Alliance for AI, IoT and Edge Continuum Innovation

AI, IoT and Edge Continuum impact and relation on 5G/6G: enabling technologies and challenges

Release 4.0

AIOTI WG Standardisation

January 2025

Executive Summary

This report highlights several IoT and Edge Computing vertical domain use cases collected by the Alliance for AI, IoT and Edge Continuum Innovation (AIOTI) and determines the specific requirements they impose on the underlying 5G/6G network infrastructure. These use cases and requirements can be used by Standards Developing Organizations (SDOs), such as 3GPP, ITU-T, ISO, and IEEE as requirements for automation in vertical domains focusing on critical communications.

In addition to these use cases also emerging topics in the area of (Beyond) 5G technology are as well introduced.

The Release 2.0 of this report included 6 additional use cases in the areas of: (1) use of drones, (2) 5G cloud-RAN, (3) Health-Critical Remote Operations, (4) preliminary 6G use cases.

The Release 3.0 of this report included 6 additional use cases in the area of Edge-Cloud Orchestration in the Section 2.13.

The Release 4.0 of this report includes 14 additional use cases in the areas of: (1) Digital Twin, (2) autonomous urban transportation, (3) critical Infrastructure support applications (smart health and connected vehicles), (4) preliminary 6G use cases, (5) use of drones, (6) smart manufacturing and automation, (7) service trust and liability management, (8) Edge-Cloud orchestration and (9) smart agriculture.

Table of Content

Executive Summary 2
Table of Content 3
Table of Figures 5
List of Tables 6
Abbreviations 7
1. Introduction 10
2. Human Centric and Vertical Services and Use cases for Beyond 5G 12
2.1 Robotic automation 12
2.1.1 Transport Infrastructure Inspection and Maintenance 12
2.2 Edge Computing and Processing 15
2.2.1 Functional Splitting for Edge Computing 15
2.2.2 Quality of service assurance-related requirements and framework for virtual reality delivery using mobile edge computing supported by IMT-2020 18
2.3 Digital Twin 24
2.3.1 Digital Twin in Industry 4.0 24
2.3.2 EVOLVED-5G: "Efficiency in FoF Operations with Novel Predictive Maintenance applied on Digital Factory Twin 29
2.4 Extreme pervasiveness of the smart mobile devices in Cities 34
2.4.1 Smart City Edge and Lamppost IoT deployment 34
2.4.2 Multi-tenant real time AI video/audio analytics 36
2.5 Autonomous Urban Transportation 41
2.5.1 Intelligent Assistive Parking in Urban Area 41
2.5.2 5G-VICTORI: UC #1.1: Enhanced Mobile Broadband under High Speed Mobility 44
2.5.3 5GMETA: Driving Safety & Awareness 49
2.6 Maritime Transportation 52
2.6.1 VITAL-5G based use case: 5G Connectivity and Data-Enabled Assisted Navigation Using IoT Sensing and Video Cameras 52
2.7 Critical Infrastructure support applications 62
2.7.1 Smart Infrastructure Monitoring 62
2.7.2 AURORAL HEALTH PILOT for Strengthening Preparedness In Health-Critical Remote Operations 65
2.7.3 ERATOSTHENES: Smart Health 73
2.7.4 ERATOSTHENES: Connected Vehicles 77
2.8 Smart Manufacturing and Automation 81
2.8.1 Factory of Future Use Cases 82
2.8.2 5G Applied to industrial production systems 90
2.8.3 5G-VICTORI: UC #2: Factories of the Future 94
2.9 Service Trust and Liability Management 102
2.9.1 E2E Service Trust and Liability Management for Verticals 102
2.9.2 5G COMPLETE: Example: UC#4: Advanced Surveillance/Physical Security Service 104
2.10 5G cloud-RAN 108
2.10.1 Virtualized base station for 5G cloud-RAN 108
2.11 Preliminary 6G use cases 112
2.11.1 Hexa-X 6G based Use cases 112
2.11.2 RISE-6G: Control for RIS-based localisation and sensing 122
2.12 Drones 127
2.12.1 Connectivity during crowded events use case, when drones are used 127
2.12.2 An innovative fire detection pilot solution using 5G, Artificial Intelligence and drone technology 131
2.12.3 5G-INDUCE: Drone assisted network performance and coverage monitoring for industrial infrastructures 139
2.13 Edge-Cloud Orchestration 142
2.13.1 CODECO P1: Smart Monitoring of the Public Infrastructure 143
2.13.2 CODECO P2: Vehicular Digital Twin for Safe Urban Mobility 147
2.13.3 CODECO P3: MDS across Decentralised Edge-Cloud 150
2.13.4 CODECO P4: Demand-side Management in Decentralized Grids 153
2.13.5. CODECO P5: Wireless AGV Control in Flexible Factories 157
2.13.6 CODECO P6: Automated Crownstone Application Deployment for Smart Buildings 161
2.13.7 5G COMPLETE: UC#3: 5G Wireless Transport services with MEC capability provided to NOs 164
2.13.8 5G-INDUCE: ML-Supported Edge Analytics for Predictive Maintenance 168
2.13.9 AI@EDGE: Edge AI assisted monitoring of linear infrastructures using drones in BVLOS operation 169

2.14 Smart Agriculture 174
2.14.1 COMMECT: Monitoring of Pest Insect Traps 174
2.14.2 COMMECT: Securing crops and equipment 176
3. Emerging Topics 180
3.1 Digital Twin 180
3.2 Deep Edge, Terminal and IoT Device Integration in B5G communication infrastructure 186
3.3 Edge, Mobile Edge Computing and Processing 187
3.3.1 Functional Splitting: allowing dynamic computing power allocation for signal processing 190
3.4 Network and Server security for IoT and edge Computing 193
3.5 Plug and Play Integrated Satellite and Terrestrial Networks 195
3.5.1 Satellite connectivity for global IoT coverage 196
3.5.2 Evolution to 5G IoT over satellite 197
3.5.3 IoT devices 197
3.5.4 IoT communication satellites 198
3.6 Autonomous and Hyper-connected On-demand Urban Transportation 198
3.7 Opportunities for IoT Components and Devices 200
3.7.1 Approach for components 201
3.7.2 Approach for devices 202
3.7.3 Requirements for IoT devices 203
3.8 EU legislative framework 204
4. Conclusions and Recommendations 205
4.1 Requirements 205
4.2. Emerging Topics 225
ANNEX I Reference 226
ANNEX II Template used for Use Case description 228
ANNEX III KPIs defined in Networld2020 (SNS) Strategic and Research Innovation Agenda (SRIA) 2021 – 2027 231
Annex IV Siemens White Paper "5G communication networks: Vertical industry requirements" 237
Contributors 239
Acknowledgements 240
About AIOTI 240

Table of Figures

Figure 1: Use case in GeoSciFramework: Early Earthquake Warning (EEW) system 15
Figure 2: Use case in E2Clab: Smart Surveillance system 16
Figure 3: Virtual reality QoE-influencing factor categories, copied from [ITU-T G.1035] 19
Figure 4: A conceptual architecture of the VR service framework, copied from [ITU-T SG13 Y.3109] 21
Figure 5: Potential Italian utilizer companies attitude towards 5G 24
Figure 6: Physical Layout – 5G Connection 27
Figure 7: Network & Application Architecture 27
Figure 8: Advanced Maintenance Scenario 28
Figure 9: Condition Management and AR Support Scenario 28
Figure 10: FOF IoT System Architecture 32
Figure 11: NCSRD site testbed setup 33
Figure 12: COSMOTE - NCSRD sites testbed setup 33
Figure 13 Block Diagram 39
Figure 14 Architecture 39
Figure 15: a) UC # 1.1 eMBB, b) UC # 1.1 Critical CCTV 46
Figure 16: Onboard network architecture 47
Figure 17: Positioning of hardware and sensors on a ship 54
Figure 18: Data-enabled assisted navigation service flow diagram 55
Figure 19: Accurate electronic navigation maps creation service flow diagram 55
Figure 20: Predictive maintenance and sanity checks service flow diagram 56
Figure 21: High-level architecture of the VITAL-5G system 57
Figure 22: 5G Galati site coverage simulation map with the Use Case interest area representation 58
Figure 23: Examples of AURORAL services 69
Figure 24: AURORAL coverage area of rescue 70
Figure 25: Normal Flow of operation 70
Figure 26: Complete block diagram for complete range of rescue drones 71
Figure 27: Selected target key performance indicators of 5G according to ITU-R (cf. [ITU-R M.2410-0]) 82
Figure 28: Exemplary application areas of 5G in the factory of the future 83
Figure 29: Overview of selected industrial use cases and arrangement according to their basic service requirements 84
Figure 30: Overview of selected main stakeholder groups participating in 5G-ACIA 84
Figure 31: Overview of selected main stakeholder groups participating in 5G-ACIA 86
Figure 32: 5G-enabled smart factory scenario 86
Figure 33: UC facility plan and configuration at ADMIE facilities 95
Figure 34: UC # 2 Digitization of Power Plants URLLC 96
Figure 35: Smart Factory and Energy Services over Private Networks 97
Figure 36: Application flows and 5G slices for Smart Factory services 97
Figure 37: a) 5G network deployed at ADMIE facility for Patras trials, b) robotic camera for the high voltage environment with live streaming over 5G, c) various interconnected sensors at the high voltage facility 99
Figure 38: High-level architecture of UC #2 100
Figure 39: UC#4 - Demo Deployment (NTUA/COSMOTE Facilities) 106
Figure 40: Summary of Hexa-X use case families and use case, source: EC 112
Figure 41: Clustering of Hexa-X Key Performance Indicators s and Key Value Indicators, copied from 122
Figure 42: Schematic of 5G positioning architecture, based on (DSM+21), supporting both UL and DL measurements 124
Figure 43: Example of RTT-based localisation (left), constraining the UE on the intersection of circles (2D) or spheres (3D); and localisation based on DL-AoD measurements (right), constraining the user within a sector of each BS 126
Figure 44: Use case architecture 128
Figure 45: High level architecture 129
Figure 46: 3GPP-compliant 5G architecture 140
Figure 47: The CODECO K8s framework and its components 143
Figure 48: CODECO P1 system architecture. 145
Figure 49: P2 UML diagram 149
Figure 50: P3 single cluster representation 152
Figure 51: P3 multi-cluster architecture representation 152
Figure 52: P4 system architecture 155
Figure 53: P4 UML use-case diagram 156
Figure 54: P5 value-proposition canvas 158
Figure 55: P5 system architecture, one cluster 159
Figure 56: CODECO P6 system architecture 163
Figure 57: P6 UML Use-case Diagram 163
Figure 58: UC#3 - Demo Deployment (NTUA/COSMOTE Facilities) 166
Figure 59: Use case 3 context 172
Figure 60: Example of use case 3 scenario 172
Figure 61: Data Flow in a Digital Model 181
Figure 62: Data Flow in a Digital Shadow 181
Figure 63: Flow in a Digital Twin 182
Figure 64: Digital Twin (DT) schema, copied from [GaRo12] 182
Figure 65: Mapping between physical and cyber/digital worlds, copied from [KrKa18] 183
Figure 66: 5C Architecture for implementation of Cyber-Physical System, copied from [CiNe19] 184
Figure 67: Applications and techniques associated with each level of the SC architecture, from [CiNe19] 184
Figure 68: Integration of industrial technology, information technology, and intelligent, copied from [KrKa18] 185
Figure 69: Application Scenarios, copied from [JML20] 186
Figure 70: Conceptual diagram of the IoT architecture with different splitting options for the 5G complex metrics calculation system[5] 191
Figure 71: Overall layered architecture of the edge-based data-intensive IoT system. 192
Figure 72: 5G/Satellite Coverage 195
Figure 73: Integrated terrestrial and satellite IoT networks 196
Figure 74: 3GPP Release 17 timeline, copied from 3GPP 197

List of Tables

Table 1: RTT, Bandwidth and Packet Loss for Weak-interaction VR, copied from [ITU-T SG13 Y.3109] 23
Table 2: RTT, Bandwidth and Packet Loss for Strong-interaction VR, copied form [ITU-T SG13 Y.3109] 23
Table 3: UC # 1.3 Rail Critical Services - Rail Signaling Requirements and KPIs 45
Table 4: UC # 1.3 Rail Critical Services - Point machine Requirements and KPIs 46
Table 5: UC # 1.1 Requirements foreseen in FRMCS and 5G landscape 47
Table 6: UC # 1.3 Network Characteristics Requirements and KPIs 48
Table 7: Data captured in Use case 2 51
Table 8: KPIs for Use case: Driving Safety & Awareness 52
Table 9: Involved stakeholders and their role 53
Table 10: Use Case Network requirements for Distributed sensor data ingestion, fusion & post-processing NetApp 60
Table 11: Use Case Network requirements for Remote inspection & risk assessment NetApp 60
Table 12: Use Case Network requirements for Data stream organization NetApp 61
Table 13: Use Case Network requirements for On board data collection & interfacing for vessels NetApp 61
Table 14: UC # 2 Key UCs requirements and KPIs 98
Table 15: UC # 2 Network functional requirements and KPIs 99
Table 16: High-Level 5G Deployment Scenario UC #2 100
Table 17: CCTV services report from tests done at the Field Demo in Patras 101
Table 18: Enhanced Security 107
Table 19: High availability of Vertical Service 107
Table 20: Lifecycle management of Vertical Services 107
Table 21: Low delay/latency 107
Table 22: High bandwidth 108
Table 23: Localisation measurements and requirements for 3D positioning 126
Table 24: UAV control and non-payload communication requirements, copied from [SiBa23] 137
Table 25: UAV payload communication Requirements, copied from [SiBa23] 137
Table 26: Communication requirements from Drone based applications, , copied from [SiBa23] 137
Table 27: Mapping of functional to non-functional requirements 141
Table 28: Comparison of 5G and 6G attributes 141
Table 29: High-bandwidth wireless transport network links 167
Table 30: Resilience 167
Table 31: Use case 4 identified risks and envisaged mitigations actions 171

Abbreviations

2D	Two Dimensional
3GPP	3rd Generation Partnership Project
4G	4th Generation
5G	5th Generation
5G-NPN	5G Non-Public Network
ABS	Anti-lock Braking System
ACL	Access Control Lists
ADApp	Autonomous Driving Application
AF	Application Function
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
AIOTI	Alliance for IoT Innovation
App	Application
AR	Augmented Reality
AS	Application Server
ASF	Authentication Server Function
AVP	Automated Valet Parking
BDA	Big Data Analytics
BICMOS	Bipolar Complementary Metal—Oxide-Semiconductor
BLE	Bluetooth Low Energy
BMS	Building Management System
BVLOS	Beyond Vision Line of Sight
C-ITS	Cooperative-Intelligent Transportation System
CAD	Connected and Automated Driving
CAGR	Compound Annual Growth Rate
CAM	Cooperative Awareness Message
CAPEX	Capital Expenditure
CC	Cloud Computing
CCAM	Connected and Automate Mobility
CNN	Convolutional Neural Network
CPS	Cyber–Physical Systems
CRAN	Cloud Radio Access Network
CSS	Car Sharing Service
D2X	Device to everything
DoF	Degree of Freedom
DoS	Denial-of-Service
DTw	Digital Twins
EEW	Early Earthquake Warning
eMBB	Enhanced Mobile Broadband
EPON	Ethernet Passive Optical Network
ESP32	Espessif Systems Processor 32
ETSI	European Telecommunication Standardisation Institute

FFT	Fast Fourier Transform
FL	Federated Learning
FoF	Factories of the Future
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GSM	Global System for Mobile communications
HPC	High Performance Computing
I&M	Inspection & Maintenance
IDS	Intrusion Detection System
IEM	Interaction of Employees and Machines
IIoT	Industrial Internet of Things
IoRT	Internet of Robotic Things
IoT	Internet of Things
IP	Internet Protocol
ITS	Intelligent Transportation System
LDM	Local Dynamic Map
LoRa WAN	LoRa Wide Area Network
LOS	Line Of Sight
LP-WAN	Low Power Wide Area Network
LTE	Long Term Evolution
LTE-V2X	LTE Vehicle to Everything
MCU	MicroController Unit
MEC	Multi-access Edge Computing
MES	Manufacturing Execution System
MIMO	Multiple Input, Multiple Output
ML	Machine Learning
mMTC	Machine-Type Communications
MQTT	Message Queuing Telemetry Transport
MUD	Manufacturer Usage Description
NACF	Network Access Control Function
NB-IoT	Narrowband IoT
NFR	Network Function Registry
NFV	Network Function Virtualisation
NoLOS	Non-Line of Sight
NoSQL	Not only Structured Query Language
NPN	Non-Public Network
NR	New Radio
NSSF	Network Slice Selection Function
NTN	Non-Terrestrial Networks
OBU	On-Board Unit
OEM	Original Equipment Manufacturer
OGC	Open Geospatial Consortium
OPEX	Operational Expenditure

OT	Operation Technology
OTA	Over The Air
PCF	Policy Control Function
RP-an	reference point between AN and NACF
RP-au	reference point between AN and UPF
RP-tn	reference point between UE and NACF
RP-ud	reference point between UPF and data network
RSU	Road Side Unit
RUL	Residual Useful Life
SAS	Service Alerting System
SCADA	Supervisory Control and Data Acquisition
SDO	Standards Developing Organization
SDO	Standards Developing Organizations
SME	Small Medium Enterprise
SMF	Session Management Function
SNS JU	Smart Network and Services Joint Undertaking
SOI	Silicon-On-Insulator
TC	Technical Committee
TCP	Transmission Control Protocol
TIoT	Tactile Internet of Things
TMC	Traffic Management Center
TSC	Time Sensitive Communication
TSN	Time-Sensitive-Networking
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
UPF	User Plane Function
uRLLC	Ultra-reliable and Low-latency Communications
USM	Unified Subscription Management
UTM	Unmanned Traffic Management system
V2V	Vehicle to Vehicle
vApp	Vertical Application
VR	Virtual Reality
VRU	Vulnerable Road Users
WAVE	Wireless Access in Vehicular Environments
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WSDN	Wireless Software Defined Network
XML	Extensible Markup Language

1. Introduction

As emphasized in reports published by AIOTI, the IoT is projected to consist of 50 billion devices by 2020 [Evans11] ranging from connected temperature sensors to autonomous vehicles. The vast scope of different device types from different verticals corresponds with highly diverse requirements for the communication infrastructure. While battery-driven sensors need a highly energy efficient communication technology, industrial IoT applications call for ultra-reliable connections with a minimum latency.

Important to mention that the ubiquitous nature of IoT devices has triggered a change to the models of managing and controlling the flow and transmission of data. The new concepts are moving from the widespread use of cloud-based infrastructure models, which are dominated by leading Internet companies, towards IoT edge mesh distributed processing, low latency, fault tolerance and increased scalability, security, and privacy.

As of today, these diverse requirements are covered by several wireless communication technologies (e.g. WLAN, Sigfox®, ZigBee, LoRaWAN, NB-IoT) which all have their specific strengths and weaknesses and that are making the IoT somewhat of a "rag rug".

This is where the 5G and beyond 5G becomes to be relevant, with its highly flexible architecture designed to be adaptable to almost any use case in the IoT space using advanced techniques like network slicing and NFV, see e.g., [Networld2020-SRIA[1]], [5GPPP-Vision], [5GPPP-verticals]. By offering a unified communications platform for the IoT, 5G has the potential of being a catalyst for IoT growth – and vice versa.

The "IoT Relation and Impact on 5G" AIOTI report [AIOTI-IoT-relation-5G] focused on highlighting emerging topics and specific IoT vertical domain use cases and determine the specific requirements they impose on the 5G network infrastructure.

This report focuses on highlighting new emerging topics and specific IoT vertical domain use cases and determine the specific requirements they impose on 5G and as well beyond 5G network infrastructure. These use cases and requirements can be used by SDOs, such as 3GPP, ISO, ITU-T and IEEE as requirements for automation in vertical domains focusing on critical communications.

The Release 2.0 of this report includes 6 additional use cases in the areas of: (1) use of drones, (2) 5G cloud-RAN, (3) Health-Critical Remote Operations, (5) preliminary 6G use cases. In particular, the added use case cases are:

- Multi-tenant real time AI video/audio analytics
- AURORAL HEALTH PILOT for Strengthening Preparedness In Health-Critical Remote Operations
- Virtualized base station for 5G cloud-RAN
- Hexa-X 6G based Use cases
- Connectivity during crowded events use case, when drones are used
- An innovative fire detection pilot solution using 5G, Artificial Intelligence and drone technology.

[1] Networld2020 ETP has been renamed to NetwolrdEurope ETP, see: https://www.networldeurope.eu

The Release 3.0 of this report also includes 6 additional use cases in the area of Edge-Cloud Orchestration, which are:

- CODECO P1: Smart Monitoring of the Public Infrastructure,
- CODECO P2: Vehicular Digital Twin for Safe Urban Mobility,
- CODECO P3: MDS across Decentralised Edge-Cloud,
- CODECO P4: Demand-side Management in Decentralized Grids,
- CODECO P5: Wireless AGV Control in Flexible Factories,
- CODECO P6: Automated Crownstone Application Deployment for Smart Buildings.

The Release 4.0 of this report also includes 14 additional use cases in different areas, which are:

- ERATOSTHENES: Connected Vehicles,
- ERATOSTHENES: Smart Health,
- EVOLVED-5G: "Efficiency in FoF Operations with Novel Predictive Maintenance applied on Digital Factory Twin,
- 5G-VICTORI: UC #1.1: Enhanced Mobile Broadband under High Speed Mobility,
- 5G-VICTORI: UC #2: Factories of the Future,
- 5GMETA: Driving Safety & Awareness,
- 5G COMPLETE: Example: UC#4: Advanced Surveillance/Physical Security Service,
- 5G COMPLETE: UC#3: 5G Wireless Transport services with MEC capability provided to NOs
- RISE-6G: Control for RIS-based localisation and sensing,
- AI@EDGE: Edge AI assisted monitoring of linear infrastructures using drones in BVLOS operation,
- 5G-INDUCE: Drone assisted network performance and coverage monitoring for industrial infrastructures,
- 5G-INDUCE: ML-Supported Edge Analytics for Predictive Maintenance,
- COMMECT: Monitoring of Pest Insect Traps,
- COMMECT: Securing crops and equipment.

2. Human Centric and Vertical Services and Use cases for Beyond 5G

This section describes the IoT vertical domain use cases that are being developed in IoT focused projects. Moreover, this section describes he specific requirements that these use cases impose on the underlying network infrastructure.

The use cases listed in this section have been described using the use case description template provided in Annex II.

2.1 Robotic automation

2.1.1 Transport Infrastructure Inspection and Maintenance

2.1.1.1 Description

This use case refers to the Transport Infrastructure Inspection and Maintenance (I&M) via the use of advanced automation and robotic systems. Such systems include various functionalities that are performed and executed in an autonomous nature and include navigation, sensor usage, robotic systems positioning, autonomous operations etc. The parts of such robotic 'missions' include various levels of communications at various stages of the mission including: i) mission communication (pre-mission), ii) control of vehicle and components during mission (measuring equipment, sensing etc.), iii) results consolidation (during and post-mission). The communication needs of these do not necessarily include real-time data communications in all cases and largely depend on the robotics equipment (hardware and software), their setup (design level) and inspection and maintenance mission (real-time or off-line).

The different types of missions running in a transport environment (such as those of highways, tunnels and bridges) include various components that execute various tasks during a robotic inspection and maintenance mission. In this scenario, this will include: i) a local control station, ii) a robotic vehicle, iii) a remote operations centre. During a mission execution there are different levels of communications taking place between these sub-systems. These are included below:

I) **Local Control Station:** usually at the close vicinity of the robotic system, in the range of 10-50m distance. This is usually responsible for the control of the mission and the actual robotic system, often providing directly commands to it. Direct communication limitations and latency issues often make system designers limit the real time-ness of these communications and make these as less critical as possible. This results into a mission being transferred to the robotic system offline and very limited communications between the local control station and the robotic vehicle take place afterwards. Requirements for such scenarios include transmission of kb of information with low latency.

II) **Robotic Vehicle:** usually includes the communication of the on-board robotic system components and sensors that need to communicate with each other during the mission of the robot. This currently usually includes WiFi, Zigbee, Bluetooth or other communications with short-range requirements. This type of communication includes low-latency commands to control the vehicle and trigger various components/actuations to perform the mission. Then data communications include the gathering of results locally or at the local control station. As such data are usually quite large in size (could be GB of information), their communication out of the robotic system is currently avoided and transmitted off-line (after the mission end). The communication of a local control station is not foresee here as described above.

III) **Remote Operations Centre**: this is usually located in large distance from the mission execution, often several kilometres away (may be 10-50km away or several more) and is usually an operations centre of the transport operator or manager. This type of communication requires the robotic vehicle or the local control station (both at the site of the inspection) to communicate the mission status, progress, detections and inspection information to a remote location.

For purposes of robotic control, the latency should be extremely low (keeping data size also low), while the bandwidth requirement may be higher for cases that we wish to transmit sensing information remotely (high bandwidth required, with mid-latency).

2.1.1.2 Source

The use case above is driven by pilot experiments in the PILOTING - 871542 project (H2020, ICT) in which INLECOM Innovation leads the highway tunnel inspection cases. PILOTING develops an integrated and robust robotics platform targeted for the Inspection and Maintenance (I&M) of infrastructures of the Oil&Gas (refineries) and transport (Tunnels and Viaducts). Its ultimate goal is to increase the efficiency and quality of inspection and maintenance activities in order to keep the necessary safety levels in these ageing infrastructures. PILOTING will establish large-scale pilots in real industrial environments to directly reply to main I&M challenges through the demonstration of: increasing rate of inspection and maintenance tasks, improving coverage and performance, decreasing costs and time of operations, improving inspection quality and increasing safety of operators.

2.1.1.3 Roles and Actors

Highway Operators (responsible for the structural condition of the infrastructure).

Inspection personnel (performing the inspection tasks).

Robotics companies and SMEs (developing robotics, communication systems and platforms).

2.1.1.4 Pre-conditions

Power requirement locally at the inspection site.

Existing network coverage are limited and possibly unfeasible in many cases (such as tunnels).

Optical fibre communications sometimes are also needed.

No line-of-sight communications is often the case.

2.1.1.5 Triggers

Inspection is needed to be performed in a highway system (tunnel, bridge etc.) as part of a planned or emergency situation.

2.1.1.6 Normal Flow

Inspection mission is transferred from the local station to the robotic system.

Robotic control is communicated to the robotic system.

Inspection results are communicated locally (at site) or remotely (far).

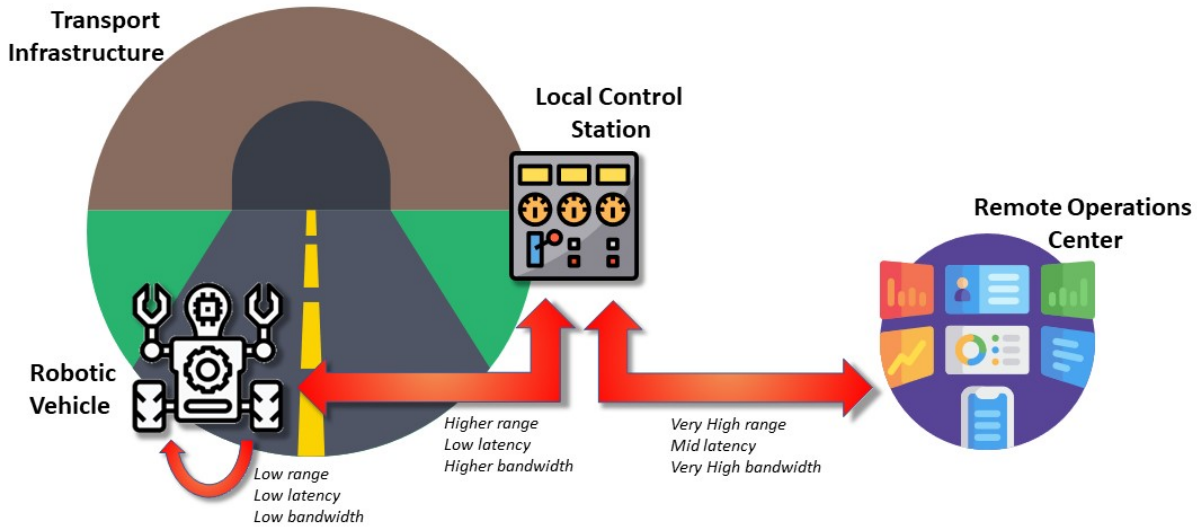
2.1.1.7 Alternative Flow

None

2.1.1.8 Post-conditions

Inspection personnel and highway management is analysing the results of the Inspection performed and takes decision on intervention actions required.

2.1.1.9 High Level Illustration



2.1.1.10 Potential Requirements

Functional Requirements

Real-time communications between local control station and robotic vehicle.

Low latency for onboard and local control station communications.

Low latency but high bandwidth communication for the remote operations centre.

Large files size (GB of information) to be transferred from robotic vehicle to the remote operations centre.

Reliable communications at all levels.

Non-Functional Requirements

Secure communications between all scenario actors.

Interoperability between communication protocols (linked also with the possibility to use. standard communication protocols between the systems).

2.1.1.11 Radio Specific requirements

2.1.1.11.1 Radio Coverage

Radio cell range

Does the radio link cross public spaces? Or is it constrained to indoor or customer premises?

Radio link crosses public spaces and includes indoor and outdoor premises.

Is Multicell required?

A Multicell may be required for remote connectivity at a regional level

Is handover required? Seamless? Tolerable impact in delay and jitter?

100 Milliseconds delay can be tolerated.

Mobility: maximum relative speed of UE/FP peers

Robotic vehicle moving around 5-50km/h.

2.1.1.11.2 Bandwidth requirements

Peak data rate: 1000Mbps

Average data rate 100Mbps

2.2 Edge Computing and Processing

2.2.1 Functional Splitting for Edge Computing

2.2.1.1 Description

In this section three use cases related to Functional Splitting are briefly described. As described in detail in Section 3.3.1 the functional splitting concept is often applied to the 5G network[2], but with this vision, the concept goes beyond the network functional splitting and can be applied to other fields dealing with signal processing[3]. It is also considered an enabler for the computing continuum as the signal processing tasks can be distributed in different parts of this continuum.

In the URBAURAMON project, the main challenges associated to the signal processing functional splitting are related to the planned problem and the resources planned in the network (i.e. sampling, windowing, weighting, compression, filtering, etc.). For instance, for audio processing and using ESP32 MCU (Espressif Systems Processor 32 MicroController Unit) in the node, functions like audio sampling, windowing are managed. Sequentially, by performing Fourier transform and some other simple operations or functions related to filtering the output information of these functions is forwarded to the Edge in order to finish the computing process. At this point, possible delays in the communication need to be considered, but using simple/lightweight protocols (such as MQTT), and using controlled audio/processed chunks, affordable delays (i.e. not too high)[5] can be obtained, allowing real-time processing/monitoring. This procedure can be as well used for video processing and other temporal related signals, but then it is required to redefine the splitting options such that specific video processing complexities are taken into account (e.g. redefining FFT to FFT2D, applying 2D filtering per frame, etc.).

In the case of GeoSciFramework project, an Early Earthquake Warning (EEW) system is developed. In particular, **Figure 1** shows the use case as an EEW system. In this system, Seismic sensors transfer data continuously to a centralized data centre where data are processed. When P-waves are identified, an earthquake warning is emitted to warning broadcasting users.

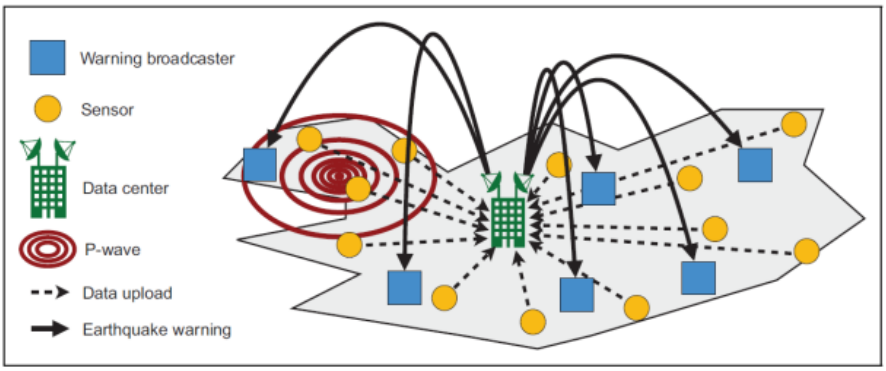


Figure 1: Use case in GeoSciFramework: Early Earthquake Warning (EEW) system

Finally, in the use case of E2Clab/OverFlow project, the image processing in a smart surveillance system for counting persons/detecting a specific person or for free parking space detection[4][5] in a Smart City can be distributed between the Edge infrastructures (such as Raspberry Pi nodes with cameras, computing and storing resources located where the data is originated), Fog infrastructures (the gateways –a number of geographically-distributed resources located on the data path between the Edge and the Cloud- processing information, aggregated from multiple neighbouring Edge devices as a way to further reduce data volumes that need to be transferred

[2] D. Harutyunyan and R. Riggio, "Flexible functional split in 5G networks," 2017 13th International Conference on Network and Service Management (CNSM), Tokyo, Japan, 2017, pp. 1-9, doi: 10.23919/CNSM.2017.8255992.

[3] D. Wubben et al., "Benefits and Impact of Cloud Computing on 5G Signal Processing: Flexible centralization through cloud-RAN," in IEEE Signal Processing Magazine, vol. 31, no. 6, pp. 35-44, Nov. 2014, doi: 10.1109/MSP.2014.2334952.

[4] J. Nyambal and R. Klein, "Automated parking space detection using convolutional neural networks," 2017 Pattern Recognition Association of South Africa and Robotics and Mechatronics (PRASA-RobMech), 2017, pp. 1-6, doi: 10.1109/RoboMech.2017.8261114.

[5] G. Amato, F. Carrara, F. Falchi, C. Gennaro and C. Meghini, "Deep learning for decentralized parking lot occupancy detection", Expert Systems with Applications, 72, pp 327-334, 2017. URL: https://github.com/fabiocarrara/deep-parking (Visited on 04/07/2021)

and further processed on Clouds), and Cloud infrastructures (which provide virtually "unlimited" computing and storage resources used essentially for backup and data analytics for global insight extraction in a centralized way). **Figure 2** shows a pipeline for the workflow between these elements.

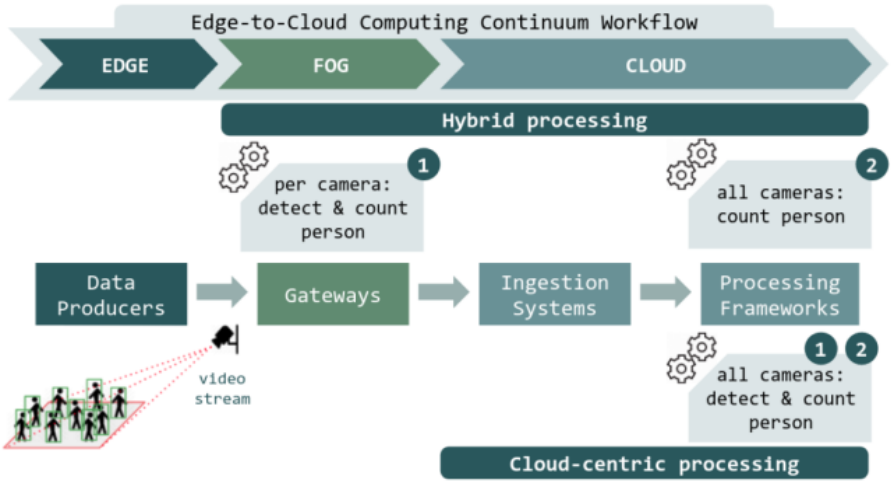


Figure 2: Use case in E2Clab: Smart Surveillance system

2.2.1.2 Source

GeoSciFramework project (funded by NSR US)

Overflow project (funded by ANR France)

URBAURAMON project

2.2.1.3 Roles and Actors

Actors & Roles in the three use cases

Citizens & Vicinity. People who lives (near) a critical infrastructure and needs to be protected or informed about potential risk that could affect their lives.

Governmental bodies. Stakeholders required to organize the society and provide insights at higher level.

Civil Protection Organization. Stakeholders dedicated to mobilizing and organize the citizens in emergency situations.

2.2.1.4 Triggers

GeoSciFramework project

The trigger used in this use-case is the appearance of a soft earthquake with p-wave or tsunami as a risk, or it is detected in the critical infrastructure.

Overflow project

The trigger for this use-case is the appearance of an event for searching some kind of people (or a specific person –or even a parking space-).

Urbauramon project

The trigger for this use-case is the continuous monitoring of the psychoacoustic annoyance. When a problem appears (i.e. high psychoacoustic annoyance), the system start recording and streaming the audio to the server.

2.2.1.5 Potential Requirements

Functional Requirements

GeoSciFramework project

Real-time communication in case of emergency.

Reliable communication between the stakeholders.

Scalable communication to interconnect different critical infrastructures.

Standard-based communication between critical infrastructures to align emergency information exchange.

Requirements for data processing: Streaming of geodynamic data from sensors using specific tools, as mentioned in the Section 3.3.1.

Requirements for data storage: Spatial and temporal data is stored in Cassandra database (NoSQL).

Requirements for data analysis and visualization: Spatial and temporal data analysis with Python notebooks (Jupiter/Zeppelin); Data exploration, analysis and visualization using dashboards with Grafana/Kibana.

Overflow project

Analysis/computation requirements:

Stream analysis: data should be analysed in real time to monitor different aspects of the city (environment, traffic...).

Spatial and temporal data: The nature of the data generated through sensors has embedded spatial and temporal data (e.g. When was the measure generated and where?).

Open and accessible data: These huge amounts of data have to be open and/or accessible for its use. This also brings privacy and security challenges.

Batch processing and learning from data: In addition to real-time data processing ,huge amounts of data can be also analysed off-line (optimising public transport routes, etc.).

Storage requirements:

Storage in real time: Multiple sensors generate data with high velocity that has to be stored almost in real time.

Replicated storage system: Dependability vs provision of replicated storage.

Infrastructure requirements:

Heterogeneous environment: The architecture of a Smart City involves connecting heterogeneous environments with different protocols and technologies (sensors, storage system, backend, frontend...).

Data locality: It is not necessary to send all data around the world but rather process it locally and send aggregates.

Fault detection system for IoT system: Detect wrongly configured devices, disconnected wires, explain accurately occurrences of combined faults. Detect and explain high energy consumption.

Scalable system: It has to be scalable (able to add new sensors and input sources), including the ability to ingest new data with a structure that is not known in advance.

Urbauramon project

The requirements for the operation of this system is the deployment of Fipy nodes with microphones for audio gathering and soundscape description. Also, the Edges for signal processing according to the necessities of the system.

For the signal processing, the Fipy nodes have been improved providing a I2S wrapper for micropython programming in order to develop the Fipy node firmware (kernel space) that is based on ESP32 Xtensa. The Fipy node allows data communication with different protocols (WiFi, BLE, Sigfox, LoRa, and LTE-M/NB-IoT). For signal processing, also FFT and sound-metric parameters for soundscape description (i.e. Loudness, Sharpness, Roughness and Fluctuation Strength) have been implemented. The user space allows the selection of the specific functional split (i.e. A for sampling and windowing, B for sampling/windowing and FFT and C for sampling/windowing/FFT and metric computation).

The Edge (Raspberry Pi-based) will compute the resting part of the whole processing in each functional splitting.

2.2.2 Quality of service assurance-related requirements and framework for virtual reality delivery using mobile edge computing supported by IMT-2020

2.2.2.1 Description

Most of the provided text related to this use case is based and/or copied from [ITU-T SG13 Y.3109].

Cloud VR (Virtual Reality) may become one of the preferred enhanced mobile broadband (eMBB) service for many IMT-2020 commercial carriers. VR is a rendered version of a delivered video and audio scene in six degrees of freedom (DoF). The rendering is designed to mimic the visual and aural sensory stimuli of the real world as naturally as possible to an observer or user. VR usually, but not necessarily, requires users to wear an HMD to completely replace the user's field of view (FoV) with a simulated visual component and headphones to provide the user with the accompanying audio. Some form of head and motion tracking of the user in VR is usually also necessary to allow the simulated visual and aural components to be updated in order to ensure that, from the user's perspective, items and sound sources remain consistent with the user's movements [b-3GPP TR 26.918]. To maintain a reliable registration of the virtual world, VR applications require highly accurate, low-latency tracking of the device at about 1 kHz sampling frequency [b-ETSI TR 126 928].

The adoption and growth of new VR services requires high performance, reliability and scalability of IMT-2020 systems and their multimedia enablers. It is important for VR service providers and network operators to be aware of the exact VR QoS (clause 3.1.8) requirements before deployment of VR service. From the network operator point of view, the exact QoS requirements can be used for efficient network QoS planning, QoS provisioning, QoS monitoring and QoS optimization [ITU-T Y.3106] and [ITU-T Y.3107]. From the VR service provider point of view, the exact QoS requirements can help to assure end-to-end (E2E) VR service QoS. Both VR service providers and network operators are required to understand the typical VR service use cases and specific QoS requirements, then, based on these requirements, they can further specify QoS assurance-related requirements and a framework for VR service deployment in IMT-2020.

The QoE is also very important for the success of VR service. [ITU-T G.1035] identifies and describes 12 QoE-influencing factors for VR services. These influencing factors, as illustrated in **Figure 3**, are divided into three categories: human; system; and context.

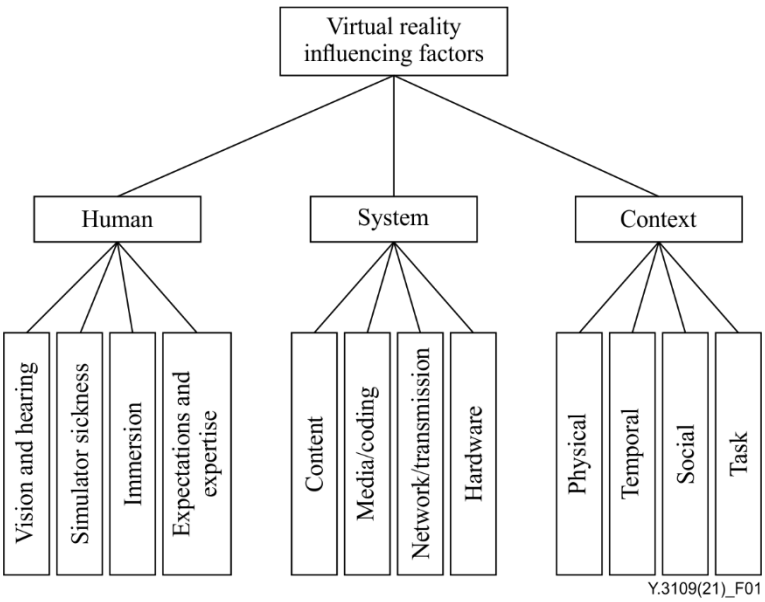


Figure 3: Virtual reality QoE-influencing factor categories, copied from [ITU-T G.1035]

According to the interaction level, VR services can be classified into those of weak- and strong-interaction [ITU-T G.1035]. NOTE - The classification of VR services, use cases and service requirements are described in Appendix II of Y.3109.

One of the most important characteristics of IMT-2020/5G is that the cloud and network converge. The basic requirements of cloud and network convergence include: unified definition, orchestration of network resources and cloud resources to form a unified, agile and flexible resource supply, operation and maintenance system. Specific QoS assurance-related functionalities and mechanisms are needed to ensure that the delivered VR service meets the quality characteristics or objectives defined elsewhere.

2.2.2.2 Source

ITU-T SG13 Y.3109 (formerly Y.qos-ec-vr-req) "Quality of service assurance-related requirements and framework for virtual reality delivery using mobile edge computing supported by IMT-2020", published in April 2021.

This Recommendation specifies quality of service (QoS) assurance-related requirements and a framework for virtual reality (VR) delivery using mobile edge computing (MEC) supported by International Mobile Telecommunications-2020 (IMT-2020). It summarizes the QoS assurance-related function and mechanism requirements for VR cloud, VR edge, VR client, VR QoS management and control. A high-level framework of VR delivery using MEC supported by IMT-2020 is given to assist the understanding of VR QoS assurance-related functions and mechanisms.

This Recommendation refers to MEC only in the context of VR delivery. Therefore, any other use of MEC lies outside the scope of this Recommendation.

The QoS planning for VR services, typical VR use cases and guidelines for deployments of VR services are described in appendices.

NOTE: Quality of service assurance is intended in the Recommendation as "functionalities or mechanisms that enable service providers to make statements with a degree of confidence that the service meets the quality characteristics or objectives specified elsewhere."

2.2.2.3 Roles and Actors

A conceptual architecture of the VR service framework consists of a VR cloud (VR service provider), VR edge and VR client (please see Section 2.2.2.9). Logical distribution of the VR service into three components assures QoS for VR service delivery to users distributed throughout different locations in the IMT-2020 network.

2.2.2.4 Pre-conditions

Considered that the virtual reality delivery system specified In ITU-T SG13 Y.3109 is applied. VR usually, but not necessarily, requires users to wear an HMD to completely replace the user's field of view (FoV) with a simulated visual component and headphones to provide the user with the accompanying audio.

2.2.2.5 Triggers

This use case is triggered when a rendered version of a delivered video and audio scene need to be realised.

2.2.2.6 Normal Flow

VR services can be seen as AFs in IMT-2020. The QoS requirements of the VR service can be realized by interacting with an IMT-2020 PCF through service-based interfaces [ITU-T Y.3102] and [ITU-T Y.3104]. VR AFs can interact with a CEF to provide session-related information (e.g., QoS requirements) via application signalling. It can also influence traffic routing by providing session-related information to the PCF in support of its rule generation.

The VR cloud, acting as the VR service provider, may be located in an external data network (DN). It generates the VR media on the fly based on incoming tracking and sensor information. Cloud VR rendering capability is deployed on the cloud so that high-quality three dimensional (3D) rendering effects on lightweight VR terminals and encoding of the full view or FoV media before network transmission can be made. MEC coordination is implemented through IMT-2020 CEF interaction, and the encoded media is transmitted over the IMT-2020 network. The VR cloud can also monitor and collect VR QoS parameters and report QoS parameters to IMT-2020 PCF to optimize VR QoS.

In the VR client, the tracking and sensor information is delivered in the reverse direction. In the VR HMD device, the VR media decoders decode the media, implement local VR rendering and display to the user. The VR client can also monitor and collect VR QoS parameters and report QoS parameters to IMT-2020 PCF to optimize VR QoS.

The VR edge is located in a trusted DN and near to the VR client. The VR edge is responsible for interaction with PCF, CEF and MEC coordination, VR edge logic processing, VR edge rendering and media transmission over the IMT-2020 network. The physical deployment guidelines of VR edge location are described in Appendix III. The VR edge can redirect VR content requests to other VR edge nodes or the VR cloud when local content is not available.

2.2.2.7 Alternative Flow

None defined.

2.2.2.8 Post-conditions

A rendered version of a delivered video and audio scene in six degrees of freedom (DoF) is realised.

2.2.2.9 High Level Illustration

The high-level illustration of the VR rendering scenario is sown in **Figure 4**.

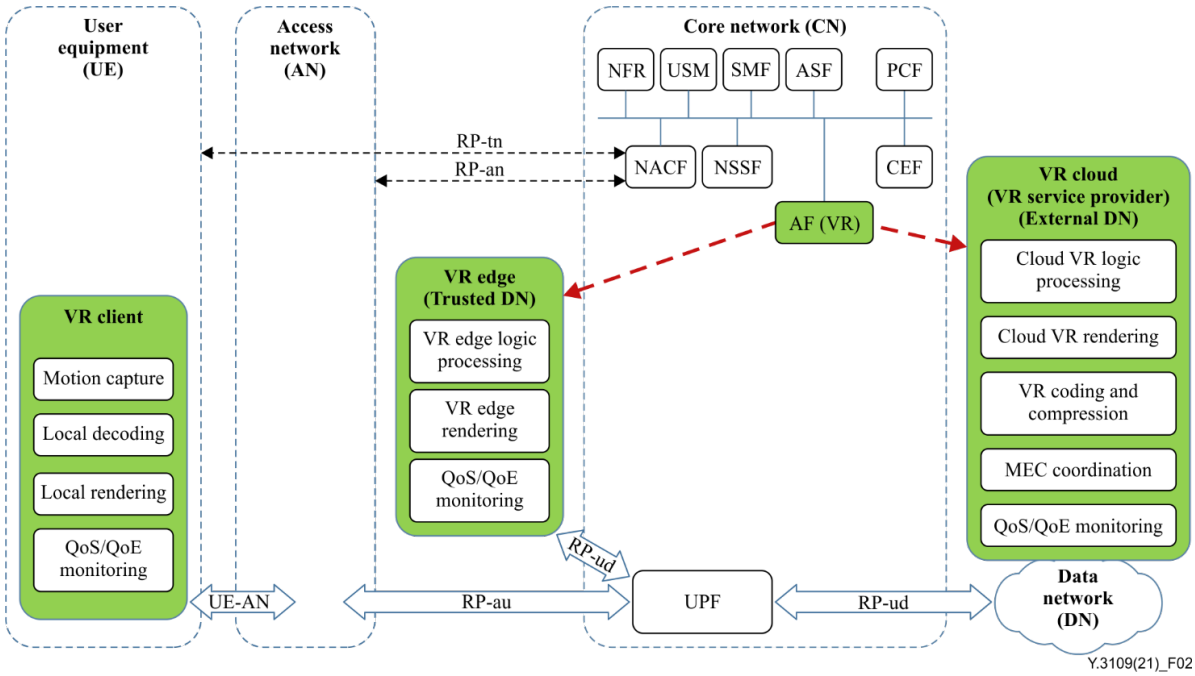


Figure 4: A conceptual architecture of the VR service framework, copied from [ITU-T SG13 Y.3109]

The following entities and interfaces are depicted in **Figure 4**:

CEF: capability exposure function

NFR: network function registry

PCF: policy control function

USM: unified subscription management

NACF: network access control function

NSSF: network slice selection function

SMF: session management function

ASF: authentication server function

AF: application function

UPF: user plane function

RP-tn: reference point between UE and NACF

RP-an: reference point between AN and NACF

RP-au: reference point between AN and UPF

RP-ud: reference point between UPF and data network.

2.2.2.10 Potential Requirements

The following requirements are copied and/or based on the VR related requirements specified in ITU-T specifications, see [ITU-T SG13 Y.3109].

Functional Requirements

VR cloud

Req_1. The VR cloud is required to act as an IMT-2020 AF and to interact with an IMT-2020 PCF to exchange VR QoS subscription information. The subscription information for a VR service may contain bandwidth, delay, loss rate, etc.

Req_2. The VR cloud is required to support generation of realistic images and sounds to emulate a real environment or create a synthetic one for the VR user with immersive experiences.

Req_3. The VR cloud is recommended to support cloud VR logic processing and cloud VR rendering to ensure the QoS of VR client and to lower requirements for VR client performance and costs.

Req_4. The VR cloud is recommended to support cloud encoding and compression mechanisms such as [ITU-T H.264], [ITU-T H.265] and [ITU-T H.266] to lower the network bandwidth requirement.

Req_5. The VR cloud is required to support MEC coordination, which includes VR content delivery and distribution to VR client and VR edge through the IMT-2020 network.

Req_6. The VR cloud is recommended to monitor and collect VR QoS parameters and report QoS parameters to an IMT-2020 PCF to optimize VR QoS.

VR edge

Req_7. The VR edge is required to act as an IMT-2020 AF and interact with an IMT-2020 PCF to exchange VR QoS information.

Req_8. The VR edge is required to support caching of VR content received from a VR cloud.

Req_9. The VR edge is required to support edge VR logic processing and cloud VR rendering to ensure the QoS of the VR client and to lower requirements for VR client performance and costs.

Req_10. The VR edge is required to be located closely to the VR client and support VR content delivery to the VR client through the IMT-2020 reference point between the UPF and data network (RP-ud) interface.

Req_11. The VR edge is required to redirect VR content requests to other VR edge nodes or the VR cloud when local content is not available.

Req_12. The VR edge is recommended to monitor and collect VR QoS parameters and report QoS parameters to the IMT-2020 PCF to optimize VR QoS.

VR client

Req_13. The VR client is required to support local decoding and local rendering to ensure immersive VR experiences.

Req_14. The VR client is required to support motion and position capture and report this information to the VR edge and VR cloud.

Req_15. The VR client is recommended to monitor and collect VR QoS parameters and report QoS parameters to the IMT-2020 PCF to optimize VR QoS.

VR QoS management and control

Req_16. It is required to support capability exposure function (CEF) and network slice selection or instantiation, e.g., eMBB slice, according to VR QoS subscription information.

Req_17. It is required to support VR QoS planning for VR service, which includes estimation of network coverage, capacity and resource requirements.

Req_18. It is required to support VR QoS provisioning, which includes translation of a VR service-centric service level agreement [ITU-T E.860] to resource-facing network slice descriptions, unified and E2E QoS control, QoS interworking and mapping, as well as efficient E2E QoS provisioning.

Req_19. It is required to support VR QoS monitoring, which includes collection of the QoS parameters, status and events of the provisioned slice, VR cloud, VR edge and VR client.

Req_20. It is required to support VR QoS optimization, which includes intelligent VR QoS anomaly detection, VR traffic prediction and routing optimization, VR QoS anomaly prediction and VR QoS optimization to provide and assure a desired service performance level during the lifecycle of the service.

RTT, Bandwidth and Packet Loss

The below tables, **Table 1** and **Table 2** are copied from [ITU-T SG13 Y.3109]

Table 1: RTT, Bandwidth and Packet Loss for Weak-interaction VR, copied from [ITU-T SG13 Y.3109]

Parameter	Level		
	Fair experience	Comfortable experience	Ideal experience
RTT	20 ms	20 ms	20 ms
Bandwidth	60 Mbit/s	140 Mbit/s	440 Mbit/s
Packet loss ratio	≤9E-5	≤1.7E-5	≤1.7E-6

Table 2: RTT, Bandwidth and Packet Loss for Strong-interaction VR, copied form [ITU-T SG13 Y.3109]

	Level		
	Fair experience	Comfortable experience	Ideal experience
RTT	20 ms	15 ms	8 ms
Bandwidth	80 Mbit/s	260 Mbit/s	1 Gbit/s
Packet loss ratio	≤1E-5	≤1E-5	≤1E-6

2.3 Digital Twin

2.3.1 Digital Twin in Industry 4.0

2.3.1.1 Description

Industry 4.0 paradigm is becoming a standard approach towards advanced, efficient and sustainable manufacturing. In that key state-of-the-art technologies such as the Internet of Things (IoT), Wireless and Mobile Communication (including 5G), cloud computing (CC), big data analytics (BDA), and artificial intelligence (AI) have greatly stimulated the development of smart manufacturing environments. An important prerequisite for smart manufacturing is cyber–physical integration, which is increasingly being embraced by manufacturers. As the preferred means of such integration, cyber–physical systems (CPS) and digital twins (DTws) have gained extensive attention from researchers and practitioners in industry. [KrKa18]. For such reason the need for a comprehensive environment to demonstrate potentiality and execute tests and proof of concepts, it was recommended the development of a use case able to demonstrate how a brown field manufacturing environment could be connected via 5G Infrastructure to Implement a Digital Twin for monitoring, simulation and control purposes.

Another important reason was the need to demonstrate how 5G technologies could be utilized in factory environment to overcome issues like difficult cabling/connection, flexibility of the Infrastructure, high performances in terms of speed and latency.

Moreover, it was demonstrated how MEC (Multi-access Edge Computing) functionalities could provide valuable support to critical operations in real time monitoring and control. Relevance of availability of such environment for dissemination and tutoring purposes is demonstrating by the following chart, see **Figure 5**, as result of a survey of "Osservatori of Politecnico di Milano"[6] , showing how 5G adoption In Industrial domain is today perceived as not relevant by stakeholders.

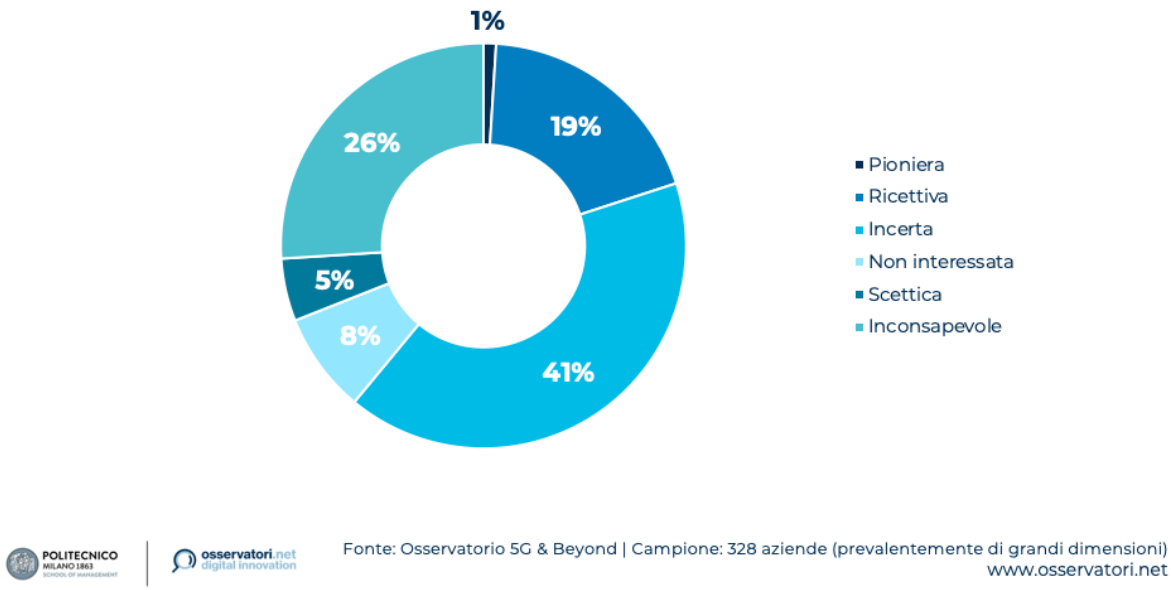


Figure 5: Potential Italian utilizer companies attitude towards 5G

With the 2016/588 communication of September 14, 2016, European Commission identified the timely deployment of 5G as a strategic opportunity for Europe, highlighting the need for a coordinated approach and a common timetable for the introduction of the 5G that foresees starting immediately the implementation of the 5G through concrete actions that pursue the following objectives:

[6] Osservatorio 5G & Beyond: la Ricerca 2020

a) to promote preliminary experiments under the 5G-PPP and pre-commercial trials;

b) to encourage Member States to develop national roadmaps for the deployment of the 5G;

c) ensure that each Member State designates at least one main city as "5G-enabled" by the end of 2020.

The MISE (Italian Ministry of Economic Development) issued a Call for proposals on 16 March 2017: In order to realise the EC "5G Action Plan" project proposals were lunched aimed at achieving, the following specific ministerial authorization for pre-commercial trials for innovative 5G networks and services in the spectrum portion 3.7 - 3.8 GHz in specific areas (among them Milan Metropolitan Area).

The actual experimentation started in Q4 of 2018 when Politecnico di Milano as major academic partner, in partnership with Vodafone Italia as main partner and other 25 industrial and academic partners won a tender to develop and deploy in the metropolitan area of Milan a preliminary project aimed at implementing pre-commercial experiments for 5G innovative networks and services. The project supported 41 use cases in 7 application domains.

Among them the Use Case 31 - 5G enabled Industry 4.0 process optimization and asset management use case, is addressing:

Advanced Maintenance Execution System - Massive data collection feeding: a preventive/predictive maintenance system able to support operators intervention with AR applications and an asset management system able to estimate future working trends (e.g. RUL – Residual Useful Life)

Self-Reconfigurable and Adaptive Production Systems - CNN (Convolutional Neural Network) based machine learning algorithms identifying: Specific operational conditions detection and Production process reconfiguration or production re-scheduling to optimize performances

Key advantages from the 5G technology are:

Wireless connection of sensors at high speed, low latency of the data transmission. This can support hard real time application or massive data transmission.

Availability of the Edge Computing platform (MEC) for fast processing close to the plant premises.

Use case was implemented in Industry 4.0 Lab @ School of Management of Politecnico di Milano. For more details on the description of the Digital Twin concept, as mentioned in the Section 3.1.

2.3.1.2 Source

As stated above, use case was executed in the context of the MISE (Italian Ministry of Economic Development) issued a Call for proposals on Mar 16, 2017. Vodafone Italy was main contractor and Politecnico di Milano was main scientific partner. Use case was one of the 2 experimentations in manufacturing domain (the other one was focused on robotic). References are available at 5G in Milan: News & Information | Vodafone 5G and Vodafone 5G - Process automation, cloud control for Industry 4.0. Further developments were carried out in the context of the H2020 EU funded Qu4lity project.

2.3.1.3 Roles and Actors

Intended stakeholders are:

Mobile networks and telco Operators and Internet Service Providers, aiming to demonstrate how 5G Infrastructure can bring tangible advantages in Industry and specifically in manufacturing domains, providing evidence to sceptical stakeholders.

Industry and Manufacturing Companies, specifically SMEs, willing to familiarize to 5G adoption in production environment.

2.3.1.4 Pre-conditions

Availability of a 5G coverage in indoor environment. Optical fiber connection in proximity of the line for (optional) installation of a MEC (Multiaccess Edge Computing) local implementation. No specific requirement is requested on the line/machines as use case embeds "AI40A-5G: Industry 4.0 data driven architecture over 5G" [TaCa19] developed at Industry 4.0 Lab @SOM POLIMI.

2.3.1.5 Triggers

Use case was developed to demonstrate how a 5G infrastructure could allow to deploy in a brown field environment a fully compliant Industry 4.0 environment without invasive cabling intervention and providing excellent features in reliability and performance terms. Digital Twin implemented was fully able to provide support for monitoring and controlling a manufacturing environment. Developed test site is utilized for evangelization and technology transfer mainly for SMEs and for educational purposes at POLIMI.

2.3.1.6 Normal Flow

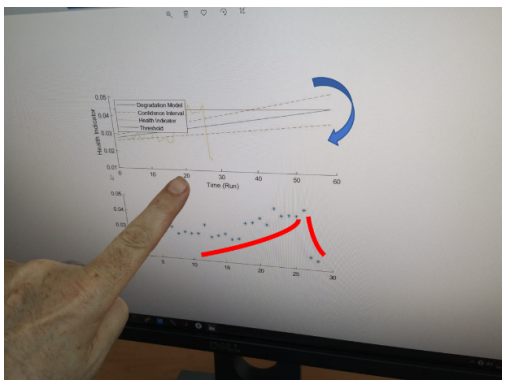
Use case is structured in two distinct flows, both of them leveraging 5G data transmission from sensors to backend and MEC functionalities.

Advanced Maintenance Execution System:

Data collected from the field and conveyed via 5G infrastructure are validated, features extracted and support creation/refinement of a Naive Bayes Prediction Model to estimate component residual useful life

A reasoner process running on a virtual machine located in the MEC, implement a forecasting algorithm to identify and display residual life of the component (specifically head of a driller and a press piston)

Computed prediction is pushed to mobile devices connected through 5G



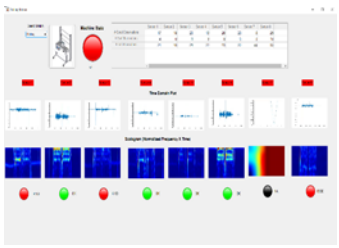
Self-Reconfigurable and Adaptive Production:

Data collected from the field and conveyed via 5G infrastructure are validated, features extracted and support creation/refinement of a CNN (Convulational Neural Network) model to recognise working conditions and correlations to identify likely situations and status

A reasoner process running on a virtual machine located in the MEC, implement a decision algorithm based on Forest Tree algorithm to identify conditions and if needed to suggest actions. Combinations of 40+ signals are considered

Results of analysis are displayed on local monitors, actions are conveyed to the line MES (Manufacturing Execution System) to change production planning, if requested AR (augmented reality) supported operator is activated and specific action are requested

AR worker is guided to execute specific actions like checks or maintenance interventions.



2.3.1.7 Alternative Flow

None

2.3.1.8 Post-conditions

Three main objective are pursued in the use case:

Real time projection of RUL (Residual Useful Life) of a component

Combined novelty detection and intervention support system (re-scheduling and intervention)

AR support to operators in the field

2.3.1.9 High Level Illustration

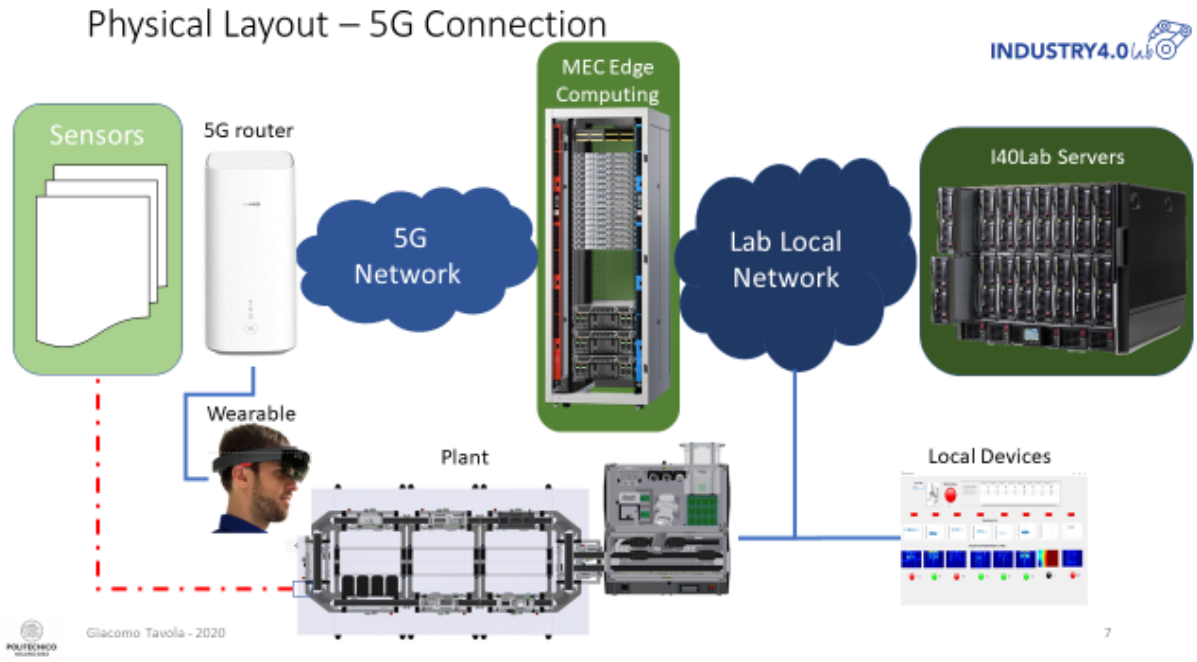


Figure 6: Physical Layout – 5G Connection

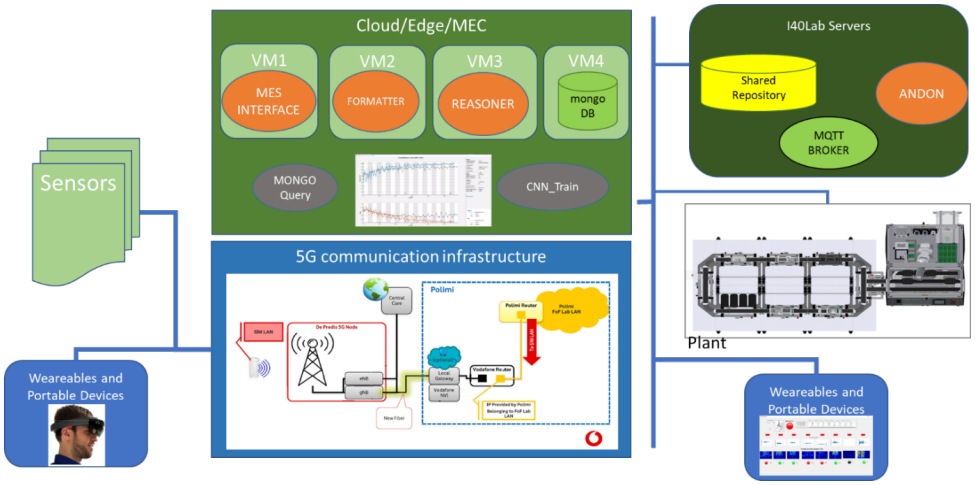


Figure 7: Network & Application Architecture

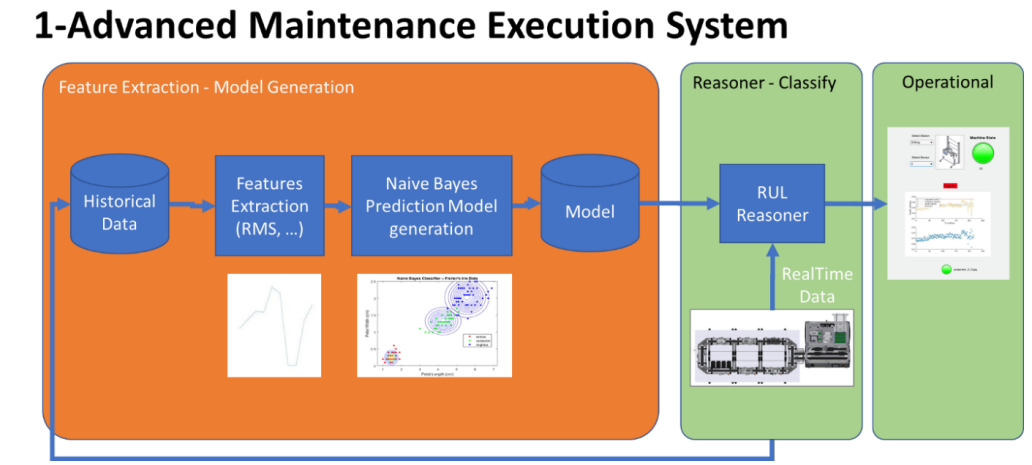


Figure 8: Advanced Maintenance Scenario

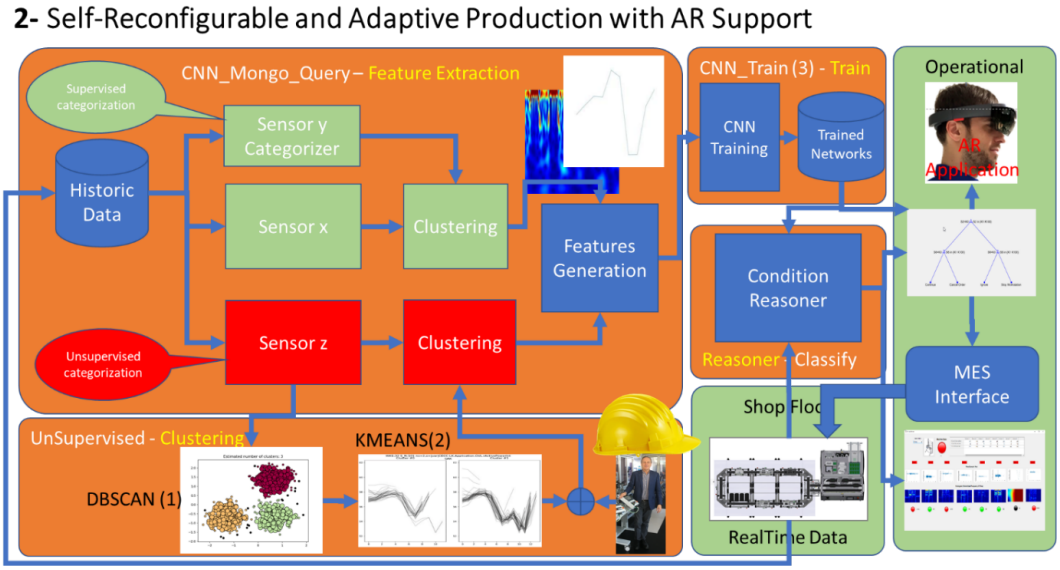


Figure 9: Condition Management and AR Support Scenario

2.3.1.10 Potential Requirements

Functional requirements

MEC (Edge Computing) infrastructure required to provide operational environment for Computer Intensive application as model creation/update, features extraction, forecast calculation.

As most of the activities are indoor in possibly harsh conditions, it is required a careful analysis of propagation and signal interference

Non-functional requirements

Possible consideration includes:

Reliability of communications considering environment conditions (electromagnetic interferences or signal reflection or Faraday effect)

Security and privacy is required to safeguard private and sensitive production data. Non repudiation mechanisms need to be implemented. Possible private networks or sliced.

2.3.1.11 Radio Specific requirements

2.3.1.11.1 Radio Coverage

Radio cell range: Mainly indoor

Is Multicell required? No

Special coverage needs: i.e., maritime, aerial: No

2.3.1.11.2 Bandwidth requirements

Peak data rate 100 Mb/s

Average data rate 10 Mb/s

Is traffic packet mode or circuit mode? TBD

2.3.1.11.3 URLLC requirements

Required Latency 10 ms one way

Required Reliability 99.9 %

Maximum tolerable jitter TBD

2.3.1.11.4 Radio regimens requirements

Desired and acceptable radio regimens TBD

Other requirements: No

UE power consumption TBD/NA

Is terminal location required? location accuracy? Nice to have max 1m

2.3.2 EVOLVED-5G: "Efficiency in FoF Operations with Novel Predictive Maintenance applied on Digital Factory Twin

2.3.2.1 Description

EVOLVED-5G endorses this vision through the definition of a NetApp ecosystem and proposes a functional architecture relevant to the implementation of an experimental facility blueprint (The EVOLVED-5G facility), that will provide the tools and the processes for the development and validation of NetApps, as well as any supporting network infrastructure (e.g., a 5G-NPN) and mechanisms for market releasing and collaboration (e.g., a Marketplace). Based on the facility blueprint, a requirements analysis work is depicted, maintaining a clear separation among:

Requirements that are fundamental for Industry 4.0 businesses, as expected by the vertical Apps (vApps) and NetApps.

Requirements that relate to the 5G network infrastructure, relating to both the network equipment, access and core network components as well as the orchestration and monitoring capabilities.

Physical infrastructure requirements that involve the data centre capabilities.

Requirements related to the NetApps development, validation and testing. Furthermore, EVOLVED-5G brings innovate Industry 4.0-related use cases that are also defined in this deliverable so as to help understand and visualize the importance of the proposed NetApp ecosystem and the value it will bring.

2.3.2.2 Source

Text included in subsections related to the EVOLVED-5G is copied from one or more documents that can be found via the following links:

https://evolved-5g.eu/

https://evolved-5g.eu/wp-content/uploads/2021/11/EVOLVED-5G-D2.1_v1.4.pdf

https://evolved-5g.eu/wp-content/uploads/2021/11/EVOLVED-5G-D7.2-v1.0_final.pdf

2.3.2.3 Roles and Actors

The following Stakeholders have been identified as important for the EVOLVED-5G ecosystem. This is a basic and non-exhaustive list of all the possible actors that may be interested in NetApps, that is used to further drive the requirements analysis:

SME/Industry 4.0 SME: Industry 4.0 SMEs are vertical providers and businesses that are interested in exploiting and bringing the new functionality provided by the 5G infrastructure so that it can be used in order to improve their new or existing applications (Vertical applications or VApps), exposing this functionality through the NetApps. Although main target is i4.0 SMEs, EVOLVED-5G also seeks impact on other 5G-enabled vertical industries. This broader vision makes the project to also consider SMEs from other verticals that would eventually benefit from the ecosystem.

Developers/Industry 4.0 NetApp Developer: The NetApp developer, that can be an SME or a bigger software company, focuses on developing the NetApps with the aim to exploit the capabilities of the 5G network.

Technology providers/5G Equipment Vendor and Device Manufacturer: These actors provide the hardware required in order to create a 5G infrastructure and to consume their services as end-users or during experimentation. They may be interested in making use of the NetApps for the implementation of the control software of the equipment.

Connectivity providers/5G Network Provider: Traditionally this stakeholder refers to the MNOs (Mobile Network Operator) that have control over the network infrastructure and radio spectrum allocation required in order to provide wireless communication services to end users. From the point of view of EVOLVED-5G, MNOs are more interested in the certification of certain NetApps for usage within their networks, which can be distributed through the Marketplace. Nevertheless, as the Industry 4.0 business case has a strong footprint on Non Public networks (NPN) the role of the Network Operator within EVOLVED-5G, can be assumed by a company or research organization that has D2.1 Overall Framework Design and Industry 4.0 Requirements GA Number 101016608 26 the license and expertise to operate a campus network, thus providing the validation framework to onboard the NetApps.

2.3.2.4 Pre-conditions

With the emergence of Industry 4.0, factories and manufacturers are pressured to increase their production and effectiveness by including new technologies and equipment. Industry workers are directly affected by these changes and as such they are more and more encouraged to interact with machines and collaborate using digital systems.

The Interaction of Employees and Machines (IEM) pillar aims at addressing the challenges related to this new paradigm and help the involved parties to boost their work performance. Within the scope of EVOLVED-5G project, 3 mains areas have been identified with respect to each of the 3 SME partners of the pillar:

Supporting the work of employees via autonomous chatbot-driven systems (INF).

Allowing efficient collaboration between remote workers (IMM).

Facilitating verification and certification phases (GMI). To solve each of these challenges, a suitable network infrastructure must be available within factories and 5G capabilities are at the heart of the envisioned IEM NetApps.

2.3.2.5 Triggers

Seven main research challenges that HCI has to face. First, social information processing must consider multimodal communication facets. Secondly, there is a need to investigate on the nature of the cognitive processes that mediates, the psychological paradigms that engage them, i.e., goals, beliefs, expectations, and the emotional effects on cognition. Thirdly, group interactions contribute to the development of creative ways and new ideas to solve problems (Group Cognition). Understanding the processes underlying individual and group cognition is fundamental for the development and implementation of theoretical and computational models that regulate cognitive behaviours in group interactions. Fourth, machine learning and artificial intelligence techniques must integrate contextual, multimodal and real-time processing capabilities from different types of inputs and stimuli (voice, movements of the head and body), and provide multimedia output that can adapt and meet the different users' needs, exhibiting autonomous behavior, context aware perception, and action control abilities. Fifth, databases of interactions need to be generated in order to enable researchers to train, test, and compare their systems as well as compare their performance and behaviours with humans. Sixth, the design of human–machine interfaces must focus on human end-users, their abilities, aptitudes, preferences, and desires. Moreover, interfaces must be accessible and usable by a wide variety of users. Seventh, the exploitation of intelligent, and socially believable ICT devices demands principled design methodologies that accommodate all potential users' requirements.

2.3.2.6 Normal Flow

The first IEM challenge is based on AI-driven systems to support the work of employees. Under the continuously changing conditions of a rapidly changing world, there is an increasing growth of AI's impact in Industry 4.0. Industrial AI is a systematic discipline, which focuses on developing, validating and deploying various machine learning algorithms for industrial applications with sustainable performance. It acts as a systematic methodology and discipline to provide solutions for industrial applications and function as a bridge connecting academic research outcomes in AI to industry practitioners. The capacity to support and control big flows of information is one of the most important applications of Industry 4.0, which relies on the maintenance of artificial intelligence networks that could lead to newer and innovative methodical approaches for planning and development of products. Hence, Artificial intelligence plays an important role in the efficient collaboration of Employees and Machines. Chatbots are one of the most important applications of Industry 4.0. They combine artificial intelligence and Human–computer Interaction (HCI). According to the dictionary, a chatbot is "A computer program designed to simulate conversation with human users, especially over the Internet". It uses Natural Language Processing (NLP) and sentiment analysis to communicate in human language by text or oral speech with humans or other chatbots. Furthermore, in factories, chatbots have become so common because they reduce service costs and can handle many customers simultaneously.

2.3.2.7 Alternative Flow

N/A

2.3.2.8 Post-conditions

The FoF NetApps developed during the project will increase the efficiency and safety of FoF operations. According to the FoF needs, it will allow to fully exploit the novel business opportunities such as:

Industrial grade 5G connectivity hardware and applications.

5G network anomaly and telemetry detection applications.

Applications for automated occupational safety analysis.

2.3.2.9 High Level Illustration

FoF IoT System architecture is depicted on the figure below and consists of Industrial IoT GW and Backend System Components with the following functions:

FoF IoT Management; a centralized management of IoT probes/IoT gateway with status monitoring and OTA updates options.

FoF IoT Collector; data collection function (centralized or distributed deployment) used to store KPIs and metrics from IoT probes/IoT gateway.

FoF IoT Reporter; real-time analytics and alerting.

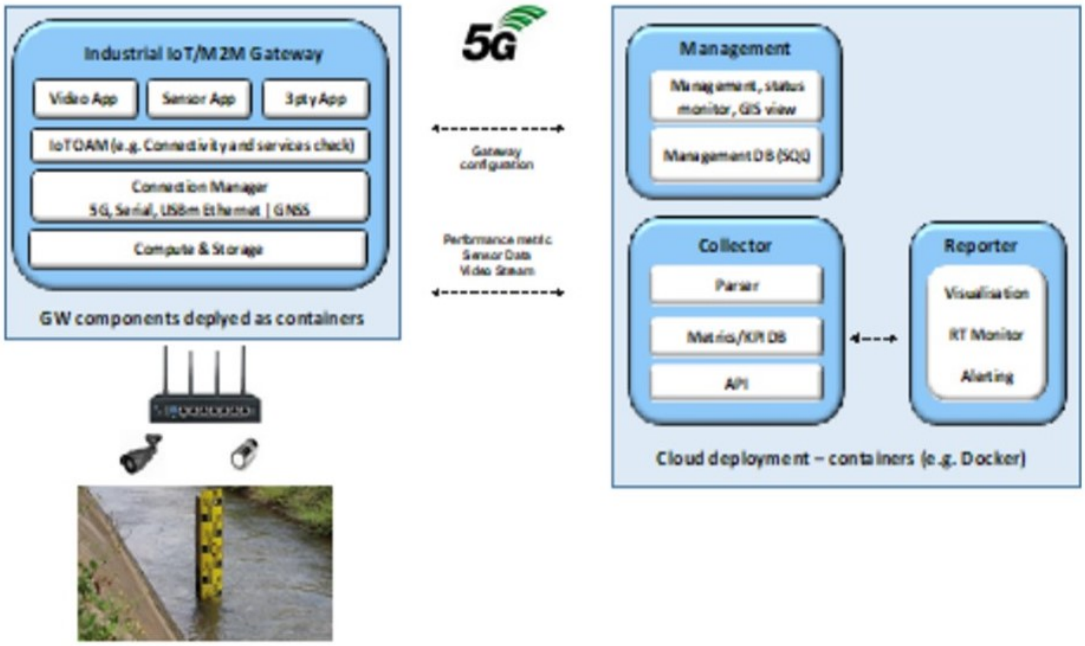


Figure 10: FOF IoT System Architecture

2.3.2.10 Potential Requirements

THE EVOLVED-5G PLATFORMS The EVOLVED-5G project makes use of two different platforms located in Athens (composed by two sites: NCSR Demokritos and Cosmote) and Málaga. The two platforms provide 5G capabilities and cloud infrastructures where Open5Genesis framework for the coordination of the experiments is deployed.

The two platforms provide support for the execution of the Validation and Certification processes, by making available their containerization environments for the deployment of the Network Applications, as well as a real 5G network that Verticals can use for the execution of additional tests more related to the specific functionality of each particular Network App.

The Athens platform is comprised of two testbeds, NCSRD and COSMOTE, which are interconnected through a 10G direct fiber link. For platform assessment, the two sites act as independent full 5G SA solutions that are evaluated using the Open5Genesis experimentation framework, which dictates the lifecycle of the experiments. As shown in Figure 1, Open5Genesis is hosted at NCSRD's premises and manages and orchestrates all the experiments. The first 5G SA network is based on the ATHONET 5G SA Core and ERICSSON BBU/RRU/RAN which is deployed at the COSMOTE campus. The second 5G SA network is deployed at the NCSRD campus and is based on the Amarisoft 5G solution.

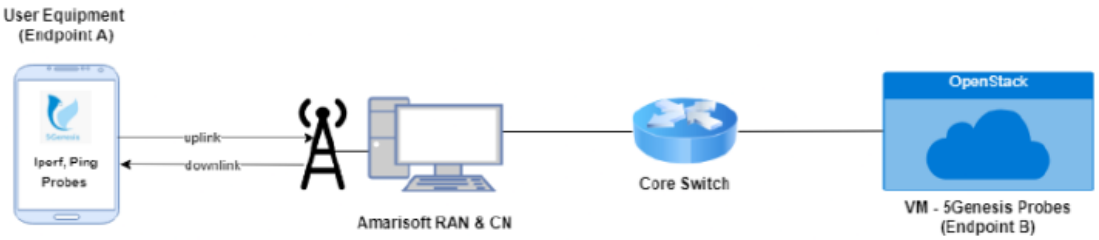


Figure 11: NCSRD site testbed setup

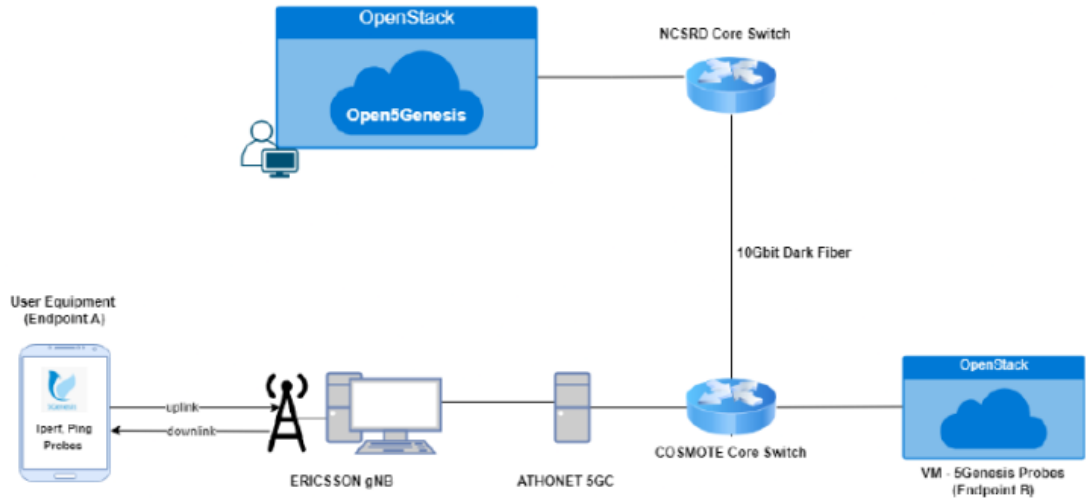


Figure 12: COSMOTE - NCSRD sites testbed setup

The framework is composed of three layers:

Management and Orchestration (MANO) layer: Handles virtualization, network slices, and virtual resources management.

Coordination layer: Responsible for the overall coordination of the experiments, including experiments' life cycle management, KPIs monitoring, and analytic results presentation.

Infrastructure layer: Handles user traffic providing 5G network connectivity.

Throughput measurements

Amarisoft/NCSRD Downlink Mean Throughput: 331.3 Mbps

Athonet-Ericsson/COSMOTE Downlink Mean Throughput: 905.73 Mbps

Amarisoft/NCSRD Uplink Mean Throughput: 48.49 Mbps, best: 214.18 Mbps

Athonet-Ericsson/COSMOTE Uplink Mean Throughput: 67.58 Mbps

Latency measurements

Amarisoft/NCSRD Mean RTT: 28.69 ms, Lowest: 9.99 ms

Athonet-Ericsson/COSMOTE Mean RTT: 15.78 ms

2.4 Extreme pervasiveness of the smart mobile devices in Cities

2.4.1 Smart City Edge and Lamppost IoT deployment

2.4.1.1 Description

This scenario demonstrates the usage of 5G networks across different verticals (domains) driven to the proliferation of smart cities. Given the market trends and spectrum capabilities, the tendency of disseminating such networks in urban scenarios has been performed by the usage of small cells, typically equipped with low-range communication Radio Access Networks (RANs). These small cells are spread across strategic geographic locations within a city, to increase bandwidth and decrease latency for the evermore demanding verticals (such as high-definition media transmission, automated driving or secure video analysis). With the purpose of facilitating the distribution of networks and computing resources at the network edge, the scenario uses streetlight poles to accommodate physical infrastructures to provide resources such as the RAN, computing and network capabilities.

Another important aspect of this type of scenario is the ability to provide a neutral hosting platform for multiple hosted clients (e.g. Mobile Network Operators (MNOs), private operators, content distribution networks). Hosted clients are entities using a portion of the resources provided by the neutral host (e.g. the lamppost owner, a city or utilities provider) which is governed by a commercial agreement including a detailed Service Level Agreement (SLA).

In this use case, the mentioned features will be showcased by exploring (i) the potential of video streaming in 5G in dense scenarios and (ii) video processing employing computer vision at the network edge. The demonstration of (i) happens with the deployment of a dedicated slice for the video transmission in a crowded location (e.g. near a football stadium or a well-known motor race) simulating a significant number of user equipment (UE) units. This way it demonstrates the interactions required to share the infrastructure between the MNO that provides 5G connectivity to their users in a dense scenario with another hosted client, in this case, a Civil Protection entity, which receives the transmission of the video and the generated alerts. The demonstration of (ii) focuses on the capability of having computation resources available at the network edge. The physical enclosure of computing hardware must be suitable for the required processing power for efficient computer vision processing.

In this particular scenario, the team aims at automatically detecting and classifying emergencies through the analysis of video streams using computer vision software, including Machine Learning (ML) algorithms. The video processing will take place at the edge of the network, exploiting its compute resources, to decrease the backhaul bandwidth usage to the core network and reduce the latency of alerts upon emergency event detections. As soon as the system identifies an occurrence or emergency, it generates an event and sends it to the monitoring platform in the cloud, namely Ubiwhere's Urban Platform. This innovative cloud solution provides a global and integrated view of a region, through centralised collection and processing of data from heterogeneous sources and city systems, while offering integrated and customisable workflows for a more efficient and coordinated response to incidents, deployed at the core network.

2.4.1.2 Source

Affordable5G H2020 5GPPP project

2.4.1.3 Roles and Actors

Mobile Network & Private Operators. Take advantage of urban furniture as infrastructure (lampposts) with neutral hosting capability for the deployment of 5G services with low OPEX and CAPEX costs.

Civil Protection Organization. Access to video streaming in crowded locations for a better operation and response, and also, an available tool to identify (using video streaming) emergencies.

Cities & Municipalities. As potential owners of the infrastructure, they can have revenues from the infrastructure renting to multiple tenants and with the installed resources/services, providing better security in the areas covered by the infrastructure.

Citizens. Citizens who live or move close to the infrastructures that see their security increased.

2.4.1.4 Pre-conditions

There are optical fibre and electricity (power) capabilities near the used infrastructure (lampposts), to support the communications and power to the installed hardware.

2.4.1.5 Triggers

The trigger for this scenario is the automatic detection of dangerous or emergencies.

2.4.1.6 Normal Flow

The video streaming will be processed in the edge, exploiting its compute resources, to identify danger or emergency events.

Once an occurrence is detected, the system generates an event and sends it to the monitoring platform, namely the Urban Platform, deployed at the core network.

After receiving the automatic event alert of a potential emergency, the Urban Platform operator can request a live feed (using the dedicated slice) of the origin video stream to avail the situation.

Besides, the Urban Platform should also be able to access the recorded images that led to the triggering of the alarm.

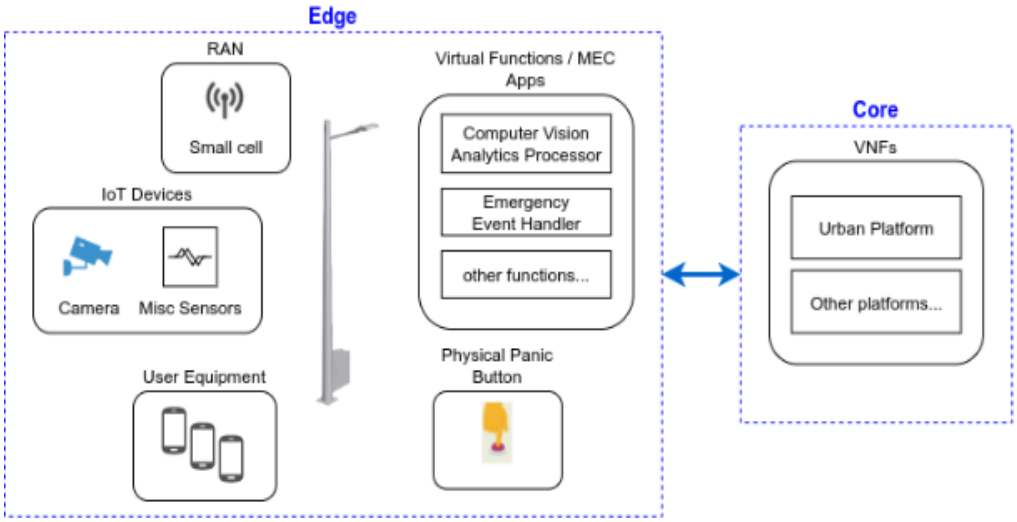
2.4.1.7 Alternative Flow

None

2.4.1.8 Post-conditions

The Civil Protection works to send all the required resources to the place where the emergency event is taking place. After the validation of a real emergency event, the Urban Platform store all the video transmission to future analysis and identification of the responsible people for the event.

2.4.1.9 High-Level Illustration



2.4.1.10 Potential Requirements

Functional Requirements

The solution should provide an environment for running software for data processing and service provisioning.

A centralised solution should allow registering specific users (authentication) under specific roles (authorisation) while keeping a log of all access attempts to external reference points (RESTful APIs, RPC daemons, etc.).

The solution should support the orchestration of services as well as lifecycle management.

The solution should allow monitoring of security-related events, e.g. network traffic connections and loads per source and destination, presence of known attack signatures, failure to authenticate, etc.

Non-Functional Requirements

The solution should be highly efficient in terms of energy consumption, computing resources and bandwidth.

The solution should support services running in lightweight VMs or Docker containers.

2.4.1.11 Radio Specific requirements

Requirement	Target
Latency (User Plane)	5 ms
Reliability	99.999%
Multi-tenant support	Yes
Dedicated slice	Yes

2.4.1.12 Other requirements

Requirement	Target
Computer vision-based automatic detection of emergency scenario	5 sec
Video bitrate per channel	30 Mbps
Video compression rate	40%
Video encoding induced latency	5 sec

2.4.2 Multi-tenant real time AI video/audio analytics

2.4.2.1 Description

Deploying at scale Smart City Services requires leveraging Edge computing to reduce processing latency and bandwidth requirements. Currently there is no shared, efficient and secure Edge as a service platform, where multiple data collectors and service providers could run their application. Use Case 2 addresses the case of smart city applications that perform distributed video and audio analytics. Instead of single service providers with own infrastructures, UC2 demonstrates a scalable, heterogeneous and multi-tenant service infrastructure for traffic analysis, surveillance, smart transportation, emergency response. A key advantage of this application scenario relates to the ability to avoid the deployment of multiple hardware platforms to address the need of heterogeneous third-party service providers. Especially in the context of a Smart City, real estate, energy constraints and more general sustainability considerations, e.g., on e-Waste, strongly Identify Infrastructure consolidation as a driver for future In-city compute systems.

In particular, this use case showcases a full processing pipeline for audio-video analysis, which comprises all the elements for: data acquisition over 5G connectivity; pre-processing for quality/performance adaptation; filtering and replication for multi-tenancy and privacy handling; and analysis.

The use case will enable effective and economically viable deployment of AI analytics at the edge In the context of Smart Cities. This will reduce the cost to deploy functions and simplify their deployment. Demonstrating the ability to run multitenant analytics applications on the same platform provides an opportunity to separate the service providers roles from those of the Infrastructure providers, allowing for specialization of the market players and Increase of the overall market value.

2.4.2.2 Source

BRAINE Project

2.4.2.3 Roles and Actors

Edge provider: edge node owner, manages the edge node

Application provider: provides the software that implements the use case, may be a "tenant" on the edge node

Cloud provider: provides the remote infrastructure

Service provider: provides the end-to-end service to implement the use case, combining the services from application, edge and cloud provider

Service consumer: buys the service from the service provider, and uses it

Service subjects: stakeholders passively involved in the service, e.g., people appearing in the monitored videos

2.4.2.4 Pre-conditions

Cameras are deployed (together with auxiliary sensors) and the functional services based on camera feeds (e.g. AI based user tracking) are operational in the BRAINE system.

Network connectivity (e.g. fiber link managed by the SDN controller) between different edge sites (or also cloud if needed) must be ensured.

5G frequency band for the 5G operations must be secured.

Various workloads including the 5G network workloads (e.g. vRAN, Core) are available in the "docker repository" and available for the Authoring system of the BRAINE to be deployed in the BRAINE edge nodes (EMDCs).

Applications:

There are several applications that fit the use case scenarios depicted In this document. We report few examples below:

Road monitoring: Vehicle flow assessment; crowd detection; etc

Emergency detection: Dangerous situations detection, e.g., road accidents; fire detection etc.

Pedestrian flow tracking: relevant for city operations planning; law enforcement etc.

In all these applications, there are the following challenges to address at the application-level:

Accuracy. Due to the extreme variability of the external conditions, Computer Vision algorithms are subject to false positives (FP) and false negatives (FN). The multi-tenant AI architecture relies over parallel computing pipelines in order to increase the overall detection performance.

Weather conditions. BRAINE algorithms and infrastructure address rapidly changing weather conditions for 24/7 working applications. In case of extreme weather conditions, performance degradation are expected for those systems relying on visual information. Audio devices might also be affected.

Applications deployment. The edge node supports multiple applications. Since the cost of running each application analysis is variable and may be application-dependent, some running applications may affect the performance of other applications, requiring performance isolation guarantees.

Below we list the challenges at hardware-level

Hardware resource limitations. The relatively limited resources of a single edge node may be quickly depleted in presence of workload spikes. This may require a high degree of cooperation among edge nodes, in case of an overloaded node. These measures may anyway affect the overall system performance and its ability to maintain the minimum QoS requirements for all edges.

Remote accesses. In the event of an edge hardware/software malfunction, the device may need to be accessible through a secure maintenance service (e.g., VPN) to restore the operative condition.

Unstable communication links. Due to the required bandwidth for video and audio analytics, even the slightest interference over the link medium can reduce the multimedia stream quality. If available in the location, wired communication interfaces may be deployed/preferred to assure a more deterministic and reliable communication link.

System reliability. In real world applications, failures might be related to unstable power supplies, sudden power line spikes, extreme temperature, vandalism, etc. In case of an edge failure, the system has to react (e.g., managed by an orchestrator) to redistribute the affected workload to other connected edge nodes and provide operations continuity.

2.4.2.5 Triggers

What are the triggers used by this use case

The use case is composed of the 'deployment' phase where vRAN is being deployed and becomes operational, and 'adaptation' phase where due to some external trigger BRAINE platform adapts the application and infrastructure workloads, including RAN deployment, to new conditions (by e.g. scaling the workload to other edge nodes). The trigger in the case of this use-case is the change of the number of active users which connect to virtual-RAN base station or the detection of object and/or anomalies in the scenes.

At the application level, changing conditions of the monitored scenario (audio/video), may require the application of different types of data pre-processing and analysis algorithms. For Instance, changing weather conditions may require the application of different analysis models, which might be more or less expensive on the computational side.

2.4.2.6 Normal Flow

The monitored subjects, e.g., pedestrians, vehicles, are monitored through the use of distributed cameras and microphones. These devices transfer data to the edge platform, which collects the data streams and performs on-the-fly analysis.

2.4.2.7 Alternative Flow

While not planned in the current use case, It Is possible to store data locally and trigger processing in a second step.

2.4.2.8 Post-conditions

When a specific type of monitoring Is terminated, the corresponding analytics applications are terminated, and the platform resources are cleared.

2.4.2.9 High Level Illustration

The use case focuses on the ability of providing the entire data processing pipeline at the edge, without relying on data transfer to a centralized cloud.

Figure 13 shows this concept, with multiple audio-video sensor devices connected to "data adapters" (orange boxes) which are then handled by a pipeline of pre-processors, e.g., privacy enforcers (green boxes), a data fusion/API layer that enables Interaction between third-party multi-tenant services and the platform, and finally the analytical services (blue boxes). Each edge deployment replicates this architecture, and while the edge platforms are connected to a central cloud aggregator, it is assumed that most data processing Is retained at the edge, thus reducing the core network bandwidth requirements.

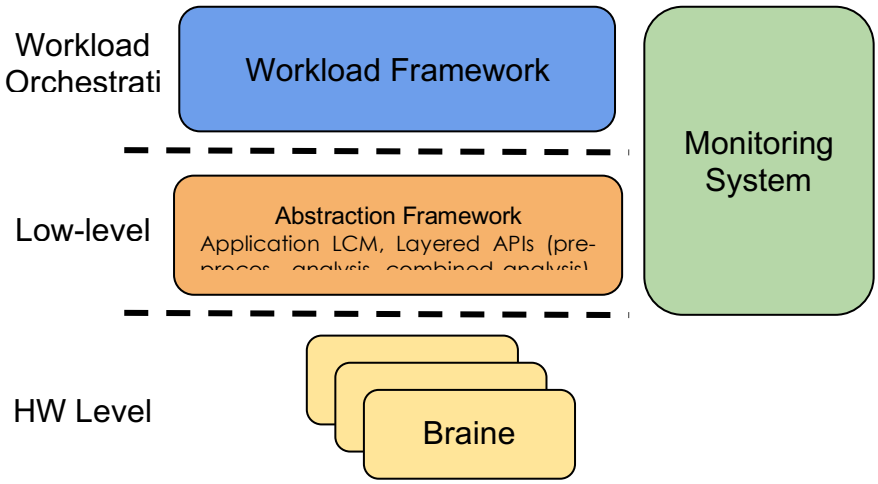


Figure 13 Block Diagram

Each edge node implements the high-level architecture depicted in **Figure 14**. On top of the hardware level, In this case the BRAINE edge platform, the service components are deployed as self-contained microservices. Platform's monitoring and workload management frameworks take care of matching the resource requirements with the available hardware resources.

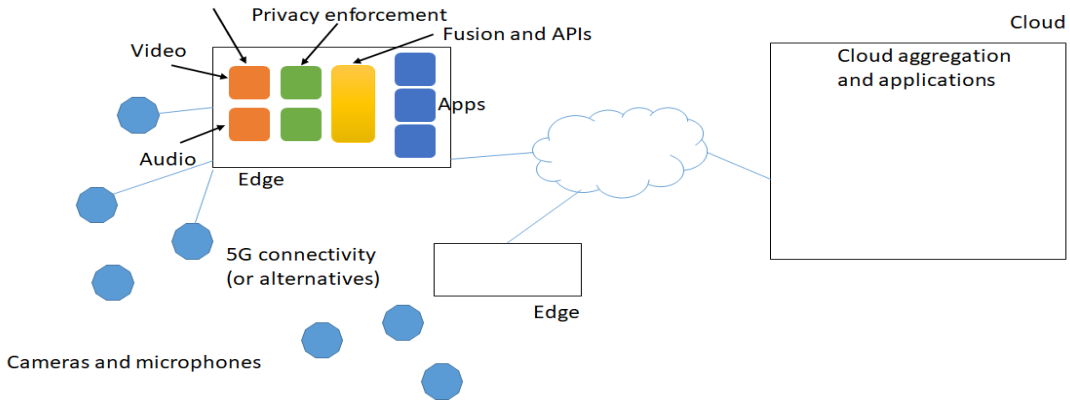


Figure 14 Architecture

2.4.2.10 Potential Requirements

This section provides the potential requirements and in particular the requirements imposed towards the underlying communication technology

Network (Bandwidth/Slicing)

Worst case is 200 Mbit/s for each camera

Computing

at least one GPU/Video accelerator (for both pre-processing and analysis)

16GB RAM

1-10TBs of storage for data

Data Exchange

Camera streams from camera to EMDC

Metadata (XML/JSON) available at the edge platform after the processing

Workload

2.4.2.11 Radio Specific requirements

2.4.2.11.1 Radio Coverage

Radio cell range

The cell coverage in a target deployment can utilize ultra-dense deployed cells or the heterogeneous cells with macro/micro presence at same time. Most of the coverage will be suitable for the outdoor location and in places the cameras can be supported by auxiliary sensors (e.g. audio). But the indoor coverage with small-cells or ultra-dense network for the e.g. hospital, factory, etc should also be considered. Besides the cell range, it Is important that cells are deployed following the concept of open-RAN networking (according to ORAN Alliance specifications). Radio range should be based on the radio units (RU) deployed, based on the technology specific to the most popular functional splits like: split 7.2, split6. The use case should also be able to operate under the novel paradigms like cell-free. The cameras would utilize either LOS or NLOS connectivity depending on its location. Connectivity for cameras would in many cases cross public spaces (like shopping malls, old town, governmental buildings, etc).

Is Multicell required?

Multi-cell is an option, and it preferably understood as cell-free operation of the network, where there is potential to allocate radio resources of multiple cells between TTI periods, i.e. not based on a single "best signal" association of the UE to the access point (AP) with handover as key mechanism enabling the change of serving cell, but more flexible allocation of UE to AP with much finer granularity. This way handovers are not required as connectivity of portable cameras (e.g. mounted on buses, robots) can be provided In a cell-free style. Multi-cell here can be both -- Indoor or outdoor. The cell-free approach has high potential of Increasing available capacity of the network.

Is handover required? Seamless? Tolerable impact in delay and jitter?

Handover Is not required in the current scenarios especially If the cell-free compliant networks are deployed.

Mobility: maximum relative speed of UE/FP peers

Considering the use-case specification the typical usage considers fixed cameras, but It is not restricted to such cameras only. If needed, cameras can be mobile and the 5G (and beyond) resource allocation should be adjusted.

Special coverage needs: i.e., maritime, aerial

No special needs

2.4.2.11.2 Bandwidth requirements

Peak data rate 100 Mbps per camera

Average data rate 20 Mbps per camera

Is traffic packet mode or circuit mode? Packet mode

2.4.2.11.3 URLLC requirements

Required Latency: below 2ms (specify if it is one way or roundtrip)

Required Reliability: 99,9999%

Maximum tolerable jitter: 0.5ms

2.4.2.11.4 Radio regimens requirements

Desired and acceptable radio regimens (describe the desired and acceptable radio regimens: i.e.: licensed - public mobile, licensed – specific license, license-exempt)

Multiple modes of spectrum access and operation are possible. The mode depends on the stakeholders business models followed.

2.4.2.11.5 Other requirements

UE power consumption

Rechargeable or primary battery?

Devices (Sensors) are expected to be plugged in power sources. Some microphones might have only battery available

Acceptable battery life: At least 1 month

Is terminal location required? location accuracy? No

2.5 Autonomous Urban Transportation

2.5.1 Intelligent Assistive Parking in Urban Area

2.5.1.1 Description

This use case presents a solution for intelligent assistive parking in urban areas in order to reduce or redirect unnecessary traffic, avoid traffic congestion and reduce emissions in populated areas. It can reduce traffic-related injuries caused by a lack of attention when looking for vacant parking spaces on the roadside and save drivers' time.

It is based on a use case that was submitted by an AIOTI member to the ISO/IEC 22417:2017 IoT use cases.

The tagline is that most car owners and citizen possess something that is of great value to others; areas that can be used as parking space. Many do not use this space during normal workdays, as they are using their car to drive to their workplace, resort, etc. This privately owned vacant spot represents an idle fond and could help solve many of the challenges associated with lack of free space in urban areas and meet market dynamics. The following conditions are assumed

Private owners of car space or similar vacant areas wishing to profit from renting out available car space

Car drivers in search of parking space have access to a larger resource pool

Car park owners, markets and event managers are able to offer this solution as an extra service for their customers, in addition to identifying nearby areas that are still vacant

City officials benefit from smart city tools, and get a real time view of occupancy of available parking space reduced traffic and pollution in urban areas, in addition to getting access to statistical information about parking

This use-case demonstrates integrating transport information between smart house, assistive living and eHealth to achieve increased predictability for the usage of the infrastructure and areas around the parking space. Intelligent parking for residents with particular needs is especially suited for health buildings and clusters of housing estates tailored for user groups like cancer patients and people with various physical disabilities like wheelchair dependent.

In order to address the needs of the individual residents, management of parking space and proximity to access points is tailored to user-defined profiles. **Safety, predictability, reliability, accessibility and comfort** are elements that are incorporated when implementing load balancing and resource administration of parking space and available areas. Access control and appraisal systems are functionality that needs to be supported. This is affected by what kind of user that wants to use the parking space.

Visitors need to be kept separate from residents, but the needs of the user and preferred actions will have an impact on the recommended parking space/placement. **Moreover, healthcare and blue lights agencies must receive particular priorit**y.

In a typical solution, prioritized parking space, booking, heating management, traffic analysis, customized and messaging services based on biometric data are adjusted according to stored rules. Home control centres operate both, locally and interact with external services and communication units. The sensors report proximity and temperature, which are accessible for the health house and made available to the virtual neighbourhood. A mobile app report status for the parking space and report status from the health home. Both booking and configuration of units in the virtual neighbourhood are available through the mobile app.

2.5.1.2 Source

ISO/IEC 22417:2017 IoT use cases [ISO/IEC TR 22417:2017]

2.5.1.3 Roles and Actors

Vehicle user Person that needs a parking space close to their destination

Parking space stakeholder. Property owner having one or more parking space available at certain times during the week.

Blue light agencies. Certain agencies that must have access to parking spaces when on emergency calls.

Cloud service. Runs the cloud service application that manages parking monitoring system set up and operation.

Smart city Management System allowing municipality to exploit available resources in order to reduce traffic congestion and pollution thereby improving living conditions and policing regulations.

2.5.1.4 Pre-conditions

It is assumed that parking sensors lack a visual user interface or have a limited user interface. During the operation of the system no user interface is needed but another device, with a user interface, must be used for the system set up and authorization process through the device's web browser or a through a native application running in the device.

The pre-conditions are the following

Parking sensors connected to cloud

Device with UI, e.g. a laptop or a smartphone connected to cloud.

Control system connected to device with UI through some kind of local connectivity method, e.g. Bluetooth or USB.

2.5.1.5 Triggers

A user is driven to a hospital under emergency, and a parking place must be allocated. The use does not have an account to the reservation system.

2.5.1.6 Normal Flow

User (or person assisting user) logs into parking space management web site. If the user has an existing account, e.g., Google or Facebook, this could be used for the log in process.

User starts set-up process by pressing a button at the smartphone

User approves that the control system is used with the remote parking space application.

2.5.1.7 Alternative Flow

No alternative flows are defined.

2.5.1.8 Post-conditions

The parking sensor is actively monitoring which vehicle is using the space and prepare billing when booked time is over, remind car owner if overtime and additional fees applies

2.5.1.9 High Level Illustration

2.5.1.10. Potential Requirements

Functional Requirements

The functional requirements are the following

Agile and rapid creation of emergency account, automatically created by a blue agency

Non-Functional Requirements

The non-functional requirements are the following

Availability

Real-time

Predictability

Post emergency settling (e.g. evidence of emergency)

Security and privacy

The smart parking industry is facing several challenges related to non-functional requirements, when preparing an area suitable for shared parking:

regulatory challenges: if an area is set to be used for a different purpose, this needs to be communicated and receive permission. An area planned used for a building cannot be redefined as suitable for parking without some kind of planning and reallocation.

insurance: insurance companies are very weary of unplanned use or other parties getting access to a site that is not assigned for commercial use. If a car is damaged by a visitor using shared parking or if the batteries of an electric car placed on a parking spot is ignited, who will be responsible? The owner of the parking space or the current temporary user.

responsibility: the same applies to when a car is parked for too long. Or perhaps even has been placed in the wrong parking space. Or if the car is blocking for other vehicles - and in worst case scenarios - are blocking for emergency vehicles such as ambulances.

payment: there are usually limitations on how much an owner of a unlicensed parking space can own by renting it. The amount may differ between municipalities and countries, but there need to be some kind of taxation system being assigned and reporting

risk: allocating an area for parking, also means that one communicates the availability of a location to third parties. These third parties can be considered as unknowns and can also pose as a security threat when gaining access during daytime or when the area is indicated free to use.

privacy: the mobile app, accompanying cameras, GPS position with more. All of these can be part of a parking space area and may represent a threat to the privacy. One thing is the driver using the area for parking, another thing is the owner of the parking site that may use the information for other purposes than originally intended.

Parking areas can be classified as:

I: unregulated parking

II: roadside and sidewalk

III: open parking/assigned parking space

IV: restricted parking/barrier

V: building/garage

Just as important, the properties of the area used for parking:

is it paid access, is it free to park, what cost is prepared? will the cost differ depending on the time of day?

is the site monitored using camera

are there sensors installed - not only parking sensors, but also motion sensors and other equipment that identifies arrival and departure

is the area illuminated, what kind of light is used, is the area soundproof?

does the area support trucks and motorhomes, or is suitable for micro-mobility solutions like bicycles and electric scooters

do the parking space support charging - and what kind of effect, voltage, and cost is relevant

are there considerations regarding fumes or other toxic gases - will this influence who can park and for how long

what properties does the ground exhibit, such as grass/clay, gravel, asphalt/concrete

Furthermore, there are other technology-related considerations, such as:

What is beneath and above the parking space

Will there be electronic interferences

Will it be future proof, for instance supporting electric paint or indirect charging

What about cables - standards, dimensions etc.?

How about support for network and 5G?

How will Wi-Fi and z-wave function?

Will the structure serve as a faraday cage?

Based on this, a matrix describing the parking space can be defined, and each area can be allocated a unique id that can be used for tracking and assisting expert systems in selecting the most suitable parking space based on a number of parameters such as cost, priority, distance, size of vehicles, special demands from the owner of the space or the driver etc. what about the different sizes of the parking space?

European, American and Asian cars differ in size and needs. is the parking space placed in uphill locations, near a corner, close to an exit door, is it thin and narrow, long and wide, is it close to a backyard or just available for a particular use - such as for janitors or homecare service?

2.5.2 5G-VICTORI: UC #1.1: Enhanced Mobile Broadband under High Speed Mobility

2.5.2.1 Description

UC #1.1 proposes a multi-technology infrastructure to provide connectivity to a train as it moves along a railway track. Three to four points along the tracks around the city of Patras were chosen to guarantee the coverage required to ensure seamless connectivity for the demonstrated services. The target distance was more than 1 km for a back and forth rail journey. This part of the track was chosen in order to ensure connectivity to the main 5G-VINNI infrastructure at the University of Patras (UoP) premises. On the other hand, this connection requires LoS for the backhaul network from UoP to the track. Additionally, LoS is mandatory to ensure strict alignment for the track to train connectivity.

The services will be provided while the moving train crosses the Patras city centre, through heterogeneous technologies, establishing high capacity low latency connections. High capacity is needed for the former services, to provide high quality of service to passengers, whereas for the latter low latency / ultra-reliable connections are needed support the transmission of real time data obtained from various sources to the train operations, driver and control centre.

2.5.2.2 Source

Text included in subsections related to the 5G-VICTORI is copied from one or more documents that can be found via the following links:

https://www.5g-victori-project.eu/about-5g-victori/use-cases/uc-1-1/

https://www.5g-victori-project.eu/wp-content/uploads/2020/06/2020-03-31-5G-VICTORI_D2.1_v1.0.pdf

https://www.5g-victori-project.eu/wp-content/uploads/2021/09/2021-07-31-5G-VICTORI_D3.1-Prel-Test-Cases-for-Trp-Services_v1.0.pdf (Page 20-24)

https://www.5g-victori-project.eu/wp-content/uploads/2022/05/2022-04-11-D2.4-5G-VICTORI-end-to-end-reference-architecture.pdf (Page 40)

5G-VICTORI deliverable D4.3, "Field Trials as showcase events and vertical business validation", September 2023

2.5.2.3 Roles and Actors

The 5G-VICTORI use case "Enhanced Mobile Broadband (eMBB) under High Speed Mobility" will extend the capabilities of the Patras 5G-VINNI facility to demonstrate eMBB functionality through heterogeneous access technologies for on-board network connectivity in a railway setup. Both business (e.g. infotainment services to passengers) and critical operations services will be provided over a unified, orchestrated 5G infrastructure.

The main stakeholders involved are:

Railway infrastructure and Train operators that require multiple/versatile network services for performing their own critical communication, performance and business services. • Telecom Operators/Carriers (or other engineering companies) that deliver network infrastructure solutions and usually (depending on the agreements) also communication services to Railway and Transport operators.

Passengers usually served directly by Telecom Operators/Carriers. In the context of 5G-VICTORI, we consider a set of 5G technologies integrated, interoperating and deployed together to provide a holistic solution for railway communications addressing also the vision of Future Railway Mobile Communication System (FRMCS), where:

Railway & Train operators, still require the same multiple/versatile network services.

Telecom Operators/Carriers deliver a single network infrastructure/solution and/or services to Railway & Train operators.

2.5.2.4 Pre-conditions

N/A

2.5.2.5 Triggers

Table 3: UC # 1.3 Rail Critical Services - Rail Signaling Requirements and KPIs

Req ID [U/F-TYPE-RQ#]	Description [Descriptive text]	Priority [H/M/L]	KPIs and Parameters [to be measured]
U-FU-3101	The rail signaling part of the Rail Critical Services uses an IxChariot traffic generator which **shall** send traffic over a demo 5G cellular network between "Performance Endpoints" (Endpoints). The Endpoints are located both in the Office (train station) and on the Train, sending traffic in both downlink (office to train) and uplink (train to office).	H	Check that traffic can be sent between IxChariot Performance Endpoints.
U-FU-3102	The rail signaling traffic generator is based on one Console and up to 10 active Endpoints (the minimum license possible). The Console handles the IxChariot application with licenses, users and endpoints. The Console is a Windows application, which **shall** be installed and run on a computer in the Office.	H	Check that the IxChariot Console can be installed and run on an office Windows computer.
U-FU-3103	The rail signaling traffic generator is based on one Console and up to 10 active Endpoints. The Endpoints handle the IxChariot traffic generation and reception, with KPIs figures such as bitrate and latency. A first Performance Endpoint **shall** be installed and run on a computer in the office, a computer supporting a platform like Windows, Linux, Android tablets and phones, IoT HW like Raspberry Pi, and VMs.	H	Check that a first IxChariot Performance Endpoint can be installed and run on an onboard computer, using for example MS Windows.
U-FU-3104	The rail signaling traffic generator is based on one Console and up to 10 active Endpoints. The Endpoints handle the IxChariot traffic generation and reception, with KPIs figures such as bitrate and latency. A second Performance Endpoint **shall** be installed and run on a computer on the train, a computer supporting a platform like Windows, Linux, Android tablets and phones, IoT hardware like Raspberry Pi, and Virtual Machines.	H	Check that a second IxChariot Performance Endpoint can be installed and run on an office computer, using for example MS Windows.

Table 4: UC # 1.3 Rail Critical Services - Point machine Requirements and KPIs

Req ID [U/F-TYPE-RQ#]	Description [Descriptive text]	Priority [H/M/L]	KPIs and Parameters [to be measured]
U-FU-3181	The signal from a real interlocking has to be copied in a way that does not interfere with existing admissions of the signaling system. For this a certified network test access point (TAP) shall be applied to the wired communication channel of the interlocking.	H	Check that the relevant signaling data is copied by the TAP.
U-FU-3182	The data stream copied by the TAP will contain lots of data that is not important for the Signal/Point Machine of 5G-VICTORI. A fake endpoint controller shall be implemented, which takes the raw data from the TAP, processes it and then transmits it to the 5G-VICTORI network. The endpoint shall also be capable of monitoring relevant data to measure other KPIs.	H	Check that the endpoint sends correct data to the 5G-VICTORI network. Check that KPIs are monitored.
U-FU-3183	The communication has to be passed from the fake endpoint controller near the interlocking system to the trackside fake object controller. The endpoint and the object controller shall use the 5G-VICTORI demo network for communication. In case of lost connectivity, the system shall log and report.	H	Check that communication can be passed from endpoint to object controller. Check that lost connectivity gets handled.
U-FU-3184	For controlling the signal and the point machine a fake object controller is required, which takes data from the 5G-VICTORI network and triggers the signal model or the point machine model. The device shall be able to communicate with the endpoint via the 5G demo network and trigger the signal/point machine accordingly. The device shall also be able to monitor relevant data to measure the KPIs for the 5G network.	H	Check that communication is processed by the object controller.
U-FU-3185	For demonstration of the correct function of the Rail Critical Service a Signal Model shall be implemented, which controls a small model signal according to the trigger sent by the controller.	M	Check that the signal model behaves as triggered by the controller.
U-FU-3186	For demonstration of the correct function of the Rail Critical Service a Point Machine Model shall be implemented, which controls a small model signal according to the trigger sent by the controller.	M	Check that the point machine behaves as triggered by the controller.
U-FU-3187	To provide evidence of the fulfilment of the KPIs a monitoring system for the communication is required, which also analyses the timings and other required indicators. A system for monitoring these shall be implemented.	H	Check that the monitored data is sufficient to check the KPIs.

2.5.2.6 Normal Flow

This use case differentiates from the prior demonstrated setup in previous 5G-PPP actions through the following contributions on the network side:

2.5.2.7 Alternative Flow

N/A

2.5.2.8 Post-conditions

The infrastructure will provide three types of services: "Business services" such as infotainment, digital mobility, travel information services, etc. A customised solution of COSMOTE Mobile TV over Internet will be used for the demonstrating the context of this UC; "Performance services", including non-critical services related to train operation, including infrastructure monitoring and maintenance services. CCTV – assisted supervision of the rail tracks health and maintenance provisioning is the main performance services to be tested. Cameras mounted on the train are capturing images/video of the tracks, viewed in real time at an emulated Railway Operations/Monitoring Centre – or peer viewer; and "Critical services", where Mission-Critical Push-to-Talk (MCPTT) and Mission Critical Data (e.g. between the controller(s) at the train/ operations centre and the driver/ on-board staff, etc.) are used as indicative applications of this type in the context of this UC.

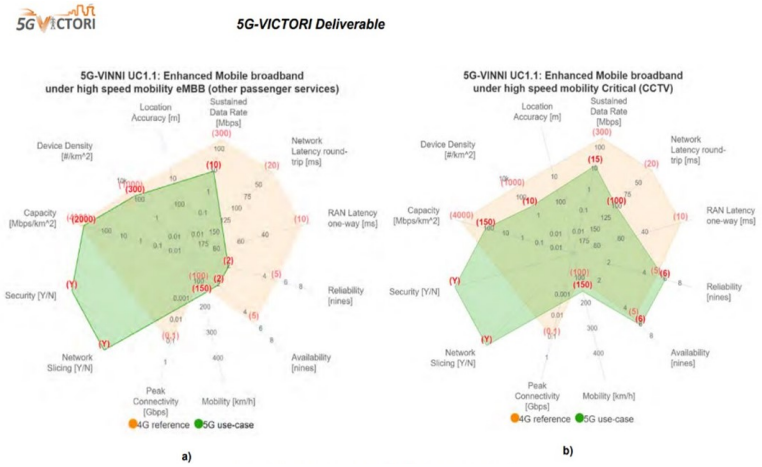


Figure 15: a) UC # 1.1 eMBB, b) UC # 1.1 Critical CCTV

2.5.2.9 High Level Illustration

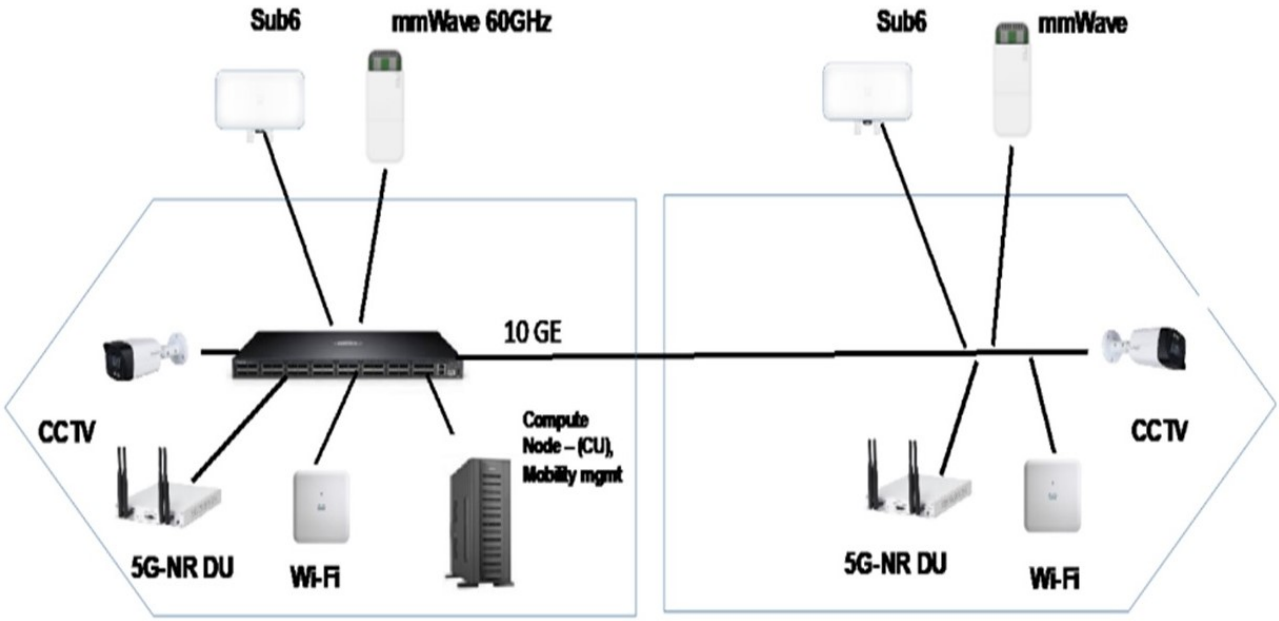


Figure 16: Onboard network architecture

The University of Thessaly (UTH) provides Sub-6 nodes to provide additional means to ensure the communication. Each stanchion has a pair of mmWave and/or Sub-6-GHz Access Points (APs) pointing in one or the other direction of the track, as shown in **Figure 16**.

To maximize connectivity and minimize the disconnection times between handovers from the train to the track APs, the proposed scheme requires antenna modules to be installed both at the front as well as at the rear of the train. IHP's mmWave solution will be able to ensure the connectivity as the train moves in such high-mobility environment. The mmWave nodes will feature beam tracking capabilities to convey data rates of at least 1.3 Gbps over the complete corridor of coverage.

2.5.2.10 Potential Requirements

The 5G-VICTORI track-to-train communication is using a heterogeneous wireless network, consisting of sub-6GHz technologies, through IEEE 802.11ax devices, and V-Band 60 GHz mmWave links. The resource heterogeneity will assist in exploring the diversity that accessing different spectrum provides, allowing the setup of robust track-to-train communication links.

Table 5: UC # 1.1 Requirements foreseen in FRMCS and 5G landscape

UC # 1.1: Enhanced Mobile Broadband Under High Speed Mobility Vertical: Transportation – Rail			Services			
			Future Train operation services (URLLC)	Critical (CCTV)	Other Passenger Services (eMBB)	MCPTT
	UC Requirement - KPI	Units				
1	Latency (min. between user service end-points)	ms	20-100 ms	100 ms	Non Critical	20 ms
2	User Datarate (Max.)	Mbps	100 kbps	10-15 Mbps (Uplink)	~10 Mbps / passenger	100 kbps
3	Reliability (%) - Min/MAX	%	99.9999% (SIL4)	99.9999% (SIL 4)	Not Critical	99.99% (SIL2)
4	Availability (%) - Min/MAX	%	99.9999% (SIL4)	99.9999% (SIL 4)	Not Critical	99.99% (SIL2)
5	Mobility	km/h	50-150 km/h	50-150 km/h	50-150 km/h	50-150 km/h
6	Traffic Density (Traffic demand per specific area)	Mbps / area surface	Non Critical	150 Mbps	max. 1-2 Gbps, assuming 5-10 Mbps/ passenger @ train or station, Total: 100-300 passengers in a cell coverage area, ~max. ave. 1-2 Gbps	Non Critical
7	Device Density (#Devices per specific area)	Devices/ area surface		(non-critical) 2CCTV cameras / train, 5 trains in area of coverage	100-300 passengers/ users per cell coverage area	5 trains in area of coverage
8	Location Accuracy	m	1 m			
	Additional Requirements					
9	Packet Loss Ratio	Num	10^{-6}	0.005	Non Critical	10^{-6}
10	Bit Error Rate		Mission critical	Mission critical	Non Critical	Critical
11	Security (Y/N) ("Carrier Grade")	Y/N	Y	Y	Y	Y
12	Type of Device		IoT devices/ Cameras/ Gateways	CCTV Cameras	Smartphones	KCC clients/ UEs
13	Type of Connection (i.e. Ethernet, WLAN, Zigbee)		5G/NB-IoT/Wi-Fi	5G/Wi-Fi	5G/Wi-Fi	5G/Wi-Fi
14	Battery Lifetime		Non Critical	Non Critical	Non Critical	Non Critical

Table 6: UC # 1.3 Network Characteristics Requirements and KPIs

Req ID [U/F-TYPE-RQ#]	Description [Descriptive text]	Priority [H/M/L]	KPIs and Parameters [to be measured]
F-PE-3201	The Rail Critical Services and other on-board vertical services, using the same 5G air-interface frequency spectrum band 3.8 GHz and the same 5G CPE gateway, **shall** show good performance isolation between the different vertical services, using slicing and QoS.	H	Check isolation between different vertical services using the same 5G air-interface spectrum band.
F-PE-3202	The onboard 5G Customer Premises Equipment (CPE) modem **shall** supports doppler up to at least a train speed of 100 km/h. The reason is to make the 5G connectivity periods longer than what a non-doppler capable modem offers (5G connectivity only when the train stands still).	M	Check that the onboard CPE can connect to the 5G cellular network at a train speed of at least 100 km/h and convey data between onboard and office.
F-PE-3203	The Rail Signaling traffic that are used for the 5G demo purposes onboard the train **shall** have access to a 5G cellular network bitrate between the train and office of around 200 kbps.	M	Check that rail traffic signaling can use a bitrate of around 200 kbps over the 5G cellular network.
F-PE-3241	The HD CCTV cameras that are used for the 5G demo purposes onboard the train **shall** each have access to a 5G cellular network bitrate between the train and office of around 5 Mbps, i.e. 10 Mbps for two HD CCTV cameras.	M	Check that each onboard HD CCTV camera can use around 5 Mbps over the 5G cellular network.

2.5.2.11 Radio Specific requirements

2.5.2.11.1 Radio Coverage

Radio cell range

Does the radio link crosses public spaces? Or is it constrained to indoor or customer premises?

Sub-6 GHz units demonstrated very high coverage (close to 1 km outside the target area of coverage) without LoS. This feature would render them a fit solution for the cases where the terrain only provides nLoS links.

mmWave was able to connect up to 75 m away from the nodes

The coverage is constrained to private places (the railway track) in Patras

Is Multicell required?

Is handover required? Seamless? Tolerable impact in delay and jitter?

Handover or mobility management is required for the connectivity in the track to train communication between Sub-6 and mmWave nodes that are deployed along the rail track.

The mobility management framework needs to cope with handovers in the same technology (change in the association of the onboard mmWave unit **T1**/**T2**), as well as changes across different technologies (handover between different stanchions). The mobility management framework is programming dynamically the flows in the P4 software switches either on the train, or the operation room, so as traffic entering/exiting the track-to-train network is always depicted in the same manner at the two endpoints. To this aim, the flows are set to mangle packet headers (MAC and IP layer) as they go through the switch, and the output port for the ingress/egress traffic is determined by each flow.

Cross-technology handover: Instantaneous losses (lasting less than 500 ms) for packets currently in transit to the network.

2.5.2.11.2 Bandwidth requirements

Sub-6 the most stable setup (and given the mobility of the train) was achieved with the 3x3 MIMO setup for the 802.11ac cards, allowing effective throughput when using a static setup of up to 550 Mbps. Throughput of up to 900 Mbps was observed in the 4x4 MIMO setup, but in a highly unstable manner, and hence the 3x3 setup was used.

Towards being able to achieve higher Modulation and Coding Schemes (MCS) in higher distances, directional panel antennas were used and mounted on the stanchions. The antennas were configurable for their sector size to 60, 90 or 120 degrees (and respective gains of 21, 20 and 19 dBi). Through extensive testing, the 90-degree configuration yielded the highest throughput in higher distances and was selected for the final demonstration.

mmWave (60 GHz)

The mmWave nodes are COTS 60-GHz 802.11ad-compliant devices (Mikrotik wAP 60Gx3). They utilize Qualcomm QCA6335 chip for digital signal processing, supporting up to MCS8 according to the IEEE802.11ad standard. The radio-frequency (RF) front-end is based on Qualcomm's QCA631 chip with three 6x6 phased-array antennas supporting beam steering in 2D. With three sectors, the modules are capable of 180° coverage in azimuth. However, a **net data rate of 1 Gbps** is possible because of 1 GbE connection.

Is traffic packet mode or circuit mode?

The traffic is packet mode.

2.5.2.11.4 Radio regimens requirements

Desired and acceptable radio regimens

Unlicensed schemes due to the use of ISM bands at both Sub-6 and mmWave (60 GHz unlicensed)

2.5.2.11.5 Other requirements

Is terminal location required? location accuracy?

Onboard 5G Network demonstrating the connectivity within the onboard network and the connectivity between the onboard (standalone) network to the 5G-VINNI facility (control room) while the multi-technology (Sub-6 GHz and mmWave) backhaul network is operational.

5G UEs are laptop with Quectel RM500Q-GL modem and **Google Pixel 6 phone** for connecting to the 5G network onboard the train.

static testing:

5G-NR throughput test: peaking at 109Mbps for SISO configuration, for 2x2

MIMO up to 230Mbps were observed, RTT=~ 14ms

Mobility Testing:

5G-NR throughput test: variations between 50-109Mbps, RTT depending on the technology backhaul (mmWave backhaul RTT=~ 14ms, Sub-6 GHz RTT=~ 14 – 25 ms)

2.5.3 5GMETA: Driving Safety & Awareness

2.5.3.1 Description

This use case will provide different services for road end users and public/private companies (such as municipalities or motor insurances) based on the information collected from the vehicle. These innovative services may include, for instance, an emergency-call service for road users, or more simply a road condition or traffic sign notification service that feeds the database of the municipality for fixing the road, or even a motor insurance that protects its clients.

2.5.3.2 Source

Text included in subsections related to the 5GMETAI is copied from one or more documents that can be found via the following links:

https://5gmeta-project.eu/use-case-driving-safety-awareness/

https://5gmeta-project.eu/wp-content/uploads/2024/05/D2.2.pdf (Page 78)

https://5gmeta-project.eu/wp-content/uploads/2024/05/D2.3.pdf

2.5.3.3 Roles and Actors

Third Parties especially from the CCAM ecosystem

Road users , Service Providers, Traffic operators.

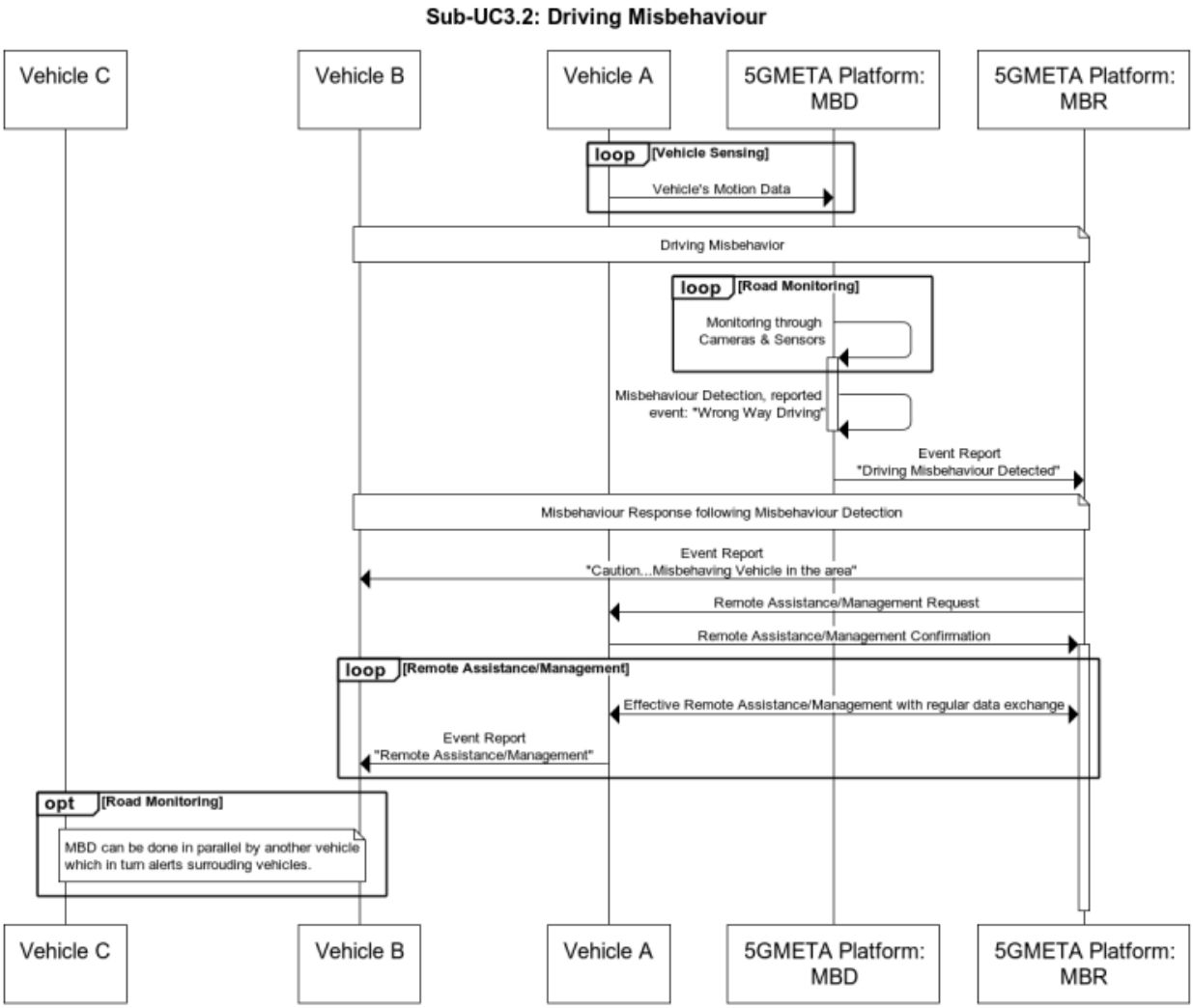
2.5.3.4 Pre-conditions

Third Parties should interact with the 5GMETA platform in order to perform those operations. The main operation exposed are the Data Consumption, and the Event Generation

2.5.3.5 Triggers

2.5.3.6 Normal Flow

In case of in-vehicle safety of life, this use case needs 5G Ultra Reliable Low Latency Communications (URLLC), since the vehicle is supposed to prevent surrounding vehicles to avoid any possible collisions and ultimately make an emergency call to the hospital. This use case also needs 5G enhanced Mobile Broadband (eMBB), as the vehicle will collect a significant volume of data regarding its immediate environment, including, for instance, traffic signs and road conditions. The resulting data will be processed in a second phase by a centralized entity which may in turn feed the database of the municipality and the insurance.



2.5.3.7 Alternative Flow

N/A

2.8.3. 8 Post-conditions

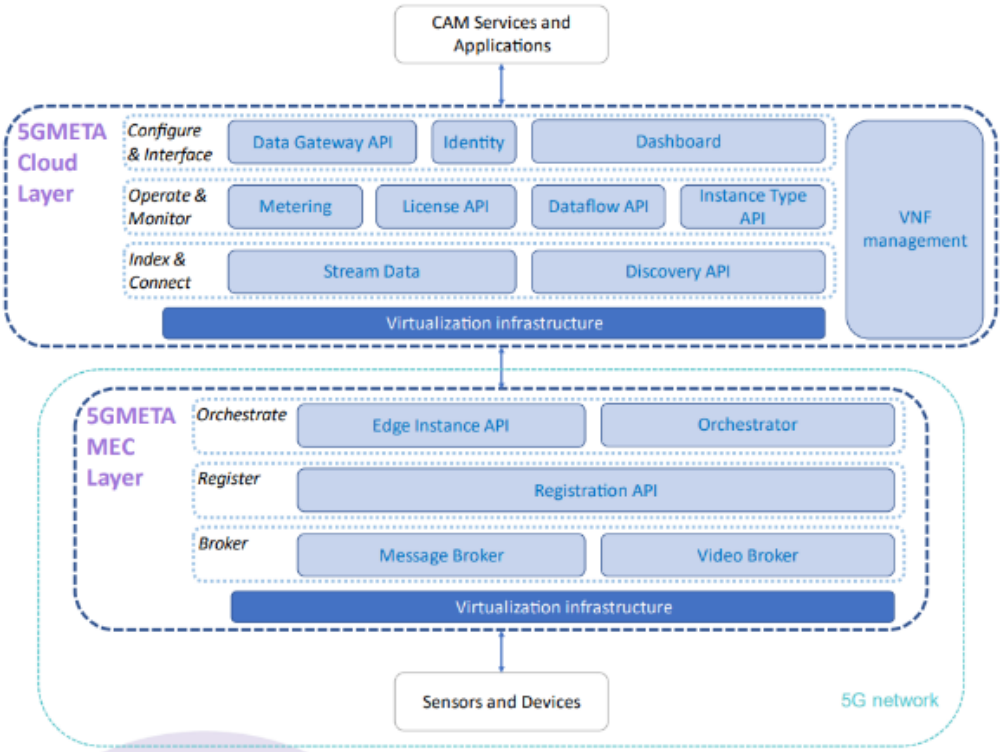
Table 7: Data captured in Use case 2

Data category	Data type	Device used to collect the data	Description of data
Vehicle identification data	ID	ECU	Unique identifier of the vehicle
Vehicle position and dynamics	Position	GNSS	Absolute positioning (lat., lon.)
	Heading	GNSS+IMU	Orientation of the ego-vehicle
	Speed	Odometer / GNSS+IMU	Speed of the ego-vehicle
	Drive Direction	IMU	Going forward or backward
Sensors' vehicle external data	Camera video stream	Camera	High-definition (1080p) video streams
	LIDAR point Cloud	LIDAR	High-definition (>32 channel) LIDAR data
Trip Information	Planned route	Navigation system	List of edge to cross
	Destination and ETA	Navigation system	Arrival point
Roadside infrastructure	Hazardous Event	RSUs	Stationary vehicle, incident, roadworks, etc.
	Road signs	Static information	
	Video flows from fixed cameras	Camera	High-definition (1080p) video streams
External information	Information about planned public events	Open data	Expected number of participants and the opening time

2.5.4.9 High Level Illustration

Figure 3 shows the reference architecture of the 5GMETA platform highlighting the functional building blocks that comprise the cloud and the MEC layers.

The 5GMETA cloud acts as the entry-point for data consumption by presenting a dedicated interface towards the CAM Services and Applications (Configure & Interface). Additionally, it offers the data consumers the ability to monitor their data usage (Monitor). It also provides an interface for indexing and discovery services for the data producers aka Sensors and Devices (Index & Connect). Finally, it ensures the management and orchestration of the MEC layer (Operate).



2.5.4.10 Potential Requirements

Table 8 shows the list of KPIs of UC3 with a general description and their target values.

Table 8: KPIs for Use case: Driving Safety & Awareness

Evaluation metric	Description	Target values
Latency	End-to-end latency between misbehaving vehicle and MEC/Cloud services. Low latency is required for road safety	< 100 ms
Reliability	Communication reliability between misbehaving vehicle and MEC/Cloud services. High reliability is required for road safety	> 99.9%
Misbehaviour Detection latency	Time needed for detecting driving misbehaviour starting from the moment when all needed data are available	< 200 ms
Misbehaviour Response latency for ETSI Basic Services	Time needed to alert surrounding vehicles from the moment when all needed data are available	< 100 ms

2.6 Maritime Transportation

2.6.1 VITAL-5G based use case: 5G Connectivity and Data-Enabled Assisted Navigation Using IoT Sensing and Video Cameras

2.6.1.1 Description

The Use Case focuses on the deployment of an Internet-of-Things (IoT) sensing system and video cameras aboard ships and barges (cargos) as well as in a river port (Galati) to implement a data-enabled assisted navigation application. The Galati port is the second-biggest port in Romania and the largest port on the Danube. It is a part of the Rhine-Danube Trans-European Transport Network (TEN-T) Corridor and serves as a point of entry for significant marine traffic from the Black Sea to continental Europe. As a result, navigation in a river port presents far more functional difficulties than it does in a seaport.

The suggested Use Case application will enable safer river port operation and greater security regarding ship movement, even in adverse weather and water conditions. Several CNFR NAVROM ships will be used for the Romanian test case study. NAVROM is a Romanian river transport firm which carries more than 10 million tons of goods each year, both internally (Galați, Constanța, Cernavoda, Medgidia, Mahmudia, etc.) and internationally (Ukraine, Moldavia, Bulgaria, Serbia, Croatia, Hungary, Slovakia, Austria, and Germany), being one of the important river ship owners in Europe.

The use of technologies for communication and voyage monitoring is required when operating ships as a means of improving any weak points. Therefore, improved communication is needed between ships and dispatchers as well as between ships and ports of operation in order to prevent stationary downtime caused by navigation errors and to, respectively, reduce the transport of empty units as much as possible while achieving a higher percentage of loading. This can be done by connecting the dispatcher's office and/or the safety of the navigation department in real time with the radio and video navigation equipment of the sensors that monitor the operating parameters of the ship. Additionally, a connection between the fleet operation department's decision-making units and ships is essential for improving sailing safety.

The interoperability of wireless protocols over a private 5G Orange network will be enabled by all sensors and cameras, allowing for the expansion of the sensing system's Internet access. The ship and barges will be equipped with several sensors, including GPS, humidity, smoke, and engine power sensors that are mounted in the machine room. These sensors supply pertinent data to the ship's local monitoring systems, such as velocity, heading, water and wind speed, etc., enabling the captain and crew to make the best decisions and aiding onboard diagnosis. Access to live video streaming from the surroundings through high-definition video cameras will be achieved using a 5G network, which offers high connectivity and low latency.

The Use Case targets three distinct services:

Data-enabled assisted navigation: The service makes use of the Internet of Things sensing technology and video cameras emplaced in Galați port and on the NAVROM vessel. For specific data collection from the NAVROM vessel, *Onboard data collection & interfacing for vessels NetApp* is used. *Data stream organization NetApp* is used to classify the data stream, assign the appropriate slice (URLLC or mMTC) in accordance with the data supplied from the vessel, and provide interfaces for sending warnings and classifying events.

Accurate electronic navigation maps creation: The service utilizing distributed sensor data intake, fusion, and post-processing allows estimating the safe distance for a ship. The data are provided by *Onboard data collection & interfacing for vessels NetApp* and analysed by *Distributed sensor data ingestion, fusion & post-processing NetApp* and include velocity, heading, water and wind speed, and GNSS (Global Navigation Satellite System) data.

Predictive maintenance and sanity checks: The service uses monitoring and onboard diagnostics data provided by *Onboard data collection & interfacing for vessels NetApp* and processes them using *Remote inspection & risk assessment NetApp* to limit human error and potential misjudgements.

2.6.1.2 Source

H2020 – ICT- 2020 VITAL-5G: "Vertical Innovations in Transport And Logistics over 5G experimentation facilities" European project

2.6.1.3 Roles and Actors

Roles relating to/appearing in the Use Case are described in **Table 9.**

Table 9: Involved stakeholders and their role

	Actor	Role
Consumer roles	Network Function Developer	Developer of virtual network functions (VNFs)
	Network Function Tester	Tester and validator of VNFs
Providers roles	VITAL-5G Facility Administrator	Administrator of one of the VITAL-5G testbeds
Business roles	T&L Service Provider	Offers services in the T&L sector to T&L end users relying on the capability of the 5G network and making use of one or more NetApps from the VITAL-5G catalogue, running in virtual environments hosted at the T&L facilities and/or in the cloud.
	System Integrator	Liaise with several other stakeholders across the value chain, from the technology providers, mobile network operators (MNOs), facility owners, NetApp developers, VITAL-5G Platform Business, T&L service designers and experimenters, with the aim of delivering an operational and validated T&L service.
	T&L NetApp Provider	Offers VITAl-5G NetApps to facilitate the creation of 5 G-enabled services.
	VNF Provider	Developer of VNFs. This profile is similar to NetApp developer but applied to different technical areas. NetApp providers focus on service applications, while VNF providers focus on network-related functions.
	T&L Facility Owner	5G network/connectivity provider
	Network Operator	MNO/MNVO (mobile virtual network operator), whose network is used to provide a 5G network to enable the T&L services
	Cloud Provider	Provider of cloud/edge computing services
	VITAL-5G Platform Operator	Administrator of the VITAL-5G Platform Offers experimentation as a service, consultancy and NetApp repository marketplace.
	Technology Providers	Provision/upgrade of 5G-connected/controlled devices for freight logistics to enable reliable, low-latency 5G connectivity for T&L services
	T&L End Users	Buys from T&L service provider.

2.6.1.4 Pre-conditions

The main pre-condition is the installation of the Internet-of-Things (IoT) sensing system and video cameras in a river port (Galati) and on ships and barges (cargos), which will enable the interoperable wireless protocols over a private 5G network.

Figure 17 illustrates the placement of the components that will be used on the ship, including:

Hardware:

AIS transponder (SAAB R4 or Periskal PM-1);

HIKVISION DVR and video cameras;

CAN-BUS interface for Caterpillar (Diesel Mecanica Constanta);

PLC (Siemens IoT 20xx or Raspberry PI);

ACTISENSE DST 2 converter.

Sensors:

Depth sensor type Airmar SS505.

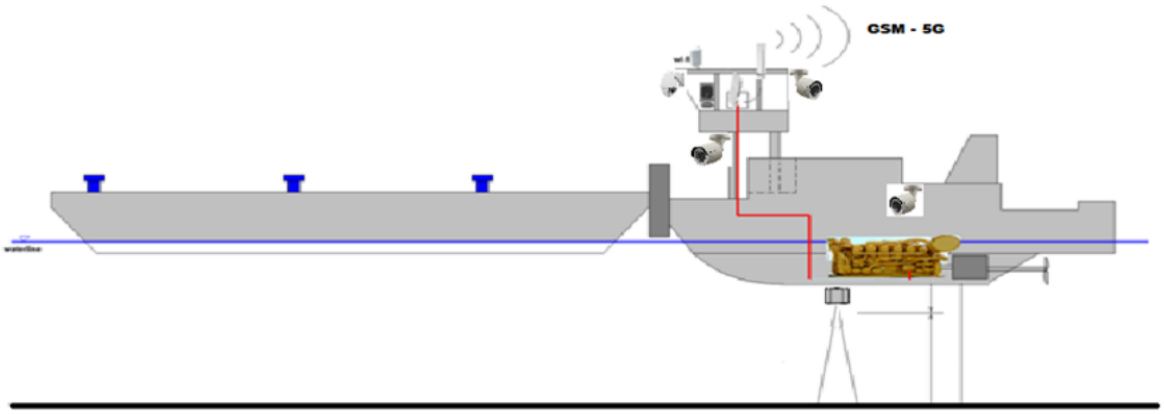


Figure 17: Positioning of hardware and sensors on a ship

(Figure copied from VITAL-5G D1.1 Report on use case requirements, page 42)

2.6.1.5 Triggers

The triggers for this Use Case consist of occurrences of dangerous navigation events, e.g., vessel collisions, tows striking bridges, ships or barges stuck in the river due to sandbanks or shallow water depth, difficulties, under typical waterway conditions (storms, high water and flood events).

2.6.1.6 Normal Flow

Data-enabled assisted navigation:

The details of data flows and interactions between the NetApps and the vessel of this service related to assisted navigation service are illustrated in **Figure 18**.

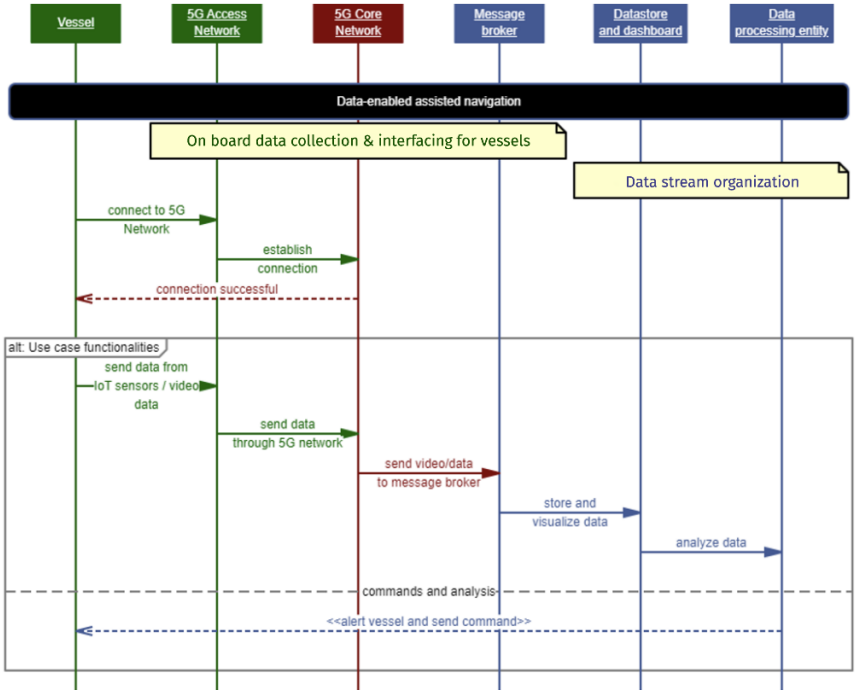


Figure 18: Data-enabled assisted navigation service flow diagram

(Figure copied from VITAL-5G D1.1 Report on use case requirements, page 32)

Accurate electronic navigation maps creation:

The details of data flows and interactions between the NetApps, the vessel and the port entities of this service related to safe distance estimation service are illustrated in **Figure 19**.

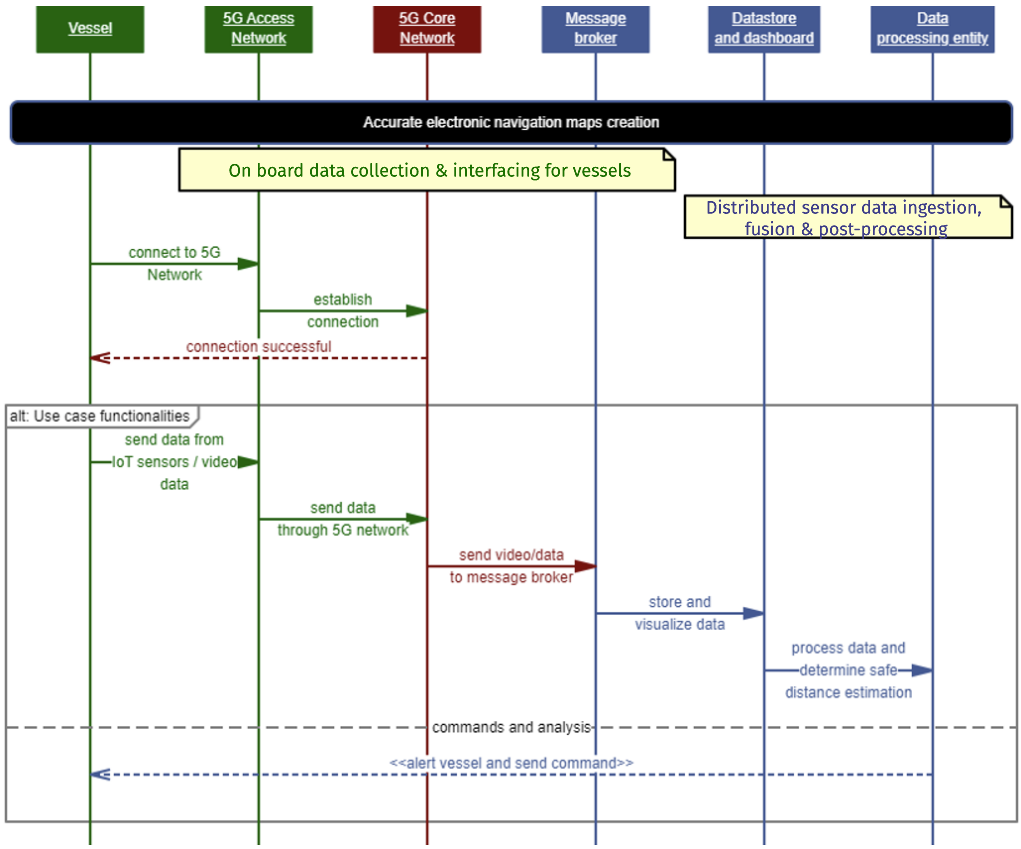


Figure 19: Accurate electronic navigation maps creation service flow diagram

(Figure copied from VITAL-5G D1.1 Report on use case requirements, page 33)

Predictive maintenance and sanity checks:

The details of data flows and interactions between the NetApps, the vessel and the port entities of this service related to predictive maintenance are illustrated in **Figure 20**.

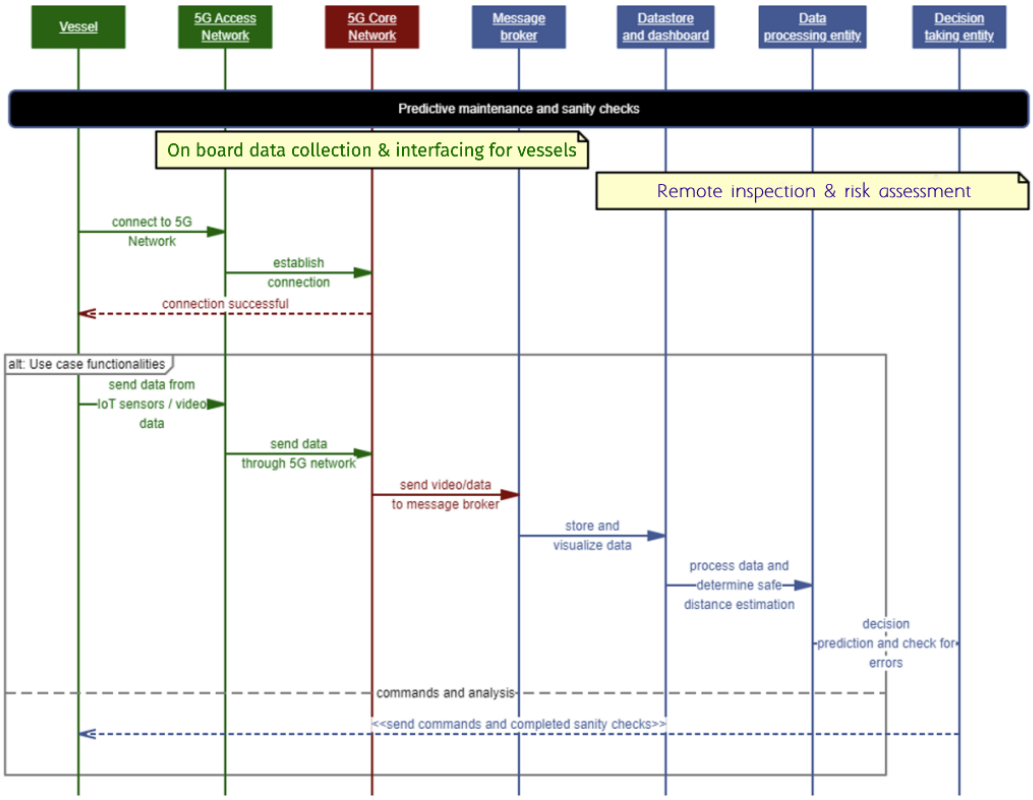


Figure 20: Predictive maintenance and sanity checks service flow diagram

(Figure copied from VITAL-5G D1.1 Report on use case requirements, page 34)

2.6.1.7 Alternative Flow

N/A

2.6.1.8 Post-conditions

The following objectives are included in the Use Case:

Decreasing risky navigation incidents by gathering and delivering sensor and video data with Data Stream Organization NetApp.

Reducing logistic costs as a result of smart decisions made using onboard diagnosis and monitoring tools through Onboard data collection & interfacing for vessels NetApp, therefore minimizing the impact of potential human error.

Achieving a more accurate electronic navigation map with Distributed sensor data ingestion, fusion & post-processing NetApp.

2.6.1.9 High Level Illustration

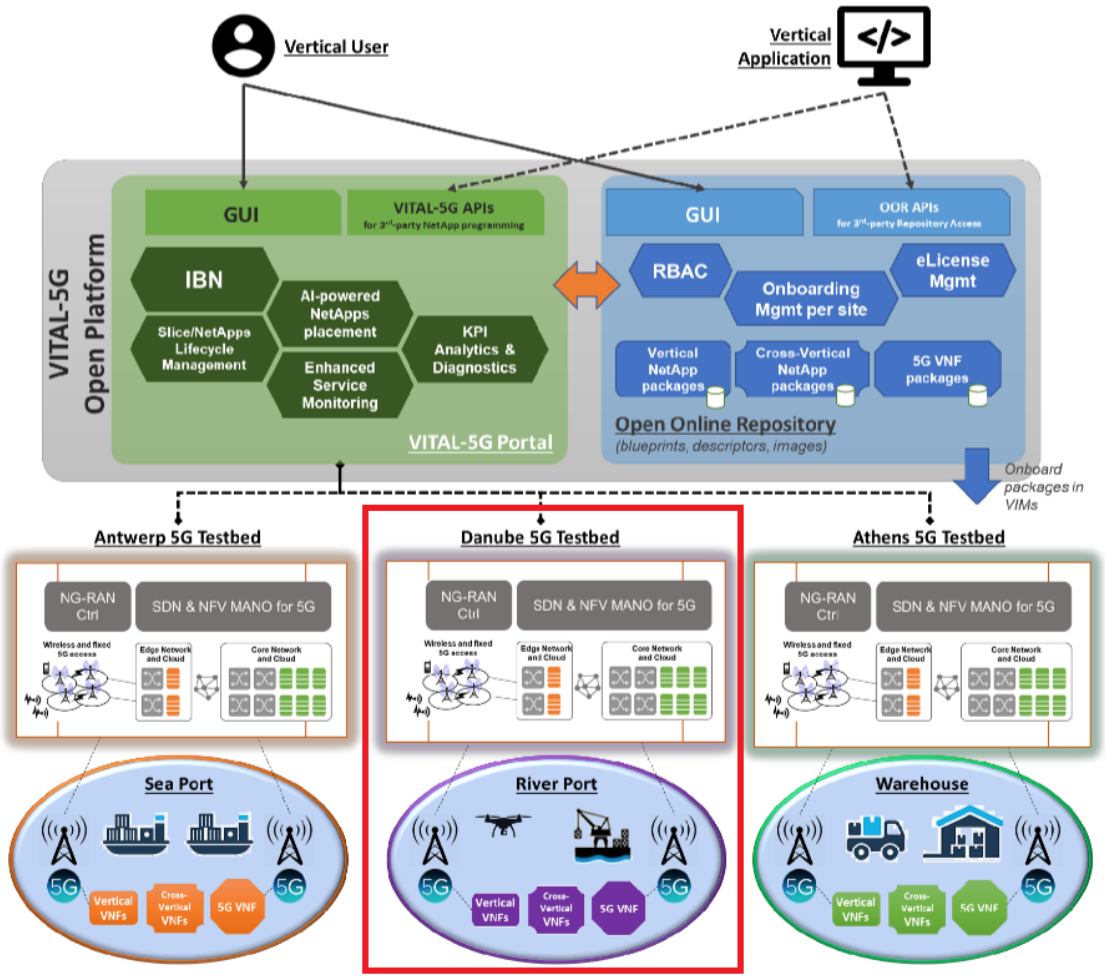


Figure 21: High-level architecture of the VITAL-5G system

(Figure copied from VITAL-5G D1.2 System Specifications and Architecture, page 69)

2.6.1.10 Potential Requirements

N/A

2.6.1.11 Radio Specific requirements

The Romanian testbed will be designed and built as an adaptive 5G system which consists of a 5G core network (5GC) and a 5G access network (NG-RAN), evolving to 3GPP Release 16.

The existing capabilities, already deployed in the Orange network, include:

5G RAN and Core components, software and hardware;

5G transport network (IP/MPLS/SR/DWDM);

Orchestration, OSM related;

Security network and services implementation;

Virtualized environment, OpenStack based and Kubernetes;

Manual Network slicing implementation.

For both 5G NSA and 5G SA services, the testbed network components for RAN, Core, Virtualization, and Network will be implemented in two phases.

Phase 1:

5G NSA implementation with the 5G NSA RAN and Core (vEPC & 5G RAN network integration), Option 3x;

two 5G sectors that cover Navrom ships' positions and headquarter, as presented in the coverage simulation output from **Figure 22**;

advanced IP/Network infrastructure, IP-FABRIC architecture network for cloud services delivery;

IP network open for transport service orchestration;

advanced telco cloud infrastructure for VNF, CNF and bare metal services apps, supporting IaaS/CaaS over OpenStack and Kubernetes/Docker;

orchestrator, OSM v10.

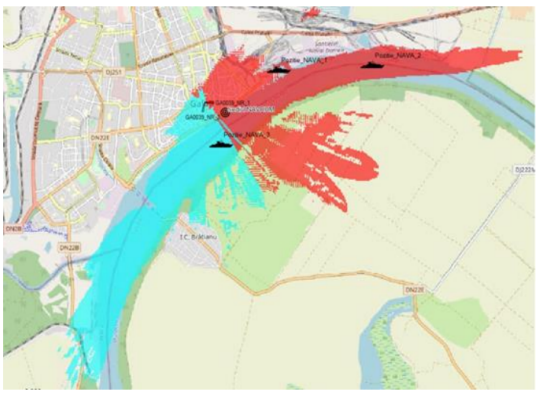


Figure 22: 5G Galati site coverage simulation map with the Use Case interest area representation

(Figure copied from VITAL-5G D3.1 Report on VITAL-5G infrastructure upgrades & extensions, page 32)

Phase 2:

5G SA Option 2 with virtualized 5G core, that is 3GPP Release 16.

2.6.1.12 Radio Coverage

N/A

2.6.1.13 Bandwidth and Latency requirements

Specific requirements linked to the Use Case for each NetApp of the service are presented in

Table 10. Table 13 as KPIs for latency, throughput, availability, dependability, and connectivity.

Table 10: Use Case Network requirements for *Distributed sensor data ingestion, fusion & post-processing NetApp*

(Table copied from VITAL-5G D1.1 Report on use case requirements, page 76)

Use Case Network requirements – Distributed sensor data ingestion, fusion & post-processing						
No.	**Requirements**	**Unit**	**Y/N**	**min value**	**max value**	**KPIs and parameters to be measured**
1	Latency (in milliseconds) - Min/MAX	Msec		5	20	Latency between terminals and service end points should be less than 20ms
2	Speed (in Mbps) - Min/MAX - sustained demand	Mbps		10	500	The throughput should be at least 10 Mbps
3	Reliability (%) - Min/MAX	%		99.99%	99.9999%	Reliability > 99.99%
4	Availability (%) - Min/MAX	%		99.99%	99.9999%	Availability > 99.99%
5	Mobility (in m/sec or Km/h) - Min/MAX	Km/h		0	25	
6	Broadband Connectivity (peak UL demand)	Y/N or Mbps	Y		100	
7	Network Slicing (Y/N)	Y/N	Y			• On-demand instantiation/ deletion/ configuration of an E2E network slice and delivery of services over it. • QoS guarantees (e.g., latency, bandwidth, etc.) of a slice shall be met.
8	Capacity (Mbps/m^2 or Km^2)	Mbps/m^2			10	
9	Device Density	Dev/Km2		100	1000	

Table 11: Use Case Network requirements for Remote inspection & risk assessment NetApp

(Table copied from VITAL-5G D1.1 Report on use case requirements, page 77)

Use Case Network requirements – Remote inspection & risk assessment						
No.	**Requirements**	**Unit**	**Y/N**	**min value**	**max value**	**KPIs and parameters to be measured**
1	Latency (in milliseconds) - Min/MAX	msec		5	200	Latency between terminals and service end points should be less than 200ms
2	Speed (in Mbps) - Min/MAX - sustained demand	Mbps		10	500	The throughput should be at least 10 Mbps
3	Reliability (%) - Min/MAX	%		99.99%	99.9999%	Reliability > 99.99%
4	Availability (%) - Min/MAX	%		99.99%	99.9999%	Availability > 99.99%
5	Mobility (in m/sec or Km/h) - Min/MAX	Km/h		0	15	
6	Broadband Connectivity (peak UL demand)	Y/N or Mbps	Y		100	
7	Network Slicing (Y/N)	Y/N	Y			• On-demand instantiation/ deletion/ configuration of an E2E network slice and delivery of services over it. • QoS guarantees (not best effort / default bearer, preferably GBR)
8	Capacity (Mbps/m^2 or Km^2)	Mbps/m^2			30	
9	Device Density	Dev/Km2		10	100	

Table 12: Use Case Network requirements for Data stream organization NetApp

(Table copied from VITAL-5G D1.1 Report on use case requirements, page 77-78)

Use Case Network requirements – Data stream organization						
No.	**Requirements**	**Unit**	**Y/N**	**min value**	**max value**	**KPIs and parameters to be measured**
1	Latency (in milliseconds) - Min/MAX	msec		5	15	Latency between terminals and service end points should be less than 15ms
2	Speed (in Mbps) - Min/MAX - sustained demand	Mbps		20	1000	The throughput should be at least 20 Mbps
3	Reliability (%) - Min/MAX	%		99.99%	99.9999%	Reliability > 99.99%
4	Availability (%) - Min/MAX	%		99.99%	99.9999%	Availability > 99.99%
5	Mobility (in m/sec or Km/h) - Min/MAX	Km/h		0	25	
6	Broadband Connectivity (peak UL demand)	Y/N or Mbps	Y		200	
7	Network Slicing (Y/N)	Y/N	Y			• On-demand instantiation/ deletion/ configuration of an E2E network slice and delivery of services over it. • QoS guarantees (e.g., latency, bandwidth, etc.) of a slice shall be met.
8	Capacity (Mbps/m^2 or Km^2)	Mbps/m^2			10	
9	Device Density	Dev/Km2		100	1000	

Table 13: Use Case Network requirements for On board data collection & interfacing for vessels NetApp

(Table copied from VITAL-5G D1.1 Report on use case requirements, page 78-79)

Use Case Network requirements – On board data collection & interfacing for vessels						
No.	**Requirements**	**Unit**	**Y/N**	**min value**	**max value**	**KPIs and parameters to be measured**
1	Latency (in milliseconds) - Min/MAX	msec		5	10	Latency between terminals and service end points should be less than 10ms
2	Speed (in Mbps) - Min/MAX - sustained demand	Mbps		20	1000	The throughput should be at least 20 Mbps
3	Reliability (%) - Min/MAX	%		99.99%	99.9999%	Reliability > 99.99%
4	Availability (%) - Min/MAX	%		99.99%	99.9999%	Availability > 99.99%
5	Mobility (in m/sec or Km/h) - Min/MAX	Km/h		0	25	
6	Broadband Connectivity (peak UL demand)	Y/N or Mbps	Y		200	
7	Network Slicing (Y/N)	Y/N	Y			• On-demand instantiation/ deletion/ configuration of an E2E network slice and delivery of services over it. • QoS guarantees (e.g., latency, bandwidth, etc.) of a slice shall be met.
8	Capacity (Mbps/m^2 or Km^2)	Mbps/m^2			10	
9	Device Density	Dev/Km2		100	1000	

2.7 Critical Infrastructure support applications

2.7.1 Smart Infrastructure Monitoring

2.7.1.1 Description

Industrial Internet of Things (IIoT) describes systems that connect and integrate industrial control systems with enterprise systems, business processes, and analytics. We define as industrial systems those manufacturing plants and installations in domains like energy, telecommunications, transport and industrial production or other similar verticals.

Industrial systems perform processes that consume resources and produce, or otherwise manipulate, resources such as energy, manufactured products, transport products, area monitoring and so on. The correct execution of the process is achieved with the use of controllers which employ sensors to measure parameters of the state of the process, as well as actuators that alter some parameters (variables) of the process. A controller is a system on its own, consisting of components such as Human Machine Interfaces (HMI), desktop PCs, network components, as well as specialised hardware such as PLCs, servo controllers and drives. The focus in this scenario is on sensors deployed in the environment of the industrial systems that capture and transmit data relevant for the control of the system process. Of particular interest, are sensors that have communication and networking capabilities and that can be accessed remotely, i.e. over the Internet. This essentially constitutes IoT in the context of industrial systems (IIoT). Many of the existing industrial installations of sensors pre-date IoT which is mostly a phenomenon of the past decade, although it originates in research carried out in the 90s, which culminated in the term Internet of Things to be coined by MIT in 1999.

However, originally, industrial systems did not use IoT technologies, gradually IoT started to penetrate industrial system installations in overhauls, upgrades and re-placement of older technologies. IoT in industrial installations results in systems that are easier to connect, remotely manage and interoperate, amongst other benefits. Introducing IoT in industrial systems, however, in addition to benefits also brings risks. The risks are the results of the unintended consequences of introducing IoT in an industrial system, i.e. the risks of making such system less safe, secure or private for its stakeholders. The reasons of such unintended consequences are multiple. IoT through its connectivity opens the industrial system to new attack vectors (routes) that can be exploited by malicious actors.

IoT data can become corrupted due to non-malicious (such as sensor malfunctioning or program errors) or malicious causes, presenting the industrial system with incorrect data that can cause it to function incorrectly and create safety hazards. Industrial system data may become indivertibly exposed on the Internet, creating a privacy risk. Also, IoT designers developing IoT technologies are rarely security and privacy experts meaning that such systems might have not been designed with security, safety or privacy in mind.

In the above terms, communications are therefore considered as vital parts of Industrial IoT deployments, providing the physical connectivity and allowing for the results aggregation under any terms and conditions. 5G communications provide higher bandwidth, reliability and lower latencies which is regarded as of major support to industrial IoT systems and applications aiming digitization of infrastructures or other systems and networks. The 5G systems reliability is strongly supported by their extended quality of service and real-time communications (as opposed to best offer In WiFi). Low latency is also considered of strong support as compared to 20 or 40msec (typical) latencies in WiFi networks. Depending on the application and related requirements, the above may of course become of higher or lower value.

In applications where we have massive IoT devices (sensors) applications (e.g. in an airport, smart building etc.) operating in low-powered endpoints, not requiring high data connectivity but low latency (< 10msec) specifications could align with Narrowband IoT (NB-IoT) connections. 5G could also serve other IoT application requirements with fewer devices but higher bandwidth needs such as video surveillance enabled by 4-8k video and real-time streaming. Other applications could include smart factory environments and manufacturing with broader connectivity requirements.

2.7.1.2 Source

CHARIOT (Cognitive Heterogeneous Architecture for Industrial IoT) is an EC co-funded research project granted under the IoT-03-2017 - R&I on IoT integration and platforms as a Research and Innovation (RIA) EC topic coordinated by INLECOM. CHARIOT provides a design method and cognitive computing platform supporting a unified approach towards Privacy, Security and Safety (PSS) of IoT Systems. This publication describes the CHARIOT system architecture and particularly a Privacy and security protection method building on state of the art Public Key Infrastructure (PKI) technologies, a Blockchain ledger in which categories of IoT physical, operational and functional changes are both recorded and affirmed/approved, a Fog-based decentralised infrastructure for Firmware Security integrity checking, an accompanying IoT Safety Supervision Engine as a novel solution to the challenges of securing IoT data, devices and functionality, a Cognitive System and Method with accompanying supervision, analytics and prediction models enabling high security and integrity of Industrials IoT supported by static code analysis of IoT devices.

2.7.1.3 Roles and Actors

Security management personnel of infrastructures

Operations management

CERT/CSIRT teams (emergency response)

2.7.1.4 Pre-conditions

Monitoring of infrastructures requiring high connectivity of hundreds of IoT devices.

Relatively low latency connectivity applications supporting infrastructure monitoring and sensing devices

2.7.1.5 Triggers

Connectivity to local networks of hundreds of monitoring devices for sensing, process monitoring, user safety and comfort as well as surveillance.

2.7.1.6 Normal Flow

Data from hundreds of IoT devices reaching central control operations.

Close to real-time connectivity and data assimilation of sensing devices

2.7.1.7 Alternative Flow

None

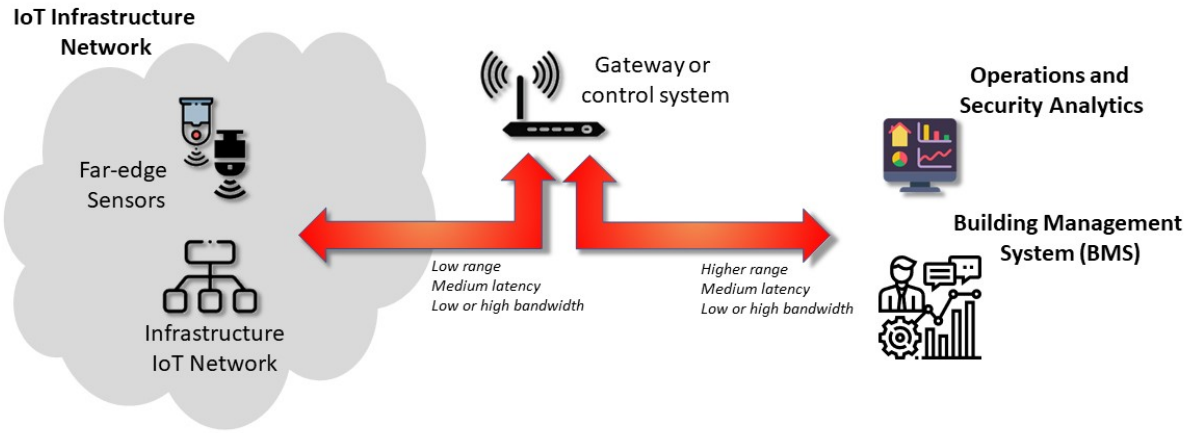
2.7.1.8 Post-conditions

Data analytics, almost real-time alerting, data communications

Actuation decisions

Security analysis and decision making

2.7.1.9 High Level Illustration



2.7.1.10 Potential Requirements

Functional Requirements

Almost Real-time communications between edge devices and local gateway or control system.

Mid-latency for collecting data from sensing devices.

Low-high bandwidth requirements (depending on sensing device).

Higher range required for results collection at security systems and/or BMS.

Reliable communications at all levels.

Non-Functional Requirements.

Secure communications between all actors and components required. Advanced level of security would be needed to replace wired applications.

Interoperability between communication protocols (linked also with the possibility to use standard communication protocols between the systems).

Power requirements could be an issue. Need to balance edge processing capabilities with power consumption. As wires provide the power now, low power consideration is needed for edge devices.

2.7.1.11.1 Radio Specific requirements

2.7.1.11.1 Radio Coverage

Radio cell range

Does the radio link crosses public spaces? Or is it constrained to indoor or customer premises?

Radio link crosses public spaces and includes indoor and outdoor premises.

Is Multicell required? No.

Is handover required? Seamless? Tolerable impact in delay and jitter? No.

Mobility: maximum relative speed of UE/FP peers No.

2.7.1.11.2 Bandwidth and Latency requirements

Peak data rate (expected):	1000 Mbps
Average data rate	100 Mbps
Latency (expected for robotic control):	50 ms
Latency (expected for remote data aggregation):	1-2 seconds

2.7.2 AURORAL HEALTH PILOT for Strengthening Preparedness In Health-Critical Remote Operations

2.7.2.1 Description

Our main intention is to provide efficient, standardised and secure communication of time-critical information for requiring situational awareness and status in rescue operations. The communication targets a broad name of stakeholders related to the first responder actions (e.g., vicinity/citizens, emergency bodies, governmental bodies, civil protection organisations and/or other related critical infrastructure and their cascading effects). To specifically build an effective emergency communication service, critical infrastructure (like 5G) must be present and support secure communication protocols. Secondary protocols (e.g., GSM, UMTS, TCP/IP, 3GPP) should also be available to emergency stakeholders and vicinity/citizens. The proposed situational awareness support system will gather data from various sources (e.g., remote control aerial vehicles, open-source data) and use techniques such as photogrammetry, machine learning and on-site reporting. The system will use Web-Based services such as OGC (Service Alerting System, Sensor Observation Service and Web, Web processing Service) to communicate alerts and current status to geographic areas using innovative communications (RSS, social media, XML, JSON).

Three main services identified as part of preparedness development:

- the use cases the scenarios are part of deals with training personnel
- planning and specifying configuration of support equipment, assist in ongoing missions
- evaluation of operation and adjust strategies for future operations.

Scenarios that are part of the use cases address support search-and-rescue operations. in looking for lost people in difficult terrain, assist in providing situational awareness in time critical situations, prepare guidance for operational managers and allow for use of transport capabilities of unmanned aerial vehicles (UAVs – in particular drones).

To successfully plan for UAV supported actions, some criteria must be fulfilled. These are all based on network coverage and communication with the UAVs:

- identification of coverage area depending on provider and signal type (2G, 3G, 4G, 5G)
- identification of coverage area in height depending on topography, vegetation and buildings
- Identification of signal strength depending on position including altitude data
- Identification of regions where coverage is so poor or lacking that a repeater drone must be sent up
- Balancing the position of drones and repeater drones based on topography and battery capacity/remaining flight time

Based on these criteria, necessary systems and training data will be the foundation for preparedness planning and inclusion in contingency strategies:

- acquisition of relevant data sets that indicate how signals behave - these are to be used for training expert systems
- obtaining the calculated position of transmitters
- choice of type of expert system and training of the network
- visualization of results in digital twin
- include 3D visualization, which can also provide the opportunity to offer a VR experience of the information

The system three main components:

1. Mission Planning Tool: This component allows the operator to define the mission objectives, specify the area of interest, and select the sensors to be used. The tool also provides the operator with a 3D map of the area, which can be used to visualize the UAV's flight path.
2. Sensor Control Module: This component controls the sensors' settings during the mission, such as the resolution, focal length, and field of view. It also manages the data acquisition and transmission from the sensors to the ground station.
3. Trajectory Planning Module: This component generates an optimized flight path for the UAV based on the mission objectives, sensor coverage, and UAV's capabilities. The trajectory planning takes into account the UAV's speed, altitude, and endurance, as well as the sensor's coverage and resolution.

Wildfires represent a significant natural risk causing economic losses, human death and environmental damage. In recent years, the world has seen an increase in fire intensity and frequency. Research has been conducted towards the development of dedicated solutions for wildland fire assistance and fighting. Systems were proposed for the remote detection and tracking of fires. These systems have shown improvements in the area of efficient data collection and fire characterization within small-scale environments. However, wildland fires cover large areas making some of the proposed ground-based systems unsuitable for optimal coverage.

To tackle this limitation, unmanned aerial vehicles (UAV) and unmanned aerial systems (UAS) were proposed along with ground sensors. The Sensors which are installed in strategic points in the park, are interconnected with the incident management platform and the drone control system. The drone operates scheduled surveillance flights as well as emergency flights in case of the sensor indications.

The system is able to detect smoke or fire, both by the sensors indications at the field and from specific algorithms that are used to analyse drones' video in real-time. In both cases the data are send to the Control Center indicating points of interest.

When a sensor identifies abnormal values of CO2 or/and temperature sends an alarm to the Control Center with the coordinate of the event. At that point two actions take place:

1. An SMS / Email is sent to the involved stakeholders with the exact location of the event
2. The drone autonomously takes-off and is directed straight ahead to the indicated location to verify the event with the help of the Ai algorithms. The drone during all operations broadcasts live to all stakeholders that are involved.

In the case of a preprogramed patrolling where the drone detects smoke or fire through the camera, it sends an alert to the control centre, and the drone, immediately rushes to where the smoke was detected to verify the incident and send the exact location info. Then the drone either returns to its base or records the progression of the fire. The result is the immediate identification of the starting point of the fire, real-time monitoring of remote areas, early visual detection of smoke and fire, and in result protection of human life.

The Use Case focuses on the deployment of an Internet-of-Things (IoT) sensing system and video cameras aboard ships and barges (cargos) as well as in a river port (Galati) to implement a data-enabled assisted navigation application. The Galati port is the second-biggest port in Romania and the largest port on the Danube. It is a part of the Rhine-Danube Trans-European Transport Network (TEN-T) Corridor and serves as a point of entry for significant marine traffic from the Black Sea to continental Europe. As a result, navigation in a river port presents far more functional difficulties than it does in a seaport.

The suggested Use Case application will enable safer river port operation and greater security regarding ship movement, even in adverse weather and water conditions.

A number of CNFR NAVROM ships will be used for the Romanian test case study. NAVROM is a Romanian river transport firm which carries more than 10 million tons of goods each year, both internally (Galați, Constanța, Cernavoda, Medgidia, Mahmudia, etc.) and internationally (Ukraine, Moldova, Bulgaria, Serbia, Croatia, Hungary, Slovakia, Austria, and Germany.), being one of the important river ship owners in Europe.

The use of technologies for communication and voyage monitoring is required when operating ships as a means of improving any weak points. Therefore, improved communication is needed between ships and dispatchers as well as between ships and ports of operation in order to prevent stationary downtime caused by navigation errors and to, respectively, reduce the transport of empty units as much as possible while achieving a higher percentage of loading. This can be done by connecting the dispatcher's office and/or the safety of the navigation department in real time with the radio and video navigation equipment of the sensors that monitor the operating parameters of the ship. Additionally, a connection between the fleet operation department's decision-making units and ships is essential for improving sailing safety.

The interoperability of wireless protocols over a private 5G network will be enabled by all sensors and cameras, allowing for the expansion of the sensing system's Internet access. The ship and barges will be equipped with a number of sensors, including GPS, humidity, smoke, and engine power sensors that are mounted in the machine room. These sensors supply pertinent data to the ship's local monitoring systems, such as velocity, heading, water and wind speed, etc., enabling the captain and crew to make the best decisions and aiding onboard diagnosis. Access to live video streaming from the surroundings through high-definition video cameras will be achieved using a 5G network, which offers high connectivity and low latency.

The Use Case targets three distinct services:

Data-enabled assisted navigation: The service makes use of the Internet of Things sensing technology and video cameras emplaced in Galați port and on the NAVROM vessel. For specific data collection from the NAVROM vessel, *Onboard data collection & interfacing for vessels NetApp* is used. *Data stream organization NetApp* is used to classify the data stream, assign the appropriate slice (URLLC or mMTC) in accordance with the data supplied from the vessel, and provide interfaces for sending warnings and classifying events.

Accurate electronic navigation maps creation: The service utilizing distributed sensor data intake, fusion, and post-processing allows estimating the safe distance for a ship. The data are provided by *Onboard data collection & interfacing for vessels NetApp* and analysed by *Distributed sensor data ingestion, fusion & post-processing NetApp* and include velocity, heading, water and wind speed, and GNSS (Global Navigation Satellite System) data.

Predictive maintenance and sanity checks: The service uses monitoring and onboard diagnostics data provided by *Onboard data collection & interfacing for vessels NetApp* and processes them using *IoT Management platform NetApp* to limit human error and potential misjudgements.

2.7.2.2 Source

AURORAL H2020 European project

H2020 – ICT- 2020 VITAL-5G: "Vertical Innovations in Transport And Logistics over 5G experimentation facilities" European project

Press release announcing an innovative fire detection pilot solution using 5g, artificial intelligence and drone technology

2.7.2.3 Roles and Actors

When planning search and rescue operations using UAVs (Unmanned Aerial Vehicles), actors involved will vary. However, they can generally be separated into public agencies such as the police and fire department, political structures such as municipalities and official department, private organizations such as Red Cross and Peoples Aid, and regulatory organisations like the Civil Aviation Authority.

These actors can be separated in general stakeholder groups:

Citizens & Vicinity. People who live (near) a critical infrastructure and needs to be protected or informed about potential risk that could affect their lives.

Critical Infrastructure. Central element source of vulnerabilities that can become real risks (natural or cyber risks).

Emergency Bodies. Stakeholders dedicated to minimizing the effects of the risks once them happens (hospitals, fireman's, etc.).

Governmental bodies. Stakeholders required to organize the society and provide insights at higher level.

Civil Protection Organization. Stakeholders dedicated to mobilizing and organize the citizens in emergency situations.

During search and rescue operations, the organisations above are part of defining various components and aspects of the mission, in particular the payload referring to equipment or devices that are carried by the UAV, such as cameras, sensors, or rescue equipment.

Furthermore, regulatory compliance and risk assessment are aspects that are considered with classifying Unmanned Aerial Vehicles (UAVs). Familiarity with airworthiness certification, licensing, and operational restrictions must exist within the organisations. In planned and ongoing missions, the actors involved will have to take into account flight capabilities with attention paid to The UAV's range, altitude, speed, endurance. Including such knowledge, required contributions include experience of control systems.

Overall, classifying UAVs from a security perspective requires a comprehensive assessment of the vehicle's capabilities, vulnerabilities, and potential impact on security, and the implementation of appropriate measures to ensure the safe and secure use of the UAV.

Mission planning: terminology

Geomap

Region with colours and values assigned to specific areas

Geolocation/geoposition

The identification of geographic location, as of an electronic device or an animal being tracked.

The latitude and longitude coordinates of a particular location. Term and definition standardized by ISO/IEC 19762-5:2008 (this standard has since been revised by ISO/IEC 19762:2016).

Geofence / geo-zone

A virtual perimeter around a geographic area, typically enforced by monitoring the positions of trackable mobile devices inside or outside the area, and determining if they cross the "fence"

A geofence could be dynamically generated (as in a radius around a point location) or match a predefined set of boundaries (such as school zones or neighbourhood boundaries).

Example of use involves a location-aware device of a location-based service (LBS) user entering or exiting a geofence.

Route planning

Coverage: This refers to the area of interest or the search area that needs to be covered during the mission.

Grid pattern: This is a search pattern that involves dividing the coverage area into a grid and searching each section systematically.

Sweep pattern: This is a search pattern that involves flying the UAV back and forth in a zigzag pattern over the coverage area.

Endurance: This refers to the duration of time that the UAV can remain airborne before requiring a battery change or refuelling.

Search and Rescue (SAR) software: This is software that helps plan and execute the search and rescue mission, including flight planning, sensor control, and data acquisition.

Geo-referencing: This is the process of assigning geographic coordinates to the images or data collected during the mission to provide accurate location information.

2.7.2.4 Pre-conditions

Example: Main pre-condition is to live a potential risk in the critical infrastructure (water, energy, transport) that could create damage to other critical infrastructure or the society (critical infrastructure attack, floorings, earthquakes, etc.).

Some data services need to be in place before it becomes operational, see **Figure 23.**

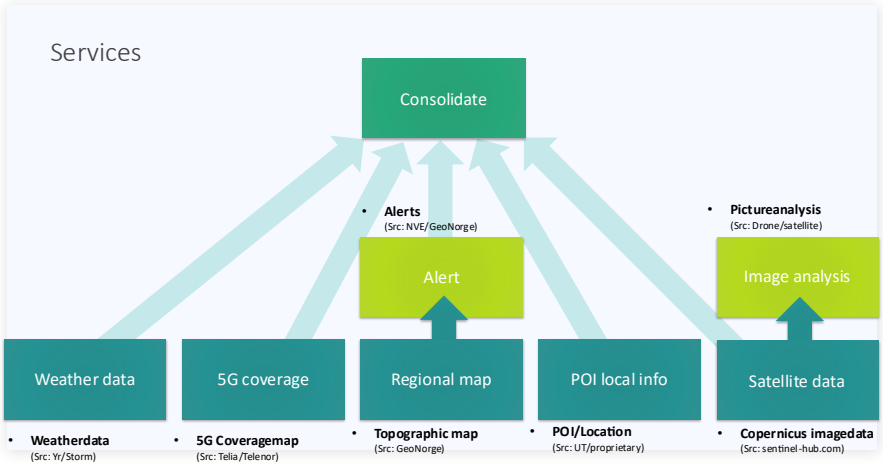


Figure 23: Examples of AURORAL services

2.7.2.5 Triggers

The triggers are when an event happen, i.e. landslide, snow avalanche, tourist missing, dement patient missing, fire, sea wave caused by stones from mountain. The Rescue centre reports to police, who engage rescue teams with local knowledge of the field, see **Figure 24.**

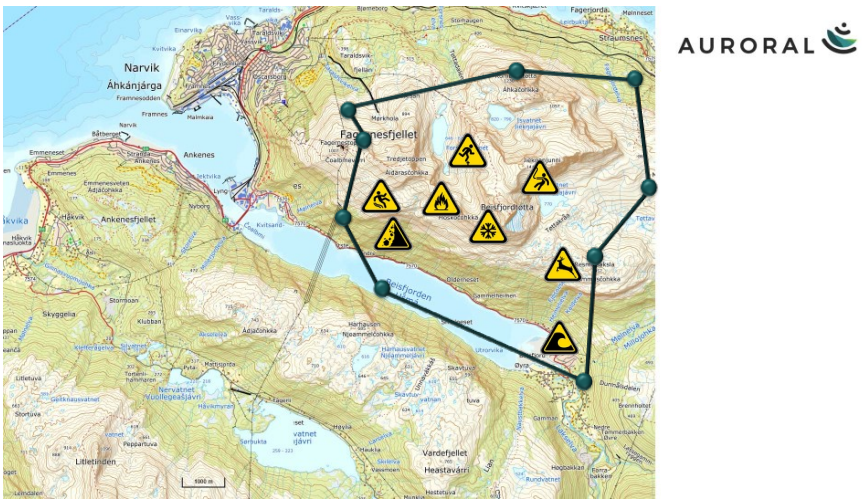


Figure 24: AURORAL coverage area of rescue

Example: The triggers used in this use-case is when the risk happens, or it is detected in the critical infrastructure.

2.7.2.6 Normal Flow

Normal flow of operations from rescue organisations through UAS and sensors using secure communication protocols to a cloud solution accessible from authoritative users shared by a digital platform and consolidated by rescue operation experts.

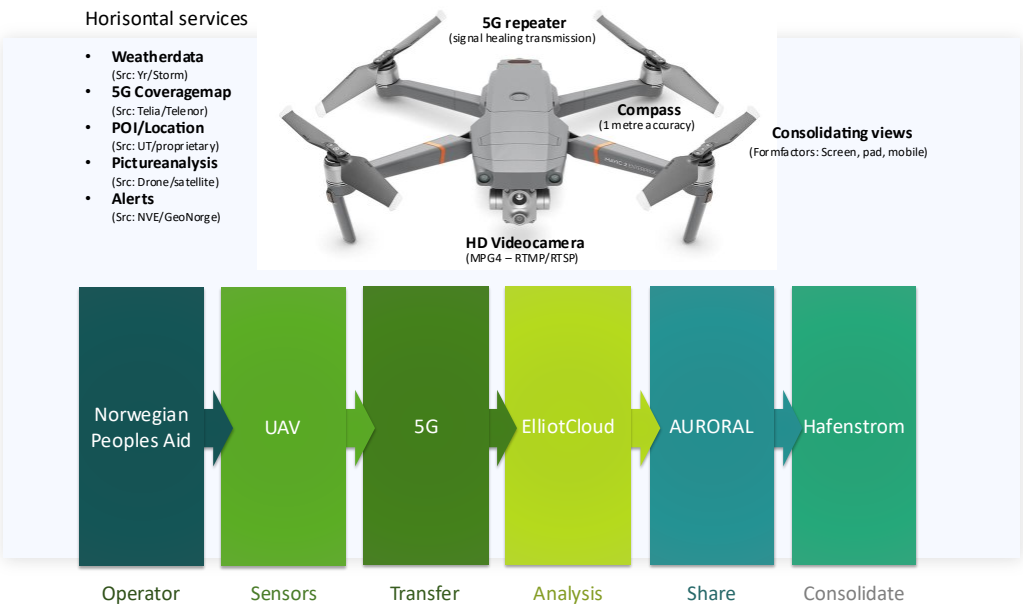


Figure 25: Normal Flow of operation

Example: Commonly, the steps are the follows:

1. Critical infrastructure systems (IoT systems, SCADAS, informational systems, risk management systems) are continuing monitoring the critical infrastructure until a potential risk is detected or could happen.
2. At this moment, the critical infrastructure communicated with other related critical infrastructures that could be affected by these risks (transport, energy, water, etc.).
3. In parallel, the critical infrastructure that is suffering the risk puts in contact with emergency bodies (in case of required) and civil protection bodies.
4. Once the risks has been minimized or solved, the critical infrastructure informs the citizens and vicinity about the risks happened and also the governmental bodies.

Our main goal is to prepare an operational model and infrastructure that supports situational awareness and provide a system that allow for assigning members and teams to mission depending on location, regions, resources and signal strength.

The service aims to offer support for search-and-rescue missions – planning, evaluating, strengthening organisation of the teams and understanding of availability and use of available systems.

Data-enabled assisted navigation:

The details of data flows and interactions related to assisted navigation service are similar the flows provided in **Figure 18**.

2.7.2.7 Alternative Flow

Not defined at the moment

2.7.2.8 Post-conditions

The post-condition is to establish normality and review the knowledge learned by rescue personnel.

Example: Once the risks have been minimized or solved, the critical infrastructure informs the citizens and vicinity about the risks happened and also the governmental bodies. Moreover, there is informative actions to the vicinity governmental bodies about the critical infrastructure situation.

The post-condition is to establish normality and review the knowledge learned by rescue personnel.

Example: Once the risks have been minimized or solved, the critical infrastructure informs the citizens and vicinity about the risks happened and also the governmental bodies. Moreover, there is informative actions to the vicinity governmental bodies about the critical infrastructure situation.

Continuous surveillance and data collection during the fire event and after. The resulting data are kept in a file (log files) and are available for further statistical analysis, patterns identification, etc. for the creation of forecasts and operational models for more efficient management of the phenomena.

2.7.2.9 High Level Illustration

Figure 26 shows the high-level figure that shows the main entities in the use case and their interaction on a high level of abstraction. Note that the High-level architecture of the VITAL-5G system, which can support as well rescue drones, can be seen in **Figure 21**.

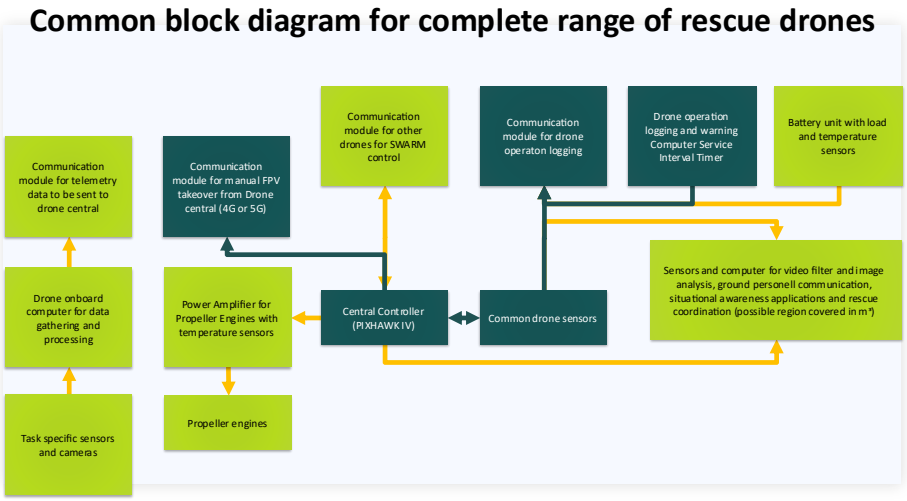


Figure 26: Complete block diagram for complete range of rescue drones

2.7.2.10 Potential Requirements

Functional Requirements

UC3.SC1-FUNC1	The mobile network must support 2 concurrent service slices		
Priority	Essential	**Justification**	Use case driven
Description	Two different services shall be supported by the Use case: 1. C2 for the drones, a uRLLC service 2. Signal measuring data transferring, a uRLLC service		
Related Component(s)	The 5G core and Access network		

UC3.SC1-FUNC2	Mobile edge capabilities must be deployed in the UO test area		
Priority	Essential	**Justification**	Use case driven
Description	The provision of the uRLLC service for the drones command and control mandates the existence of a MEC cloud of University of Oulu		
Related Component(s)	The 5G core and Access network		

UC3.SC1-FUNC3	Simultaneously support data transmission for UAVs and users		
Priority	Essential	**Justification**	3GPP r.17 22.829 UC4
Description	The 5G system shall need to optimize the resource use of the control plane and/or user plane for transfer of continuous uplink data that requires both high data rate and very low end-to-end latency.		
Related Component(s)	The 5G core and Access network and RAN		

UC3.SC1-FUNC4	The mobile network must support prioritisation		
Priority	Essential	**Justification**	Use case driven
Description	The provision of the uRLLC service with required SLA in the volume of airspace is critical for the drones' command and control (C2 link).		
Related Component(s)	The 5G core and Access network and RAN		

UC3.SC1-FUNC5	The network should provide service for the remote operator		
Priority	Essential	**Justification**	Use case driven
Description	A transmission link must be provided for the drone operator in a remote location, at least at the same level as provided for the drones.		
Related Component(s)	The 5G core and Access network, RAN		

Non Functional Requirements

UC3.SC1-NFUNC1	Approved SORA		
Priority	Essential	**Justification**	Regulation
Description	No objections from Traficom (Finnish CAA).		
Related Component(s)	Operator		

UC3.SC1-NFUNC2	Connectivity shall be provided in a secure manner		
Priority	Essential	**Justification**	Security
Description	The network deployed must be protected against denial of service attacks and other malicious attempts to compromise it		
Related Component(s)	5G network		

2.7.3 ERATOSTHENES: Smart Health

2.7.3.1 Description

In the healthcare domain, the number of IoT devices involved has increased drastically in the latest years due to the evolution of the environment to a smarter one. In ERATOSTHENES project, the Smart Health pilot is based on a remote patient monitoring system. It facilitates remote assistance and follow up on patients suffering from chronic diseases such as diabetes, COPD, or other diseases where patients, at least partly, can stay at home (e.g., COVID-19). In general, the eHealth use case enables patients to stay home during treatment and care, and foster self-care. It includes a Personal Health Gateway, which is deployed in every patient's home, that is responsible for collecting data from various medical sensors and sending them to the back-end cloud services. The services provide data to health personnel allowing for remote patient monitoring. Data is recorded in the patient's electronic health journal. Furthermore, it normalizes data according to standard eHealth ontologies to enable data analysis. During this period in ERATOSTHENES project, we showcase two use cases, for the health pilot.

In use case 1 we showcase the implementation of ERATOSTHENES, by onboarding the service provider gateway into their services within a remote patient monitoring system. In the use Case 2 we Illustrate the application of ERATOSTHENES, in dynamically establishing trust for the service gateway within the context of a remote patient monitoring system.

2.7.3.2 Source

ERATOSTHENES H2020 European project

2.7.3.3 Roles and Actors

Patient: People who receive the remote provided services by Tellu

Stakeholders: i) Industry as the supplier, ii) Sub departments of the Industry supplier or third parties organizations such as the Communication Network supplier/provider/operator, IoT device manufacturer, IoT platform provider, iv) operators of the transport network,

Emergency Bodies: Hospital

2.7.3.4 Pre-conditions

The main precondition is to live a potential cyber-attack, faulty operation or communication, connectivity issue, authorization fault and/or data leakage in the operation of the remote patient monitoring system that could result in casualties, data leakage and faulty or delayed communication transmitted to the remote patient.

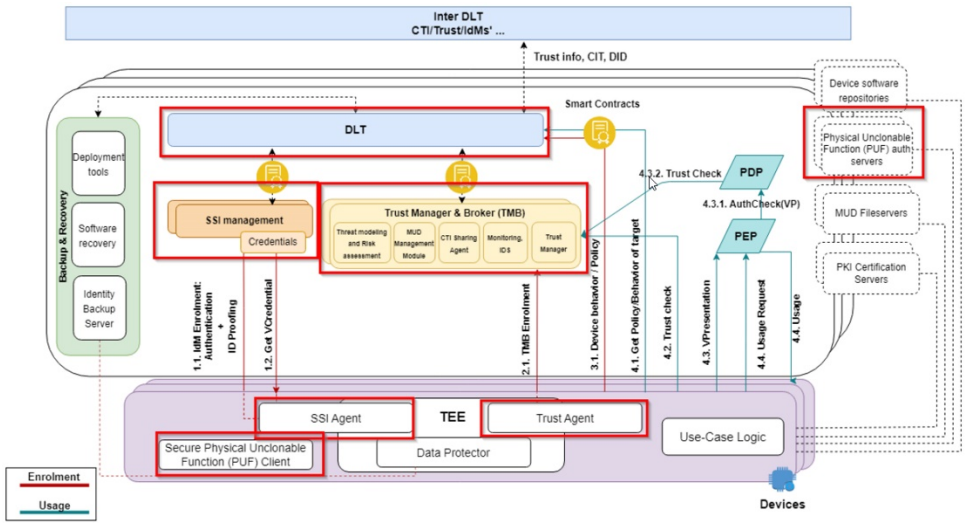
2.7.3.5 Triggers

Malicious action to modify or in any case alter the initially intended purpose of the remote patient monitoring application and system. Inherited system malfunction relating to user authorization that could lead to personal data leakage. Delayed or malfunctioning communications with the remote station (and sensing/communication system) that could result into delayed communication to the patient or the remote sensing platform. Intentional cyber-attack, to create limited or total denial of service under the scope of damaging the patient or the health platform.

2.7.3.6 Normal Flow

The data flow for the Use Case 1 is materialised through the integration of three key technologies developed in the ERATOSTHENES project: i) Physically Unclonable Function (PUF), ii) Self-Sovereign Identity (SSI), and iii) Distributed Ledger Technology (DLT). The Physically Unclonable Function (PUF) plays a pivotal role in generating Disposable IDs (DIDs) for the device. Leveraging the Self-Sovereign Identity (SSI) framework, the device undergoes onboarding onto the system domain. Ultimately, the device registration in the Distributed Ledger Technology (DLT) is completed, ensuring its future use.

The data flow in use case 2 is based on the trust management of devices and services and is building on use case 1. In this case of Pilot 2 the main device is the Personal Health Gateway which manages a set of medical sensors attached to it and is responsible to send trusted patient medical data over the gateway to our back-end service.



ERATOSTHENES Architecture with Modules Used in Smart Health Pilot

2.7.3.7 Alternative Flow

N/A

2.7.3.8 Post-conditions

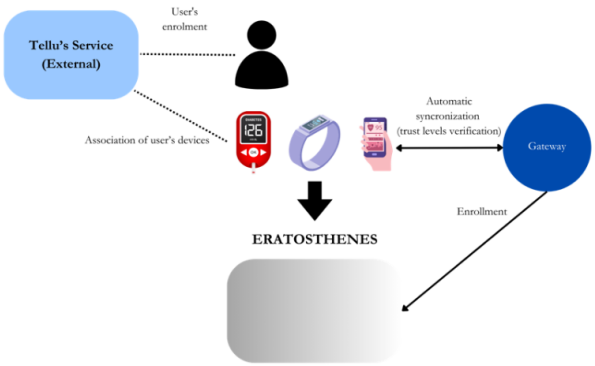
With the use of ERATOSTHENES framework, there is a significant improvement into the domain of trustworthiness and security, related to enrolment and application of medical devices. Improved in trust and identity management regarding people and devices from both the patient and the remote platform sides.

2.7.3.8 High Level Illustration

Use Case 1- Device Authentication and Authorization

A) Authenticate our own Gateway in our System

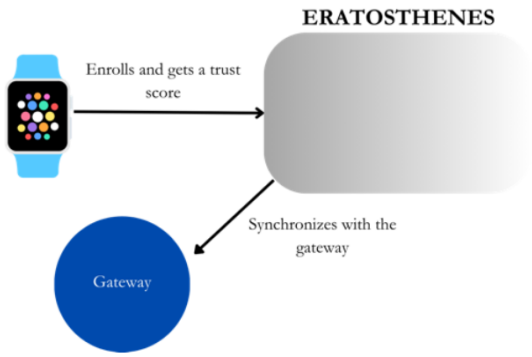
Each suite of devices, that are provided by the health service to patients, needs to be connected with a single gateway (Personal Health Gateway). Until now, the enrollment process was cumbersome and demanded manual intervention, making it difficult to scale. However, with the implementation of ERATOSTHENES, these various devices can be connected automatically by authenticating the gateway and leveraging the trust functionalities offered by the ERATOSTHENES architecture.



Pilot 2 Gateway Authentication

B) Authenticate External Gateway/Device in our own System

The objective of this use case is to facilitate the integration of a third-party device (or gateway) (e.g., an Apple Wallet) into the service platform. In alignment with the process delineated in the first use case, the third-party device would need to complete a prior enrolment in the ERATOSTHENES architecture. This enrolment enables the generation of a corresponding identifier that aids in securely incorporating the device into the platform. Thus, it ensures a seamless and secure user experience while broadening the scope of devices compatible with the health monitoring system.



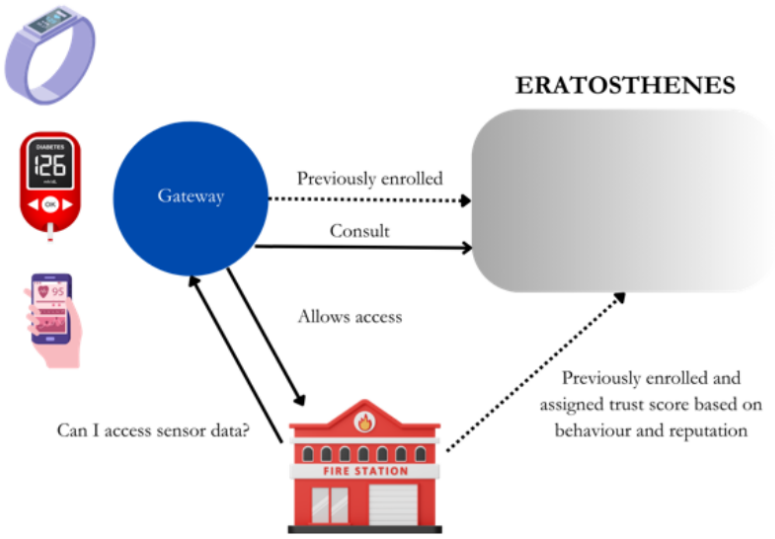
Pilot 2 External Gateway authentication

C) Authenticate External Services to Access our own Gateway/Devices

Strengthen of security measures is of major importance considering the sensitive nature of medical data. The authentication of external services can be leveraged in multiple scenarios. In general, when a third-party service provider interacts with these devices or the gateway itself, it is crucial to verify their trustworthiness. This is enabled through their prior enrolment in the ERATOSTHENES architecture, which assigns and records a level of trust for each third party.

A specific scenario that necessitates access to the health system provider's gateway is the case of emergency services. An explanatory scenario is when firefighters need to access a sensor during a fire outbreak. To facilitate this, the emergency service should have previously registered with the ERATOSTHENES system.

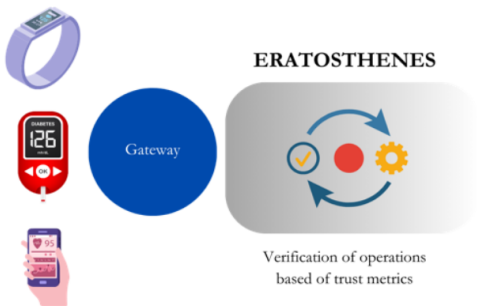
Upon registration, they are assigned a unique identifier and a trust score. When emergency access is required, the gateway can quickly consult this trust score and, if appropriate, grant immediate access.



Pilot 2 External Service Authentication

Use Case 2- Trust Management of Devices/Services

In this use case, when a device/gateway is enrolled and considered operational, the ERATOSTHENES features are utilized to sustain trust over time. This is achieved using specific trust metrics that assist in the detection of unusual behavior.



Pilot 2 Trust management of devices and services

2.7.3.10 Potential Requirements

A number of functional requirements for Pilot 2:

Consistent representation of trust relationships in personalized health devices

Assignment of trust score measurement to every device

Automatic deployment and update of software

End to End Cryptography

A number of non-functional requirements for Pilot 2:

Increase the average speed of software updates

Accuracy on detecting attacks and/or anomalies

Reduction of checking time of context condition for emergency situations

2.7.3.11 Radio Specific requirements

Only preliminary information is provided.

2.7.3.11.1 Radio Coverage

Radio cell range

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

Radio link crosses public spaces

Required scope of the multicell arrangement:

Global

Mobility: maximum relative speed of UE/FP peers

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

Special coverage needs

Healthcare

2.7.3.11.2 Bandwidth requirements

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

2.7.3.11.3 URLLC requirements

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

2.7.3.11.4 Radio regimens requirements

Desired and acceptable radio regimens

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

2.7.3.11.5 Other requirements

Requirements related to monitoring metrics of the gateway such as the OS-version, connectivity issues related to Internet speed, CPU usage, memory usage

Protection of personal identifiable information based on GDPR

2.7.4 ERATOSTHENES: Connected Vehicles

2.7.4.1 Description

In the automotive world, the number of IoT devices involved has increased drastically in the latest years due to the evolution of the environment to a smarter one. In this new smart environment, all the actors are interacting and making decisions among them. The work effort of this use case is devoted to the development, deployment, operation and validation of the IoT-based Connected Vehicle pilot in the ERATOSTHENES project. The pilot is materialised under two use cases, oriented on the V2I/V2V secure communication and the software update for vehicles. Both use cases are considered by adopting proposed project services (e.g., blockchain). Pilot 1 will demonstrate the enrolling/ bootstrapping of new Internet of Things (IoT) devices and trust verification with intrusion detection technologies, developed by the ERATOSTHENES project consortium partners. Integration tests are performed using the modules deployed in the current environment, and results are recorded to ensure the individual modules are working properly. Operation of selected modules (e.g., the Self-sovereign Identity (SSI) Management, the Trust Management Broker (TMB)) is demonstrated though Pilot 1, under the support of the Distributed Ledger Technology (DLT) through the whole ecosystem.

2.7.4.2 Source

ERATOSTHENES H2020 European project

2.7.4.3 Roles and Actors

Transport element: Smart vehicle that is under attack, and infrastructure (e.g., traffic lights) for the Vehicle to Infrastructure communication (V2X) network.

Stakeholders: i) End user as the consumer who uses the vehicle that is aligned with the ERATOSTHENS principles, ii) Industry as the supplier, iii) Sub departments of the Industry supplier such as the Communication Network supplier/provider/operator, IoT device manufacturer, IoT platform provider, iv) operators of the transport network, v) Insurance company

2.7.4.4 Pre-conditions

The main precondition is for the end-user to live a potential risk in the operation of the smart vehicle that is under attack (i.e., cyber-attack), that could result in casualties. Potential intentional attack to modify the intended purpose of the system or setup, create accident sub-pre-conditions, denial of service, limited communications etc.

2.7.4.5 Triggers

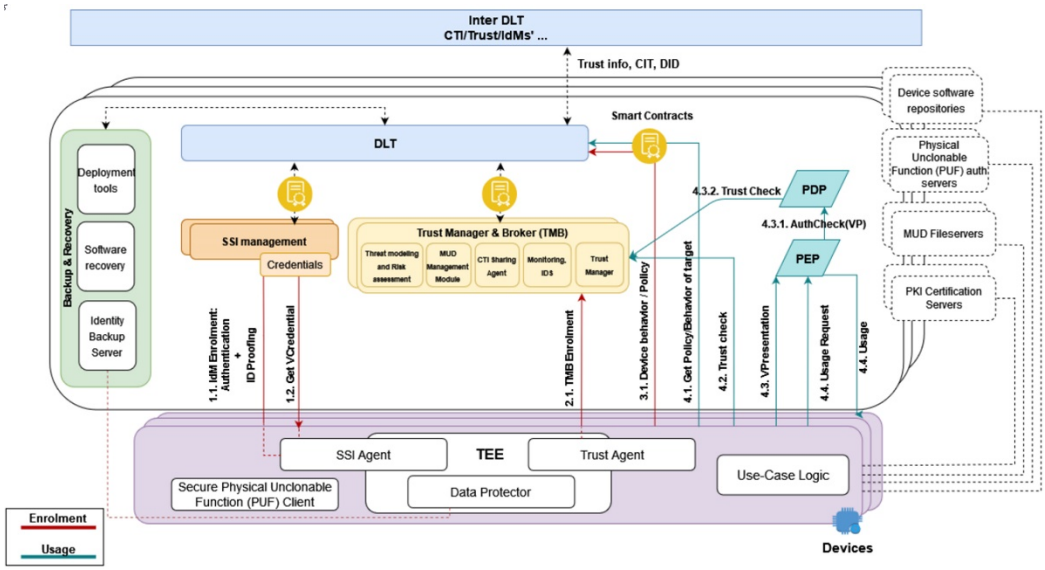
Triggers may include any smart infrastructure compromise in services provisioning (between vehicles or vehicles to infrastructure), smart infrastructure (traffic lights etc).

2.7.4.6 Normal Flow

Commonly, the steps in ERATOSTHENES are the follows:

The first stage is the initial enrolment to the network, which involves the deployment of the client modules, registration with the TMB, and authentication, to authorise the service usage.

The second stage is the use case with the interaction with the other device and the use of the ERATOSTHENES trust verification modules. This is where pilot 1's use case 1 scenario is actively run, and the attack is executed.



ERATOSTHENES Architecture with modules Used in Connected Vehicles Pilot

2.7.7.7 Alternative Flow

N/A

2.7.7.8 Post-conditions

With the use of ERATOSTHENES framework, there is a significant improvement into the detection and the response phase of the attack, which is the main industry goals.

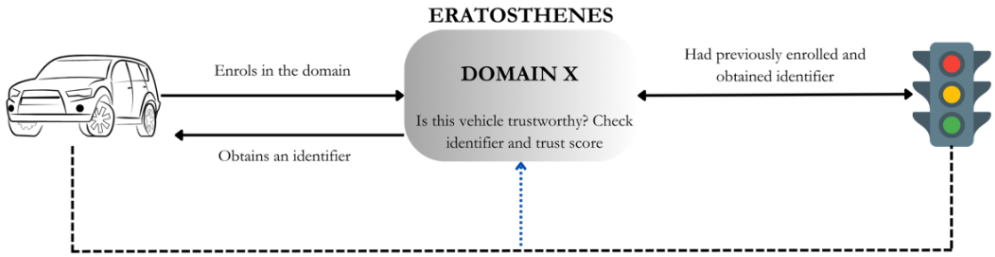
2.7.7.9 High Level Illustration

Use Case 1- Secure Connections

The objective of this use case is to enhance security during the establishment of connections between vehicles and either external roadside elements or other vehicles. To achieve this, it is crucial to determine the trustworthiness of these external elements for which the ERATOSTHENES architecture is employed. Two communication possibilities are considered:

A) Vehicle to Infrastructure

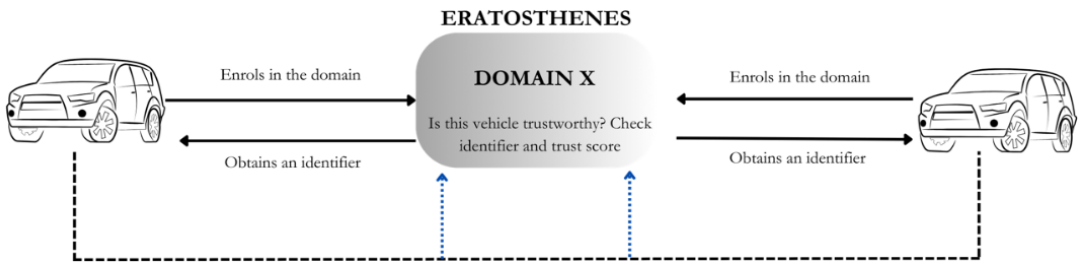
In this scenario, a vehicle, using its On-Board Unit (OBU), forms a connection with a smart traffic light. This interaction enables the vehicle, for example, to assess if it should proceed at its current speed or decelerate.



Pilot 1 V2I Communication

B) Vehicle to Vehicle

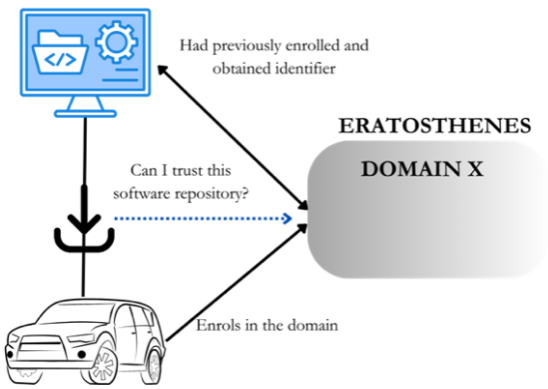
In this scenario, one vehicle seeks to establish communication with another, aiming to enhance traffic management, such as providing information on congestion, or boost safety by alerting about potential accidents.



Pilot 1 V2V Communication

Use Case 2- Remote Software Updates

This second use case of Pilot 1 is formulated within the context of a major challenge in the automotive industry. Ensuring that smart vehicle software is appropriately updated is vital, yet these updates can potentially open gateways for malicious attacks, leading to privacy violations or even actual accidents. To mitigate this risk, it is key to guarantee that the software updates are securely sourced from a trusted repository.



Pilot 1 Remote Software update

For the deployment of the use cases the interaction of the following components is required, namely:

The *Distributed Ledger Technology (DLT)* is deployed in the ERATOSTHENES server. The ledger is used in the pilot 1 scenario to disperse trust and threat information to other domains and provide information on the local Domain to the IoT devices when requested during the bootstrapping process. It uses blockchain technology to act as secure storage between the multiple ERATOSTHENES domains.

The *Self-sovereign Identity (SSI)* Management module is deployed in the ERATOSTHENES server. It is used to verify identity information that is received from the SSI agent on both the infrastructure and vehicle IDAPTs.

The *Trust Management Broker (TMB)* is deployed in the ERATOSTHENES server. It acts as the communicator between the IDAPT client modules and the trust modules in the Domain. These are the Trust Management and Risk Assessment (TMRA), Manufacturer Usage Description (MUD) management, Cyber Threat Intelligence Sharing Agent (CTISA), and Intrusion Detection System (IDS) modules.

2.7.4.10 Potential Requirements

Functional Requirements

Integration of Advanced driver-assistance systems Platform Tool client with ERATOSTHENEES modules

Reliable and scalable communication of ERATOSTHENES server to support the Distributed Ledger Technology (DLT)

Reliable integration of ERATOSTHENES sub modules with its clients counterpart (e.g., Self-sovereign Identity (SSI) Management module.

Reliable integration of Trust Management Broker (TMB) in ERATOSTHENES server, which acts as a communicator between the IDAPT client modules and the trust modules in the Domain (e.g., Trust Management and Risk Assessment (TMRA), Manufacturer Usage Description (MUD) management, Cyber Threat Intelligence Sharing Agent (CTISA), and Intrusion Detection System (IDS) modules) .

The system should be able to detect and respond (e.g. mitigate) to attacks.

Non-Functional Requirements

Reliable communication between the emergency bodies due to the information nature.

Secure and Privacy-Preserving Information Sharing

Efficient resource utilization (device/network)

2.7.4.11 Radio Specific requirements

2.7.4.11.1 Radio Coverage: Not applicable

Expected maximum and typical radio range:

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

Radio link crosses public spaces

Required scope of the multicell arrangement:

Global

Is handover required?

Mobility: maximum relative speed of UE/FP peers

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

Special coverage needs

Transportation

2.7.4.11.2 Bandwidth requirements

Network load (kb/s): To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

2.7.4.11.3 URLLC requirements

Required Latency, reliability and Maximum tolerable jitter:

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

2.7.4.11.4 Radio regimens requirements

Desired and acceptable radio regimens:

To be performed when in the full use case environment with final versions of ERATOSTHENES modules

2.7.4.11.5 Other requirements

To be performed when in the full use case environment with final versions of ERATOSTHES modules.

CPU usage (%)

Time between first message send/receive

Time between message receive/ present on HMI

Time for any message (not just first)

Total time for message through system (ms)

Timely response to attacks (detailed fully in trials plan)

2.8 Smart Manufacturing and Automation

5G supports communication with unprecedented reliability and very low latencies, and also massive IoT connectivity. This paves the way for numerous new use cases and applications in many different vertical domains, including the automotive, healthcare, agriculture, energy and manufacturing sectors. In manufacturing in particular, 5G may have a disruptive impact as related building blocks, such as wireless connectivity, edge computing or network slicing, find their way into future smart factories.

The fourth stage of the Industrial Revolution, also termed "Industry 4.0", is the next era in industrial production, aiming at significantly improving the flexibility, versatility, usability and efficiency of future smart factories.

Industry 4.0 integrates the Internet of Things (IoT) and related services in industrial manufacturing and delivers seamless vertical and horizontal integration down the entire value chain and across all layers of the automation pyramid [KaWa13] – here named Industrial IoT (IIoT). Connectivity is a key component of Industry 4.0 and will support the ongoing developments by providing powerful and pervasive connectivity between machines, people and objects. Moreover, wireless communication, and in particular 5G, is an important means of achieving the required flexibility of production, supporting new advanced mobile applications for workers, and allowing mobile robots and autonomous vehicles to collaborate on the shop floor – these being just a few examples.

Some of the target key performance indicators of 5G as specified by the International Telecommunications Union (ITU) are summarized in **Figure 27** (cf. [ITU-R M.2410-0]).

In order to support the three service types defined above and the diverse requirements of the anticipated 5G use cases by a common cellular infrastructure, network slicing, a new concept introduced in 5G, will allow simultaneous but isolated provisioning of diverse services by the same network infrastructure.

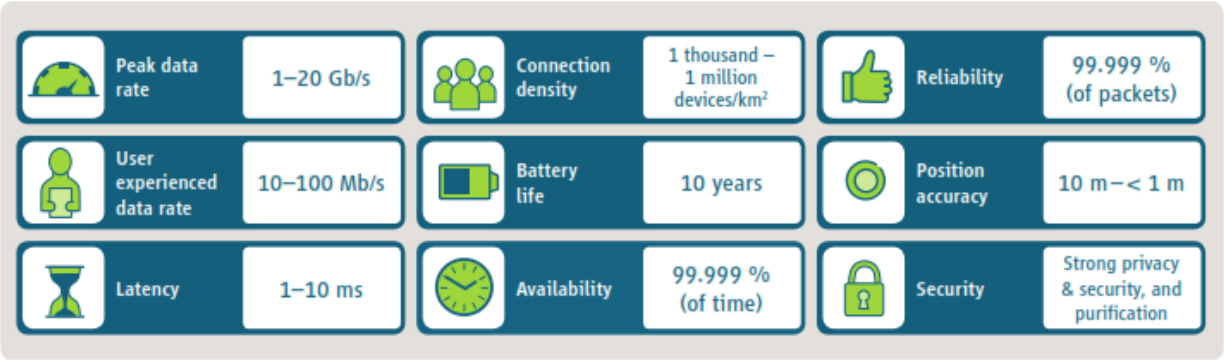


Figure 27: Selected target key performance indicators of 5G according to ITU-R (cf. [ITU-R M.2410-0])

Industry 4.0 and the Role of 5G

The fourth stage of the Industrial Revolution, also termed "Industry 4.0", is the next era in industrial production, aiming at significantly improving the flexibility, versatility, usability and efficiency of future smart factories. Industry 4.0 integrates the Internet of Things (IoT) and related services in industrial manufacturing and delivers seamless vertical and horizontal integration down the entire value chain and across all layers of the automation pyramid [KaWa13]. Connectivity is a key component of Industry 4.0 and will support the ongoing developments by providing powerful and pervasive connectivity between machines, people and objects. Moreover, wireless communication, and in particular 5G, is an important means of achieving the required flexibility of production, supporting new advanced mobile applications for workers, and allowing mobile robots and autonomous vehicles to collaborate on the shop floor – these being just a few examples.

5G Roadmap

The 3GPP began work on the specification of 5G in early 2017. The standardization work has been divided into two major phases: standardization of the fundamental 5G building-blocks has already been completed in June 2018 (Release 15), and further enhancements added by the end of 2019 (Release 16). According to 3GPP SA2 the Release-17 work made good progress, which most of the study items are over 95% complete. The study focus related to IIoT is on enhanced support of standalone non-public networks "SNPN" (TR23.700-07) and on enhanced support of Industrial Internet of Things related to Time Sensitive Communication (TSC) (TR23.700-20) including enhancements for support of deterministic applications etc. to IEEE Time-Sensitive-Networking (TSN) which is supported by 5G-ACIA work items for manufacturing industries.

Looking ahead to 2026, digitalization revenues from 5G for ICT players are estimated to exceed 1,200 billion USD, of which approximately 234 billion USD is accounted for by the corresponding vertical manufacturing [ErLi17]. In business terms, this constitutes an incredibly large and fast-growing market.

2.8.1 Factory of Future Use Cases

2.8.1.1 Description

5G has the potential to provide (wireless) connectivity for a wide range of different use cases and applications in industry. In the long-term, it may actually lead to convergence of the many different communication technologies that are in use today, thus significantly reducing the number of relevant industrial connectivity solutions.

Just as there is an ongoing trend towards Time-Sensitive Networking (TSN) for established (wired) Industrial Ethernet solutions, 5G is likely to become the standard wireless technology of choice, as it may for the first time enable direct and seamless wireless communication from the field level to the cloud.

Figure 28 illustrates different examples of where the benefits of 5G can be used in a factory in the future. Promising application areas range from logistics for supply and inventory management, through robot and motion control applications, to operations control and the localization of devices and items. Interestingly, 5G is likely to support various Industrial Ethernet and TSN features, thereby enabling it to be integrated easily into the existing (wired) infrastructure, and in turn enabling applications to exploit the full potential of 5G with ease.

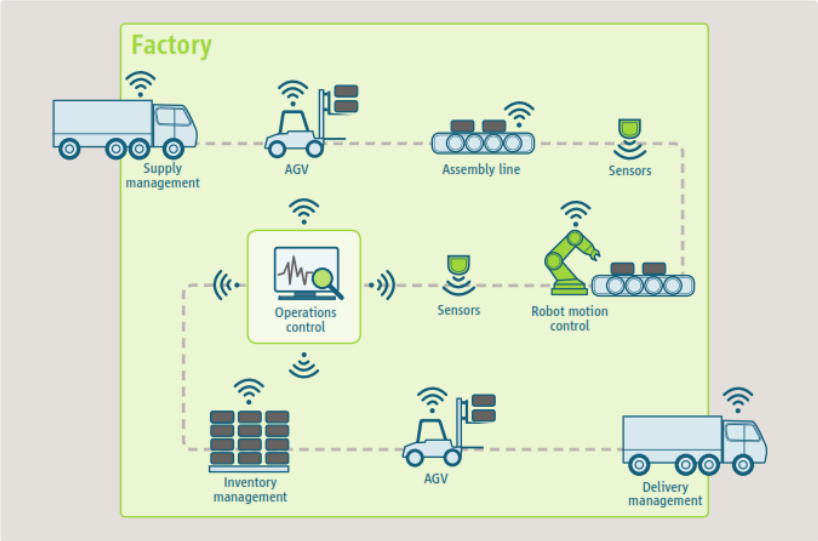


Figure 28: Exemplary application areas of 5G in the factory of the future

Certain more concrete use cases for the "Factory of the Future" have already been defined and analysed by 3GPP, with considerable support from a number of vertical industry players, in technical report TR 22.804 [3GPP TR 22.804].

In this respect, wireless communication and in particular 5G may support achievement of the fundamental goals of Industry 4.0, namely, to improve the flexibility, versatility and productivity of future smart factories. An illustrative overview of some of the use cases outlined in TR 22.804 is shown in **Figure 29**, in which the individual use cases are arranged according to their major performance requirements, classified according to the basic 5G service types eMBB, mMTC and URLLC. As can be seen, industrial use cases, such as motion control or mobile robotics, may have very stringent requirements in terms of reliability and latency, whereas others, such as wireless sensor networks, require more mMTC-based services. However, use cases and applications also exist that require very high data rates as offered by eMBB, such as augmented or virtual reality.

Among all listed use cases, motion control appears the most challenging and demanding. A motion control system is responsible for controlling moving and/or rotating parts of machines in a well-defined manner. Such a use case has very stringent requirements in terms of ultra-low latency, reliability, and determinism. By contrast, augmented reality (AR) requires quite high data rates for transmitting (high-definition) video streams from and to an AR device. Process automation lies somewhere between the two, and focuses on monitoring and controlling chemical, biological or other processes in a plant, typically extended, involving both a wide range of different sensors (e.g. for measuring temperatures, pressures, flows, etc.) and actuators (e.g. valves or heaters).

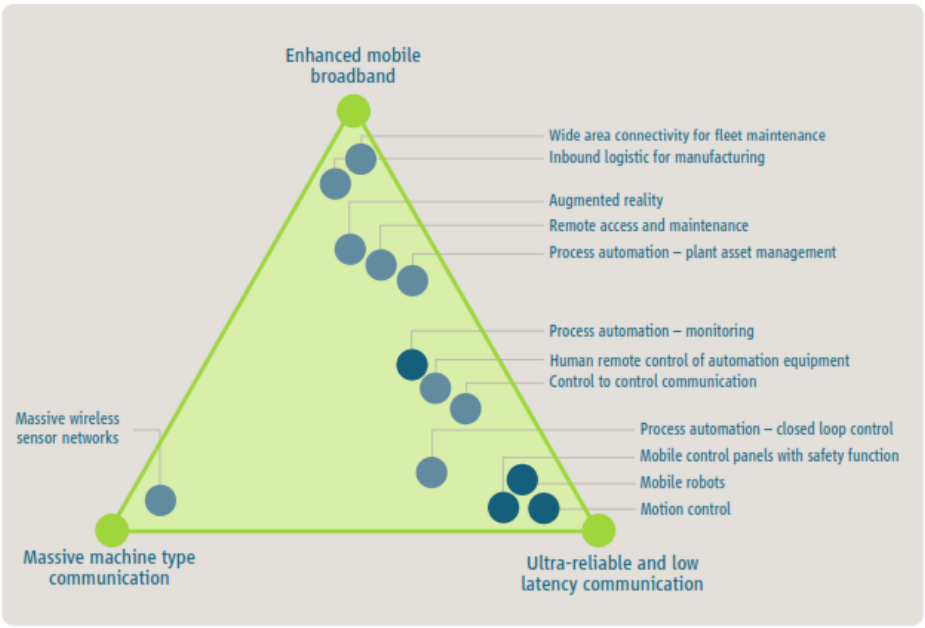


Figure 29: Overview of selected industrial use cases and arrangement according to their basic service requirements

2.8.1.2 Source

White Paper "5G for Connected Industries and Automation", 5G Alliance for Connected Industries and Automation (5G-ACIA), a Working Party of ZVEI

References Highlight_Issue_2_FLIP_BOOK_3GPP_March 2021, page 4-5

2.8.1.3 Roles and Actors

The 5G Alliance for Connected Industries and Automation (5G-ACIA) has been established to serve as the central and global forum for addressing, discussing, and evaluating relevant technical, regulatory, and business aspects with respect to 5G for the industrial domain. It reflects the whole ecosystem and all relevant stakeholder groups as shown in **Figure 30**.

OT industry (industrial automation, machine builders, end users, etc.), =

ICT industry (chip manufacturers, network infrastructure vendors, mobile network operators,

Academia and other groups, =

3GPP (ETSI) as main SDO for 5G standardization and regulation,

Various national and international associations and regulations.

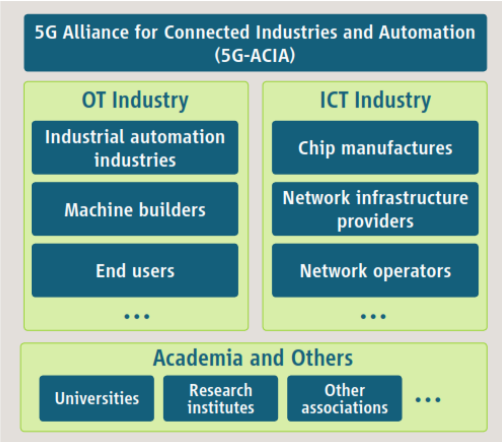


Figure 30: Overview of selected main stakeholder groups participating in 5G-ACIA

2.8.1.4 Pre-conditions

Pre-condition is already given as Industrial IoT is already in trail and implementation phase for various Industrial use cases. Business case and implementation depends on each industry use cases and status of brownfield vs Greenfield status of the industry /verticals.

2.8.1.5 Triggers

The triggers of the use-cases for Industrial IoT is given by the need of the verticals to have a very flexible, highly reliable and available with lowest latency, very secure and cost effective infrastructure to replace cable solutions where possible.

2.8.1.6 Normal Flow

The main domains of a 5G system are access, transport, management, cloud, and applications (including network functions and 3rd party applications). Traditionally, access, transport and management have been key areas in the cellular industries. Cloud and applications are traditional IT areas that have progressively become an integral part of cellular systems. The access domain provides wireless connectivity between the devices and the access nodes (e.g. a base station (BS)). The transport domain enables connectivity between remote sites and equipment/devices. The transport networks are interconnected via backbone nodes that carry information from the access nodes to the data centres, where most of the data is stored and the network is managed. An exemplary 5G system architecture for a smart factory scenario is shown in Figure 32. It illustrates that 5G may provide both communication within the factory and with other factories.

5G systems comprise control and data planes. Most of the control plane intelligence (mobility management, session management, etc.) resides in the data centre, while most of the data plane intelligence resides in the access network (scheduling, Quality-of-Service (QoS), multi-user).

Similarly, to TSN, a 5G network contains a management and application domain, which may partly run on cloud technologies. The network management entities in 5G systems automate and manage a range of lifecycle management processes. Furthermore, they coordinate complex dynamic systems consisting of applications, cloud, transport and access resources. Finally, applications, including many network applications, can run in cloud environments (with the exception of dedicated functions in the access nodes). The applications can be logically centralized or distributed, depending on the requirements. 5G can be characterized as a modular communication system, with in-built privacy and security, which is built upon the cloud approach and can be flexibly configured to meet different service requirements.

2.8.1.7 Alternative Flow

An alternative flow of a wireless technology is given by WiFi, especially latest version WiFi6.0 for certain Industrial IoT use cases. However, WiFi will be different in certain features, performance and system parameters depending on the business model.

2.8.1.8 Post-conditions

The specific interests of the industrial domain will be addressed more thoroughly in 3GPP Release 17 and 18, although some features have already become available in Release 15 and 16. **Figure 31** shows the roadmap for the 3GPP standardization of Releases 16, 17 and 18 (Source: Puneet Jain, 3GPP Working Group Chair SA2).

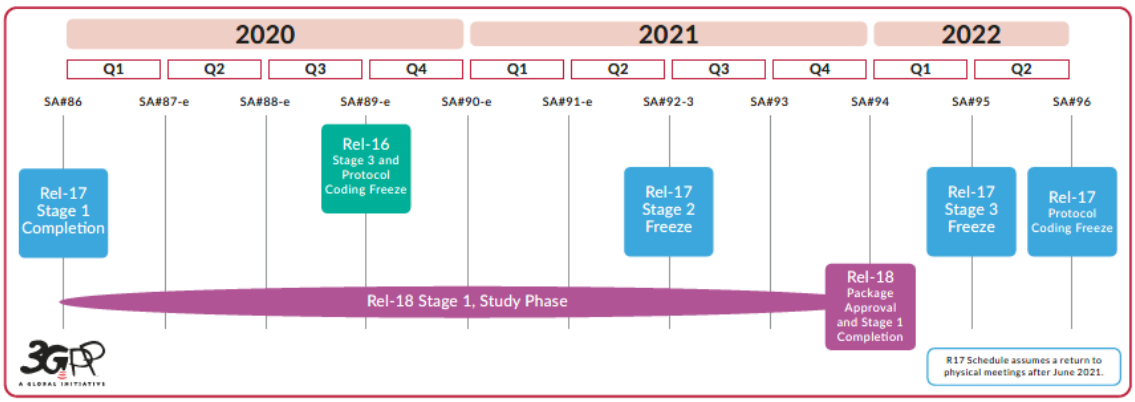


Figure 31: Overview of selected main stakeholder groups participating in 5G-ACIA

2.8.1.9 High Level Illustration

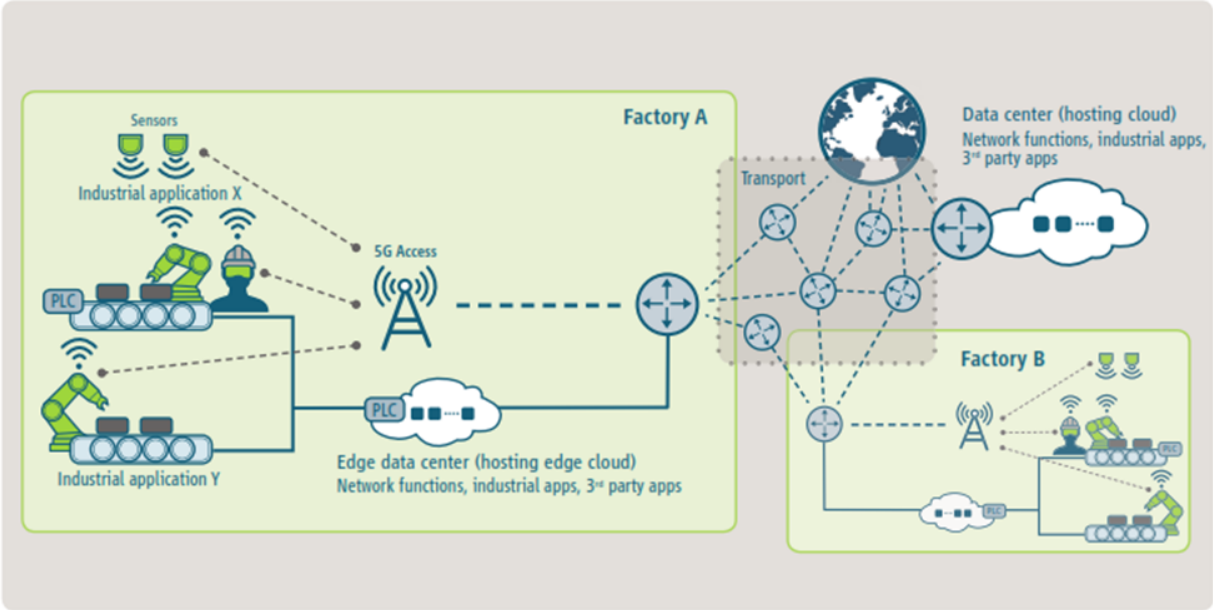


Figure 32: 5G-enabled smart factory scenario

2.8.1.10 Potential Requirements

Functional Requirements

Certain more detailed performance requirements of selected factory / process automation use cases (those indicated with a blue circle in Figure 29) are provided in

Table (see also 3GPP TR 22.804 for further information). As can be seen, industrial use cases may have the highest requirements in terms of availability and latency/cycle time and are often characterized by somewhat small payload sizes. The cycle time is the transmission interval in periodic communication, which is often used in industrial automation. The latency is usually smaller than the cycle time.

Table 8: Selected use cases and associated key requirements

Use case (high level)		Availability	Cycle time	Typical payload size	# of devices	Typical service area
Motion control	Printing machine	>99.9999%	< 2 ms	20 bytes	>100	100 m x 100 m x 30 m
	Machine tool	>99.9999%	< 0.5 ms	50 bytes	~20	15 m x 15 m x 3 m
	Packaging machine	>99.9999%	< 1 ms	40 bytes	~50	10 m x 5 m x 3 m
Mobile robots	Cooperative motion control	>99.9999%	1 ms	40-250 bytes	100	< 1 km^2
	Video-operated remote control	>99.9999%	10 – 100 ms	15 – 150 kbytes	100	< 1 km^2
Mobile control panels with safety functions	Assembly robots or milling machines	>99.9999%	4-8 ms	40-250 bytes	4	10 m x 10 m
	Mobile cranes	>99.9999%	12 ms	40-250 bytes	2	40 m x 60 m
Process automation (process monitoring)		>99.99%	> 50 ms	Varies	10000 devices per km^2	

In this respect, "availability" refers to the "communication service availability". This means that a system is considered to be available only if it satisfies all other required quality-of-service parameters, such as latency, data rate, etc. Comparison of the 5G requirements listed in **Figure 27** with those in

Table **8** shows that these requirements are addressed in Release 16 and future releases, in particular Release 17 and 18.

Non-Functional requirements

Support of Functional Safety:

Functional safety is one of the most crucial aspects in the operation of industrial sites. Accidents can potentially harm people and the environment. Safety measures must be applied in order to reduce risks to an acceptable level, particularly if the severity and likelihood of hazards are high. Like an industrial control system, the safety system also conveys specific information from and to the equipment under control. Some industrial network technologies are able to transport both industrial control information and safety-critical information. This could be achieved by implementing functional safety (e.g. based on suitable safety protocols) as a native network service, which would ensure proper safety provisioning.

A 5G system applied in industrial automation should also support functional safety. It is important for the safety design to determine the target safety level, including the range of applications in hazardous settings. In accordance with this level, safety measures can be developed for and used by 5G based on proven methods.

Security:

Previous industrial real-time communication systems – generally wired and often isolated from the Internet – were not normally exposed to remote attacks. This changes with increasing (wireless) connectivity as required for Industry 4.0 and offered by 5G. The use of wireless technologies requires that consideration be given to a wide range of types of attack: local versus remote, and logical versus physical. These attacks threaten the areas referred to above of reliability, dependability, availability and safety, resulting in risks to health, the environment and efficiency. Specifically, logical attacks exploit weaknesses in the implementation or interfaces (wired and wireless) by performing side channel analyses. Physical attacks focus on hacking of/tampering with devices by exploiting physical characteristics (and ultimately breaking a critical parameter, for example a key). The 5G industrial solutions must be protected against local and remote attacks (both logical and physical), as these can be automated and then carried out by anyone against a large number of devices (for example, bots performing distributed denial-of-service attacks). Local and isolated management of devices is therefore to be made possible in order to assist in the prevention of remote attacks.

In addition, device authentication, and message confidentiality and integrity are crucial for industrial communication systems. While data confidentiality is very important in order to protect company IP and prevent industrial espionage, data integrity becomes of paramount concern for industrial applications. This particularly applies to machine-to-machine communication in which data is used to either feed the control loop or control actuators. In this context, checks for data manipulation are not usually applied, resulting in compromised data being accepted as long as the values lie within a valid data range. This can lead for instance to machine failure or quality issues if not detected.

Finally, the security architecture must support the deterministic nature of communication, scalability, energy efficiency, and low latency requirements for industrial applications.

Cost efficient and flexible processes:

Production and operational processes must become more cost-efficient and flexible. Reductions in CAPEX and OPEX could be attained through reduced engineering costs (e.g. by the provision of on-demand infrastructures, system automation, etc.). Achieving flexibility in processes can be done by using virtualization, process modularization, and cloudification.

One example are local data centres that support critical industrial applications by way of an edge computing approach. In this case, existing infrastructures must be modified to tackle the new challenges. For instance, industrial applications can be deployed locally within an edge data centre to reduce latency.

2.8.1.11 Radio Specific requirements

Spectrum and operator models:

The availability of a suitable spectrum is an important aspect in the deployment of 5G services for industrial applications. In order to meet extremely demanding latency and reliability requirements, a licensed spectrum is highly preferred. Alternative means of accessing a licensed spectrum may exist, for example through regional licenses or by subleasing from (nationwide) mobile network operators; these differ in their benefits and drawbacks. It is important for suitable spectrum usage options and operator models to be found that take the specific requirements of the industrial domain into account and represent a fruitful basis for the success of 5G in industry. More Radio specific requirements are available in various White Papers.

2.8.2 5G Applied to industrial production systems

2.8.2.1 Description

As the world volatility and uncertainty increases, more the focus and relevance of flexible, connected and context aware production systems. This requires not only that all the processes and machines are sensorized and connected to advanced production execution systems (MES), but also that all this connectivity is as unobtrusive as possible, ideally wireless. This is where 5G plays a major role for the factory of the future.

In Industry 4.0 production systems, there are sensors measuring all aspects of production, which are sent through a powerful communications network to a server in the cloud or in the edge, that stores them, to be then processed by big-data algorithms, from which detailed information about the entire production process is extracted.

With this project, we want to aggregate IoT and 5G connectivity to bring the best technologies to the Industry in order to address typical challenges in the shop floor, improve Industrial processes (flexibility, efficiency, productivity, time sensitive communications, etc.) and build a base to new business models and circular economy promotion.

Under this scope three main use cases where defined:

Use Case Next Generation Industrial Infrastructure: Fault detection is a challenge in industry and issue prediction is the way to prevent quality issues while increasing efficiency and productivity in order to improve manufacturing competitiveness. In order to monitor machines and processes it is necessary to install sensors capable of acquiring metrics such as temperatures, pressure, humidity, level, vibrations, energy and others. With the high number of sensors that is currently being added to a system, there are challenges such as device management, high cable density and data processing. This highly increases solution cost and limits its usage. There is a clear need to offer the means for devices to be connected, especially legacy ones, due to the many emerging applications resulting from the next generation of wireless communication, of which 5G is the most remarkable[7].

To overcome these connectivity challenges, there is a consensus in exploring in factory environments: i) 5G wireless communications, enhanced with gateways for legacy equipment; ii) decentralization from cloud to edge; and iii) data exploration with pattern recognition, correlations and algorithms for improved efficiency.

Use case Smart wearables: In a factory environment, accidents like slips and falls on the factory floor are an important health issue[8]. On some working areas, there are safety risks related with objects, and cleanliness issues of the floor that potentiate safety hazards. To prevent hazards such as falls and slipping, safety shoes could have sensors to detect these safety risks and advise users. At the same time, information can be used in mapping the potentially dangerous areas on the shopfloor in order to advise and offer a warning regarding which areas must be cleaned. Again, 5G is the key of this use case for sending the data wirelessly to a cloud and to give the necessary geolocation for mapping the areas. For achieving this, our use case includes the software development to map risky areas and Apps for mobile devices (e.g., smartphones).

Use case Energy Management: Bosch is already carbon neutral since 2020, nevertheless is continuously looking for improvement opportunities. Thus, there is a need to improve energy management by developing advanced systems able to provide opportunities advice the users via data monitoring, correlations and rules.

2.8.2.2 Source

Augmanity PT2020 project

Interim information in a company: Critical Manufacturing - Augmanity

2.8.2.3 Roles and Actors

Industry IT personnel. The IT personnel in the industry will have to cope with new technology in premise, dealing with possible different network scenarios and operation/business models, even new technical terminology.

Industry i4.0 personnel: Responsible for defining the use cases, setting up the sensors network and manufacturing execution systems able to cope with the additional connectivity and data volume.

Industry operator: Using wearables or information made available coming from sensors and edge systems, providing additional predictive directions.

Network operator. Supplier of the 5G infrastructure, fully responsible for respective management or just for a part of it, depending on the business model.

University Researchers. In this project involved in use case research and development of new solutions, coordinating infrastructure requirements and implementing new technologies.

Hardware vendor. Responsible for the high-level hardware requirements definition, configuration, and architecture setup.

[7] https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

[8] https://www.who.int/news-room/fact-sheets/detail/falls

National network authority. Responsible for the criteria for policy definition, including bandwidth assignment and bidding rules.

2.8.2.4 Pre-conditions

Pre-condition to have a fully productive operational use case exploitation is to have 5G coverage in the relevant machines/areas where the use cases are to be implemented/developed. A stepwise approach is being used where we start with traditional sensor connectivity to machines / processes as a first phase, including data acquisition and analysis. In parallel the activities towards providing 5G connectivity take place, so that the use cases can be migrated, as soon as the 5G connectivity conditions are met.

2.8.2.5 Triggers

Most of the use cases under exploration require constant dataflow, in order to detect patterns in sensor data behaviour. A machine learning algorithm will process this data continuously, detecting patterns classified as issues, enabling early problem detection.

In case of slip and fall detection, the sensor will have an AI module, enabling near real-time situation classification (slippery condition detection), enabling pro-active alert to end user.

2.8.2.6 Normal Flow

Commonly, the steps are the follows:

Critical infrastructure systems (IoT systems, MES, informational systems): machine data (production counters, condition monitoring sensors data) is permanently being collected.

An edge-based pipeline is permanently monitoring the machine data / sensors data until a potential situation is detected, where an issue prediction can be issued (based on trained data patterns). Alternative: a used wearable is continuously collecting data and detects a pattern, where a prediction condition can be issued.

At this moment, an alert is generated so that the industrial operator can react timely, either replacing a part, doing a machine maintenance or whatever appropriate measure needs to be taken.

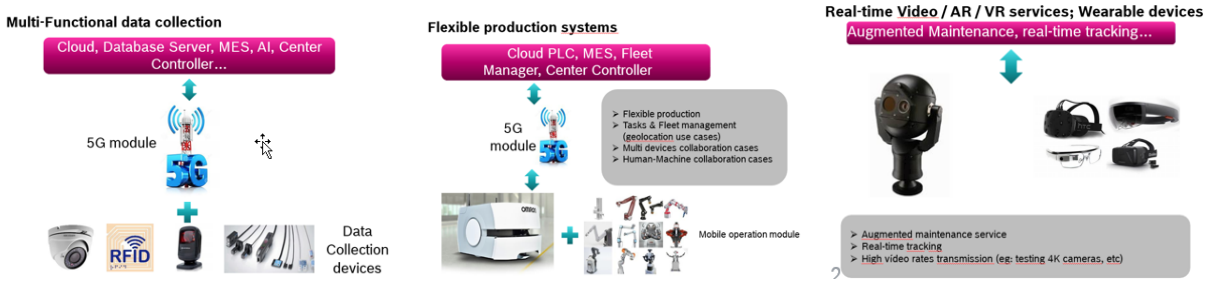
2.8.2.7 Alternative Flow

2.8.2.8 Post-conditions

Periodically there is the need to check for new conditions that lead to machine breakdown: they could need to be further classified and model trained/updated in order to improve prediction ability. The overall objective of the project is to develop such a long term assessment.

2.8.2.9 High Level Illustration

There are three basic scenarios:



2.8.2.10 Potential Requirements

Functional Requirements

Near Real-time communication with the stakeholders (especially critical for wearables / automatic moving machines like AGVs).

Reliable communication between machines and systems.

Scalable communication between systems to interconnects different critical infrastructures.

Flexible/transparent communication cell allocation as we may have machines relocation, as well as moving machines (AGVs, mobile robots, etc).

Non-Functional Requirements.

Secure and reliable communication between the different systems.

Interoperability between communication protocols (linked also with the possibility to use standard communication protocols between the systems).

2.8.2.11 Radio Specific requirements

The requirements below are mostly a collection of the collective requirements of the three major cases highlighted above. Most stressful use case is usually (but not always) the real-time video use case.

2.8.2.11.1 Radio Coverage

Radio cell range

Indoor full coverage, in a metallic environment. Typical expected coverage would be a minimum of 35 m^2 at the factory floor, but larger would be better.

Does the radio link crosses public spaces? Or is it constrained to indoor or customer premises?

Coverage indoor at factory premises.

Is Multicell required?

Multicell is expected due to coverage requirements. Handover is not essential at these use cases, but handover use cases are being developed.

2.8.2.11.2 Bandwidth requirements

Peak data rate

Uplinks of 2Gbps in the video use case per cell. Will less cells, uplink bit rate will need to increase.

Average data rate

Average very near the peak data rate.

Is traffic packet mode or circuit mode?

If circuit mode, is isochronicity required?

All traffic is packet mode, but timing constrains exist.

2.8.2.11.3 URLLC requirements

Required Latency Round trip of 20msec

Required Reliability Not clear since the protocol to be used is to be developed. But 1 failure per month.

Maximum tolerable jitter 3-4 msec

2.8.2.11.4 Radio regimens requirements

Desired and acceptable radio regimens

Due to Portuguese legislation, public spectrum will have to be used. Ideally, license-exempt would be possible.

2.8.2.11.5 Other requirements

UE power consumption

Rechargeable or primary battery?

Acceptable battery life

Devices in the current scenarios will be mains-powered. Future secondary scenarios will require battery life in some cases on the order of month.

Is terminal location required? location accuracy?

Current scenarios expect 50 cm location range. Further secondary scenarios would require extreme location – on the 5cm range.

2.8.3 5G-VICTORI: UC #2: Factories of the Future

2.8.3.1 Description

The main objective of this UC is to automate the monitoring process and improve inspection methods and maintenance procedures of energy utilities as Factories of the Future, both for cost/time reduction and quality improvement. The idea is to showcase how 5G technology can integrate and deliver services able to support these diverse applications simultaneously.

These services are mainly grouped into three classes: maintenance, security and operation services. Maintenance activities require support of low cost, energy efficient sensors, planted in a distributed and heterogeneous infrastructure.

Security and operation services ask for low latency trip signals and high bandwidth for CCTV. More specifically, three different scenarios will be demonstrated:

The application of mMTC-banded IoT architectures for preventive maintenance and monitoring of the factory assets.

The support of uRLLC-type applications for real time monitoring and automation in an industrial environment.

The provision of eMBB services for smart CCTV surveillance applications.

2.8.3.2 Source

Text included in subsections related to the 5G-VICTORI is copied from one or more documents that can be found via the following links:

https://www.5g-victori-project.eu/about-5g-victori/use-cases/uc-2/

https://www.5g-victori-project.eu/wp-content/uploads/2022/05/2022-04-11-D2.4-5G-VICTORI-end-to-end-reference-architecture.pdf (Page 41-44)

https://www.5g-victori-project.eu/wp-content/uploads/2020/06/2020-03-31-5G-VICTORI_D2.1_v1.0.pdf (Page 56-59)

5G-VICTORI deliverable D4.3, "Field Trials as showcase events and vertical business validation", September 2023

2.8.3.3 Roles and Actors

Providers (VISP), Network Operators (NO), Security and operation services, Factories.

2.8.3.4 Pre-conditions

To support the Smart Factory services, where each one of them imposes a substantially different set of KPIs, QoS mechanisms and schemes to the overall architecture, three dedicated slices are going to be instantiated concurrently on the network. Each slice corresponds to a different service:

A slice responsible for the timely collection of HV power cable sensor data from the two ADMIE sites at Rio and Antirio.

An eMBB slice for providing high-bandwidth communications to address sensor data collection, fusion and storage to the cloud.

An eMBB slice for providing high-quality live video streaming dedicated to smart facility monitoring and inspection.

2.8.3.5 Triggers

2.8.3.6 Normal Flow

The deployment of the new infrastructure brought by the 5G-VICTORI project involves installation of sensing devices at the predefined locations and powered through either battery/solar cells or connected to the power supplies provided by ADMIE (**Figure 33**). The cells providing the gateway of the collected data are installed (software defined NB-IoT cell, COTS LoRaWAN gateway, Wi-Fi AP) along with the edge data centre and the remote connection to the 5G-VINNI facility.

The figure below shows the placement area that was selected for the demo following initial site surveys between the Rio (B1) and Antirio (B2) terminal stations. Indoor installations have already been performed in B1, however a major power cut need to be planned in order to perform the outdoor installations of the antennas.

Figure 34: UC facility plan and configuration at ADMIE facilities

2.8.3.7 Alternative Flow

N/A

2.8.3.8 Post-conditions

Figure 35 show the spider diagram accounting on the KPIs to be fulfilled. As already mentioned, note that these reflect the vertical (ADMIE/ digital utilities – energy) requirements considering not only the current (restricted to SW and network capabilities) services but the foreseen future ones, thus not all of them are subject to demonstration. Further refinement of these KPIs will be provided in the context of WP3, with the explicit definition of the applications to be demonstrated.

As initial estimation, for the demonstration of UC # 2, cameras (2 Full HD /4K cameras) will be considered for the Rio-Antirio facility premises, and 50 sensors of different types (motion control, humidity, temperature etc.) will be spread in the ADMIE facility of 2000 m2 . For KPI measurement purposes sensors will be distributed across the facility in different density configurations.

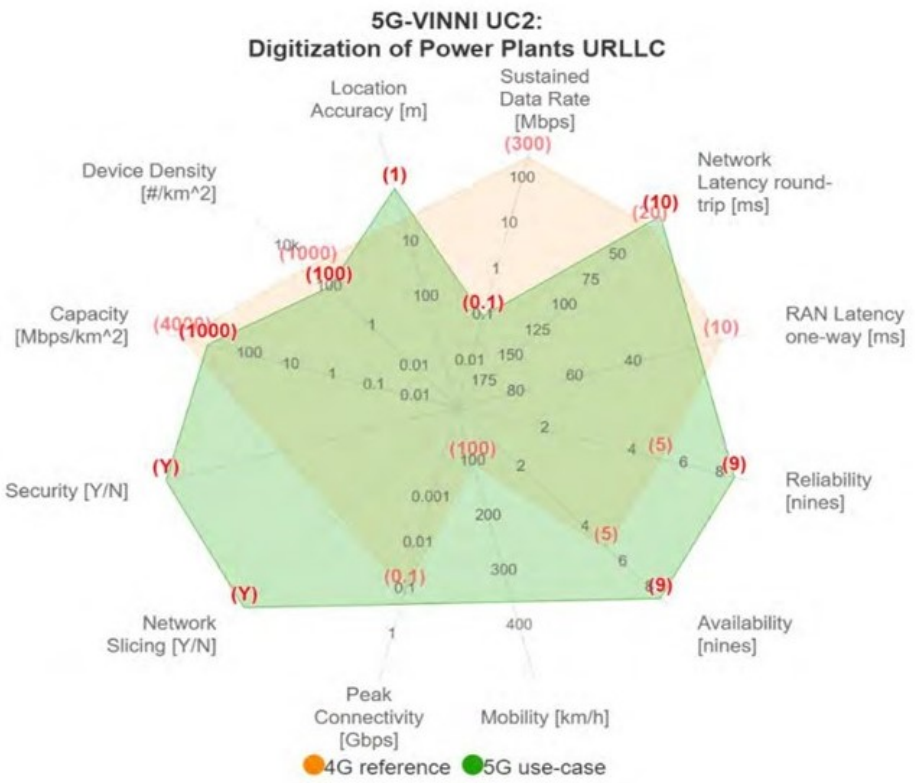


Figure 35: UC # 2 Digitization of Power Plants URLLC

2.8.3.9 High Level Illustration

Low latency services with flexible 5G architecture (Smart Factory) A smart private network of energy efficient sensors and the corresponding management system, able to support preventive maintenance techniques, is demonstrated. Preventive maintenance applications requiring high frequency timestamped sampling will be considered.

Due to the large volume of data, originating from different sensors spread at the facilities, needed to support the preventive maintenance applications, low-cost and low-power devices without strict latency requirements must be used. 5G NR is used for the transmission of the collected data to the ADMIE central facility where the ADMIE data management platform will coordinate the correlation and analysis of the collected time-stamped information from various sites. 5G NR will interconnect the UEs of technicians that look after the area.

Figure 5-7 illustrates how the specific services are mapped on Patras5G architecture and how it is orchestrated by the OSM at UoP premises. Specifically, as shown in the figure, the MEC enabled Factory of the Future gives access to the ADMIE personnel to access the ADMIE digital infrastructure (application and data) via two types of services corresponding to two UPFs and two slices that will be discussed below.

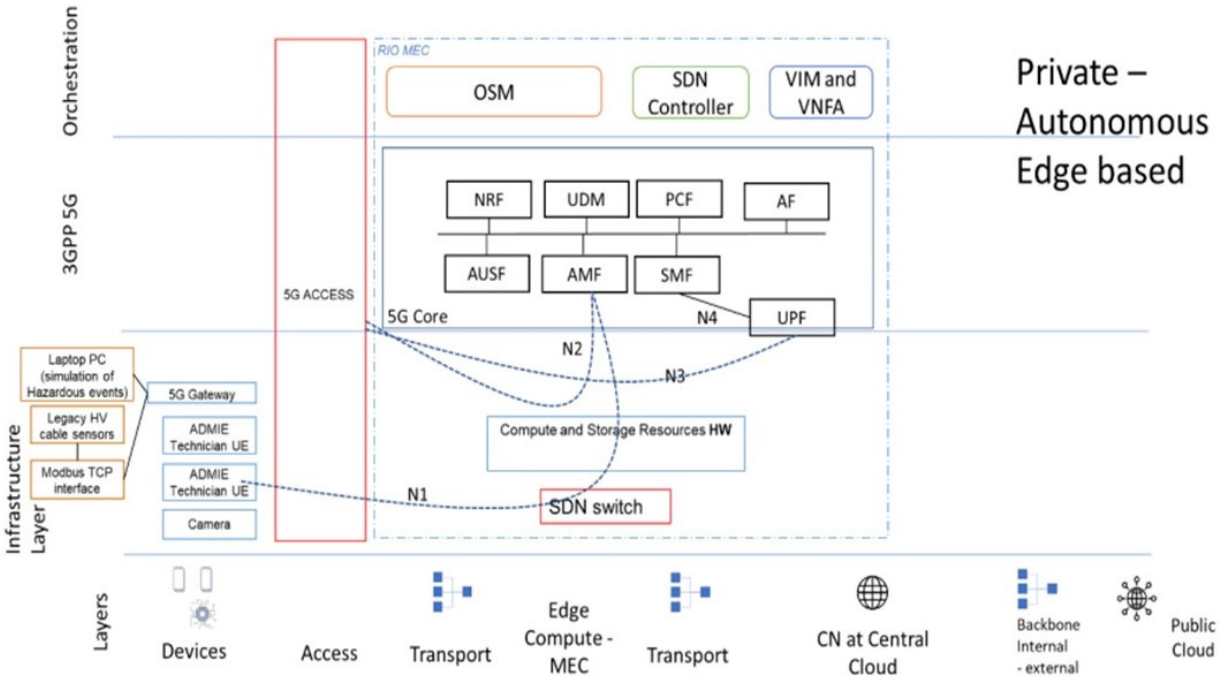


Figure 36: Smart Factory and Energy Services over Private Networks

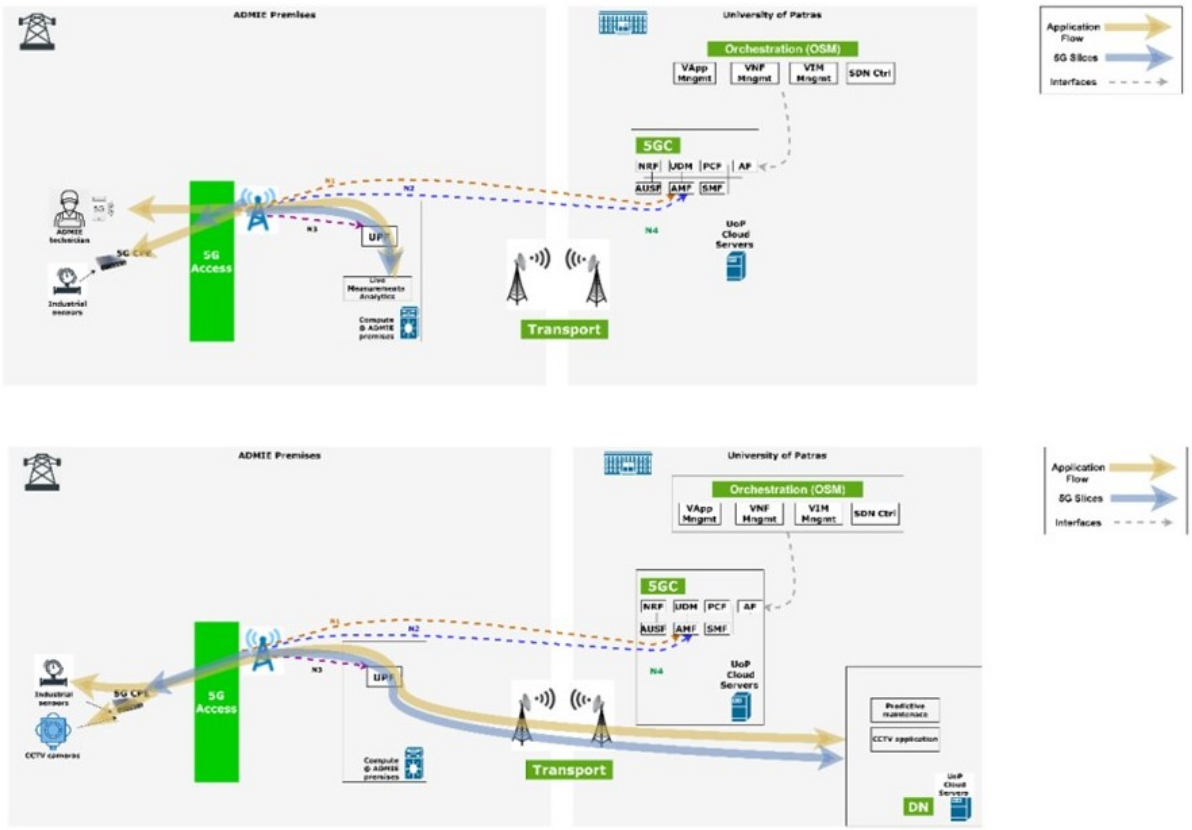


Figure 37: Application flows and 5G slices for Smart Factory services

2.8.3.10 Potential Requirements

The service performance requirements for the main communication services categories foreseen in the forthcoming smart factory/ digital utilities and 5G landscape are summarised in **Table 14.**

Table 14: UC # 2 Key UCs requirements and KPIs

Vertical: Smart Factory			UC # 2 – Digitization of Power Plants		
			Monitoring & Alerting Services (URLLC)	Maintenance Services (mMTC)	CCTV(as eMBB type of service)
UC Requirement - KPI		Units			
1	Latency (min. between user service end-points)	ms	10 ms	Not Critical	100-150 ms
2	User Datarate (Max.)	Mbps	0.1 Mbps (per device)	1-100 kbps (per sensor)	10-15 Mbps (Uplink, per HD/4k camera)
3	Reliability (%) - Min/MAX	%	> 99.9999999% (SIL 7)	>99%	99.9999 % (SIL 4)
4	Availability (%) - Min/MAX	%	> 99.9999999% (SIL 7)	>99%	99.9999 % (SIL 4)
5	Mobility	km/h	0 km/h	0 km/h	0 km/h
6	Traffic Density (Traffic demand per specific area)	Mbps/ area surface	Low, not critical 1000 Mbps/ 2000 m^2	Low, not critical 1000 Mbps/ 2000 m^2	20-100 Mbps / 2000 m^2
7	Device Density (#Devices per specific area)	Devices/ area surface	Low, not critical 100 Dev over 2000 m^2	100 Dev over 2000 m^2	Low, not critical 20 cameras/ 2000 m^2
8	Location Accuracy	m	non critical because the deployment is static thus the sensors' location is already known	non critical because the deployment is static thus the sensors' location is already known	non critical because the deployment is static thus the sensors' location is already known
Additional Requirements					
9	Packet Loss Ratio	Num	10^{-9}	10^{-6}	0.005
10	Bit Error Rate		Mission critical		Mission critical
11	Security (Y/N) ("Carrier Grade")	Y/N	Y	Y	Y
12	Type of Device		IoT devices/ Cameras/ Gateways	IoT devices/ Gateways	CCTV Cameras (possibly FHD/4K)
13	Type of Connection (i.e. Ethernet, WLAN, Zigbee)		5G/NB-IoT/Wi-Fi	5G/NB-IoT/Wi-Fi	5G/Wi-Fi
14	Battery Lifetime		Non Critical	up to 10 years	Non Critical
15	User Datarate (Max.)	Mbps/ samplin g point	Non Critical	2-10 Mbps	Non Critical

Table 15: UC # 2 Network functional requirements and KPIs

Req.ID [U/F-Type-RQ#]	Description [Descriptive text]	Priority [H/M/L]	KPIs and Parameters [to be measured]
S-FU-5301	**Air Interface – Access Network** Towards delivering the required network coverage for the specific devices, it is needed to design and develop antennas operating at 5G/ Wi-Fi & NB-IoT frequency bands.	H	• Antenna operation at 5G, Wi-Fi and/or NB-IoT support.
S-FU-5302	**Distributed Pools of (Compute/Network) Resources** Towards achieving the stringent QoS targets as well as efficient resource utilisation, it is necessary to enable instantiation of network, compute and storage resources optimally selected from a common resource pool that is physically distributed. This requires that the deployment is based on distributed (at different geographical locations, e.g. in the notion of edge computing) pools of resources (i.e. DCs) where the allocation is based on specific QoS and resources requirements.	H	• Capability for instantiation of network and compute resources for a specific service over geographically distributed pools of resources. It shall be possible to use various Edge and Core DCs to host different parts of the Power Plants Monitoring and Preventive Maintenance Applications. • Monitoring of distributed resources pools from a common platform.
S-FU-5303	**Multi-Tenancy** The 5G facility needs to support simultaneously multiple tenants and multiple services, with various QoS, requirements, etc., over a single infrastructure. Since it can be possible that different departments make use and have access rights to different monitoring and maintenance applications/ information over the same ADMIE facility (e.g. one department can control the CCTV cameras, and another one can be in charge of monitoring the cable status), it shall be possible from the 5G facility to allow the creation of multiple tenants for this scenario.	H	• Delivery of services with the requested QoS to multiple tenants over a single network deployment.

2.8.3.11 Radio Specific requirements

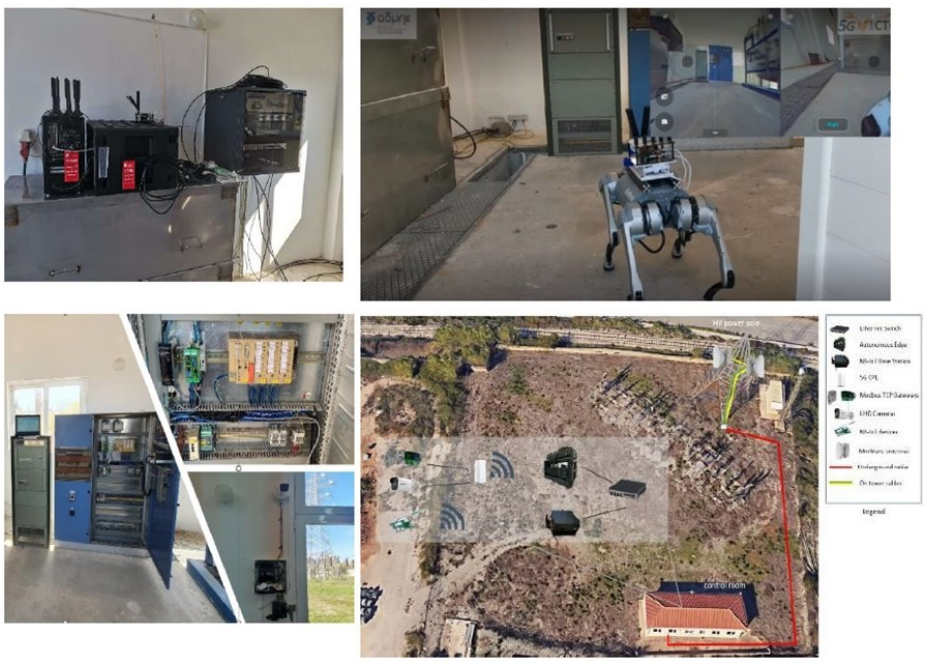


Figure 38: a) 5G network deployed at ADMIE facility for Patras trials, b) robotic camera for the high voltage environment with live streaming over 5G, c) various interconnected sensors at the high voltage facility

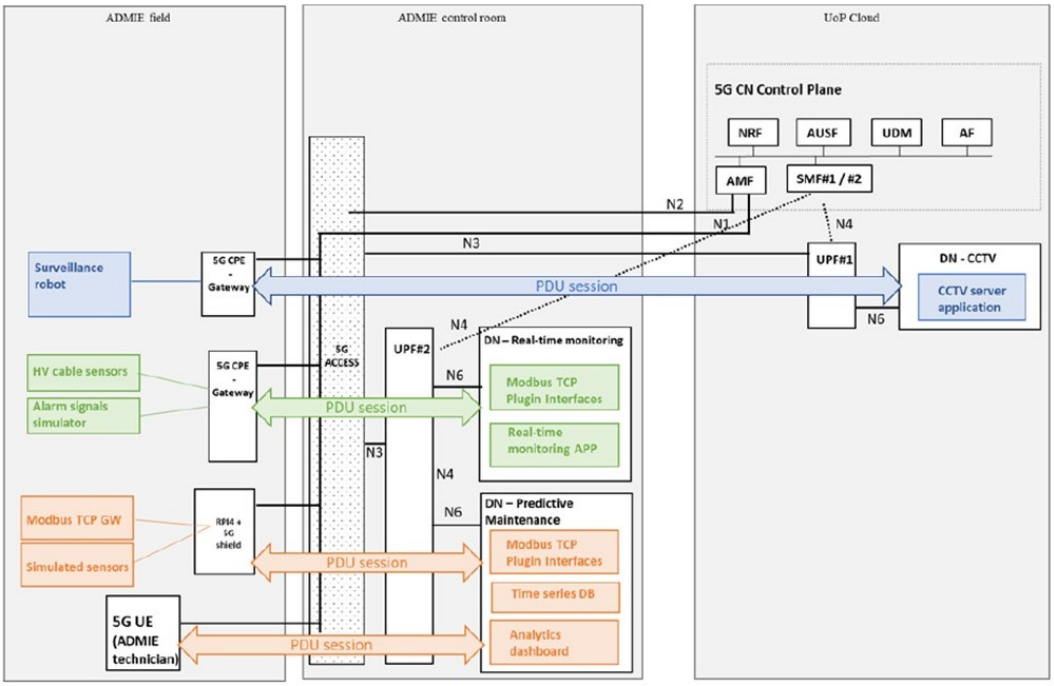


Figure 39: High-level architecture of UC #2

CCTV monitoring of facilities over 5G provides live video feed when technical personnel is present or an event occurs, while not compromising other Industry 4.0 applications running in the background. For the demonstration of this service, two UHD CCTV cameras are installed inside the HV cable control room and a third robotic camera is used inside the Smart Factory facility. The purpose of the Facility CCTV Monitoring service on high-level is the following:

Provide network slice customized for CCTV monitoring.

Demonstrate that CCTV Streaming is conveyed over 5G with the required characteristics, regardless of other services and background traffic.

Table 16: High-Level 5G Deployment Scenario UC #2

Scenario Description Template – Lab		
Radio access technology (RAT)	5G VINNI _3 (AW2S)	5G VINNI_4 (Callbox Classic)
Standalone / Non-Standalone (if applicable)	SA	SA
Cell Power	33 dBm	20 dBm
Frequency band:	n78	n78
Maximum bandwidth per component carrier	100 MHz	50 MHz
Sub-carrier spacing	30 KHz	30 KHz
Number of component carriers	n/a	n/a
Cyclic Prefix	n/a	n/a
Massive MIMO	n/a	n/a
Multiple-Input Multiple-Output (MIMO) schemes (codeword and number of layers)	4x4 MIMO	2x2 MIMO
Modulation schemes	Downlink: 256 QAM Uplink : 256 QAM	Downlink: 256QAM Uplink: 256QAM
Duplex mode	TDD	TDD
TDD uplink/downlink pattern	7 Down / 2 Up timeslots	7 Down / 2 Up timeslots
Contention based random access procedure/contention free	n/a	n/a
User location and speed	n/a	n/a
Background traffic	n/a	n/a
Computational resources available	n/a	n/a

Table 17: CCTV services report from tests done at the Field Demo in Patras

Field	Description
Test Case ID	**EDCv01**
Facility, Site	5G-VINNI, ADMIE site
Description	This test case demonstrated the provisioning of a CCTV network slice for critical assets monitoring over a private 5G network, where the CCTV equipment are connected over the mmWave backhaul to the UoP cloud (e.g. ADMIE offices) where the Open5GS Core Network and facility CCTV monitoring service were instantiated.
Executed by	Partner: ADMIE, ICOM, UoP
Purpose	Smart CCTV surveillance services for industrial environments over 5G
Scenario	**EDCv01**
Slice Configuration	CCTV slice
Components involved	MEC server (Autonomous Edge + gNB) CCTV camera Mobile surveillance robot with 5G connectivity Network switch mmWave 10Gbit Link UoP DC
KPIs collected (Metrics collected)	CCTV camera datarate, mobile surveillance robot camera datarate, CCTV streaming latency, CCTV maximum packet loss ratio
Tools involved	wireshark
Results and KPIs **Primary** **Complementary**	Video streaming latency: Min = 0.9 s/ avg = 2.32 s / max latency = 5.01 s (including application processing overhead) CCTV camera datarate: Min = 6.5 Mbps / avg = 9.33 Mbps / max bitrate usage = 12.78 Mbps 5G-enabled mobile surveillance robot camera datarate: Min = 0.4 Mbps / avg = 1.5 Mbps / max bitrate usage = 2.5 Mbps Aggregated datarate: Min = 7.3 Mbps / avg = 11.03 Mbps / max bitrate usage = 15 Mbps
Target metric/KPI and verification (pass/fail)	Seamless provisioning with no interruption time achieved, throughput expected results achieved

2.8.3.11.1 Radio Coverage

Radio cell range

Specification of expected maximum and typical radio ranges (indicate if LOS/NoLOS)

10000 m2 with multipath

Does the radio link crosses public spaces? Or is it constrained to indoor or customer premises?

Constrained to an outdoor private area

2.8.3.11.2 Bandwidth requirements

CCTV camera data rate: Min = 6.5 Mbps / avg = 9.33 Mbps / max bitrate usage = 12.78 Mbps

5G-enabled mobile surveillance robot camera data rate: Min = 0.4 Mbps / avg = 1.5 Mbps / max bitrate usage = 2.5 Mbps

Aggregated data rate: Min = 7.3 Mbps / avg = 11.03 Mbps / max bitrate usage = 15 Mbps

2.9 Service Trust and Liability Management

2.9.1 E2E Service Trust and Liability Management for Verticals

2.9.1.1 Description

5G networks play a fundamental role in the implementation of pervasive and digital services with anytime-anywhere connectivity. They are envisaged to be extremely flexible and dynamic to fulfil the myriad of use cases for Verticals with very different requirements such as ultra-low latency or ultra-reliability.

Some of these Verticals must comply with stringent safety and cybersecurity legal obligations that need to be translated into requirements for underlying services for data communication and processing. For example, some vertical industries are considered as Operators of Essential Services (OES) by the European Network and Information Security (NIS) Directive because their interruption would have a significant impact on the functioning of the economy or society[9]. As such, they have to protect themselves against cyber-attacks and need to delegate or enrich some of these controls with services provided by 5G E2E Service Providers. Domain-specific regulation or standards like ISO 14971 for Health[10] or SEVESO[11] for industry also impose controls that can be translated into requirements for privacy, isolation of processing or network component certification levels.

Moreover, the strategy to implement the highest level of security is unrealistic. For instance, some requirements may be incompatible. Most use cases do not need the strongest security level, while Verticals will be reluctant to pay for services that they do not need and do not use.

The difficulty to track the support of security requirements and demonstrate responsibilities in the multi-party and multi-layer 5G architecture hinders the adoption of 5G E2E Services. Therefore, the way to define and measure the effectiveness of security of components forming the service used by Verticals is needed. And the definition of liability and responsibilities when security breaches occur is essential to support confidence between parties and compliance with regulation.

2.9.1.2 Source

INSPIRE-5Gplus H2020 European project

2.9.1.3 Roles and Actors

Vertical. Vertical industry entity subcontracting E2E services for its main activity, needs to demonstrate that used services meet regulations or standards related to security, privacy, etc.

E2E Service Provider. Provides services spanning over multiple domains consuming services offered by Domain Service Providers.

Domain Service Provider. Provides services within particular domain e.g. communication domain, edge computing domain, device management domain, cloud domain, etc.

Component Provider. Provides components (infrastructure, devices, software) used by service providers to build services (can be distinguished as Infrastructure Provider, Software Vendor, etc.).

[9] European Commission. EU Network and Information Security (NIS) Directive (EU 2016/1148) - http://data.europa.eu/eli/dir/2016/1148/oj

[10] ISO 14971:2019 Medical devices — Application of risk management to medical devices. https://www.iso.org/standard/72704.htm

[11] European Commission. SEVESO III Directive (2012/18/EU) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012L0018

2.9.1.4 Pre-conditions

Vertical has defined the service that should be delivered by E2E Service Provider. The definition also covers different security measures, that are required to achieve Vertical's security objectives (for example access control, service isolation, security monitoring).

Security controls and the ways to monitor them are included in Service Level Agreement (SLA).

E2E Service Provider translates needed security properties into domain-specific requirements that have to be fulfilled by Domain Service Providers.

The liability relations are expressed in Stakeholder Responsibility, Accountability and Liability descriptor for the E2E Service with indication of properties committed by each actor involved in service delivery (E2E Service Provider, Domain Service Providers, Component Providers). The signature of commitments, as well as the usage conditions, are necessary to achieve the liability criteria.

2.9.1.5 Triggers

The first trigger used in this use-case is when the E2E service requested by Vertical is activated. During its operation, security controls are monitored on request of Vertical. When anomaly is detected or security breach occurs, the most likely responsible parties with the appropriate accountability need to be identified and reported (cf. Alternative Flow).

2.9.1.6 Normal Flow

During E2E service activation the steps are following:

1. Domain Service Providers in each domain deploy needed services with required security properties.
2. The evidence of effectiveness of applied security controls are exposed using tools provided by Domain Service Providers.
3. The evidence is aggregated by E2E Service Provider and exposed towards Vertical.

During E2E service operation:

4. Vertical can request evidence of effectiveness of applied security controls.
5. The evidence is collected and exposed using tools provided by Domain Service Providers.

2.9.1.7 Alternative Flow

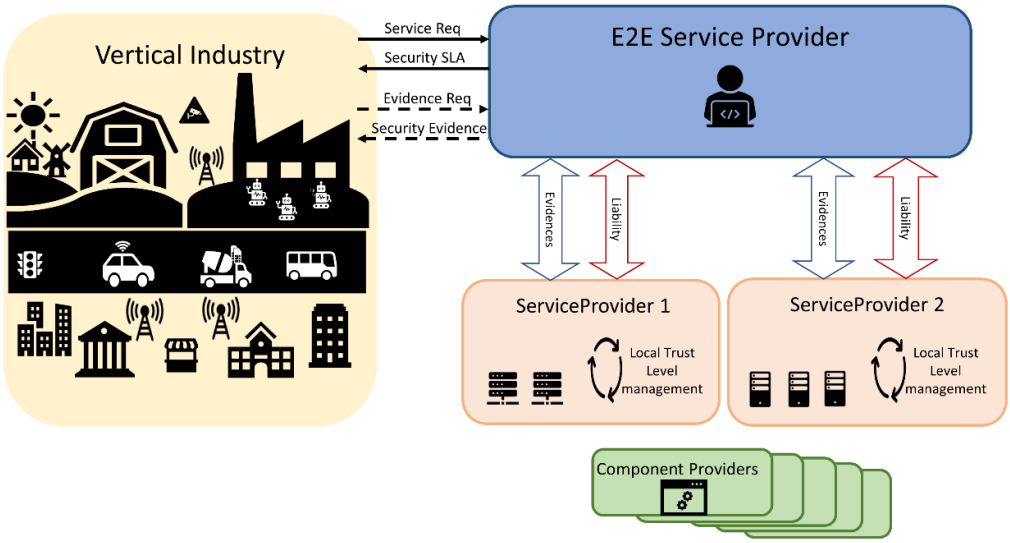
When anomaly is detected or security breach occurs:

1. The evidence of the occurred problem is collected and root cause of the problem is investigated.
2. E2E Service Provider uses agreed Stakeholder Responsibility, Accountability and Liability descriptor to identify responsible parties based on the root cause.
3. The problem is mitigated based on the identified root cause and the liability of E2E Service Provider towards Vertical.
4. Incident liability negotiation can be held among the responsible parties (E2E Service Provider, Domain Service Providers, Component Providers).
5. If the negotiations fail, parties may go to court.

2.9.1.8 Post-conditions

During E2E Service operation, security controls are monitored on request of Vertical. Security SLA and Stakeholder Responsibility, Accountability and Liability descriptor may need to be updated/renegotiated based on experience from the incident resolution.

2.9.1.9 High Level Illustration



2.9.1.10 Potential Requirements

Non-Functional Requirements.

Security enablers to provide required security properties (e.g. isolation, confidentiality, anomaly detection).

Security enablers to verify that a required property is really and correctly provided (e.g. Infrastructure Attestation Framework) – certification of these enablers (the *requirement related to "Trust in ICT infrastructure" indicated in Networld 2020 (SNS) Strategic and Research Innovation Agenda (SRIA)*).

Security enablers to define liability relation (e.g. Stakeholder Responsibility, Accountability and Liability descriptors) and the system for its management.

2.9.2 5G COMPLETE: Example: UC#4: Advanced Surveillance/Physical Security Service

2.9.2.1 Description

In the context of this use case, an innovative 5G-based advanced end-to-end surveillance/physical security solution is considered, exploiting the capabilities of the 5G-COMPLETE architecture, esp. with regards to 5G FWA technologies, orchestration of resources, edge processing, etc. which affects the quality and the reliability of the monitoring/surveillance service. Such solutions have direct applicability on various verticals, such as smart cities, public safety and facilities with multiple distributed "sites" (municipalities, factories, warehouses, University campuses, hospitals, Telco infrastructure sites, etc.).

To render the solution attractive to the stakeholders, a long list of requirements shall be met such as: ease in installation/operation (wireless connectivity supported), fast service deployment, scalability and customization, camera vendor/model independency (e.g. wired and wireless, bullet and PTZ (Pan Tilt Zoom), indoor and outdoor cameras supported), 24x7 monitoring, low-cost deployment and operation (reuse of existing cameras allowed, without additional h/w at site and associated support costs, reduced need for human resources for monitoring purposes, etc.), Graphical environment (WebGUI) for info visualization (sites' info over google maps, snapshots/videos per site and per camera, statistics (e.g. alerts/site, per object), playback, live streaming, camera configuration), automated storage in secure cloud/backend infrastructure,

smart alerting, including enhanced notifications, only when specific objects detected, voice announcements, etc., in real/near real-time; voice announcements may reduce the need for the security staff to watch all the cameras' activity via the monitors/screens 24x7. However, there are specific capabilities/features that pose highly demanding requirements to 5G-COMPLETE, such as:

Object detection, classification and smart tracking; the list of objects (e.g., vehicles, humans) to be detected/tracked to be customized by the end-user

Multiple cameras' synchronization, considering that a camera's movement could be triggered not only by motion/object detection events, but also by external events e.g., by a "signal" sent by an activity detector; especially, in case of mass deployment of the solution.

Such capabilities are falling into the focus of the 5G-COMPLETE framework because they necessitate the deployment/utilization of distributed compute resources and edge processing capabilities to support ultra-low latency (for smart tracking), flexibility/scalability in deployment and network/compute resources' allocation, virtualized transport network resources from multiple VISPs that are provisioned on demand, to achieve fast response times as well as high levels of reliability and availability, guaranteed QoS, enhanced security, along with an increasing set of smart capabilities. Non-real time "services" such as camera snapshots, camera content visualization, statistics extraction, camera configuration, alerting, voice announcements, etc., could be performed at the backend.

2.9.2.2 Source

Text included in subsections related to the 5G COMPLETE is copied from one or more documents that can be found via the following links:

https://5gcomplete.eu/wp-content/uploads/2023/05/D2_2.pdf (Page 50)

2.9.2.3 Roles and Actors

(Vertical) Service Customers, Service Providers (CSP, DSP, NSaaS Provider), VISP Aggregators.

2.9.2.4 Pre-conditions

Current status, Problem statement limitations of today's situation.

2.9.2.5 Triggers

Currently, commercial surveillance/physical security solutions are mainly based on closed platforms, (to support live streaming, video/snapshots storage, line/area crossing, remote configuration, cloud storage, etc.), followed by limitations/restrictions, such as the following: local processing (camera or site-level), limited flexibility in service provisioning, network and compute resources availability, expandability both in terms of number of cameras and HW/SW upgrades, maintenance and support overhead, utilization of own storage/cloud infrastructure for security reasons, camera specific service quality and reliability.

2.9.2.6 Normal Flow

5G-COMPLETE aims to deliver a paradigm for the support of aforementioned capabilities/scenarios and to demonstrate the lifecycle management of an advanced surveillance/ physical security service over:

A multi-domain deployment consisting of distinct Edge and Cloud compute domains providing:

Advanced Security at Edge Cloud deployment (e.g. trusted boot and secure execution for Workloads) addressing the user requirement for high security.

Diversification in terms of resources selection and capabilities, by exposing HA functions for the Advanced Surveillance/ Physical Security Services Workloads that need low processing delay and low end-to-end network latency.

A 5G FWA domain providing:

High availability and resilience through mesh architectures.

High capacity and low latency.

An orchestration layer capable of:

Collecting and processing the topology, the capabilities and characteristics of the multiple compute domains to higher Network Operation/ Digital Service provisioning layers.

(Co-)Provisioning the transport network resources, on-demand with specific QoS. characteristics reflecting the "Slice" requirements and taking into consideration the actual placement of services' components that have to be interconnected.

Performing service lifecycle management across the multiple roles and provisioning layers.

2.9.2.7 Alternative Flow

2.9.2.8 Post-conditions

2.9.2.9 High Level Illustration

The 5G-COMPLETE network deployment that will support this UC is shown in the following architectural diagram.

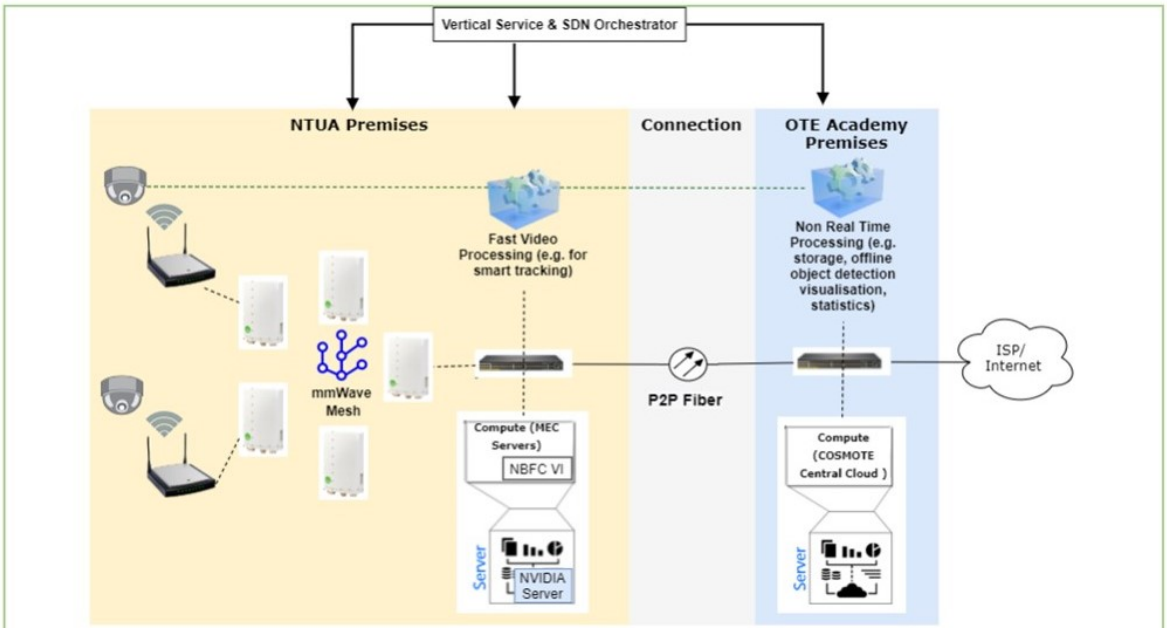


Figure 40: UC#4 - Demo Deployment (NTUA/COSMOTE Facilities)

In the context of this UC, Slicing is considered at end-to-end Vertical Application layer which includes the transport network part as well as the virtualized compute resources provisioning for the specific service deployment. Slicing is required in order to preserve isolation between services delivered to Service Customers (e.g., object tracking, object classification, camera movement upon object detection), and to maintain the QoS guarantees (e.g. latency, bandwidth).

Slicing information is provided by the Service Customer and captured at the Digital Service Provider level through suitable templates. Regarding the templates, the end-to-end Network Slice description and its requirements are formalized in the Network Slice template, following the 3GPP specification. According to the 3GPP Network Slice Network Resource Model, the end-to-end Network Slice is composed of different subnets and each of them can target a technology-specific domain. Un this specific case, we consider the Vertical Services and the transport network NSS, containing the related information in terms of requirements and subnets components.

2.9.2.10 Potential Requirements

Table 18: Enhanced Security

VU-OTH-20	Enhanced Security
Priority	Essential
Description	Enhanced security is required at the distributed pools of compute resources in order to ensure that the application components and software/data repositories are not compromised by malicious parties.
Success Criteria	Success Criteria: • Security is ensured at compute resources domain.
Use Case	UC#4

Table 19: High availability of Vertical Service

VU-OTH-21	High Availability of Vertical Service
Priority	Essential
Description	High Availability of the Vertical Service is needed.
Success Criteria	Success Criteria: • Ensuring 99.99%-99.9999%availability for 24x7 monitoring.
Use Case	UC#4

Table 20: Lifecycle management of Vertical Services

VU-PERF-19	Low Processing Delay
Priority	Essential
Description	Low processing latency is needed for specific functionalities (e.g. object detection/classification at high FPS (Frames per Second) from multiple cameras simultaneously).
Success Criteria	Success Criteria: • To simultaneously process all cameras' high FPS stream without delay (with respect to the real-time content).
Use Case	UC#4

2.9.2.11.2 Bandwidth requirements

Table 21: Low delay/latency

VU-PERF-17	Low Delay/Latency
Priority	Essential
Description	Low Delay/Latency is required between the cameras and the processing unit (i.e. MEC), which is critical for the real-time dispatching of object-tracking related commands (to be executed by the camera).
KPIs	KPI: <20ms
Use Case	UC#4

Table 22: High bandwidth

VU-PERF-18	High Bandwidth
Priority	Essential
Description	High Bandwidth is required to provide the capacity needed for a high number of cameras served from a specific FWA node (for live streaming, object tracking, etc.).
KPIs	KPI: > 8 Mbps per camera (depending on cameras' capabilities)
Use Case	UC#4

2.9.2.11.3 URLLC requirements

VU-OTH-21	High Availability of Vertical Service
Priority	Essential
Description	High Availability of the Vertical Service is needed.
Success Criteria	Success Criteria: • Ensuring 99.99%-99.9999%availability for 24x7 monitoring.
Use Case	UC#4

2.10 5G cloud-RAN

2.10.1 Virtualized base station for 5G cloud-RAN

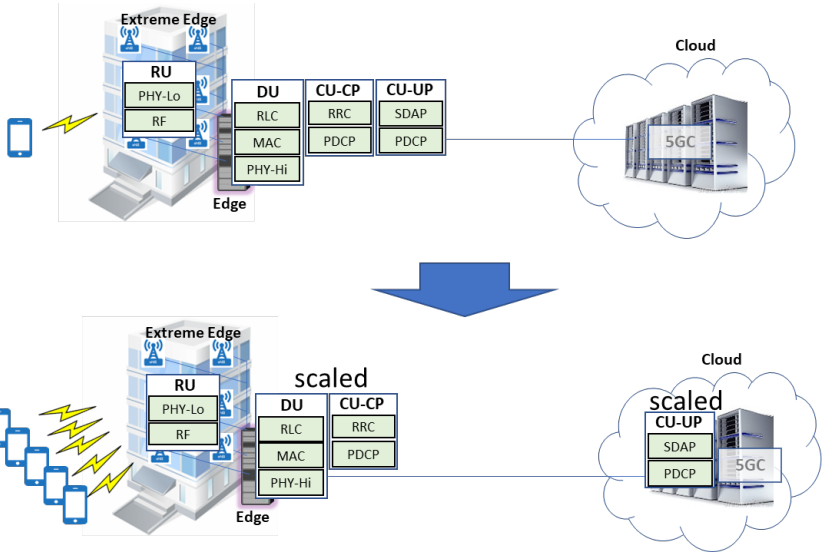
2.10.1.1. Description

The intention of the use case, which is a part of the MORPHEMIC project, is to investigate the intelligent deployment of the 5G cloud-RAN (Radio Access Network) in the multi-cloud environment with the aid of proactive and polymorphic capabilities of the MORPHEMIC, a multi-cloud orchestrator. It will give RAN unprecedented capabilities to seamlessly operate in multiple private and public clouds with ability to scale according to current and future needs. The anticipated benefits for the end customer will include reduction of Total Cost of Ownership (TCO), due to the multicloud deployment, higher availability of the service, due to the predictive analysis of application data as well as programmability of the deployment due to the expressive CAMEL modelling language and inclusion of application data in the deployment decision making.

Potential customers are the entities which desire to build private 4G/5G connectivity on their premises such as smart factories, airports, etc.; nationwide 4G/5G coverage such as Mobile Network Operators (MNO); 5G based solution providers. Customers of the first and second type belong to the communication service providers market. Their main focus concerns a reliable and affordable communication services. Third type of the customer belong to the vertical industries and utilize customization tools to design the target RAN deployment, fitting proprietary business scenarios.

The use case focuses on the scenario where RAN components migrate between Edge (private cloud) and Cloud given the contextual change in the RAN operations. The example shown in the figure below illustrates the case where all RAN components are deployed locally at the Edge while 5GC (5G Core) resides in the Cloud. This scenario is viable for the low user throughput, which due to some simplification can be translated to the low number of users. However, when the number of users increases, the load on CU increases as well.

The need for the scaling CU arises. Since the Edge offers limited resources, it can be necessary to migrate CU (Centralized Unit) (especially CU-UP -user plane) component to the Cloud (given that low latency performance for user applications is not required). The act of scaling access network across different clouds (private and public in this case) is facilitated by the MORPHEMIC platform with the use of mentioned polymorphic and proactive adaptation mechanisms making it seamless.



2.10.1.2. Source

MORPHEMIC H2020 European project

2.10.1.3 Roles and Actors

Telecom operator – integrates cloud-RAN into its 5GS (5G System),

End users – subscribers connecting to RAN (and 5GS) via user equipment or IoT devices,

Mobile equipment manufacturer – the manufacturer of the IoT and mobile phones,

Cloud provider – provider of public and/or private cloud infrastructure on which Cloud-RAN can be deployed,

Cloud-RAN vendor – provider of the cloud-RAN software to be operated by the operator and deployed on cloud infrastructure.

2.10.1.4 Pre-conditions

5G frequency band for the 5G operations must be secured,

Network connectivity between different cloud sites must be ensured.

2.10.1.5 Triggers

The use case is composed of the 'deployment' phase where cloud-RAN is being deployed and becomes operational and 'adaptation' phase where due to some external trigger MORPHEMIC platform adapts the RAN deployment to new conditions. The trigger in our case is the influx of the users which connect to cloud-RAN base station.

2.10.1.6 Normal Flow

Commonly, the steps are the follows:

Cloud-RAN is being modelled in the CAMEL modelling language which can be then processed by MORPHEMIC platform,

Cloud RAN is being deployed at the Edge and becomes operational. This step can be called a 'deployment' phase,

Due to the influx of the users, MORPHEMIC recognizes the need to scale the cloud-RAN,

The ‘adaptation’ phase starts. MORPHEMIC, through the scaling process, is moving CU-UP (Centralized Unit - User Plane) to the available resources in the public cloud as the local resources at the Edge private cloud are already consumed,

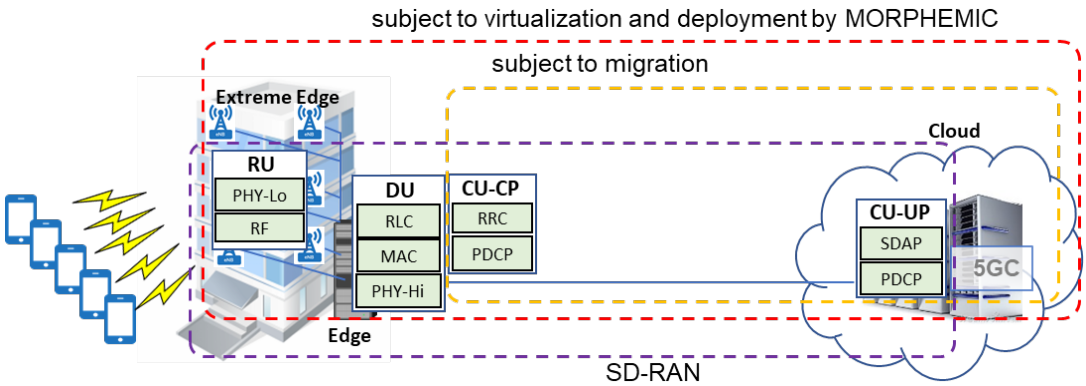
2.10.1.7 Alternative Flow

The alternative flow would be similar to the one described in X.6. however basing on downscaling the solution in case the user departure. In this case, CU-UP component would be moved to the Edge from the cloud location.

2.10.1.8 Post-conditions

The cloud-RAN can serve more users.

2.10.1.9 High Level Illustration



2.10.1.10 Potential Requirements

Functional Requirements

To support modelling of the interconnection dependencies between components,

To not exceed certain communication delay in communication between components,

To not exceed certain response time to the user or other systems.

Non-Functional Requirements.

To have the high availability configuration with redundancy of the components,

To scale resource available for the application up and out at run time,

To support secure functioning of the cloud-RAN components e.g., isolate traffic/communication from other applications, allow secure communication with the component, apply anti-DDoS firewall,

To place some of the components within geographical region e.g., Poland,

To be able to optimize cost during the deployment and redeployment.

2.10.1.11 Radio Specific requirements

2.10.1.11.1 Radio Coverage

Radio cell range

Specification of expected maximum and typical radio ranges (indicate if LOS/NoLOS)

The use case is going to be performed in the lab environment as a proof of concept (PoC). For this reason the expected radio range is about 10 meter.

Does the radio link crosses public spaces? Or is it constrained to indoor or customer premises?

Radio link is constrained to indoor (lab) premise.

Is Multicell required?

Multicell is not required.

Is handover required? Seamless? Tolerable impact in delay and jitter?

Mobility: maximum relative speed of UE/FP peers

Mobility of the end user is not required.

Special coverage needs: i.e. maritime, aerial

No special coverage is needed.

2.10.1.11.2 Bandwidth requirements

Peak data rate 57 Mbps.

Average data rate 50 Mbps.

Is traffic packet mode or circuit mode?

The traffic is packet mode.

If circuit mode, is isochronicity required?

2.10.1.11.3 URLLC requirements

Required Latency

50 ms one way for Control Plane.

50 ms one way for User Plane.

Required Reliability

Achieving high reliability is important however not key for this use case.

Maximum tolerable jitter 100ms

2.10.1.11.4 Radio regimens requirements

Desired and acceptable radio regimens

Desired and acceptable radio regiments is licensed- specific license for testing purposes acquired from the national regulator.

2.10.1.11.5 Other requirements

UE power consumption

Rechargeable or primary battery?

Mobile phone with rechargeable battery is used.

Acceptable battery life

Acceptable battery life span should support related lab tests including data transmission before and after the RAN redeployment. It is estimated to be around 1h.

Is terminal location required? location accuracy?

No.

2.11 Preliminary 6G use cases

2.11.1 Hexa-X 6G based Use cases

Disclaimer: The text Included in this section is copied from "Deliverable D1.2 Expanded 6G vision, use cases and societal values", EC H2020 Hexa-X, 30-04-2021, see URL (retrieved on 27 March 2023)

2.11.1.1 Description

Hexa-X describes several families of 6G based use cases, see the summary in **Figure 41.** More details are described below.

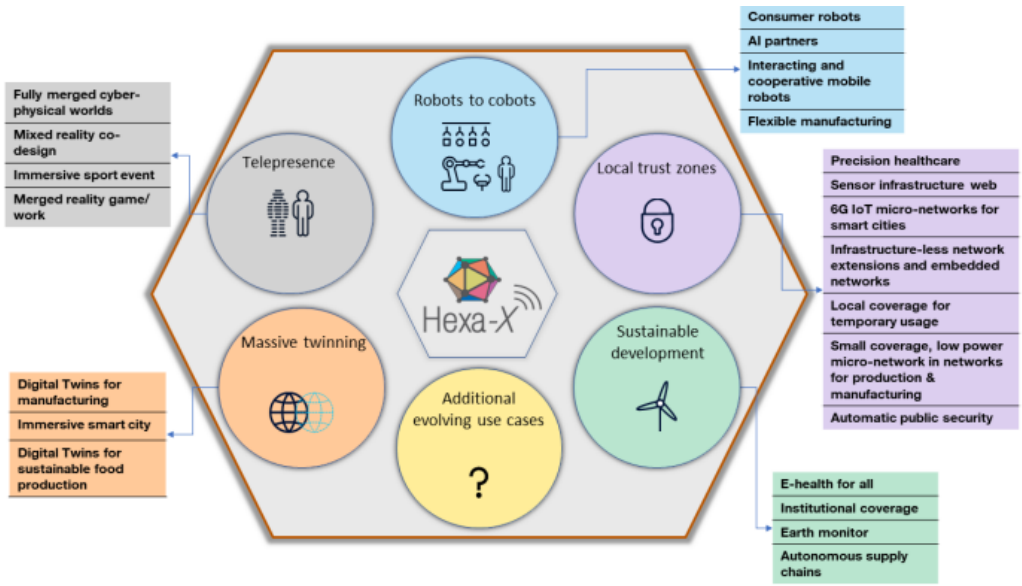


Figure 41: Summary of Hexa-X use case families and use case, source: EC

2.11.1.1.1. Sustainable development 6G use case family

The development of the 6G system heralds applications that go far beyond the user- and vertical-centric applications of current and former generations. Sustainability is explicably the foremost research challenge addressed by this use case family, both in terms of environmental sustainability as well as sustainable development of human societies.

The use cases that are belonging to this Hexa-X use case family are:

E-health for all

We face a number of health challenges today, some of the most important ones to save lives are addressed in UN SDG #3 – "ensure healthy lives & promote wellbeing for all".

However, the demographic, economic and environmental development expected on a global scale the coming decade will add and emphasize additional challenges to address, while technology development will increase expectations. The associated targets of UN SDG #3 aim to ensuring access to reproductive & universal healthcare, reduce maternal & child mortality, end epidemics such as acquired immunodeficiency syndrome (AIDS), tuberculosis, malaria and other preventable diseases (for example water borne parasites) as well as reduce death and illness caused by drug abuse, traffic, and pollution and to promote mental health.

Institutional coverage

The ultimate goal must be to include all communities with high-grade wireless services – this is true digital inclusion for networks. A more realistic goal is perhaps to make sure that schools, hospitals, etc. around the world can have access to full 6G services, even in developing countries and remote rural areas of developed countries.

This goes far beyond video services and includes immersive and precise communication such as telepresence, remote virtual education and medicine. In many areas, deployment of fiber communication may be cost prohibitive, for example, due to long distances in remote areas or islands, or because of inaccessible areas due to political instabilities.

Autonomous supply chains

To ensure a fully integrated autonomous supply chain, the demand of scoping, ordering, sourcing, packaging, routing and delivery must be automated using local and central AI agents continuously optimizing the process, for example, in relation to unexpected events such as natural events, disasters or political circumstances. 6G will enable fully automated supply chain, at reasonable cost and complexity. With global end-to-end lifecycle tracking of goods from production, shipping, distribution, usage and recycling, a higher resource efficiency and reduced material and energy consumption can be achieved. The use of 6G-connected micro tags on goods can simplify tracking, customs, safety checks, and bookkeeping, allowing it to be done without manual interference.

2.11.1.1.2 Massive twinning 6G use case family

Massive twinning, i.e., the application of the more fundamental Digital Twin (DT) concept in a wide set of use cases, will gain importance. Massive twinning is designed to lead us towards a full digital representation of our environment, extending the use in production/manufacturing (as it has started today), but also, for example, in the management of our environment, in transportation, logistics, entertainment, social interactions, digital health, defence and public safety.

Digital Twins for manufacturing

The use of DTs will continue to grow in industrial/production environments, leading to Massive Twinnning. It will enable us to go beyond the current levels of agility of production, enabling more efficient interaction of production means to encompass a larger extent of the respective processes, and also to achieve the transfer of massive volumes of data, and, often, extreme performance and reliability.

In the realm of production and logistics, DTs can be used for many beneficial applications. For instance, the following sub-cases can be identified:

Managing infrastructure resources.

New products need to be designed and automatically be linked to their DT

The cooperation among multiple DTs in a flexible production process will also be needed, as it ensures anomalies in the real world are detected and mitigated through reconfigurations of the communication system or dynamic adaptations of the production process, or a combination of both.

Another practical usage of digital representations is to follow the history through "digital threads": the history of every part of the system can be used to learn, to replace parts, etc.

Immersive smart city

City liveability is a concept that is determined by large parameter sets, which are weighted. The sets correspond to wide application areas, relevant to the city infrastructure (for example, roads, rails, buildings, networks), the ambience/environment (for example, climate, air quality), healthcare aspects (for example, management of health system, quantified self), education and culture issues, the stability/safety, and many others. The effective management of all these factors, on various time scales, opens technical challenges, potential from a societal perspective, and business opportunities. Technical challenges are associated with aspects related to the volume of traffic that needs to be transferred, the associated time scales and reliability, etc. Societal value lies in the potential of perceiving, predicting and managing hazards or other less critical situations. Business opportunities occur for operators and other ICT players, by assisting cities in the accomplishment of their goals.

Digital Twins for sustainable food production

One of the UN SDGs is to end hunger, to achieve food security, while maximizing the sustainability of the production. Massive twinning is a valuable concept in this direction, especially, in the light of the challenges for mankind in our time, for example, higher populations, climate aspects, and need for enhanced efficiencies. The main challenge is that "remote", "rural", "in-sea, close to shore" areas need to be provided with higher network capacity and performance than today. This is essential for monitoring in real time the conditions at the level of micro-locations (microclimate, soil conditions), inspecting and developing optimized and targeted plant treatments (including disease combatting), experimenting with various actions or strategies (for example, removal of plants, alternate cultivations, spraying strategies), or enforcing actions, including the control of semi-autonomous ground robots. Human expert knowledge will benefit from the closely synchronized digital representation of the physical world, not only for inspecting, but also for experimenting with actions in the digital realm, and, ultimately, impacting the physical world. Therefore, in this use case, the fully synchronized digital representation is the key to optimize agricultural production through improved management and prevention of threats.

2.11.1.1.3 Immersive telepresence for enhanced interactions 6G use case family

This use case family consists in being present and interacting anytime anywhere, using all senses if so desired. It enables humans to interact with each other and with the other two worlds, and physical and digital things in these worlds.

Fully merged cyber-physical worlds

Mixed Reality (MR) and holographic telepresence will become the norm for both work and social interaction. Via holographic telepresence it will be possible to make it appear as though one is in a certain location while really being in a different location – for example, appearing to be in the office while actually being in the car. Other example use cases include facilitating collaboration and performing remote home-working beyond office type of work by white-collar workers, improving diagnosis during tele-consultations and enhancing teacher-student interactions in eLearning classes. This can also mean virtual traveling to far-away places and telepresence meetings with friends and family. The user would experience the world where his/her hologram is, through very rich sensing of multiple sorts, synchronized to devices on his/her body for an enhanced sensory experience.

Mixed reality co-design

Mixed reality co-design means remote collaboration and "experience before prototyping". This may for example apply to a factory scenario where two people are remotely designing something intricate together with some physical objects and some virtual objects. A MR reality co-design system will allow designers to cooperatively design innovative virtual products in a virtual-real fusion of worlds.

Context awareness as an integral part of the MR codesign process will allow designers to focus on the design itself and its relationship with the external environment. MR co-design will link into new forms of man-machine interaction such as capturing the designer's head or eye movement, emotional state, facial expressions, and body parameters such as heart rate or blood pressure. Such an approach can be subsumed under the term "spatial computing". Moreover, the co-design context can be captured by spatial mapping and imaging technology.

Immersive sport event

Current sport simulators utilize motion capture technology to create life-like renderings of real players. With the advent of XR gaming, this will be further expanded to allow 3D rendering of any simulated sports event. With 6G, it will be possible to motion capture actual games in real time to create a DT of the whole game, which can be experienced live from any angle, by hundreds of millions of people worldwide. The majority of viewers would likely be satisfied with a classical overview, determined by professional camera operators and thus, the bulk of the information can be broadcasted single-to-multipoint.

However, the 3D rendering also allows end users to experience the game from any angle with a 360° view, for example, following a specific player, or watching the game from the ball's point of view. In these cases, the processing would have to take place locally to allow high fidelity rendering of the interesting field of view. AI models could also assist in predicting the near-future motion of the players merging real-time footage with pre-rendered models. The experience could be to watch the game from a virtual bleacher while interacting virtually with your friend while watching the game.

Merged reality game/work

Gaming in a public or in a dedicated space is experiencing a shared merged reality with a massive amount of people where the distinction between reality and virtuality has been blurred. Some objects or other players in the game are present in the physical world, others are digitally enhanced with visual, haptic or olfactory sensation while yet others are fully digital but appear to be real. Players in the same game share a common merged experience and exchange synchronized sensory information that is authentic or synthetic. Digital meetings can take place where the user participate with a hologram avatar of himself/herself, making him/her appear fully present. Tactile and sensory feedback can be delivered to participants, and visual information is immersively experienced through a smart contact lens, for example. Digital co-creation is easily handled in the virtual domain, simplifying remote work and training.

2.11.1.1.4 From robots to cobots 6G use case family

The 6G system provides the technical fabric to go beyond pure command-and-control of individual robots. Instead, it empowers robots to become "cobots" in that they form symbiotic relations among each other to fulfil complex tasks efficiently or better cater to the needs and demands of humans in day-to-day interactions. Trustworthiness and digital inclusion are core values in human-machine and machine-machine interaction. By collaborating and building symbiotic relations, complex tasks can be fulfilled in a sustainable fashion: rather than devising more and more complex machinery and allocating more and more resources, intelligent and flexible utilization of existing capabilities to the benefit of society is at the core of this use case family. This also enables new business models for verticals: with increased flexibility in production and resource utilization and connected intelligence, machinery can perform highly individualized on-demand tasks, enabling lot size one production and fully utilizing novel production methods such as additive manufacturing. A number of research challenges are targeted with this use case family. Trustworthiness is at the core, especially as use cases in this family depend on connecting intelligence and coming to joint decisions.

Consumer robots

Numerous consumer robots will go beyond the automated vacuum cleaners and lawn mowers that we know today and become an essential part of future living. These may take the form of a swarm of smaller robots that work together to accomplish tasks or autonomous robots that provide convenience. Enabled by 6G, the robots will be, for example, equipped with video cameras streaming to a local compute server for real-time processing as well as equipped with advanced sensing and positioning features for seamless and intuitive interactions among users, robots and environment. Robots will utilize the connected AI capabilities offered by 6G for situation-aware cooperation and collaboration and assistance. Thus, we will see an increase in the number of devices and higher capacity requirements within our home networks, further demanding seamless connectivity across the resulting network of (local) networks. In the big picture, domestic robots will enable the elderly to stay in the comfort of their homes for longer and improve their quality of life.

AI partners

With the advances in AI and its embedding into 6G systems, AI agents will become more prevalent and ingrained in society, alleviating more and more tasks from humans. However, many tasks will still involve human operators actively interacting with AI partners to jointly solve tasks, not only the AI assisting the human operator, but the AI and human working as equal partners. Instead of relying on dedicated machines or specific autonomous system, the AI agent can be much more general-purpose and act as a partner which autonomously and adaptively

interacts with other agents (humans/machines), by interpreting intents and surroundings, performing challenging and risky tasks. This AI agent could be a simple stationary machine in a factory, software controlling the illumination wherever you are by communicating with other AI agents in the vicinity, either in your home, in the office, or in a public space, or it could be a group of drones autonomously collaborating to solve various tasks.

Interacting and cooperative mobile robots

In consumer-oriented use cases with multiple robots as introduced above, machines need to identify others, connect, exchange intent and negotiate action through automated communication. Examples of where robots need to coordinate with each other are, for example, awareness such that your personal butler doesn't step on your robot vacuum cleaner; in construction/building scenarios where different robots need to sync/coordinate their movements of lifting, etc.; Automated Guided Vehicles (AGVs) outdoors that need to avoid collisions; swarms of simpler robots coordinating among themselves to perform tasks through emergent action. In industrial environments, going beyond flexible modular production cells (i.e., specific areas where mobile robots and machines collaborate on a production task), some production tasks can be conducted by collaboration among mobile machinery, for example, robots collaboratively carrying some goods while being mounted on AGVs. This coordination will be conducted in three dimensions, to avoid collision and enable collaboration of robots evolving in the air, such as drones. In this use case, in addition to the coordination among the interacting entities, process data among involved entities needs to be exchanged, meeting real-time requirements and requiring synchronization: with (static) machinery when departing from a modular flexible production cell among collaborating machines while on the move, and when reaching the target production cell for the next process steps. Reliability, functional safety, latency and positioning requirements as well as high-energy performance need to be met during all steps and even if trajectories are blocked or need to be altered.

Flexible manufacturing

With increasing personalization and modularization of production (for example, lot size one production of a single, highly customized product) and flexibility of manufacturing systems (for example, mobile robots) comes the need for powerful wireless communication and localization services as well as flexible, dynamic configuration of communication services in the network.

The machinery and associated communication will be configured dynamically for each production task, either by a production system or even in a self-organizing way by direct collaboration among (mobile) production machines. This involves the orchestration of AGVs, as higher flexibility in the production process requires higher flexibility in logistics. Dynamic configuration of real-time communication services is required, potentially initiated by end systems themselves and executed in a distributed fashion. Respective communication resources and capabilities (for example, local compute, D2D communication, frequency ranges) need to be assigned through a flexible framework. High availability and functional safety requirements need to be met, and data from the production process needs to stay secure and private. This use case extends existing industrial 5G functionality in more dense industrial environments with higher flexibility, self-organization capabilities, local processing and direct communication among entities.

2.11.1.1.5 Local trust zones for human & machine 6G use case family

"Mobile" communications are up to today often "cellular" communications. Many use cases, however, require local or private communication capabilities for very sensitive information that are tightly integrated in wide-area networks. Here, network topologies beyond cellular topologies and security concepts beyond classical security architectures are required. Local trust zones protecting individual or machine specific information and independent sub-networks such as body area networks enabling advanced medical diagnosis and therapy or on-board networks of AGVs have to be dynamically and transparently integrated in wide area networks, or remain on-premises as private networks, as needed. The work towards research challenges "Connecting Intelligence", "Network of Networks", and "Trustworthiness" will contribute to building communication solutions for these use cases.

Precision healthcare

Today`s medicine typically follows a one-size-fits-all approach, in which disease treatment and prevention strategies are developed for the average person. In contrast to this, precision medicine is "an emerging approach for disease treatment and prevention that takes into account individual variability in genes, environment, and lifestyle for each person," according to the Precision Medicine Initiative. In order to understand the environment and lifestyle of persons, 24/7 monitoring of vital parameters for both the healthy and the sick through numerous wearable devices will be useful. Persons interested in their personal analytics, or "quantified self", will be able to perform self-tracking and monitoring thanks to in-body devices.

Sensor infrastructure web

A simple autonomous vehicle (with no or limited sensor capabilities) is moving around the environment, while relying on external third-party sensors as if they were on-board sensors. The vehicle obtains external data from externally available sensors, or navigation commands through the network with utmost confidence in the reliability, timeliness and confidentiality of the data, and can as well share its own sensor data. This allows aggregation of sensor data across different systems, even to devices lacking their own sensor capabilities. The network can advertise locally relevant and trusted sensor information that all connected devices, for example, vehicles, can access. 3GPP today does not allow diffusion or sharing of sensor data in predefined local environments and to networks or network parts under external security management. Depending on the implementation, this use case might require the split of network ownership, network control, network transport and network security. Finally, today it is not possible to allow a network to advertise and distribute third-party provided sensor data in well-defined local areas.

6G IoT micro-networks for smart cities

The expansion of smart cities usages (for example, energy management, traffic control, citizen safety) will entail massive deployment of communicating objects. Administrators of smart cities want to deliver the required coverage for smart city networks with minimized energy consumption and without multiplying base stations. They need self-adaptive networks, relying on objects as relays.

These micro networks would manage the flows of information from objects, robots, etc, locally interacting in a complex system. Network slices and private networks bringing their own network nodes exist in 5G. Here, micro networks of potential different ownership and with a potentially external security management might share parts of the infrastructure with wide area networks, i.e., a private network with partly owned infrastructure and a private trust policy is integrated in a public network.

Infrastructure-less network extensions and embedded networks

At the edge of network coverage, a temporary network coverage extension is required, for example, for providing connectivity between several agriculture vehicles during harvesting campaigns. The connectivity should remain even when the vehicle platoon is leaving the network coverage completely while still in the harvesting campaign. An industrial vehicle manufacturer has a fleet of its shop-floor vehicles deployed in a factory. While all or some of them are connected to the wide area network, the manufacturer wants to have reliable networking solutions between his vehicles not using the local network, i.e., a local private infrastructure-less network being established. This network might have authorized access to the spectrum of a local non-public network or a public network, thus external network control should be enabled. D2D solutions exist in LTE and 5G. Direct Mode Operation (DMO) is a typical requirement for Public Protection and Disaster Relief (PPDR). Construction work, agriculture, and tactical services — often operating at the edge of network coverage — regularly ask for coverage extending concepts beyond D2D and autonomous operation of island solutions. Mesh networks, multi-D2D might be options. Temporary, ad-hoc security solution deployments are required. Networking islands of several devices re-joining the cellular networks shall be seamlessly reintegrated. D2D could be seen as a first step, and DMO solutions are known from several standards.

Local coverage for temporary usage

PPDR and Program Making and Special Events (PMSE), roadwork and harvesting campaigns benefit from applications as massive video transmissions that often require local networking coverage fulfilling high requirements. When cellular coverage is insufficient or unavailable, local, semi-permanent, temporary, or moving network nodes enabled e.g. mounted on vehicles, drones, high altitude platforms or other means can be used. Automated licencing processes can help to guarantee access to the required spectrum resources. Today temporary deployments for PPDR and PMSE are already used. However, lowering the costs of the deployment and the administrative burden, for example, by automated licencing, might help this option to become more widely used.

Small coverage, low power micro-network in networks for production & manufacturing

A machine manufacturer wants to mutually connect a large population of sensors in his machine using – for reliability reasons – non-Industrial, Scientific and Medical spectrum. This can be done with very low-power devices and very limited coverage as an underlay network, potentially with one of the sensors getting the authorization out of the public or non-public network of which the spectrum is used. This could be seen as a shared spectrum access concept under full control of the incumbent. The incumbent might have the option to disable the spectrum usage by signalling.

Automatic public security

There will be a massive deployment of wireless cameras as sensors. With advances in AI and machine vision and their capacity to recognize people and objects (or more generally, automatically gather information from images and videos), the camera will become a universal sensor that can be used everywhere. Privacy concerns will be addressed by limiting access to data and anonymizing information. Also, radio and other sensing modalities like acoustics will be used to gather information on the environment. In short, advanced techniques will be used in security screening procedures to eliminate security lines.

A combination of various sensing modalities will be used to screen people as they move through crowded areas rather than only at entrances. Radio sensing will be an essential component of achieving this; supported by the communication systems of the future the network can sense the environment. For example, it could be programmed to automatically detect metallic objects of certain kinds that people or robots may be carrying in a crowded square. The network can sense and identify potential threats.

2.11.1.1.6 Enabling services harnessing new capabilities 6G use case family

In the initial collection of use cases, some ideas have emerged, that may not be categorized as use cases according to the definition above, but that deserve to be shared to the 6G ecosystem. They can be considered as services useful to address the use cases proposed above and, possibly additional ones. This set of novel services will develop 6G beyond the data pipe, leading to a convergence of communication, computing, data and sensing, including Artificial Intelligence.

Compute-as-a-Service (CaaS)

CaaS can be applied for storage and processing of large sensory data in an industrial environment to address specific needs, such as: (i) production process customization involving, e.g., AGV trajectory planning and moving/ static robot coordination; (ii) enhancement of production process dependability e.g., by guaranteeing full synchronicity of actions and reactions in the system. This service is aimed to be used by any devices (static or mobile, IoT, handhelds, etc.) or network infrastructure equipment that choose to delegate demanding, resource-intensive processing tasks to other parts of the network providing more powerful compute nodes, which are also of higher availability at the time of workload generation; these service-offering compute nodes can be either onboard other devices or, for example, edge cloud servers at the infrastructure side. A first example is the one of a worker performing equipment maintenance.

The worker uses special equipment (glasses, gloves, vests, etc.) useful to capture information (for example, video footage, images, sensory information) of the process. The respective workload for data fusion, sensor data processing, etc. needs to be processed in a reliable and timely fashion; however, the computational/ memory/ storage resources of the special equipment are limited. As an alternative, instead of a human, any kind of small robot (for example, AGV, unmanned aerial vehicle) of limited energy, storage and computational resources can play the role of the maintenance entity. Workload delegation to powerful nodes at the network will be essential for the stability of a closed loop system involving measurement capturing, processing, issuing an actuation policy and implementing it.

AI-as-a-Service (AIaaS)

AIaaS can be applied for intend classification and prediction in human-to-human and human-to-machine interactions, based on criteria/ features, such as: gesture, intonation, expressions, surrounding sounds, touching objects etc. This service can be consumed by applications instantiated at either user and IoT devices, or at network infrastructure submitting requests for ML-based inferencing decisions to the network (for example, to other devices or to edge cloud hosts with already trained models). A first example relates to inclusiveness of the elderly and people with motion/vision impairments, in which, for example, a person with vision impairments is equipped with wearables including sensors collecting environmental/ surroundings data. These sensory data are exploited to infer and identify objects, street furniture and possible hazards so that the user can be informed in advance and take proactive measures. Such environmental identification via object classification is useful to improve the inclusiveness and quality of life per the UN SDGs.

AI-assisted Vehicle-to-Everything (V2X)

Safety and security are of high importance for any transport system, especially road transport due to the prevalence of accidents. Several initiatives have been conducted to promote rules, technical standards and awareness campaigns to decrease the number of fatalities caused by road accidents. Moreover, studies and trials proved that AI can be exploited for making roads safer. This motivates the need to further explore the potentiality of the AI algorithms for enhanced automotive services provided by future 6G networks. The novel AI algorithms, applied to the big data collection gathered by sensors (in and outside of the cars) as well as radio stations in the operators' networks, will allow dynamic shaping, monitoring and suggesting actions/recommendations to connected vehicles' drivers — or, potentially, to directly control the automated vehicles in order to reduce the traffic caused by them. This will have an important societal impact allowing a safety improvement for drivers and passengers as well as minimizing traffic congestion. With respect to C-V2X technologies already developed and based on LTE and NR, the processing of the massive amount of data gathered through the automotive services offered by communications networks is far to be managed properly and this creates room for the introduction of AI-based algorithms to dynamically control and shape the traffic, generating a digital replica of the real traffic scenario. The real-time creation and adaptation of such digital replica encompassing an entire urban area is very challenging and requires network capabilities not currently available; in addition, the intertwining of digital and physical worlds, as foreseen in Hexa-X, will improve not only safety but also the mobility's sustainability in a human-centric fashion. Latency and location accuracy are essential for these AI algorithms in order to control real-time-like the type, the evolution and the shaping of the traffic in large scenarios like today's cities.

Flexible device type change service

The service may need to be consumed when robots or humans enter or leave a specific group of collaborating entities that act on a common task. In this case, the respective communication entity needs to adapt to the communication requirements within the respective group, potentially differing from previous device configurations. This service will enable devices to effectively and flexibly change their device type, for example, from a consumer device (like today's smartphone) to an industrial IoT device to a V2X device. As an exemplary user scenario, we consider the case that a user owns a consumer device (such as today's smartphone) that is typically used for voice/data communication in a non-safety-related context.

When the user is entering an area where V2X communication is being used (for example, on a road, on a side-walk close to a road), the user device changes its purpose (and, therefore, its type) and will enable safety-related communication; a Vulnerable Road User (VRU), such as a pedestrian, will be warned in case of danger, a vehicle will have access to Vehicle-to-Network (V2N) services through the smartphone, etc. Another example could be an industrial robot toggling between critical and non-critical actions, such as switching from welding, requiring very high localization accuracy and low latencies, to long-range movement only requiring moderate localization accuracy and latencies. This requires that a device can flexibly change its type and configuration depending on the currently active service needs. Sensing capabilities will be an advantage to predict the need for such change and appropriate timing. This service is mainly relevant to the Network of Networks and Trustworthiness research challenges.

Energy-optimized services

Users want to be given the choice of consuming "green" ICT services, with reduced environmental impact with respect to traditional services, in a holistic manner, considering not only the applications, material, etc. but also the technology and the E2E network design. As environmentally friendly users, they will be invited to consider possible trade-offs between performance, cost and environmental impact, enabling them to monitor the overall environmental impact of their products/services. Such services aim to mainly address the Sustainability and Global Service Coverage research challenges.

This service considers the energy consumption end-to-end, considering the environmental impact of all the elements involved in the service: application, network, terminal, etc. These energy optimized services will require not only energy-optimized networks, but also energy-optimized applications, appropriate upcycling of materials, etc. Providing a holistic view will require new indicators of the environmental impact and an aggregation of these indicators to reach a global view.

Internet-of-Tags

Tags will be present everywhere to facilitate everyday life. The tags will enable multiple operations: collecting information through tracking of label-tags and monitoring and acting on the environment through smarter tags, with sensing or actuating capabilities in addition to communication capabilities. For instance, tracking merchandise with basic label-tags can improve logistics; tags capable of sensing temperature/light, etc. can be monitored to optimize energy consumption for heating/lighting, etc.; tags that are activated with the manual pressure of a button can be used to switch on/off light or heating. To limit the impact on the environment, tags will not be powered but will rely on energy harvesting to enable communication between tags or between tags and network, sensing, actuating, processing of the data collected. Energy harvesting will be performed through re-using ambient or renewable energy, for example, using surrounding (already existing) or dedicated RF waves, solar energy, wind, vibration, mechanical push. Finally, "zero-environmental-cost" tags can be considered, utilizing for example printed electronics to enable ubiquitous tags, while still ensuring sustainable handling at end-of-life of tags (e.g., biodegradable). This service generalizes and extends the use of tags and the concept of energy harvesting, relying on multiple possible sources (RF waves, solar, …), going into massive deployment. It also includes communications of the tags with the network and will enable monitoring and controlling the environment.

Security as a service for other networks

Any kind of connected device will become able to establish trusted local connections, request and verify the on-demand deployment of security functions and assess the security of the end-to-end path by the composition of trusted segments. Local access provider collaborates with other network, security and application providers by means of dynamic trust links, always verifiable by end users.

2.11.1.2 Source

H2020 Hexa-X "A flagship for B5G/6G vision and intelligent fabric of technology enablers connecting human, physical, and digital worlds"

2.11.1.3 Roles and Actors

In addition to **telecom operators** and **end users** all possible actors that represent the **vertical industry domains** are involved. More details required for the implementation of each use case.

2.11.1.4 Pre-conditions

Key pre-conditions require the availability of 6G connectivity and the required network connectivity. More details required for the implementation of each use case.

2.11.1.5 Triggers

Triggers are diverse depending on the use case family and use case considerations. More details required for the implementation of each use case.

2.11.1.6 Normal Flow

More details required for the implementation of each use case.

2.11.1.7 Alternative Flow

More details required for the implementation of each use case.

2.11.1.8 Post-conditions

More details required for the implementation of each use case.

2.11.1.9 High Level Illustration

More details required for the implementation of each use case.

2.11.1.10 Potential Requirements

Figure 42 illustrates the key value areas as stated in the Hexa-X vision and associated KPIs and capabilities. Each key value area reflects multifaceted aspects for which KVIs need to be developed. The key values are sustainability, inclusiveness and trustworthiness, where sustainability is explicitly considered from two perspectives in Hexa-X. 6G in itself needs to be sustainable, which could, for example, be mapped to the network energy efficiency as a KPI. In addition, 6G is an enabler for sustainability and sustainable growth in other markets and value chains, potentially covering aspects of inclusiveness and trustworthiness. Trustworthiness as another core value for Hexa-X, in the context of security considerations for 6G. In addition, the value of new capabilities enabled with 6G needs to be captured; this includes integrated sensing, embedded devices, local compute integration and integrated intelligence, as illustrated in the lower right. Flexibility is seen as a core capability. As core capability, flexibility covers, for example, the applicability of 6G to a new value chain, including ease of deployment and operation in that environment and, consequently, the goal of enabling new business opportunities. Flexibility as new capability of 6G impacts, for example, AI-based network management and operation.

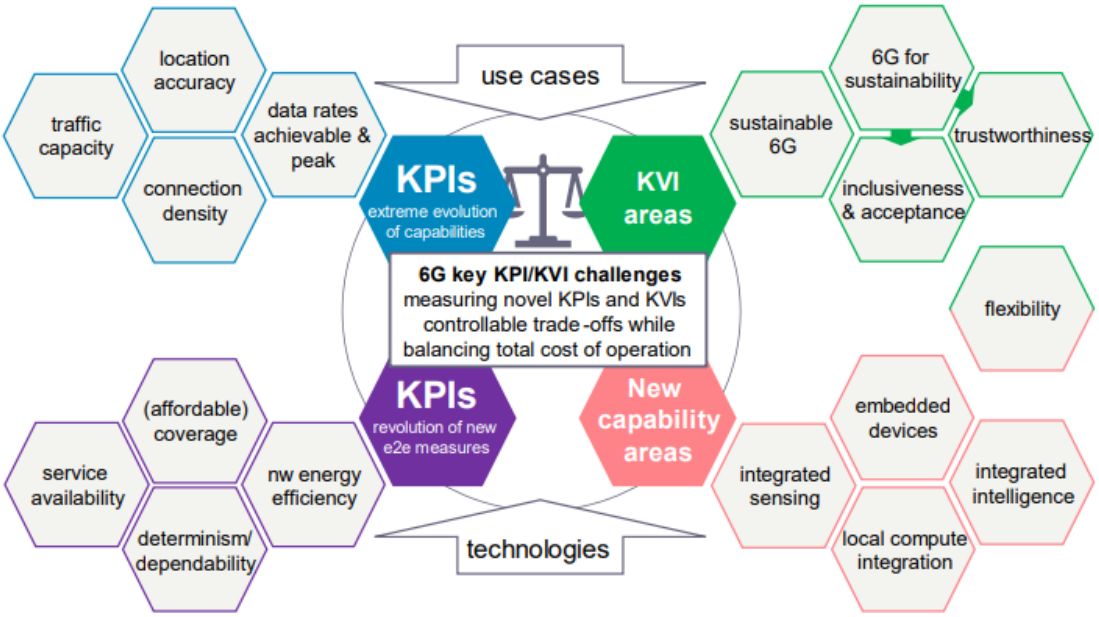


Figure 42: Clustering of Hexa-X Key Performance Indicators s and Key Value Indicators, copied from

In addition to the novel concept of KVIs, KPIs and performance goals need to go beyond what 5G can do to address new use cases discussed in the previous chapter. This includes increasing peak data rates and data rates achievable at the cell edge, density of connections, traffic capacity, and location accuracy to a substantial extent. For some performance goals, for example, dependability and determinism, service availability, affordable coverage, and network energy efficiency, the focus will shift more towards new end-to-end KPIs in specific use cases, and extreme performance in terms of data rates might be confined to specific scenarios rather than being a general, system-wide goal. Depending on the use case, novel KPIs for this end-to-end perspective will be defined. In addition, the relation between the fulfilment of KPIs and the associated total cost of operation becomes increasingly complex, given the number of stakeholders involved and the potential of networked intelligence and service-oriented ownership and business models on a local and global scale.

2.11.2 RISE-6G: Control for RIS-based localisation and sensing

2.11.2.1 Description

The design of 6th Generation (6G) wireless networks points towards flexible connect-and-compute technologies capable to support innovative services and use cases. Targeting the 2030 horizon, 6G networks are poised to pave the way for sustainable human-centered smart societies and vertical industries, such that wireless networks will be transformed into a distributed smart connectivity infrastructure, where new terminal types are embedded in the daily environment. In this context, the RISE-6G project aims at investigating innovative solutions that capitalize on the latest advances in the emerging technology of Reconfigurable Intelligent Surfaces (RISs), which offers dynamic and goal-oriented radio wave propagation control, enabling the concept of the wireless environment as a service.

The project will focus on: i) the realistic modelling of RIS-assisted signal propagation, ii) the investigation of the fundamental limits of RIS-empowered wireless communications and sensing, and iii) the design of efficient algorithms for orchestrating networking RISs, in order to implement intelligent, sustainable, and dynamically programmable wireless environments enabling diverse services that go well beyond the 5G capabilities.

RISE-6G will offer two unprecedented proof-of-concepts for realizing controlled wireless environments in near-future use cases.

2.11.2.2 Source

Text included in subsections related to the RISE-6G is copied from one or more documents that can be found via the following links:

https://rise-6g.eu/Documents/LIVRABLES/RISE-6G_WP5_D5.1_Final.pdf

https://rise-6g.eu/Documents/LIVRABLES/RISE-6G_WP2_D2.5_FINAL.pdf (Page 19)

https://hexa-x.eu/wp-content/uploads/2023/02/RISE-6G-ICT-52-and-Hexa-X-Workshop-on-6G.pdf

2.11.2.3 Roles and Actors

Base station, connected devices, users, networks providers.

2.11.2.4 Pre-conditions

2.11.2.5 Triggers

Challenges for RISE-6G:

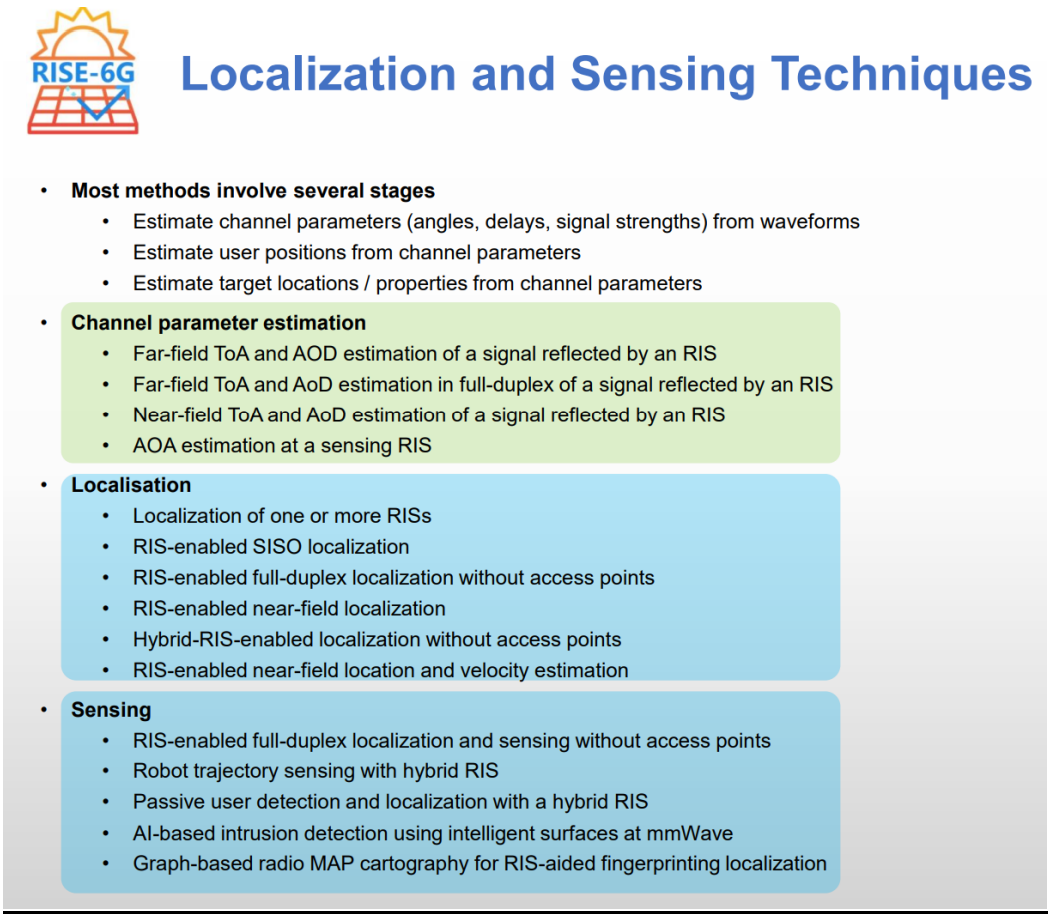
Architectures and different problem variations

RIS control strategies

Methods for localization and sensing

Attainable performance from synthetic and real data

2.11.2.6 Normal Flow



2.11.2.7 Alternative Flow

2.11.2.8 Post-conditions

2.11.2.9 High Level Illustration

As reference, in a general 5G localisation context (i.e., regardless of RIS considerations), [DSM+21], the Location Management Function (LMF) is central into the architecture, as it configures the UE using the long-term evolution (LTE) positioning protocol and must coordinate with the BS. Accordingly, a typical positioning procedure involves additional control overhead, via the Access and Mobility management Function (AMF), between the LMF, the BSs, and the UE, as shown in **Figure 43.**

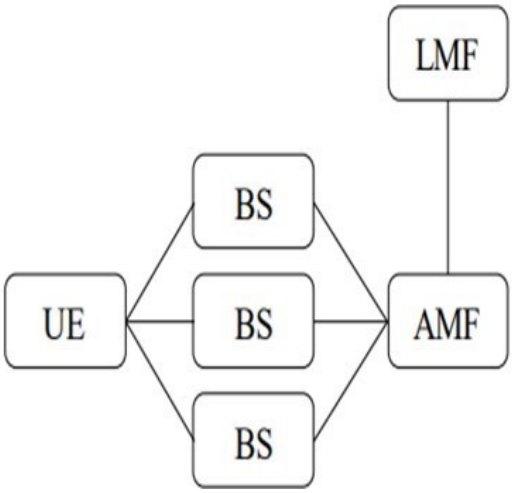


Figure 43: Schematic of 5G positioning architecture, based on (DSM+21), supporting both UL and DL measurements

Beyond, just like in a more general RIS-based communication context, the new RIS-augmented architectures envisioned to support, enable and/or optimize localization and sensing functionalities, must include the necessary components to configure and operate the RIS, namely the RIS orchestrator and the RIS controller. The RIS phase configuration indeed controls the physical radio observations that positioning is based on, and thereby any positioning strategy either requires the explicit control of the RIS configuration or must operate with the knowledge of the RIS configuration in use.

2.11.2.10 Potential Requirements

2.11.2.11 Radio Specific requirements

In the context of radio systems, localisation (synonym: positioning) is the process of determining the 2D or 3D location of a connected device (a user equipment (UE)), based on uplink (UL) or downlink (DL) measurements with respect to several base stations (BSs) [PRL+18]. The measurements are performed based on the reception of dedicated pilot signals and can be of the forms described in

Table 23**.** Observe that a combination of angle and delay measurements can be used for UE localisation and that different measurement combinations put different requirements on both the number of BSs as well as on their mutual synchronisation. For this latter reason, pure ToA measurements with a UE synchronized to a BS is impractical in real scenarios, since even small synchronisation errors lead to large localisation errors (e.g., 10 ns clock error corresponds to 3 meters error). Examples of two different measurement for localisation are shown in **Figure 44.**

Table 23: Localisation measurements and requirements for 3D positioning

Measurement	UL or DL	Number of BSs needed	Comment
Time-of-arrival (ToA) of the first path	Either	3	BSs should be synchronized with the UE
Time-difference-of-arrival (TDoA), derived from several ToA measurements	Either	4	BSs should be mutually synchronized
Round-trip-time (RTT), derived from several ToA measurements	Both	3	No synchronisation needed
Angle-of-arrival (AoA) at the BS	UL	2	Requires planar arrays at each BS
Angle-of-departure (AoD) from the BS	DL	2	Requires planar arrays at each BS
TDoA+UL-AoA	UL	2	BSs should be mutually synchronized
RTT+ UL-AoA	Both	1	No synchronisation needed

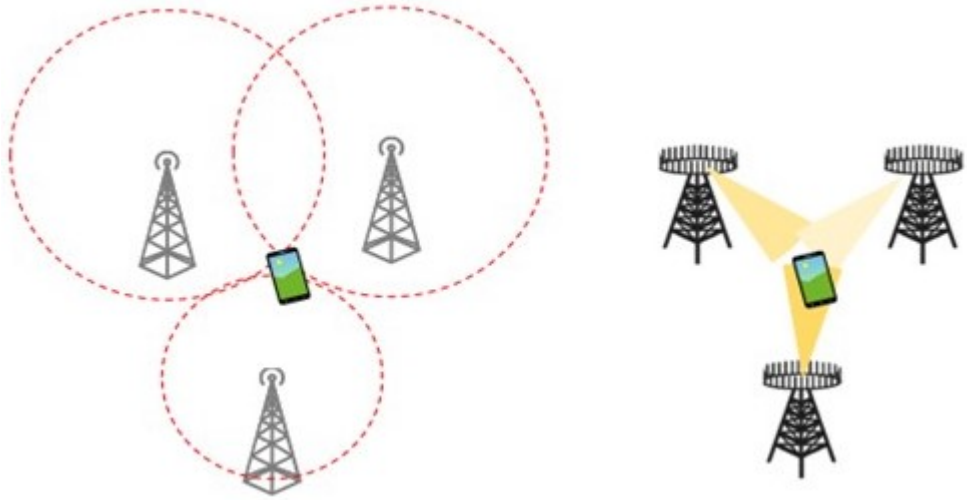


Figure 44: Example of RTT-based localisation (left), constraining the UE on the intersection of circles (2D) or spheres (3D); and localisation based on DL-AoD measurements (right), constraining the user within a sector of each BS

2.11.2.11.2 Bandwidth requirements

The amount of available bandwidth is directly related to delay resolution and thus to multipath suppression (in particular, two paths can be resolved if their delay difference is at least 1 over the bandwidth). If strong signal paths are present, say, 10 meters after the direct path, then a bandwidth of around 30 MHz is needed to resolve this secondary path. For that reason, a large bandwidth is important for accurate localisation in cluttered environments.

2.11.2.11.5 Other requirements

Transmission power: the accuracy of delay and angle measurements depends on the received signal-to-noise ratio (SNR), which is itself proportional to the transmission power. Hence, higher transmit powers lead to more accurate localisation, provided multipath can be resolved. Since localisation depends on pilot signals, an increase in SNR can also be achieved through longer transmission times.

Number of antennas: similar to bandwidth being related to delay resolution, so is the number of antennas proportional to angle resolution (the relation for a linear array is that two paths with angle difference (in radians) beyond 2/(number of antennas) can be resolved). Hence, a larger array of half-wavelength spaced elements leads to improved angular resolution.

Signal processing and hardware limitation: depending on the computational capacity and knowledge regarding the utilized beams, the delay and angle estimation performance can be improved. Moreover, hardware and calibration errors (e.g., synchronisation errors) significantly affect localisation performance, leading to a significant gap between theory and practice.

2.12 Drones

2.12.1 Connectivity during crowded events use case, when drones are used

2.12.1.1. Description

The purpose of this scenario is to demonstrate how UAVs through 5G network capabilities can improve connectivity services in a highly crowded environment e.g. during large events. The concept relies on providing end-to-end dedicated and reliable communication targeting specific user groups such as the event organisers to supervise and manage large events in an unhindered manner. At the same time, and with the proper dimensioning of the deployed solution in terms of capacity, the connectivity services can also be offered to the spectators.

Three deployment variants are envisaged in respect to connectivity extension provisioning:

In the first scenario, the drone will be carrying a 5G base station (gNB), and will have an RF backhaul link to the ground 5G Core. To implement this approach a tethered drone is required (also from C2 link radio interferences perspective), which offers unlimited power supply and secured data transfer for safer operations. This will expand the connectivity to a stadium, where a crowded event takes place or other stadium patrolling services are requiring a dedicated private connectivity.

In the second scenario, the drone will provide connectivity to the users via a relay link. This setup modifies the requirements of the drone to be used and therefore a simple (and not tethered) drone is considered. This modification changes the flight characteristics of the drone itself, with most critical the limited flight time due to the on-board batteries. Moreover, connectivity expansion is performed only in under-served areas, since the capacity of the network is not modified, but only the signal quality reception is improved.

In the third scenario, the drone will be carrying a lightweight 5G UE, which will provide connectivity to the users by creating a Wi-Fi hotspot, utilizing the 5G technologies as a backhaul between the WiFi hotspot and the gNB. In the variant, the connectivity expansion is performed in terms of the number of users, since a specific group of people will be connected at the WiFi spot and then via the 5G Backhaul to the gNB. By lifting more than one drone, the connectivity can be expanded not only in under-served areas, but also in terms of the number of users that can be connected to a specific gNB. An on-board policy controller and caching technology can reduce the bandwidth requirements, especially when the user requests refer to local services.

2.12.1.2. Source

5G!Drones H2020 European project

2.12.1.3. Roles and Actors

Users - People who connect during events in the crowd

Drone operator

Telecom operator – to provide connectivity services

2.12.1.4. Pre-conditions

Preparation stage: In addition to the common preparation stage steps mentioned in Section 3.3.1, this scenario will have the following additional steps:

Provide a portable setup comprised of UAVs, small 5G cells, other communication equipment and application servers necessary to support the broadcast and connectivity requirements..

Deploy UAV operator software pilots to application servers provided in the test facility's portable setup.

2.12.1.5 Triggers

None

2.12.1.6. Normal Flow

Preliminary flight stage

Flight stage

i. Use the Trial Controller to initiate the drone trial.

ii. Autonomous take-off of the 5G-enabled patrolling UAV (drone with camera).

iii. Autonomous take-off of the 5G network-measuring UAV (drone with UE).

iv. Drones follow the agreed flight plan to scan the area and stream the data for analysis and logging to the edge.

a. Drones report their position periodically.

b. Drones can receive information with regards to re-routing.

c. The 5G enabled patrolling UAV scans the area using its camera and provides the video feed back to the event organizers.

d. The 5G network-measuring UAV measures 5G connectivity and the signal/network quality.

v. Identify stadium areas with overloaded network capacity and initiate UAV assisted 5G connectivity.

vi. Once finished the missions the drones return to the home base and land autonomously.

2.12.1.7. Post-conditions

Analysis & reporting.

2.12.1.8. High Level Illustration

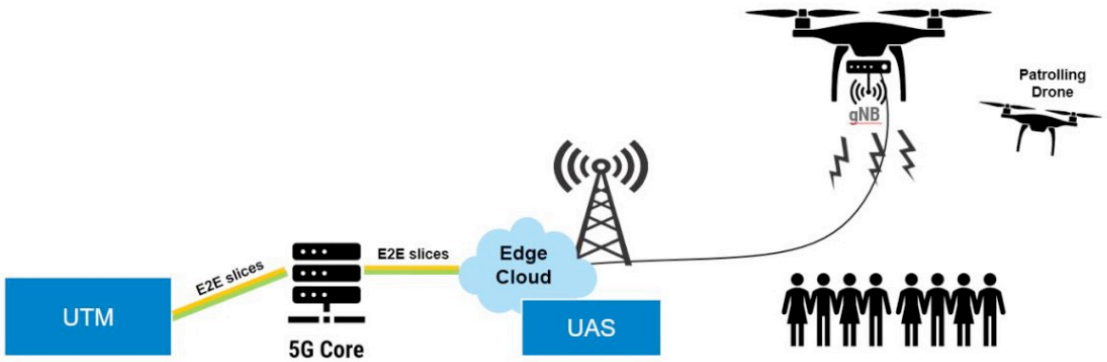


Figure 45: Use case architecture

Figure 46: High level architecture

2.12.1.9. Potential Requirements

Functional requirements

SC1-FUNC1		The mobile network must support 3 concurrent service slices	
Priority	Essential	**Justification**	Use case Driven
Description		Three different services shall be supported by the Use case: C2 of the drone, a uRLLC service. Multimedia Streaming from the Patrolling Drone, an eMBB Service. Sending radio network quality measurement data. Basic connectivity for the spectators, also an eMBB service.	
Related Component(s)		The 5G core and Access network	

UC4.SC1-FUNC2		Mobile edge capabilities must be deployed in the stadium	
Priority	Essential	**Justification**	Use case Driven
Description		The provision of the uRLLC service for the drones' command and control mandates the existence of a MEC centre in Egaleo stadium.	
Related Component(s)		The 5G core and Access network	

UC4.SC1-FUNC3		Enforcement of separation between UAVs operating in close proximity	
Priority	Optional	**Justification**	3GPP r.16 22.825 UC5
Description		The requirements defined in [13] use case 5 for collision avoidance in cases that drones are flying in close proximity are relevant and should be considered when the technology is made available. Drones C2 systems should use GPS RTK solution to improve precision of drone positions.	
Related Component(s)		The 5G core and Access network	

UC4.SC1-FUNC4		Radio Access Node on-board UAV	
Priority	Essential	**Justification**	3GPP r.17 22.829 UC2
Description		The requirements defined in [18] Use case 2 and summarized in Table 58 as Requirements for UxNB must be considered, and most importantly: The 5G system shall be able to support wireless backhaul with required quality to enable a UxNB. The 3GPP system shall minimize interference among UxNBs in close proximity. Optionally, if the technology is made available, the 3GPP system shall be able to monitor UxNB (e.g. power consumption of the UAV etc.) and provide means to minimize power consumption of the UxNB (e.g. optimizing operation parameter, optimized traffic delivery) without degradation of service provided. Until this is possible, a tethered drone can be used to resolve power consumption concerns.	
Related Component(s)		The 5G core and Access network	

UC4.SC1-FUNC6		Initial authorization to operate a UAV	
Priority	Essential	**Justification**	3GPP r.16 TS 22.825 UC1
Description		The requirements defined in [13] Use case 2 and summarized in Table 58 are relevant and must be considered when the technology implementing them is made available.	
Related Component(s)		The 5G Core	

UC4.SC1-FUNC7		Data acquisition from the UTM by law enforcement	
Priority	Essential	**Justification**	3GPP r.16 TS 22.825 UC3
Description		The requirements defined in [13] Use case 3 and summarized in Table 58 are relevant and must be considered when the technology implementing them is made available.	
Related Component(s)		The 5G Core and Access network	

UC4.SC1-FUNC8		Simultaneously support data transmission for UAVs and eMBB users	
Priority	Essential	**Justification**	3GPP r.17 22.829 UC4
Description		The 5G system shall need to optimize the resource use of the control plane and/or user plane for transfer of continuous uplink data that requires both high data rate and very low end-to-end latency. The requirements defined in [18] Use case 4 are relevant and must be considered when the technology implementing them is made available.	
Related Component(s)		The 5G Core and Access network	

UC4.SC1-FUNC9		Autonomous UAVs controlled by AI	
Priority	Essential	**Justification**	3GPP r.17 TS 22.829 UC5
Description		The UAVs shall be controlled through a UAS system and as such all requirements set in [18] Use Case 5 must be considered. Specifically, the 5G network must: Consider UAV requirements for both high uplink rate transmission and low delay downlink transmission To provide high precision positioning information to the AI system to assist the calculation and decision-making for UAV flight.	
Related Component(s)		The 5G Core and Access network	

Non-functional requirements

Safe distance from spectators

Approved Flight Plans

Certified Drone operators

Connectivity shall be provided in a secure manner

Approved Flight Plans of tethered Drones

2.12.1.9. Radio Specific requirements

5G New Radio (NR), is one of the novel and most promising components of 5G. 5GNR encompasses a new OFDM-based air interface, designed to support the wide variation of 5G device-types, services, deployments and spectrum.

OpenAirInterface (OAI) gNB: OpenAirInterface RAN (OAI-RAN) solution provided by Eurecom, both for the gNB and the UE will be deployed in the Athens platform.

The Athens platform will integrate the OAI 5GNR gNBs and UE components to perform end-to-end experimentation and KPI measurement collection. The initial deployment will be based on Non-Standalone Mode (NSA) Option 3. This assumes that a working chain of OAI software encompassing 4G radio should be available. In this context, in Athens the OAI version of 4G is already implemented and incrementally will be upgraded with 5G features as is foreseen by the 5G migration path.

2.12.1.10. Bandwidth and URLLC requirements

Network Critical Parameters	Value
Data Type	1. C2 of the drone is max 100 ms latency 2. Application data: including video streaming, images, sensor data to support event management applications 3. Basic connectivity, to support organisers as well as spectators connectivity needs in a saturated environment
Heights	Max 120 m AGL. This is an upper limit of VLL airspace according to Eurocontrol definition.
Speeds	Target horizontal speeds up to 70 km/h for all scenarios
Latency	1. C2: UAS requirement is 10 ms (one way from eNB to UAV) 2. Application data: Latency value similar to LTE ground-based users 3. Basic connectivity
Data Rates	1. C2: [60-100] kbps for uplink and downlink 2. Application data: up to 50 Mbps for UL 3. Basic connectivity: 0.5 Mbps
C2 Reliability	As low as 10-3 Packet Error Rate
Position Accuracy	1m

2.12.2 An innovative fire detection pilot solution using 5G, Artificial Intelligence and drone technology

An innovative fire detection pilot solution using 5G, Artificial Intelligence and drone technology

2.12.2.1 Description

Provide motivation of having this use case, e.g., is it currently applied and successful; What are the business drivers, e.g., several stakeholder types will participate and profit from this use case

Provide on a high level, the operation of the use case, i.e., which sequence of steps are used in this operation?

Wildfires represent a significant natural risk causing economic losses, human death and environmental damage. In recent years, the world has seen an increase in fire intensity and frequency. Research has been conducted towards the development of dedicated solutions for wildland fire assistance and fighting. Systems were proposed for the remote detection and tracking of fires. These systems have shown improvements in the area of efficient data collection and fire characterization within small-scale environments. However, wildland fires cover large areas making some of the proposed ground-based systems unsuitable for optimal coverage.

To tackle this limitation, unmanned aerial vehicles (UAV) and unmanned aerial systems (UAS) were proposed along with ground sensors. The Sensors which are installed in strategic points in the park, are interconnected with the incident management platform and the drone control system. The drone operates scheduled surveillance flights as well as emergency flights in case of the sensor indications.

The system is able to detect smoke or fire, both by the sensors indications at the field and from specific algorithms that are used to analyse drones' video in real-time. In both cases the data are send to the Control Center indicating points of interest.

When a sensor identifies abnormal values of CO2 or/and temperature sends an alarm to the Control Center with the coordinate of the event. At that point two actions take place:

An SMS / Email is sent to the involved stakeholders with the exact location of the event

The drone autonomously takes-off and is directed straight ahead to the indicated location to verify the event with the help of the Ai algorithms. The drone during all operations broadcasts live to all stakeholders that are involved.

In the case of a preprogramed patrolling where the drone detects smoke or fire through the camera, it sends an alert to the control centre, and the drone, immediately rushes to where the smoke was detected to verify the incident and send the exact location info. Then the drone either returns to its base or records the progression of the fire. The result is the immediate identification of the starting point of the fire, real-time monitoring of remote areas, early visual detection of smoke and fire, and in result protection of human life.

2.12.2.2 Source

Press release announcing an innovative fire detection pilot solution using 5g, artificial intelligence and drone technology

2.12.2.3 Roles and Actors

Citizens & Vicinity. People who lives (near) a critical infrastructure and needs to be protected or informed about potential risk that could affect their lives.

Critical Infrastructure. Central element source of vulnerabilities that can become real risks (natural or cyber risks).

Emergency Bodies. Stakeholders dedicated to minimizing the effects of the risks once them happens (hospitals, fireman's, etc.).

Governmental bodies. Stakeholders required to organize the society and provide insights at higher level.

Civil Protection Organization. Stakeholders dedicated to mobilizing and organize the citizens in emergency situations.

2.12.2.4 Pre-conditions

The main pre-condition here is the occurrence of an extreme event, such as a fire, that would result in severe social, environmental, and economic impacts.

2.12.2.5 Triggers

The triggers used in this use-case is when an extreme event is detected early enough in the critical infrastructure.

2.12.2.6 Normal Flow

What is the normal flow of exchanged data between the key entities used in this use case: devices, IoT platform, infrastructure, pedestrians, vehicles, etc.

The main goals are to provide a reliable early warning system in case of extreme environmental events. A prerequisite is the interoperability of the system and the data it produces with smart city standards, and the effective integration of legacy third-party applications and IoT subsystems and equipment already installed in cities.

The service aims to:

1) Surveillance, in real time, of large areas presenting a high level of risk and an increased possibility of fire through a network of ground sensors and UAV/Drone.
2) Immediate smoke or fire detection in 2 ways:
   a) Ground sensors: temperature, smoke, etc.
   b) On-board sensors in UAVs/drones (optical cameras, thermal cameras, sniffers) Optional
3) Timely confirmation of an outbreak using special high-end small-sized drones, equipped with a special camera, operating in the designated area.
4) Upon a true confirmation immediate alerts and notifications with emergency bodies (in case of required) and civil protection bodies.
5) Provide highly accurate information about the location, spread, and intensity of fires, allowing emergency responders to make informed decisions about how to respond
6) Continuous surveillance and data collection during the fire event and after. The resulting data are kept in a file (log files) and are available for further statistical analysis, patterns identification, etc. for the creation of forecasts and operational models for more efficient management of the phenomena.
7) Develop a holistic platform to provide Common Operational Picture (COP) with critical information to help decision-makers prioritize resources and respond more effectively reducing the damage caused by fires. Reduce the need for large-scale firefighting operations and the costs associated with them.

2.12.2.7 Alternative Flow

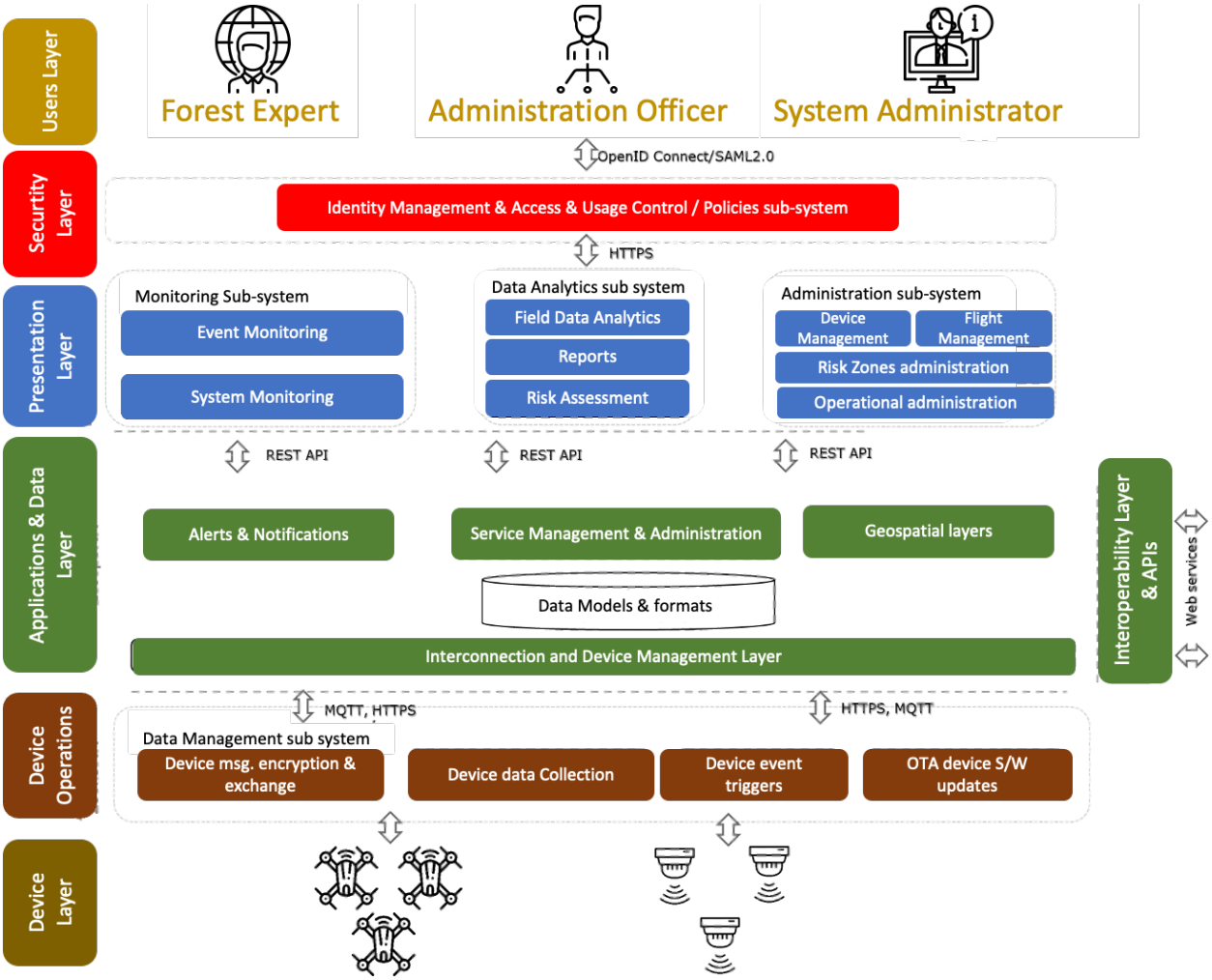
None

2.12.2.8 Post-conditions

Continuous surveillance and data collection during the fire event and after. The resulting data are kept in a file (log files) and are available for further statistical analysis, patterns identification, etc. for the creation of forecasts and operational models for more efficient management of the phenomena.

2.12.2.9 High Level Illustration

- High level figure/picture that shows the main entities used in the use case and if possible their interaction on a high level of abstraction



2.12.2.10 Potential Requirements

Functional Requirements

Real-time communication with the stakeholders in case of emergency.

Reliable communication between the stakeholders.

Scalable communication between systems to interconnects different critical infrastructures.

Standard-based communication between critical infrastructure to align emergency information exchange with new and legacy systems.

Non-Functional Requirements.

Secure communication between the emergency bodies due to the information nature.

Interoperability between communication protocols (linked also with the possibility to use standard communication protocols between the systems).

2.12.2.11 Radio Specific requirements

2.12.2.11.1 Radio Coverage

According to [MuBo22]:

"When working with a UAV, it is essential to control and receive image and video data remotely. Therefore, the line-of-sight, 4G/LTE, and SATCOM communication methods were used to secure

the capability of operating under various circumstances and the UAV operation at long distances from the ground control station due to the size of the forest area.

A typical transmission structure contains a line-of-sight ground control station using a radio connection. It includes two datalinks (the primary one, used for image and video and telemetry exchange within 180+ kilometre range, and the backup one, for telemetry only), with automatic hopping between them in case of Global Navigation Satellite System (GNSS) or signals loss and advanced encryption standard AES-256 encryption. Secure VPN technologies, including TLS, IPSec, L2T, and PPTP, are used for data transport. This method allows the ground control station to connect with the UAV regardless of range restrictions and provide reliable cellular service. The modem concurrently enrols itself in the networks of two distinct cellular network operators and then chooses the most reliable one. Line-of-sight communications have some disadvantages, considering the range and the possibility of weather interference. SATCOM has historically been considered a Beyond Line of Sight (BLOS) communication system that would guarantee a constant connection and reliable data transmission at predetermined distances. A highly directed L-band antenna ensures a small radio signature. Furthermore, it complies with BRENT, STU-IIIB, TACLANE, STE, and KIV-7 are only some of the encryption and secure communication standards. AI server computer is located in the ground control station to process received image and video data from UAVs", copied from [MuBo22].

Moreover, according to [SiBa23]:

"To achieve secure and reliable communication for drones using a cellular communication system, drones have to exchange the information with the pilot, nearby other drones or UAVs, and principally with the air traffic control system. This mechanism is called UAV Control and Non-payload Communication (CNPC) simultaneously, depending upon the applications, a drone has to transmit or receive information on a timely basis related to the assigned task, such that images, videos, and data packets from ground entities to the drone and vice-versa. This operation is known as payload communication. To de- ploy the UAVs application on a large scale the International Telecommunication Union (ITU) has categorized the CNPC in the following section:

1. UAV Command and Control Communication (C2): This type of communication includes UAV or drone's status, a real-time control signal from pilot to UAV, and flight command updates.
2. Air Traffic Control (ATC) Relay Communication: Communication between the air traffic control system and UAV operator via ATC relay.
3. Communication for Detect and Avoid Collision: Capability to sense and avoid collision from nearby UAVs and territory.

Payload communication and CNPC require different set of spectrum. Table 2 and table 3 represents the network key points for UAV's communication. These communication parameters are specified in Release 17 by the 3GPP standards.

UAV Control and Non-payload Communication:

Table 24 represents the required QoS parameters for the CNPC communication. Here, uplink (UL) data transmission represents UAV to network side messages and downlink (DL) data transmission represents network to UAV side messages. Control and command communication is duplex communication and it may be integrated with video for controlling the operation of UAVs. Therefore, when a C2 message is sent with video, the required end-to-end latency is 1 second. A positive acknowledgment message for downlink transmission is necessary in this mode. On the other hand, when a C2 message is sent without video, end-to-end latency would be less than 40 milliseconds. This mode also requires a positive acknowledgment in downlink transmission. To communicate with the ATC relay, end-to-end latency should not be more than 5 seconds. To sense and avoid the collision with other UAVs and territories, the delay for the uplink transmission should be less than 140 milliseconds and in downlink transmission required delay is 10 milliseconds. In this mode, the reliability of the network should be 99.99% for the uplink transmission and 99% for the downlink transmission.", copied from [SiBa23].

Table 24: UAV control and non-payload communication requirements, copied from [SiBa23]

Control and non-payload communication	Message interval (UP/DL)	Message size (UP/DL)(byte)	Max UAV speed (km/h)	End-to-end latency (UP/DL)	Reliability (UP/DL)	ACK (UP/DL)
Control & Command message (without video)	1 s/ >= 1 s	84–140/100	300	1 s/1 s	99.9%	Not required/Required
Control & Command message (With Video)	40 ms/40 ms	84–120/24	60	40 ms/40 ms	99.9%	Not required/Required
Communication with UTM or ATC	1 s/1 s	1500/10K	300	5 s/5 s	99.9%	Required/Required
Detect & Avoid collision with other UAV	500 ms/500 ms	4K/4K	50	140 ms/10 ms	99.99%/99%	Required/Required

2.12.2.12 Bandwidth requirements

According to [SiBa23]:

"UAV Payload Communication: The 5G cellular technology shall be capable to transmit data collected by the entity which are installed on UAVs, such as a camera to transmit images, videos, and data files. Depending upon the applications, UAVs require different uplink and downlink quality of service (QoS). **Table 25** introduces the UAV payload communication requirements. **Table 26** introduces the communication requirements from Drone based applications.

Table 25: *UAV payload communication Requirements, copied from* [SiBa23]

UAV applications	Above ground level (m)	Max UAV speed (km/h)	End-to-end latency (UP/DL)(ms)	Data Rate (UP/DL)
8K Video Real-Time Broadcasting	<100	60	200/20	100 Mbps/600 kbps
4X4K AI Surveillance	<200	60	20/20	120 Mbps/50 Mbps
Remote UAV Controller Through HD Video	<300	160	100/20	25 Mbps/300 kbps

To transmit real-time video using a UAV up to 100 meters above ground level requires a 100 Mbps data rate for uplink transmission and 600 Kbps for downlink transmission. The allowed latency is 200 and 20 milliseconds for uplink and downlink transmission respectively. Using a UAV for surveillance needs 20 milliseconds of end-to-end latency in both uplink and downlink transmission. The essential data rate for this kind of application is 120 Mbps for uplink and 50 Mbps for downlink transmission. For controlling an UAV through HD video where the speed of the UAV is less than 160 km/h, the required uplink data rate is 25 Mbps and the downlink data rate is 20 Mbps. For this kind of application, end-to-end latency is 100 and 20 milliseconds for uplink and downlink transmission, respectively.", copied [SiBa23].

Table 26: Communication requirements from Drone based applications, , *copied from* [SiBa23]

Drone based application sector	Coverage height (m)	End-to-end latency (ms)	Throughput requirements (UL/DL)
Delivery of goods	100	500	200 kbps/300 kbps
Videography and image capturing	100	500	30 Mbps/300 kbps
Security and inspection	100	3000	10 Mbps/300 kbps
Drone fleet show	200	100	200 kbps/200 kbps
Agriculture	300	500	200 kbps/300 kbps
Rescue mission	100	500	6 Mbps/300 kbps

2.12.2.13 Other requirements

Unmanned aerial vehicles, or drones, are to become an integral part of the equipment used by firefighters to monitor wildfires. They shall be used as autonomous and manual intervention remotely operated sensing platforms with AI for fire detection prevention, providing real time connectivity in a control centre. In such a holistic approach the following requirement shall be addressed

UAV types

Specialized fire **surveillance UAVs**, capable of flying in harsh weather conditions of wind, rain, extreme heat or cold, equipped with a camera that can zoom and detect fires on the fly, with an automatic health and battery status check system. The UAVs are intended for patrolling and surveillance of specific danger zones, which will be determined by the risk analysis and fire protection study.

Specialized **small confirmation drone quadcopters** for immediacy and operational risk reduction with high-end thermal and optical camera, capable of flying near high temperatures, waterproof, with automatic health and battery status check that will aim to confirm an incident on the ground.

A specialized **medium-sized UAV** that allows for ad-hoc flights on a case-by-case request basis, which should have a high-end thermal and optical camera and automatic health and battery status checks. This UAV has two (2) operational roles:

- Monitoring for smoke and fires
- Event confirmation from a local sensor or surveillance UAV

Drone Charging/Landing-Take-off Bases

The aim is for the drones to be constantly within the geographical area they are expected to operate so that they are always 'ready' to flight and thus reducing response time required. These bases must necessarily be equipped with a meteorological station that collects data in real time such as humidity, temperature, wind speed, etc. These indications must be visible both from the operations centre and from the pilots. The pilots and the operations centre, in consultation with the flight controller are taking into account all the parameters (meteorological data, flight restrictions of the drone), in order to decide whether or not the flight can be carried out. Thus, all data that the pilots process with the flight controller contribute to the commissioning or de-commissioning of the flights. Such data are recorded in a data storage kept in the operations centre. Data can be sent via 3G/4G/5G and/or WiFi with PC support on the base.

For the proper and uninterrupted operation of the bases, a charging power supply unit (UPS) capable of meeting the requirements for continuous power supply for at least 8 hours is mandatory.

Unmanned Aircraft System (UAS)

The information system consists of autonomous functional units (subsystems) that complete the infrastructure and communicate through well-defined standards and interfaces (APIs). Such subsystems of the system are:

Drone/UAV flight and control unit

Take-off/landing and charging base monitoring unit

Weather update unit

Civil aviation aircraft and drone/UAV air traffic information unit

Infrastructure orchestration and cloud interoperability extension module

2.12.3 5G-INDUCE: Drone assisted network performance and coverage monitoring for industrial infrastructures

2.12.3.1 Description

Use case targets 5G network performance and coverage monitoring - data collected through monitoring of the 5G network serve as a key factor in a continuous process of network optimisation, thus assuring the required (high) level of QoS and QoE for the industry/business process to run properly. The solution also enables drone assistance to add height relation perspective of the 5G monitoring metrics and to provide real-time video streaming with the purpose of identifying potential sources of performance drop (e.g., sources of radio interferences, metal obstacles causing signal scattering, etc.).

2.12.3 2 Source

Text included in subsections related to the 5G-INDUCE is copied from one or more documents that can be found via the following links:

https://www.5g-induce.eu/

https://private.5g-induce.eu/Documents/PublicDownload/144

Drones in B5G/6G Networks as Flying Base Stations

2.12.3.3 Roles and Actors

Industry/business, drone assistance.

2.12.3.4 Pre-conditions

The identified challenges can be narrowed down two five main issues, namely energy availability, mobility and path planning, positioning of nodes, security and privacy issues, and the offered quality of service. As the nature of the interfaces among the relaying equipment and the next-generation cellular network core is highly compartmentalized (assuming an ETSI TS 123 501 V15.2.0-compliant 5G architecture), drone BSs belong to the RAN layer as UE instances.

2.12.3.5 Triggers

All challenges, especially security and quality of service, are affected by this compartmentalized, "blackbox" approach, as the 5G core has no authoritative access to the radio-layer.

2.12.3.6 Normal Flow

The 5G-INDUCE project is envisaged to offer a variety of services and components as add-ons to the 5G core architecture presented in Section 2 and described on a high-level (considering interfaces among the management and network orchestration (MANO) and the virtual/physical infrastructure and the NFVO) in Figure 6. 5G-INDUCE offers a full-stack NetApp management platform to orchestrate services and functionalities, mainly in the industrial domain. Orchestration enhancement can support data confidentiality, securely encrypt critical infrastructure management and monitoring, and reliable operator–drone communication interfaces.

The scenarios are strongly related to the targeted NetApps of the 5G-INDUCE project and are aligned with its goal of establishing easily extensible yet secure and QoS-aware next-generation cellular connectivity in critical scenarios. All aforementioned use-cases rely on novel orchestration algorithms for the deployment of services over containerized realms.

The challenges currently faced by the entire research and industrial landscape range from security and privacy to licensing and AI-related issues, namely explainability and legislative/ethical concerns in regard to automated piloting, no-fly-zones and potential collisions; all these areas require more research in the near future, as little to no work has targeted the aforementioned parameters in a networking context. It can be easily deduced that the complexity of said issues will increase, even more so with the increase in network heterogeneity and the additional requirements entailed.

Low-earth orbit satellites (and constellations thereof) also seem to be a rather promising technology in terms of supporting ubiquitous connectivity for NR networks. With this in mind, future protocols, frameworks, and even hardware modulators and demodulators shall be designed to support satellite-to-drone connectivity where applicable. Consequently, standardization for all developments targeting the aforementioned challenges is going to be a direct focus of all relative standardization groups and institutes in the coming years.

2.12.3. 7 Alternative Flow

2.12.3. 8 Post-conditions

2.12.3.9 High Level Illustration

As the presented work constitutes an output of the 5G-INDUCE H2020 project, parallels are drawn—where applicable—between the examined use cases and challenges.

The core elements of the 3GPP 5G architecture are defined in ETSI TS 123 501 V15.2.0 (2018-06). As demonstrated in Figure 2, the core 5G services (implemented in the form of network functions (NFs)), are the network slice selection function (NSSF), the network exposure function (NEF), the network repository function (NRF), the policy control function (PCF), the unified data management (UDM), the application function (AF), the authentication server function (AUSF), the access and mobility management function (AMF), the session management function (SMF), the user plane function (UPF), the data network (DN), the radio access network (RAN), and the user equipment (UE). In the context of the presented work, the most important components can be narrowed down to the AMF, the RAN and the UE.

The AMF is responsible for registration and connection management, as well as ensuring reachability and managing UE mobility. As demonstrated in Figure 1, the supported mobility for 5G networks reaches up to 500 km/h, and up to 100 km/h for the upcoming 6G networks. Handling node mobility is enabled by this network function. The RAN utilizes radio transceivers (gNodeB/gNB instances) to facilitate cellular connectivity; gNBs provide the New Radio (NR) user plane and control plane protocol interfaces with the UE. According to 3GPP, a device utilized by an end-user to facilitate communication with another user or service is a UE, which is in turn connected to the gNB.

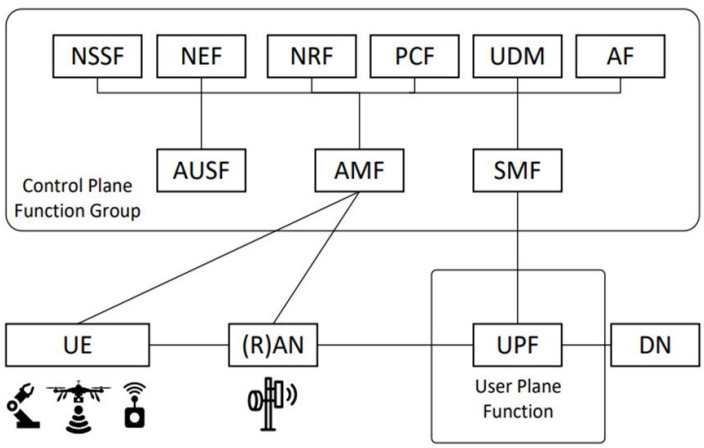


Figure 47: 3GPP-compliant 5G architecture

2.12.3.10 Potential Requirements

B5G/6G, a major driving force behind the vision of 6G, involves the deployment of connected and autonomous vehicle systems (CAVs) and drone communications. Research efforts in the field of CAV and drone-based communication systems have been steadily increasing in both academia and industry, targeting strict requirements, especially ultra-low latency and unprecedented communication reliability. As the industry is shifting towards wireless, real-time and high-throughput networking, drone base stations are envisaged to constitute pivotal assets. Table 28 showcases the main differences between 5G and 6G networks and the main improvements with regard to their core attributes.

Table 27: Mapping of functional to non-functional requirements

List of 5G-INDUCE **Functional** requirements	Prevailing **Non-functional** Requirements (ISO/IEC 25010)							
	Functional Suitability	Performance Efficiency	Compatibility	Usability	Reliability	Security	Maintainability	Portability
GPR.A (Generic platform impl.)	○	○	○	○	○	○	○	○
GPR.B (Generic OSS implementation)	○	○	●		○			
GPR.C (Generic NAO implementation)	○	○		○	○			
GPR.D (User Interfacing and sharing)	○			●		●	○	○
GPR.E (Security capabilities)	○		○		●	●		
GPR.F (Generic services' use cases)	●					○	○	●
GPR.G (Data processing and regulations)	○		●			○		
MSR.A (End user NAO interface)	○			●		○	○	
MSR.B (NAO)	○	○		○	○			
MSR.C (NAO-OSS Interface)	○		○					○
MSR.D (OSS)	○	●	○		○			
MSR.E (OSS-Network Orch. interface)	○		●				○	○
MSR.F (Network Orchestrator)	○	○	○		○			○

Table 28: Comparison of 5G and 6G attributes

Attribute	5G	6G
Peak Frequency	110 GHz (W-band)	10 THz
Peak Spectral Efficiency	30 bps/Hz	100 bps/Hz
Peak Data-rate	20 Gbps	1000 Gbps
End-to-End Latency	10 ms	1 ms
Connection Density	1 million per sq. kilometer	10 million per sq. kilometer
Supported Node Mobility	500 km/h	1000 km/h

2.13 Edge-Cloud Orchestration

The main goal of CODECO is to research, implement and validate a novel cognitive, cross-layer and highly adaptive Edge-Cloud management framework, which will enable flexible and effective orchestration of decentralized data workflows, dynamic offloading of computation and adaptive networking services across the Cloud/Edge computing continuum. CODECO will be validated in the scope of **six innovative use cases** that are destined to showcase the value-added Cloud/Edge functionalities of the CODECO framework, including functionalities like latency and power efficiency optimization, real-time computation adjustments, as well as flexible and adaptive networking infrastructures from the far Edge to the Cloud. The use cases are aimed at demonstrating the whole range of CODECO functionalities and features in a wide array of deployment configurations serving the needs of different stakeholders like infrastructure providers and Cloud/Edge application developers.

The initial CODECO containerized application orchestration framework composes of modular micro-services illustrated in **Figure 48**, to support the following aspects:

Automated configuration, related with application setup and application runtime across Edge-Cloud, by taking into consideration compute, network, and data aspects. Automated configuration is handled by the CODECO *Advanced Configuration and Management (ACM)* component.

Data as a resource. CODECO addresses, via its *Metadata Manager (MDM)* component data as a resource in the sense that available snapshots from the overall Edge-Cloud infrastructure, integrating different perspectives (application, user, system, data, network) at different instants of the CODECO operational workflow can be provided to different CODECO components, to assist in detecting relevant changes.

Dynamic scheduling and workload migration is supported by the CODECO component *Scheduling and Workload Migration (SWM)*. SWM integrates a novel concept by Siemens, seamless computing, including a novel scheduler for Kubernetes (K8s) that considers data-network-computation requirements to provide a best match between application requirements and available infrastructure (nodes, their computational and data properties, as well as network nodes and links), and to schedule and re-schedule application workloads across single cluster and federated cluster environments, considering application and user requirements.

Context-awareness and privacy preserving decentralised learning, supported in the component *Privacy-preserving Decentralised Learning (PDLC)*. CODECO relies on context-awareness to be able to achieve a joint data-network-compute orchestration, and on privacy-preserving decentralised learning and inference to best support readjustment of aspects such as the processing capability, computational resources, networking resources and interconnections in real-time.

Infrastructure adaptation based on a cross-layer data-compute-network approach. Via the CODECO *Network Management and Adaptation component (NetMA)*, CODECO assists in adapting not just computational (node resources) but also the networking infrastructure interconnecting such nodes.

CODECO as a framework shall support the setup of applications across clusters (the so-called K8s application deployment) and the cluster runtime management operations for single and multi-cluster environments. Users relying on CODECO during an application deployment are named as **user DEV** in CODECO. Users relying on CODECO during the cluster runtime management are referred to as **user MGT.**

Components that are expected, at the current initial stage of development (M6) to be co-located with the K8s control plane are ACM and SWM. All the other components are expected to reside in both worker nodes and if required, they may also operate on the K8s control plane.

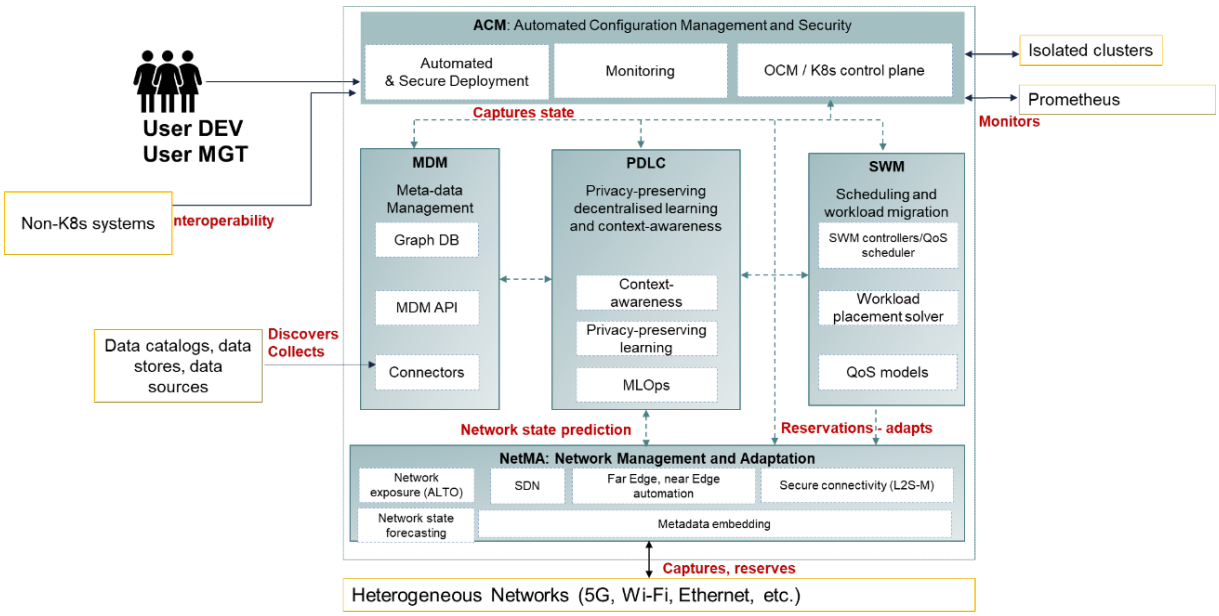


Figure 48: The CODECO K8s framework and its components

2.13.1 CODECO P1: Smart Monitoring of the Public Infrastructure

Contact: University of Göttingen, Tingting Yuan (tingting.yuan@cs.uni-goettingen.de), Xiaoming Fu (fu@cs.uni-goettingen.de)

2.13.1.1 Description

In recent years, there has been a remarkable increase in the use of Smart City solutions aimed at benefiting both residents and visitors. Those usually are achieved by leveraging advanced technology and data analytics to monitor traffic/ detect pedestrians, etc. The data collected from various sensors and devices is transmitted and analysed to optimize traffic patterns/ city planning and improve the quality of life for everyone. Now, with CODECO we can achieve a more connected, efficient, and sustainable solution. CODECO addresses the demand for handling large amounts of data in smart cities, including those with low latency demands. It is capable of orchestrating data flow across diverse features, both in terms of computation and networking. Besides, CODECO ensures a smooth and secure integration of data across Edge-Cloud environments. This ensures that data flows seamlessly and securely from Edge devices to the Cloud and vice versa, enabling end-to-end integration of smart city services. CODECO's decentralized approach to orchestration, along with its ability to deploy services in isolated, self-sufficient containers, offers great flexibility and adaptability. This means that smart city services can be deployed and executed in any environment, and the networking infrastructure can adapt to the needs of the services and the surrounding environment. This helps in creating a more resilient and adaptable smart city infrastructure.

The global purpose of P1 is to improve traffic flow and pedestrian safety in the city of Göttingen and assist in strengthening the existing Smart City concept through the implementation of a road monitoring and analytics system at the far Edge. This system comprises two parts: traffic monitoring at the city periphery, and pedestrian distribution monitoring in the city centre. By collecting and analysing at the Edge valuable data on traffic and pedestrian behaviour, this use case aims to optimize management, reduce congestion, and enhance overall pedestrian safety and comfort, while also providing valuable insights for city planning.

In the initial phase of the pilot, P1 will focus on two specific zones in Göttingen: the city periphery, which experiences high volumes of vehicular traffic, and the city centre, where pedestrian activity is most concentrated. On a first phase of operation, these two areas shall be considered to integrate a single cluster (together with the Cloud server(s) operated by the city and UGOE). On a second phase, the two areas shall be configured as two distinct clusters.

The periphery of the city will be equipped with a combination of thermal cameras, computing units, and communication units. This will enable the real-time collection and analysis of traffic data, tracking vehicle counts and congestion levels. These insights will be used to optimize traffic flow, reduce bottlenecks, and improve overall traffic efficiency. In parallel, the city centre will see a combination of LiDARs, computing units, communication units, and using data analytic techniques to track pedestrian movement patterns and density. The data collected will be crucial for improving pedestrian safety, managing crowd flow, and informing city planning initiatives. The back-end data centre can obtain real-time processing results at the Edge and visualize them to the public. As the pilot progresses, the data gathered will be evaluated and used to adjust traffic patterns, modify transport routes, and potentially redesign city layouts to better accommodate pedestrian and vehicular flow.

This pilot scenario, combining technological advancement and data-driven decision-making, is the first step towards transforming Göttingen into a truly smart city, enhancing the quality of life for its residents and visitors alike.

Edge nodes co-located with the cameras represent Kubernetes (K8s) worker nodes; the control plane is expected to reside in the Cloud. Hence, in the context of this use-case, CODECO shall be used to orchestrate (reallocate) resources across Edge-based environments, to assist in the degree of control decentralisation.

2.13.1.2 Source

HE-CODECO project

2.13.1.3 Roles and Actors

Actors:

GOV and municipalities can monitor traffic and get analytics on patterns (e.g., traffic, volumes of cars, bikes, etc.).

Network Infrastructure provider offers network connection.

Cloud/Edge infrastructure provider offers computation and storing resource for analytics.

User (developer, subscriber, e.g., Citizen) can get information about traffic.

Roles:

Transportation planning and management: The government and municipalities will have access to real-time traffic analytics, including abnormal alarms, as well as long-term traffic pattern analytics. By automatically collecting and analysing data on traffic behaviour, they can gain insights that can inform decision-making and improve city planning, enhancing traffic safety and efficiency.

Property development and investment: The infrastructure provider and deployer need to carefully consider the selection, deployment, and maintenance of the system, considering the feasibility and costs associated with each step. Once the system is deployed, the infrastructure provider conducts testing and validation to ensure that it is working effectively and providing the desired results.

Advertising and marketing: The citizen will have access to real-time traffic information through downloadable apps or public boards, enabling them to plan their travel and make informed decisions about their routes.

A summary of the business impact for the different proposed user journeys is as follows:

User Journey #1 Transportation planning and management: The real-time traffic data collected by the road usage monitoring system can be used to optimize transportation planning and management in the city. This can benefit businesses that rely on efficient transportation and logistics, such as delivery services, public transportation companies, and trucking companies.

User Journey #2 Property development and investment: The pedestrian distribution monitoring part of the system can provide valuable insights into foot traffic patterns in different areas of the city.

This information can be used to make data-driven decisions about property development and investment. Real estate companies and property developers can use this data to identify high-traffic areas and make informed decisions about where to invest in new properties or develop existing ones.

User journey #3 Advertising and marketing: The data collected by the system can also be used for advertising and marketing purposes. For example, businesses can use the data to identify high-traffic areas and strategically place their ads in these locations. This can help businesses reach their target audience more effectively and potentially increase sales.

2.13.1.4 Pre-conditions

Specific equipment and Edge nodes placed across the city in specific locations and are dimensioned with specific constrains in terms of computational and networking resources.

Application workload and respective datasets need to be uploaded, or adequate traffic needs to be generated e.g., by the installed cameras.

2.13.1.5 Triggers

Specific nodes in the infrastructure go down, or new nodes enter the living system – critical changes to the infrastructure.

2.13.1.6 Normal Flow

Figure 49 provides a high-level perspective on the proposed system architecture considering one cluster deployment, detailing both non-CODECO and CODECO components. The K8s control plane with the respective CODECO nodes is represented to run in the Cloud but may also be deployed at the near Edge. The worker nodes are deployed in Edge nodes co-located with cameras across the city.

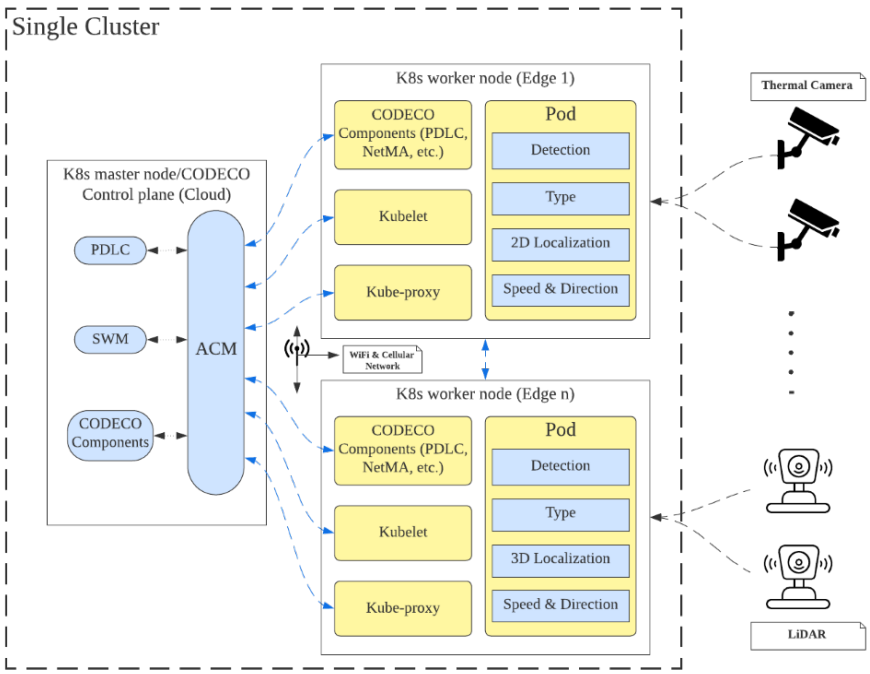


Figure 49: CODECO P1 system architecture.

As illustrated, there are CODECO components and non-codeco components.

Non-CODECO components deliver highly accurate and timely traffic indicators such as vehicle counting, traffic density, and traffic flow by using thermal camera sensors. With this data, cities can have an overview of the number of vehicles entering/leaving Göttingen, monitor traffic patterns, and use the information to reduce congestion. This information can also be used to identify potential bottlenecks or problem areas in the transportation system, allowing officials to proactively address issues before they become major problems. In addition, this information

could be used to optimize existing infrastructure to better meet the needs of residents and visitors. These components will also deliver highly accurate and timely pedestrian distribution indicators such as pedestrian counting, pedestrian density, and pedestrian distribution heat map by using the LiDAR sensor. It can be a valuable tool for city planning. On the one hand, it can help the city to have an overview of the number of pedestrians in some key areas in Göttingen city centre. On the other hand, it can help to understand pedestrian traffic patterns: Heat maps can provide the city with a visual representation of where pedestrians tend to congregate, move, and dwell in public spaces. By analysing these patterns, the city can identify high-traffic areas and prioritize them for improvements, such as new crosswalks, street furniture, or public amenities.

CODECO Components shall be placed both at the Cloud (K8s master node) and Edges (K8s worker nodes). For each location chosen for implementation, we will outfit it with an Edge device equipped with an array of sensors such as thermal cameras or LiDAR systems (rf. To section 2.1.2). In this use-case. An Edge node will be the same as a K8s worker node. This arrangement ensures the autonomous computational and data processing capabilities of each Edge device, all while remaining interconnected within the larger network. The data collected by these devices, including video and point Cloud data, must be pre-processed, and stored locally. This local storage of data is a crucial step that allows for future reference, audits, and given the sensitivity of the data to outflows from the specified area.

2.13.1.7 Alternative Flow

N/A

2.13.1.8 Post-conditions

Once the risks have been mitigated or circumvented, the system continues in operation. The user gets information via a dashboard; but the change in the infrastructure is agnostic to the user.

2.13.1.9 High Level Illustration

See **Figure 49**.

2.13.1.10 Potential Requirements

2.13.1.10.1 Deployment KPIs

Minimize bandwidth costs: we want to consider the bandwidth usage of each compute node and factor that into our decision-making process when deciding where to place workloads. We may also want to consider the bandwidth costs associated with network connections, such as those incurred when data is transferred between nodes. Overall, our goal would be to choose a deployment strategy that minimizes our bandwidth costs while still meeting our performance and reliability requirements.

Bandwidth cost: < 10G/month/camera

Overall detection and counting accuracy: >= 80%

System latency: <= 40ms

Rate of occurrence of failure (ROCOF): <= 5%

2.13.1.10.2 Non-functional requirements

Privacy protection in video collection and transmission; GDPR Compliance.

2.13.2 CODECO P2: Vehicular Digital Twin for Safe Urban Mobility

Contact: I2CAT, Jordi Marias (jordi.marias@i2cat.net)

2.13.2.1 Description

P2 makes use of the CODECO framework to support a Vehicular Digital Twin aimed to improve the safety of *Vulnerable Road Users (VRU)* in Urban Environments. Any mobility oriented Digital Twin requires the extensive deployment of ultra-reliable low latency services around the area it supports. Starting from the V2X communication capabilities to Computer Vision (CV) detectors capable of tracking all the moving parts within the mobility environment.

For this reason, the current use case relies on *V2X Roadside Units (RSUs)* and cameras to gather all the necessary information to track vehicles and pedestrians and then feed it to the vehicular Digital Twin, which will detect dangerous situations or behaviours and alert them.

The deployment and scalability of this service has challenges around the infrastructure side, where the information should be processed as close as possible to the V2X nodes and ensure low latency communications. This, in turn, translates to always having a fresh track of all the moving parts.

The pilot scenario focuses on the mobility environment of the interior and adjacent street of a UPC campus known as "Campus Nord" in Barcelona, which is located next to the I2CATs offices. This environment offers an interesting balance with walkable pedestrian zones that include bike lanes, as well as car lanes on the adjacent street. It encompasses a mix of various transportation modes, with *Vulnerable Road Users (VRUs*) playing a central role. However, VRUs can find themselves in dangerous situations when sharing spaces with cars. Which addresses the UC being presented.

This scenario presents an ideal testing ground due to its size, allowing for the examination of multiple areas and their respective control measures. Additionally, it provides a diverse representation of all transportation modes commonly found in urban environments. Consequently, this scenario offers the perfect setting to assess and address the challenges associated with different modes of transportation, ensuring the safety and efficiency of urban transportation networks.

2.13.2.2 Source

HE-CODECO project

2.13.2.3 Roles and Actors

Actors:

VRUs. A VRU, refers to vehicles or transport users who lack physical protection while navigating roadways, making them more susceptible to harm. They require heightened caution from both them and drivers to ensure their safety on the streets. Their role is to move around and expect to be advised when engaged in dangerous situations. Their goal is to prove that they can be safer thanks to the infrastructure services and the notification through V2X.

Pedestrians: They will be equipped with a smartphone and tracked by the camera. Are the most vulnerable ones.

Light Mobility Vehicles (bike or electric scooter): Equipped with an OBU or smartphone and tracked by a camera. They tend to get in riskier situations due to its speed and fragility.

Cars: Equipped with an OBU. Can find themselves in dangerous situations when sharing mobility spaces with lighter, more vulnerable, modes of transportation. Their role is to move around the car lanes and engage in risky behaviours with VRUs and to proof that the dangerous situations are avoided when detected by the system and notified.

Cameras: The cameras, which will be connected to the corresponding service. Will spot VRUs that are not connected. And notify them of their position and track to the infrastructure. Their role is to detect the position and trajectory of all the moving entities that are not connected.

To then pass this information to the infrastructure. Their goal is to make sure the use case works even when there are some vehicles or pedestrians not connected.

V2X RSUs. They will be the point of contact from the vehicles and UC users and the infrastructure. There will be some of them to ensure full coverage of the use case scenario. They will need to ensure minimum latency to the infrastructure. Their role is to serve as point of contact between the infrastructure and the V2X environment. Their goal is to make sure the messages emitted by the OBUs, or the infrastructure are mutually received.

Roles:

Governmental entities, policy makers, will have the availability to see a real time low-latency digital twin of the moving entities around the designated urban public space. Check dangerous behaviour and immediate notifications when any incident happens (along with the place where the incident happened and how it happened).

ICT (industry, mobile communications, and Cloud providers) will use CODECO to achieve reliability and low latency.

The **academic and researcher stakeholders** will be capable of ensuring through the proper research the viability of a system of Vulnerable Road User Awareness. And provide solid information that reduces/eliminates incidents with that kind of users.

The **developers** (Edge, IoT) and especially the **early adopters** will run around the campus as VRU. And will receive an audio-visual notification. On the other side other early adopters will be using conventional cars that will also notify collisions.

A summary of the business impact expected is as follows:

One potential business case for this technology is in the public sector. Municipalities and other government agencies responsible for mobility could use this technology to monitor and reduce the number of incidents involving vulnerable road users and other vehicles. By providing real-time data on the movements of these users, the application could help city planners design safer roads and intersections.

Another potential business case is in the insurance industry. Insurance companies could use the data collected by the application to improve their revenue by accurately assessing risk and reducing the number of claims. The positional and camera data provided by the application could also help insurance companies more accurately determine fault in the event of an accident.

The automotive industry is also a potential market for this technology. Car manufacturers are always looking for new features to include in their vehicles, and a V2X Vulnerable Road User awareness application could provide an extra layer of safety for drivers. This technology could be particularly useful for vulnerable vehicles such as bikes, electric scooters, and motorcycles.

2.13.2.4 Pre-conditions

Object detection (cars, pedestrians).

2.13.2.5 Triggers

Movement changes, time-based.

2.13.2.6 Normal Flow

The heterogenous sensor-V2X related modules of the present use case interact with each other following the structure shown on **Figure 50**.

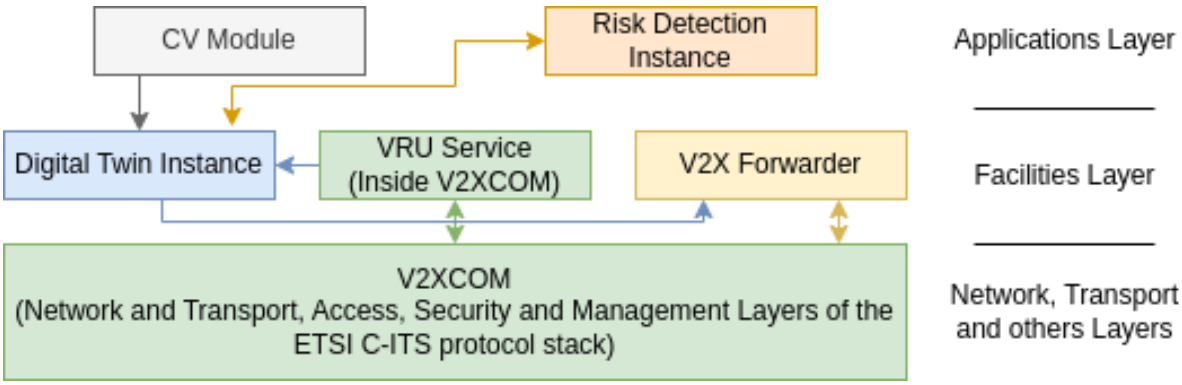


Figure 50: P2 UML diagram

In addition to the functionalities described in the previous section, it is essential to outline the various information flows between the modules:

1. **V2XCOM to V2X Forwarder**: All packets, regardless of the Facilities standard they belong to, are transmitted to the V2X Forwarder. Each packet is accompanied by information specifying the Radio Access Technology (RAT) it originates from or the unicast IP in the case of conventional mobile communications. The V2X Forwarder then determines whether to forward the message to other RATs and unicast Ips (using the V2XCOM module) or ignore it altogether.
2. **Digital Twin to V2X Forwarder**: Certain packets received from the V2XCOM module may be ignored by the V2X Forwarder. This occurs because the V2X Forwarder awaits queries from the Digital Twin to aggregate multiple messages and achieve the same effect as directly forwarding the packets.
3. **VRU Service (V2XCOM) to Digital Twin**: Whenever a new Vulnerable Road User (VRU) Awareness Message (VAM) is received, it undergoes processing, and its information is directly stored in the Digital Twin. Digital Twin serves as a repository for VRU-related data.
4. **Digital Twin to Risk Detection Instance**: The Risk Detection Instance continually receives updates on the positions and trajectories of all moving entities from the Digital Twin. With each update, the Risk Detection Instance assesses the potential for dangerous situations. If a hazardous situation is identified, the Risk Detection Instance notifies relevant parties.
5. **CV Module to Digital Twin**: The CV Module continuously processes images captured by associated cameras and extracts positional information from the detected nodes. This positional information is promptly stored in the Digital Twin, allowing for comprehensive data integration.

These information flows ensure efficient communication and coordination between the modules, enabling the exchange of crucial data for the proper functioning of the system.

2.13.2.7 Alternative Flow

N/A

2.13.2.8 Post-conditions

Once the risks have been mitigated or circumvented, the system continues in operation. The user gets information via a dashboard; but the change in the infrastructure is agnostic to the user.

2.13.2.9 High Level Illustration

See **Figure 50**.

2.13.2.10 Potential Requirements

2.13.2.10.1 Deployment KPIs:

Latency: Average latency (V2V, V2P or V2I) < 50ms.

Age of Information (AoI): Average AoI < 70ms; Average Peak AoI < 200ms

Penalty Age of Information: The penalty function is the L2-Norm between the estimated trajectory and the real one.

Average Penalty Age of Information: < 20.

Average Peak Penalty Age of Information: < 50.

Processing time: < 5 ms.

Neighbourhood Awareness Ratio: must be 100% for distances < 100 meters. There is a tolerance of missing a neighbour for distances from 100 to 300 meters. (Nar above 80%).

2.13.3 CODECO P3: MDS across Decentralised Edge-Cloud

Contact: Telefonica, Luis Contreras Murillo (luismiguel.contrerasmurillo@telefonica.com)

2.13.3.1 Description

P3 focuses on the smart and efficient distribution of media content (e.g., video streaming, gaming, Augmented Reality/Extended reality (AR&ER) across a multi-domain, multi-cluster Edge-Cloud. The use-case therefore leverages on a combined optimization of both connectivity (from the underlying transport network) and computational resources (supporting the MDS streamers and distribution logic).

P3 promotes a tighter computational/networking integration and optimizes the overall resource usage while reaching a good level of *Quality of Experience (QoE)*. To reach this, the use-case focuses on an interaction between a *Media Delivery System (MDS),* via CODECO, and the CODECO component NetMA which shall rely on a decentralized concept of the IETF ALTO protocol[12] to expose capabilities (e.g., topological information together with associated metrics, available resources, or functions) that promote joint adaptation.

The key aspects to be demonstrated concern:

- demonstrating the CODECO informed orchestration of virtualized delivery points with the purpose of selecting the most appropriate Edge facility- according to specific constraints in both the Edge-compute (CPU, RAM, or storage) and the network sides (i.e., latency, bandwidth),
- obtaining a real-time, updated view of the network status, for instance due to optimizing the delivery, for triggering on-demand instantiation of Edge delivery points.

2.13.3.2 Source

HE-CODECO project

2.13.3.3 Roles and Actors

Actors:

MDS platform owner.

Network Infrastructure owner.

Cloud/Edge infrastructure owner.

[12] https://datatracker.ietf.org/wg/alto/about/

MDS content owner.

MDS subscriber.

Roles:

The primary actor is the application-service provider (and network capability client). There are also two secondary actors: the application-service client, and the network operator.

A summary of the business impact is as follows:

To fulfil the ever-changing demands of their clients, companies in the telecommunications sector are continually working to improve their services. Customer turnover is one of the most important issues that service companies must deal with. The revenue and profitability of a firm can be significantly impacted by high customer turnover rates. Service providers are making investments in technology that can raise the quality of the customer experience (QoE) to deal with this problem.

One way to reduce costs without a great investment is optimizing the use of the resources available. To archive this, this use case uses exposure capabilities to allow the network client to select the best path according to the nodes and path characteristics and the internal client information. By this, the telecom operator increases service satisfaction improving QoE. This solution allows better resource use, reducing delivery expenses and optimizing the capabilities available in both network and Edge-Cloud.

2.13.3.4 Pre-conditions

Application workload and respective datasets need to be provided.

Pre-authorization of users needs to be in place.

2.13.3.5 Triggers

Specific nodes in the infrastructure go down, or new nodes enter the living system – critical changes to the infrastructure.

Workload migration is triggered by CODECO (SWM component).

2.13.3.6 Normal Flow

For the CODECO MDS use case, an initial system architecture is defined, which is subject of refinement along the implementation of the use case and the development of the different CODECO components.

For each of the service situations, i.e., single-cluster and multi-cluster, two different system behaviours are exercised.

In the single cluster, understood as baseline case, the MDS will interact with the CODECO components with the objective of optimizing the content delivery considering network metrics in addition to the MDS view of the delivery resources. Such interaction between MDS and CODECO will imply the interaction with the different components (NetMA, SWM, MDM, etc) for multiple purposes. In the following figures, only the NetMA component is highlighted for the only purpose of remarking the interaction with this component for retrieving network information (by leveraging on ALTO).

The operation of P3 in a single cluster is represented in Figure 51. In the single-cluster case, once the end-users request a service to the MDS (step 1), the MDS logic interacts with the CODECO components for retrieving information about the network metrics applicable to the different existing delivery points (step 2). Once this information is retrieved, the MDS analyses the combined compute and network information, including the availability of contents, and takes a decision on what is the more convenient delivery point to serve the end-users (step 3). With that, the end-users access the selected delivery point.

On the other hand, the multi-cluster case is exercise for the optimal instantiation of delivery points across the Edge-Cloud continuum motivated by the presence of end-users in each area. As before, the interaction between MDS and CODECO components implies the interplay with different components, even though only NetMA is highlighted for simplicity.

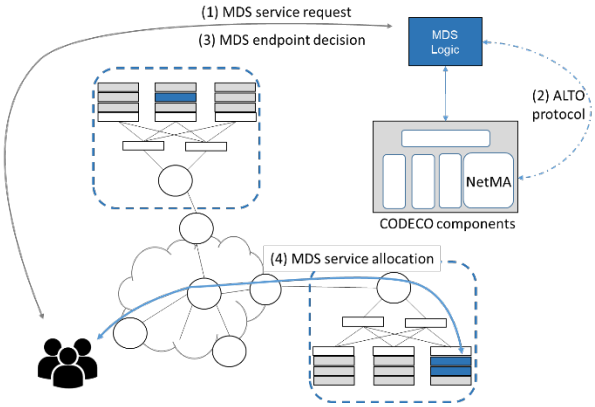


Figure 51: P3 single cluster representation

In the multi-cluster case, the MDS identifies a (potential) end-user base that can drive an optimization of the delivery system (step 1). To identify the more convenient node where deploy a new delivery endpoint in the Edge-Cloud continuum, the MDS logic interacts with the CODECO components to retrieve potential sites where deploy the endpoint collecting both network and compute metrics (step 2). After processing all that data, the MDS logic will decide where to instantiate the new delivery point, optimized from that perspective. The new endpoint will be interconnected with the Origin MDS node as well with the rest of the MDS footprint by means of L2S-M overlay for feeding contents, etc. (step 3). Once the new endpoint is available, the requests coming from the end-users will be served as described in the single-cluster case.

Note that the motivations for the placement of new delivery endpoints can be triggered by other processes and situations, e.g., as for a workload migration triggered by SWM.

As said, the use case will be refined along the progress of the project, so different situations could be documented as part of the single- and multi-cluster cases.

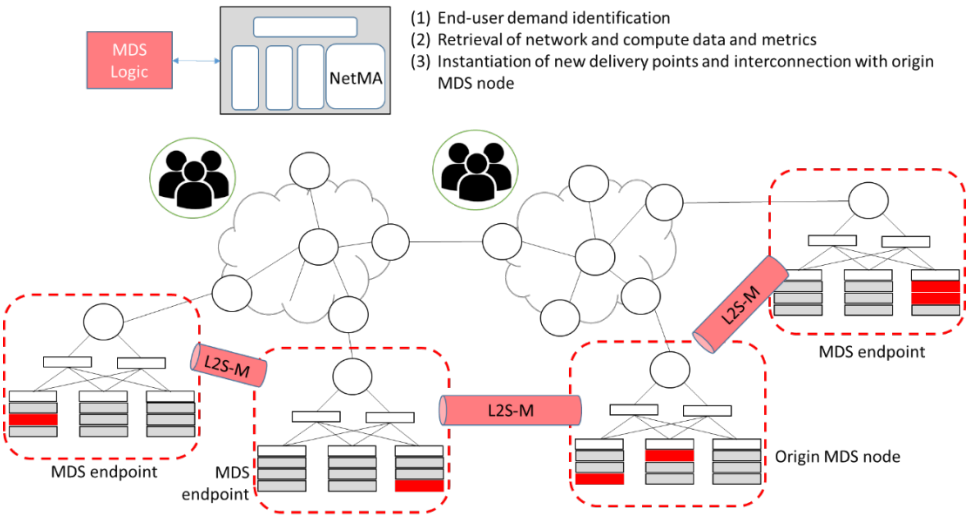


Figure 52: P3 multi-cluster architecture representation

2.13.3.7 Alternative Flow

N/A

2.13.3.8 Post-conditions

After the instantiation of new delivery points to serve end-users, content delivery is optimized and proceeds as indicated in the service.

2.13.3.9 High Level Illustration

See **Figure 51** and **Figure 52**.

2.13.3.10 Potential Requirements

2.13.3.10.1 Deployment KPIs:

Efficiency level achieved in the usage of both computer and network resources.

Reaction time reduction in terms of adaptation execution.

2.13.3.10.2 Non-functional requirements:

Endpoint Authentication: Even the information is not critical, it is needed an endpoint authentication to avoid data poisoning.

Interoperability: System should be multi-vendor and do not have dependencies with the hardware/software used to deploy the UC.

Maintenance: System should be easy to maintain and update, having clear documentation about its parts, how it works and how to update it.

Reliability: System should be able to detect a fall and recover from it. Also, should have a failure-resistant deployment.

2.13.4 CODECO P4: Demand-side Management in Decentralized Grids

Contact: UPM, David Jimenez (djb@gatv.ssr.upm.es)

2.13.4.1 Description

The proposed use case for the distributed energy management system focuses on implementing an active demand response decentralized management system for building decarbonization. It aims to optimize energy usage, improve sustainability, and enhance the resilience of buildings by integrating renewable energy sources and enabling intelligent demand response actions.

The use case also emphasizes the joint orchestration of computational and networking resources to ensure efficient coordination and management of energy-consuming devices and the networking infrastructure within buildings. It focuses on achieving a holistic view of data in the IoT-Edge-Cloud continuum, enabling comprehensive monitoring, analysis, and replication of energy-related data.

CODECO framework leverages the power of K8s to build a decentralized energy management system. By integrating worker nodes (which in this use-case have a correspondence with Edge nodes) and employing the CODECO's developed tools like ACM, PDLC, and modular functionalities, P4 aims at achieving efficient resource utilization, scalability, resilience, and adaptability in energy management operations integrating the energy-related IoT systems and the computing needs.

2.13.4.2 Source

HE-CODECO project

2.13.4.3 Roles and Actors

Actors:

Prosumers

Energy Communities

Aggregators

DSO

Cloud/infrastructure providers

Roles:

Energy service provider: UPM aims to be climate neutral by 2030. To this end, it seeks synergies between generation and energy consumption between its different campuses and its buildings. It leverages Edge computing capacity to make its associated generation and consumption forecasts, and scheduling and optimization models. From them, it decides how to group the different energy assets to achieve the best performance in terms of decarbonisation. This calculation is executed in the Cloud and associated to the physical environment (cluster) defined, where IoT data collected on the real-time operation to take the necessary corrective measures on planning.

Energy community: UPM acting as an energy community wants to offer energy aggregation (offering network flexibility and balance services to the system operator and distributors) and charging services for electric vehicles.

A summary of the business impact is as follows:

The business case for a distributed energy management system lies in its ability to optimize energy usage, enhance grid resilience, and enable the integration of renewable energy sources. By decentralizing energy management, such a system allows for efficient utilization of distributed energy resources, including solar panels, wind turbines, and energy storage devices.

With increasing concerns about climate change and the need to transition to a low-carbon economy, the market demand for distributed energy management systems is growing. This demand is driven by factors such as government regulations promoting renewable energy adoption, rising energy costs, and the desire for energy independence and resilience.

The market analysis reveals a significant potential for growth in the distributed energy management system market. The system caters to various sectors including residential, commercial, and industrial, where energy consumers seek ways to reduce costs, improve sustainability, and contribute to environmental goals. Additionally, the integration of advanced technologies, such as IoT, AI, and blockchain, into these systems further enhances their capabilities and market attractiveness.

Key market players in the distributed energy management sector include energy service companies, technology providers, utilities, and energy aggregators. These players offer a range of solutions, including energy monitoring and control platforms, demand response management systems, and virtual power plant solutions.

The impact of distributed energy management systems is multifaceted. They enable consumers to reduce their energy bills through optimized energy usage and by leveraging locally generated renewable energy.

Additionally, these systems contribute to grid stability and resilience by balancing energy supply and demand in real-time, reducing the strain on centralized power infrastructure. Moreover, distributed energy management systems foster the integration of renewable energy sources, accelerating the decarbonization of the energy sector. They facilitate the transition from a traditional centralized energy model to a decentralized and democratized energy system.

Overall, the high-level market analysis reveals a growing demand for distributed energy management systems driven by energy cost savings, sustainability goals, and the need for resilient energy infrastructure. The market presents opportunities for innovative solutions and collaboration among stakeholders to transform the energy landscape towards a more sustainable and efficient future.

One way to reduce costs without a great investment is optimizing the use of the resources available. To archive this, this use case uses exposure capabilities to allow the network client to select the best path according to the nodes and path characteristics and the internal client information. By this, the telecom operator increases service satisfaction improving QoE. This solution allows better resource use, reducing delivery expenses and optimizing the capabilities available in both network and Edge-Cloud.

2.13.4.4 Pre-conditions

Application workload and respective datasets need to be provided.

Pre-authorization of users' needs to be in place.

2.13.4.5 Triggers

CODECO alerts on abnormal pattern detection

On-demand requests for optimization.

2.13.4.6 Normal Flow

The system architecture represented in Figure 53 is still in a very initial stage of development. Nonetheless it shall rely on CODECO, leveraging a combination of Edge computing, Cloud computing, and K8s for efficient resource allocation, data processing, and decision-making. The architecture consists of the following components:

Edge Devices: These are devices located at various energy generation and consumption points, equipped with sensors, and connected to the local energy infrastructure. Examples include smart meters, renewable energy sources (e.g., solar panels, wind turbines), and energy storage systems. Each Edge device acts as a worker node within the K8s system, capable of performing computations and data processing independently.

Master Node: The master node serves as the central control plane within the K8s system. It manages and orchestrates the distributed resources and tasks across the Edge devices. The master node is responsible for coordinating energy generation, consumption, and optimization algorithms, as well as collecting and analysing data from the Edge devices.

Energy UC Cluster: The Energy UC cluster consists of the master node and multiple worker nodes (Edge devices). It provides a scalable and resilient infrastructure for managing the decentralized energy system. The K8s cluster handles workload scheduling, resource allocation, and load balancing to optimize energy management tasks.

Figure 53: P4 system architecture

The initial proposed workflow for P4 is illustrated in **Figure 54**, for a single cluster deployment.

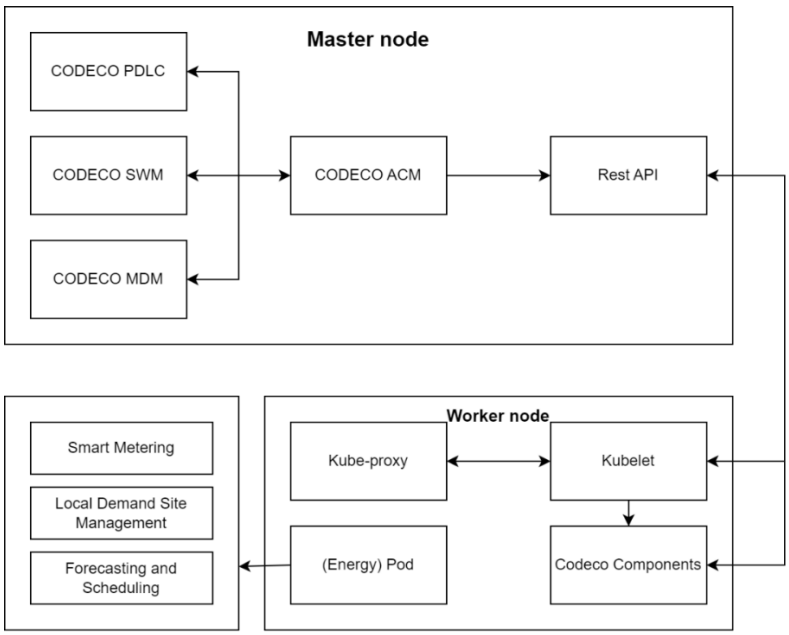


Figure 54: P4 UML use-case diagram

This UML diagram illustrates the flow of data and control in a decentralized energy demand side management system. The sensors collect energy-related data, which is transmitted to the Edge device for local management execution. The local manager handles real-time decision-making and control tasks. For more complex optimization functions, some computing is offloaded to the Cloud, where advanced algorithms or machine learning models can be applied to optimize energy consumption, load balancing, or other energy-related tasks. Internally in each of the pods, there are three specific use-case components:

Smart Metering.

Local Demand Site Management.

Forecasting and Scheduling.

2.13.4.7 Alternative Flow

N/A

2.13.4.8 Post-conditions

Optimized energy consumption.

2.13.4.9 High Level Illustration

See **Figure 53** and **Figure 54**.

2.13.4.10 Potential Requirements

2.13.4.10.1 Deployment KPIs:

Number of buildings involved. (>3)

Energy assets integrated. (>100)

Amount of kilowatt and kilowatt hours of the energy community. (30% UPM consumption)

Amount of energy saved (not bought from the grid). 10-20%

Number of energy clusters created and modified per day. (20)

CO2 emissions reduction. (>10%)

2.13.4.10.2 Non-functional requirements:

Trusted Execution Environments (TEE)

2.13.5. CODECO P5: Wireless AGV Control in Flexible Factories

Contact: Rute C. Sofia (sofia@fortiss.org)

2.13.5.1 Description

There is today an increasing need to consider Automated Mobile Robots (AMRs), of which one example are Automated Guided Vehicles (AGVs) in manufacturing environments, to support the heterogeneous and growing demand of material handling and logistics in flexible factory environments.

While current AGV fleets are based on pre-defined task assignment and pre-defined paths, there is an urgent need to provide a more flexible control to support fleets with a larger number of AGVs, and to support an increasing number of tasks/goods to be transported. By reaching a higher level of autonomy, it is possible to increase overall efficiency while reducing operational costs. The integration of wireless technologies to support the control of AGVs, e.g., 5G, Wi-Fi 6/7, becomes highly relevant and shall be explored by CODECO. However, relying on wireless implies also that the control of AGV systems is prone to interference and intermittent connectivity, thus requiring a higher degree of adaptation which CODECO is expected to provide.

Hence, in addition to the wireless connectivity aspects concerning interference mitigation, synchronization, this use-case shall also demonstrate the CODECO capability to proactively adapt the overall network energy consumption and to mitigate interference and failures.

In this context, the use-case shall explore AGVs handling goods within a warehouse, being subject to remote control and requiring real-time support. The use-case expects to be developed in three phases:

Phase 1, single cluster, static control plane.

Phase 2, single cluster (multi-master), mobile control plane.

Phase 3, federated clusters.

AGVs shall therefore expected to carry different micro-services (dockerized) for a single cluster. In this case AGVs shall correspond to Kubernetes worker nodes, while the control plane shall reside on a static node. The AGV micro-services shall be managed via CODECO, being the CODECO components placed across the control and data plane of K8s. On a second phase, the control plane shall also be deployed on a mobile node.

CODECO shall explore distributed ML approaches considering computation as close as possible to data sources; networking features (e.g., available bandwidth); energy awareness, to assist in a higher degree of autonomy. The CODECO framework will be installed across the fortiss IIoT Lab (expected to reach 10 nodes, mobile and embedded).

The experimental environment will be developed based on realistic scenarios, derived from consultation with manufacturing partners. A final demonstration involving multi-cluster domains will be provided together with an external manufacturing partner of FOR.

2.13.5.2 Source

HE-CODECO project

2.13.5.3 Roles and Actors

Actors:

AGVs (far Edge nodes) – mobile robots with different sensors (e.g., cameras, environmental sensors)

User: user DEV, developer willing to deploy the CODECO AGV App; user Operator, human operators, and respective terminals, remotely assisting AGVs.

AGV fleet Controller node.

Roles:

Deployment of micro-services in an AGV fleet: a user (DEV, developer) wants to deploy a new CODECO offered application in UC5 across an AGV fleet and wants also to manage its application workload with K8s/CODECO.

The user (DEV) shall be able to observe the existing cluster via a CODECO dashboard (9), and be able to make initial adjustments, if required (9).

AGV Fleet control – Resilient infrastructure: This user journey relates with the runtime management of the CODECO AGV Apps. The aim is to assist AGVs in autonomous navigation on indoor, blocked spaces. Key challenges concern energy optimization and support of intermittent connectivity. ICT stakeholders relevant for this use-case are mobile communications, Edge-Cloud providers.

A summary of the business impact is as follows:

The P5 value proposition (VP) canvas is provided in **Figure 55**. The application of CODECO to the context of AGV fleet decentralized control has as customer segments the CODECO target groups DEV (developers), ICT (large industry and SMEs) and AR (Academia and Research). The targeted vertical domains are Manufacturing and Logistics, which correspond to domains where there is an increasing growth in the need of automation and cognitive processes to improve the overall operations in critical environments. With the integration of Industrial IoT and ML, these sectors are experiencing a major change towards decentralisation, as observable in the concept of Manufacturing as a Service (MaaS).

Target customer	VP 1	VP2
Customer perspective	DEV: segment wants zeroconf deployment, low skill investment	ICT, AR, SMEs: zeroconf, scalability, and low cost fleet management, with energy efficiency
Competing alternative	Proprietary solution providing 99.999% reliability High investment in training	Proprietary, customized solution often tailoring 1 cluster. Federated clusters (e.g., remote locations) requires high investment (CapEx and OpEx)
Differentiators		
Performance	**Scalability**, capability of CODECO to cope with an increasing number of application deployments across variable fleet sizes (large, heterogeneous) and towards mobile devices. **Resilience and availability**, capability of CODECO to support five nines system availability in the verge of network interference and intermittent connectivity.	**Privacy,** capability of CODECO to manage a varying infrastructure across a single or different locations (multi-domain environments). **Resilience and availability**, capability of CODECO to support five nines system availability in the verge of network interference and intermittent connectivity.
KPIs	• Time to completion of a task (latency): reduction in 20% due to decentralized control. • 10% of reduction in the number of collisions. • 10% improvement of energy efficiency of the network (overall involved nodes) and eventual network lifetime.	10% improvement of energy efficiency of the network (overall involved nodes) and eventual network lifetime. 10% improvement of total setup times

Figure 55: P5 value-proposition canvas

The proposed solution in this use-case consists of CODECO and of a set of AGV fleet Apps to assist the deployment of the use-case, and to play with CODECO components. The key innovation aspects in UC5 relate with the use of context-awareness and behaviour estimation to provide a higher degree of flexibility to the overall system, thus allowing control of AGVs to be handled in a decentralized way, expected to bring benefits in large-scale environments.

In terms of performance, the application of CODECO in UC5 is expected to improve scalability, resilience, and availability in comparison to K8s, adding also novel support in mobile environments.

2.13.5.4 Pre-conditions

Active AGV fleet interconnected via wireless.

2.13.5.5 Triggers

Node (AGV) with intermittent connectivity.

Node (AGV) goes down due to battery or another failure.

Node (AGV) not capable of supporting an assigned task (e.g., lack of memory, energy, etc).

Network with low link quality.

2.13.5.6 Normal Flow

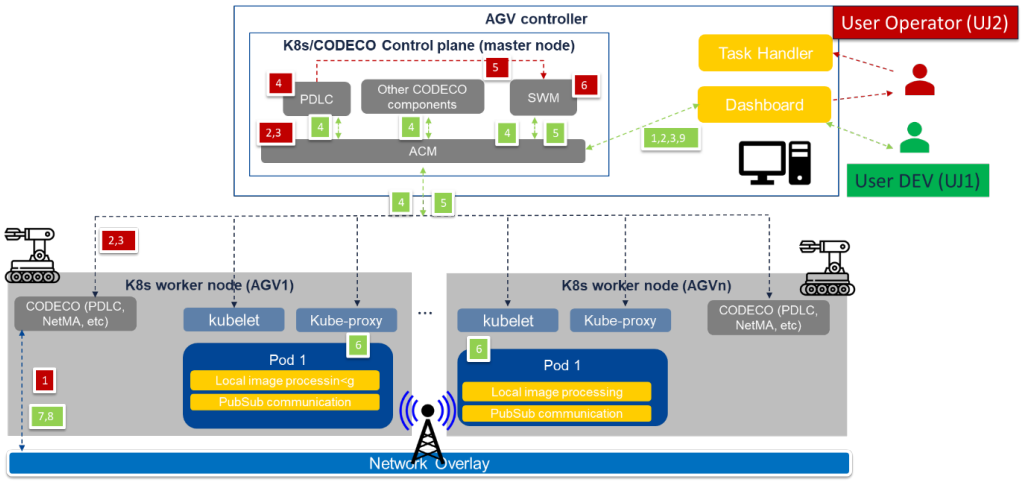


Figure 56: P5 system architecture, one cluster

Deployment of micro-services in an AGV fleet

Rf. To Figure 15. The user wants to deploy a new CODECO offered application in UC5 across an AGV fleet and wants also to manage its application workload with K8s/CODECO. For this purpose, the user starts by accessing the CODECO ACM UI (1) via the available dashboard (AGV controller). The dashboard shall interact with the ACM UI, via a specific customization for the use-case. Hence, via the dashboard the user DEV shall be able to select a pre-defined set of micro-services deployed for the use-case (2). For the initial CODECO AGV App, the UC shall provide a basic set of micro-services available, such as the ones illustrated in Figure 2. For instance, PubSub approach such as MQTT Sparkplug or NDN; micro-service for task handling; micro-service for object detection). Some of these services will be mandatory; some will be optional.

Then, the user is also requested to enter a set of requirements (3), e.g., key requirements such as latency; size of the fleet (how many AGVs to consider); type of communication (e.g., 5G, Wi-Fi); channel aspects, etc. These parameters serve the purpose of creating the so-called CODECO Application model (YAML file(s)), which is key to adequately schedule resources to be used.

Once completed, ACM stores this information (ApplicationModel, CRD format, (4)), making it accessible via the usual K8s methods to other components of CODECO, in alignment with the CODECO CRs/CRDs. SWM starts the initial placement (5). The deployment of the AGV services (ApplicationGroup) is started, being all deployment developed in a single cluster (1 Pod per worker node; 1 AGV corresponding to a worker node) set up by default with all involved nodes that are within range at an instant in time, and that may appear later in the radio range of the controller (6).

For the case of an AGV fleet based on multiple remote locations (phase 2), then ACM shall activate the procedures for federated clusters, instead of deployment on a single cluster. Further development aspects shall be considered during the development of CODECO features for federated clusters (M18-M36).

CODECO shall handle in addition the required network path handling, by taking into consideration aspects such as interference mitigation, channel properties, etc. This shall be handled via the information collected via NetMA for the wireless interconnections across AGVs (7). If required, routes shall be set to optimize the overall communication (8).

The user (DEV) shall be able to observe the existing cluster via a CODECO dashboard (9), and be able to make initial adjustments, if required (9).

AGV Fleet control – Resilient infrastructure

This user journey relates with the runtime management of the CODECO AGV Apps. The aim is to assist AGVs in autonomous navigation on indoor, blocked spaces. Key challenges concern energy optimization and support of intermittent connectivity. ICT stakeholders relevant for this use-case are mobile communications, Edge-Cloud providers.

For this deployment we will investigate existing proposals for AGV communication, e.g., derived from VDMA guidelines and shall consider both a single cluster and a multi-cluster deployment.

On a first phase, we shall consider a centralized approach where the central controller has a global perspective on the overall K8s infrastructure (data, compute, network, (1)) which is regularly updated based on data collected via different CODECO components and managed via the CODECO CRs/operators (2, 3). The CODECO PDLC performs, for this specific scenario, an analysis of robustness of the overall graph, and of the existing links in terms of energy consumption across a pair of nodes, as well as in terms of channel conditions, RTT, between two nodes (4). It can propose an adaptation of the overall communication infrastructure derived from functional and non-functional network requirements to the SWM scheduler (5) which shall then decide on whether to adapt the overall infrastructure (6). Additional re-scheduling supported by CODECO shall take into consideration aspects such as energy consumption. If an AGV is expected to run out of battery in x seconds, then its micro-services shall be passed (replicated or offloaded) to another suitable AGV, automatically selected by CODECO based on the Application model requirements provided by the user.

On a second phase, we shall consider a decentralized approach, where each AGV shall be responsible to transmit its own perspective of the K8s infrastructure at an instant in time to other AGVs. The infrastructure data (data observability, computation, network) is regularly updated by different CODECO operators (2) to the CODECO control plane, which now shall consist of a multi-master cluster. The selection of 3 master nodes per cluster, to ensure resilience, shall be done based on NetMA input (1) to ensure a stronger resilience to failures.

2.13.5.7 Alternative Flow

N/A

2.13.5.8 Post-conditions

CODECO analyses periodically the status of the overall system (data-compute-network infrastructure) continuously proposing adjustments.

Data plane continues without interruption.

2.13.5.9 High Level Illustration

See **Figure 56**.

2.13.5.10 Potential Requirements

2.13.5.10.1 Deployment KPIs:

Time to completion of a task (latency): reduction in 20% due to decentralized control.

10% of reduction in the number of collisions.

10% improvement of energy efficiency of the network (overall involved nodes) and eventual network lifetime

Number of nodes supported (at least 5); reduction in failures (resilience).

2.13.5.10.2 Non-functional requirements:

Scalability, capability of CODECO to cope with an increasing number of application deployments across variable fleet sizes (large, heterogeneous) and towards mobile devices.

Privacy, capability of CODECO to manage a varying infrastructure across a single or different locations (multi-domain environments).

Resilience and availability, capability of CODECO to support five nines system availability in the verge of network interference and intermittent connectivity.

2.13.6 CODECO P6: Automated Crownstone Application Deployment for Smart Buildings

Contact: ALMENDE; Andries Stam (andries@almende.org)

2.13.6.1 Description

In CODECO P6, we will focus on novel mechanisms for automated deployments of smart office/smart building applications on the Crownstone Platform. In this context, an application is defined as a collection of related functionalities realized by means of a set of interconnected application components which can run either in the Cloud, on the Crownstone Hub, or inside a Crownstone Node. The key issue we will address is how the CODECO technologies can help with automated deployment of multiple applications on the Crownstone platform, both in single cluster situations (where multiple Crownstone Hubs form a single manageable entity with a single user base), and in multi-cluster situations (where multiple Crownstone Hubs form multiple manageable entities with different (but potentially overlapping!) user bases).

The Crownstone platform technology has been developed within the Almende group during the past years. The five main constituents of the technology are:

1. Smart lustre terminals called **Crownstone nodes**, which can be mounted inside power outlets. Each Crownstone node has five capabilities: switching on and off (or dimming) the devices attached to the power outlet, measuring the power consumption of the device attached to the power outlet, maintaining BLE connections with wireless sensors and/or actuators, communicating with other Crownstone nodes via Bluetooth mesh, and running small apps called Microapps on the processor inside the Crownstone node.
2. USB-sticks called **Crownstone Bridges**, which are Crownstone nodes with their UART connected to USB male socket, but without the technology to switch on/off devices and measuring power consumption. Bridges are used to connect a Bluetooth Mesh network to a Crownstone Hub.
3. Raspberry Pis with a specific software stack installed called **Crownstone Hubs**. These are used to collect data from larger collections (at most 256) of Crownstone nodes, to process data, to deploy Microapps to Crownstone nodes, and to connect to the Cloud.
4. A Cloud Service called the **Crownstone Cloud,** which serves to administer and exchange information about spheres (i.e., buildings / environments with Crownstone nodes that are connected to each other), rooms, Crownstone nodes, smartphones, and their relationships.
5. A React Native based app called the **Crownstone App**, which lets your smartphone act as a beacon which can be detected by Crownstone nodes and provide a management dashboard for managing all details of the Crownstone platform within a single sphere.

The Crownstone platform was originally developed as a universal domotics solution for the consumer market. However, recently, Almende has decided to make a shift from B2C to the B2B market, offering the Crownstone platform as a universal smart building technology for office environments, industrial environments, etc. This poses completely new challenges on the technology, which are partially addressed in this use case.

2.13.6.2 Source

HE-CODECO project

2.13.6.3 Roles and Actors

Actors:

Crownstone application developers

Building managers

Roles:

A microapp developer develops a microapp to be run on subset of Crownstone in the network, and wants to deploy apps quickly without moving within Bluetooth range to Crownstone, copy-pasting MAC addresses, etc. They set relevant parameters in config file and the microapp deployment manager will make sure the microapps are correctly uploaded to the designated Crownstone.

A building manager wants to deploy applications without worrying about the network topology of Crownstone. They can push a single configuration file and FADO manager will orchestrate the deployment of the applications among the hubs. Any issues around deployment (e.g., resource problems) are fed back to building manager, if possible, with directions for fixing the issues.

A summary of the business impact is as follows:

The management and deployment of crownstones is currently highly centred around the use by consumers. This entails the use of the Crownstone app to manage crownstones, locations and schedules including constraints.

A business-oriented management scenario should enable managing organisations to organise sets of crownstones into spaces, users and (micro)applications. A typical scenario might require the sharing of all users over all buildings, while a set of crownstones cannot currently exceed 256 elements. The option to have multiple sets of crownstones recognising and tracking most if not all users(/assets) is a much-requested feature that will increase the target market.

Our crownstone platform enables the deployment of multiple different applications, developed by multiple third parties, on a single infrastructure inside a smart building, thereby avoiding that every new end user application installed in the building always introduces new hardware components to run the application on. The difficulty, however, is that we need to have better tools to manage and monitor the portfolio of installed applications in a single building or even over multiple buildings, as they share the same infrastructure. Our new tooling will build these tools to overcome this new management problem.

2.13.6.4 Pre-conditions

Medium-to-large-scale buildings with a multitude of rooms equipped with sensors and/or actuators.

Bluetooth mesh topology between crownstones and hubs

2.13.6.5 Triggers

New Crownstone setup across a building or room required.

2.13.6.6 Normal Flow

The Microapp deployment architecture illustrated in **Figure 57** can be divided in a Cloud level, a local (per building/apartment) level and AIoT level.

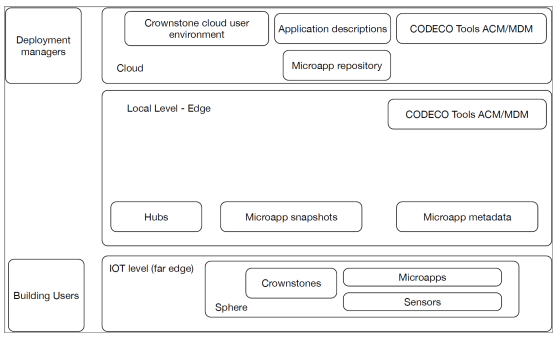


Figure 57: CODECO P6 system architecture

Crownstone are already administered in spheres. A sphere is a collection of crownstones with associated locations (e.g., rooms) and users. A digital twin of this representation is present in the crownstone Cloud.

Microapps can communicate with the crownstones and the local hub, that serves as a relay for the Cloud-based environment. Collections of microapps can be configured (together with optional added sensors) in the Cloud and adapt to the locally available resources.

The Cloud environment will be combined with the CODECO ACM/MDM functionalities to allow for this adaptive distribution and deployment of microapps. The crownstone firmware is already able to receive the microapps. The CODECO MDM functionality will be made available on the hub level to execute the configurations defined at the Cloud level.

The initial UML use-case diagram is provided in **Figure 58**.

Figure 58: P6 UML Use-case Diagram

2.13.6.7 Alternative Flow

N/A

2.13.6.8 Post-conditions

Once the new infrastructure is active, measurements can be performed in the Crownstone mesh.

2.13.6.9 High Level Illustration

See **Figure 57** and **Figure 58**.

2.13.6.10 Potential Requirements

2.13.6.10.1 Deployment KPIs:

Number of deployed Crownstone nodes over time, with CODECO, in comparison to regular operation.

Network reliability over time (K8s as baseline for deployment).

Latency

Throughput

Energy consumption

2.13.6.10.2 Non-functional requirements:

Non-invasiveness (e.g., Crownstone basic functionality always remains).

Privacy-preserving with respect to data captured by sensors related to people in the building and their behaviour.

2.13.7 5G COMPLETE: UC#3: 5G Wireless Transport services with MEC capability provided to NOs

2.13.7.1 Description

5G principles shift the Telecom industry from an equipment-based to a platform-based foundation; from network deployments operated by a single entity to multi-domain, multi-tenant deployments with multi-layer management and orchestration capabilities potentially operated by different parties; from closed networks to open systems making network capabilities, such as data and network services, easily available for customers and partners ecosystems. In other terms, 5G principles pave the way towards a dynamic, flexible way of "provisioning of services and resources as a Service". This shift is collectively reflected in architectural approaches of fully fledged 5G networks, as well as in the early identification of business roles and the associated activities.

For many business and technical reasons related to these key 5G aspects, entities holding the role of NO (mainly Telecom Operators) will be willing to lease (additional) IT/Cloud/Edge infrastructure resources, by establishing collaborations with Cloud/Edge Providers -the latter undertaking the roles of DCSP/ VISP. In this direction for instance, the GSMA and Telecom Operator driven suggestions envision a cross-operator mobile edge platform, featuring openness and inclusivity, to meet the requirements of digital transformation of various vertical industries. To this end, however aspects relating to multi-tenancy, security and (IT/ virtualisation) technologies interoperability are still under investigation.

At the same time, there is a huge trend towards high-capacity 5G wireless transport deployments over advanced (5G) mmWave and THz technologies, aiming to serve both vertical (e.g. for service employment at various vertical sites) and NO high-capacity needs (e.g. for on demand 5G wireless transport service provisioning to end users or/and for backhauling access network nodes). In the aforementioned business context, such 5G wireless transport deployments operated by VISPs can be used for providing resources as a service to NOs on-demand.

2.13.7.2 Source

Text included in subsections related to the 5G COMPLETE is copied from Deliverable D2.2 "Report on Use Cases, System requirements, KPIs and Network Architecture".

2.13.7.3 Roles and Actors

Datacentre Service Providers (DCSP), Virtualisation Infrastructure Service, Providers (VISP), Network Operators (NO), VISP Aggregators.

2.13.7.4 Pre-conditions

Current status, Problem statement - limitations of today's situation. Currently, network and compute resources (e.g., cloud, datacentre) deployments are being operated as closed platforms, with very limited flexibility in terms of service provisioning.

Telecom Operators are holding the roles of DSCP, VISP, NO and SPs cumulatively, operating internal data-centres or establishing partnerships with big cloud providers, usually in terms of hosting user applications at remote clouds. At the same time 5G wireless transport technologies still rely on fixed (with low modification capabilities) allocation of resources with minimum flexibility and basic resource sharing capabilities.

2.13.7.5 Triggers

Therefore, there is a huge gap in technologies supporting flexibly allocated (as a Service), compute and 5G wireless transport resources as virtualized services. At the same time key business aspects such as security, speed of provisioning of "anything as a Service", resilience, and QoS at various levels are still under investigation over advanced (5G) 5G wireless technologies.

Table 5-11: Provisioning of complex virtualisation services to NO.

P-FUNC-10	On-demand provisioning of complex virtualisation services to NO
Priority	Essential
Description	The VISP or SA shall be able to expose (to the NO) the capabilities, characteristics a availability of the multiple domains with which they interact, accept comp virtualisation service requests from the NO as a "compute and 5G wireless transpo network slice and (Co-)provision (along with VISPs) the resources on-demand w specific QoS characteristics reflecting the "Slice" requirements.
Success Criteria	Success Criteria • Capability to provision complex virtualisation services to NO
Use Case	UC#3

Table 5-12: On-demand allocation of 5G wireless transport network resources.

P-FUNC-11	On-demand allocation of transport network resources
Priority	Essential
Description	VISP/Service Aggregator shall be able to provide resources as a service to NOs over a flexible 5G wireless transport network deployment, upon request. The 5G wireless transport network shall therefore expose such capabilities to upper layers. Deployment of a 5G wireless transport topology and allocation of resources to serve NOs needs shall be fast.
Success Criteria	Success Criteria • Wireless transport network exposure level sufficiently developed/ interacting with SA orchestration layers. • Capability to form paths of transport network links on demand. • Capability to self-discover the necessary 5G wireless transport nodes on demand.
Use Case	UC#3

2.13.7.6 Normal Flow

5G-COMPLETE aims to deliver a paradigm for the support of the aforementioned scenarios addressing the following requirements and KPIs from the NOs side, including:

A multi-domain deployment comprising distinct compute domains providing:

Secure multi-tenant operation by incorporating advanced Security at the Edge Cloud via trusted boot and secure execution for workloads.

A Hybrid Virtualization framework offering diverse virtualization capabilities of services deployment.

A wireless transport domain providing:

Self – Organisation (not 3GPP as it refers to transport network nodes) features, leading to optimized usage of wireless resources as well as easy, quick transport services provisioning (towards the 90 minutes service deployment target)

High reliability and resilience by supporting mesh architectures

High (transport) capacity operating at the large spectrum chunks of mmWave (and sub-THz) bands meeting the high QoS requirements of multiple tenants (e.g. more than 1Gbps is needed to support gNB traffic transport (preferably 2Gbps)).

An orchestration layer capable of:

Collecting and processing the topology, capabilities and characteristics of the multiple compute domains to higher Network Operation layers.

(Co-)Provisioning the transport network resources, on-demand with specific QoS characteristics reflecting the "Slice" requirements and taking into consideration the actual placement of services' components that have to be interconnected.

2.13.7.7 Alternative Flow

2.13.7.8 Post-conditions

2.13.7.9 High Level Illustration

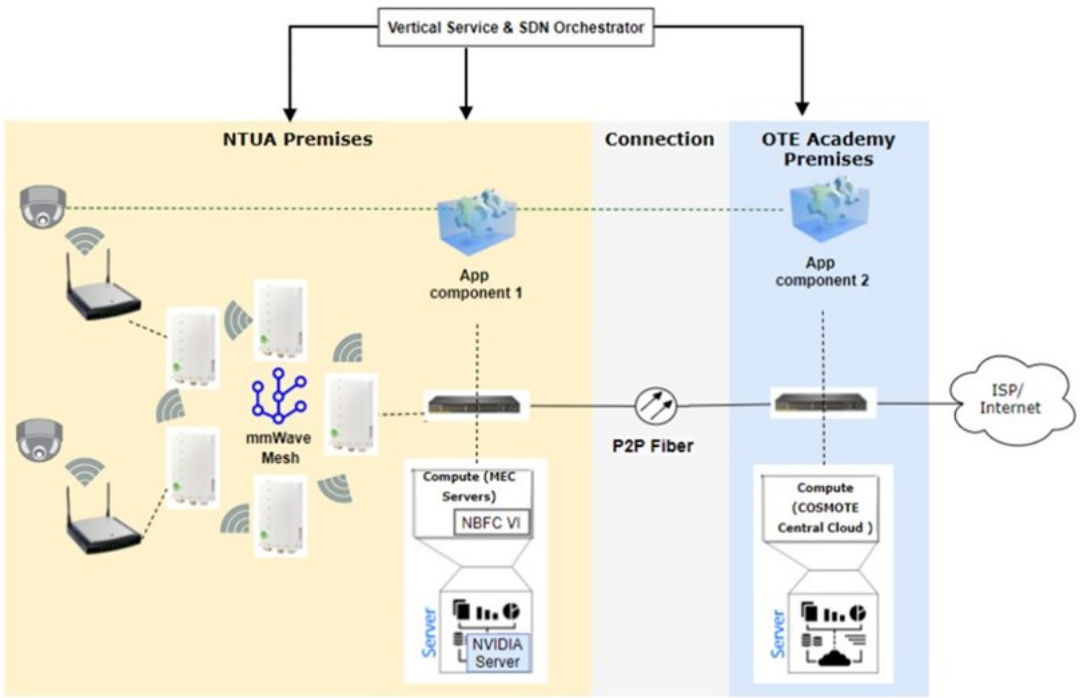


Figure 59: UC#3 - Demo Deployment (NTUA/COSMOTE Facilities)

Slicing Definition: In the context of this UC, Slicing is considered at the 5G wireless transport network part as well as through provisioning of the virtualized compute resources. Slicing information is provided by the NO level and captured at the Service Aggregation level through suitable templates.

Considering the templates, the end-to-end Network Slice description and its requirements are formalized in the Network Slice template, following the relevant 3GPP specification. According to the 3GPP Network Slice Resource Model, the end-to-end Network Slice is composed by different subnets and each of them can target a technology-specific domain, in this specific case, we consider the transport network NSS. For each specified subnet a Network Slice Subnet Template is created, thus containing the related information in terms of requirements and subnets components.

2.13.7.10 Potential Requirements

2.13.7.11 Radio Specific requirements

2.13.7.11.2 Bandwidth requirements

Table 29: High-bandwidth wireless transport network links

P-PERF-12	High-bandwidth wireless transport network links
Priority	Essential
Description	High bandwidth wireless transport network links are required in order to meet the NO high datarate requirements. Optical network can provide scalable solutions for very high datarates at the transport network segments. At the same time, wireless transport network solutions are needed in order to address numerous infrastructure deployment challenges faced by the Infrastructure Provider and NO. Datarates of up to 2Gbps to dedicated last-mile transport links (potentially providing connectivity to gNBs and high datarate Wireless Access Points, e.g. WiFi6) are required to serve the cumulative datarate requirements at the access network nodes' level. Even higher transport network data rates are needed at the transport network segments where transport links are aggregated. 1st level aggregation of at least 4 last-mile transport links is common in network deployments.
KPIs	KPIs: • Capability of last mile transport network links to provide 2Gbps transport capacity. • Capability of transport network to perform 1st level aggregation of at least 4 last mile transport network links.
Use Case	UC#3

Table 30: Resilience

P-OTH-13	Resilience
Success Criteria	Success Criteria: • Demonstrate 5G wireless transport network deployments and functionalities in support of the required resilience.
Use Case	UC#3

2.13.8 5G-INDUCE: ML-Supported Edge Analytics for Predictive Maintenance

2.13.8.1 Description

Data-driven predictive maintenance in factory settings can leverage on the combination of edge and 5G technologies to overcome current computational, performance, speed, data security and sovereignty challenges. The Network Application 4 developed by Suite5 Data Intelligence Solutions, will offer data collection, analytics and visualisation functionalities bundled in separate VNFs that will facilitate business users take advantage of data coming from their shop floor machines, sensors and other data sources, transmitted at high speed through the 5G network and processed within their premises for enhanced security and performance. In particular the experimentation will take place in two manufacturing settings provided by two 5GInduce demonstrators:

Predictive maintenance for power generator – by PPC S.A.

Data provided from a power generator machine available at the PPC premises are used to perform ML-predictive maintenance using edge analytics and federated learning.

Predictive maintenance for thermoforming machine – by Whirlpool Corporation

Edge analytics for predictive maintenance will be applied on the thermoforming machine (COMI5) in the Whirlpool premises. All big data will be transferred via 5G network to the Network Application to be processed, and the specific information will be offered to the user through a mobile device interface.

2. 13.8.2 Source

Text included in subsections related to the 5G-INDUCE is copied from one or more documents that can be found via the following links:

https://www.5g-induce.eu/index.php/outcomes/ (More information in D5.2 - Description of the Experimentation Facilities)

https://www.5g-induce.eu/#experimentation-facilities

https://private.5g-induce.eu/Documents/PublicDownload/144

2. 8.3.3 Roles and Actors

Ford factory in Valencia, Spain, interconnected through Ericsson's edge node technology to 5TONIC test-bed in Madrid.

Public Power Corporation industrial site in Lavrio, Greece, interconnected to OTE 5G laboratory infrastructures in Athens.

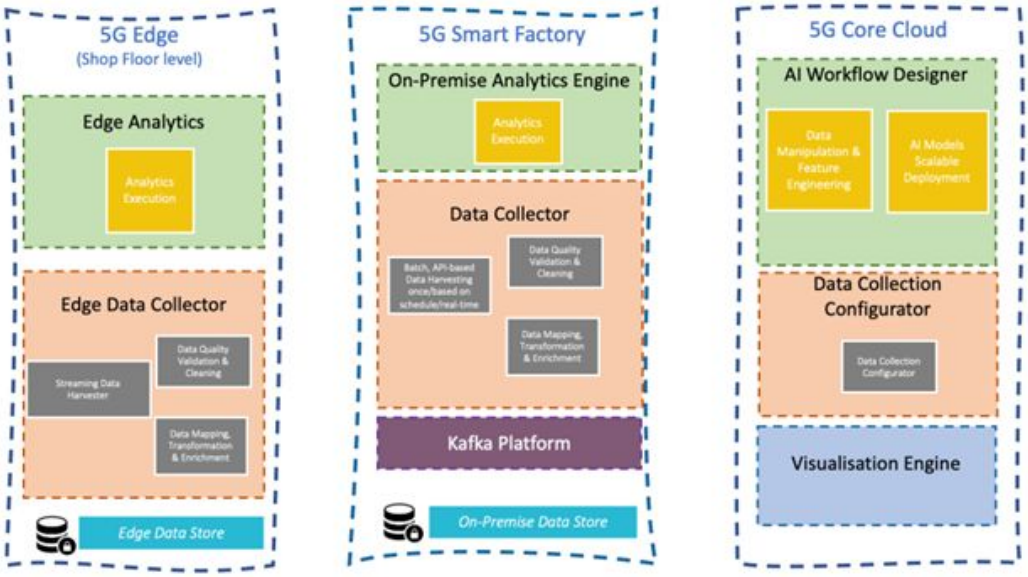
Whirlpool factory in Biandronno (Varese), Italy, interconnected to CNIT's lab infrastructure in Genoa through Wind3 network, serving also as the DevOps testbed for new Network Applications.

2.13.8.4 Pre-conditions

2.13.8.5 Triggers

2.13.8.6 Normal Flow

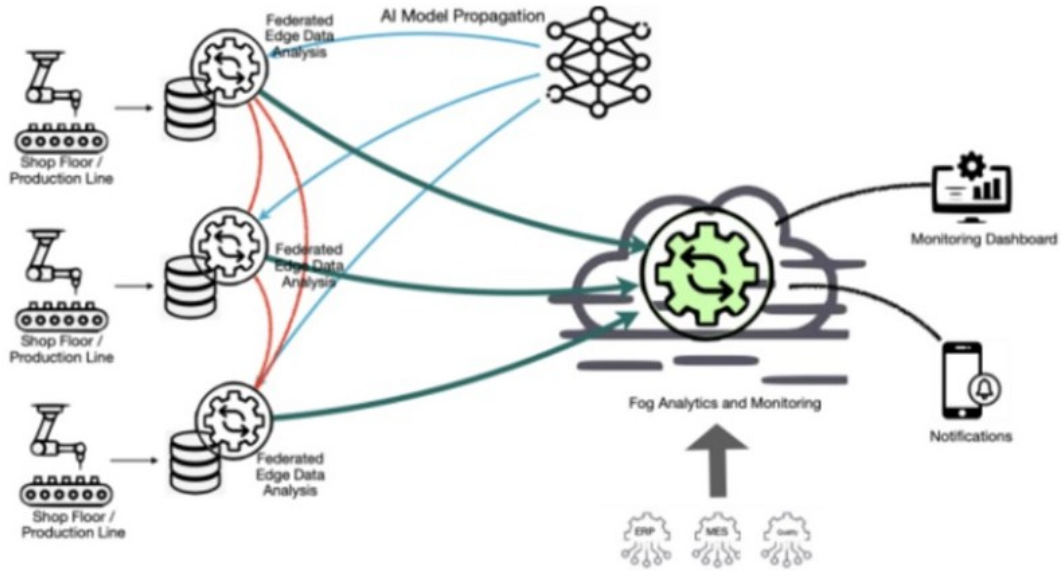
Predictive maintenance is mostly performed with data not being actually real-time nor fine-grained, using aggregations and utilising centralised infrastructures. Thus decision accuracy suffers as ideally computations should be performed at the edge to allow real-time monitoring based on analytics running on edge nodes, and be push instant notifications.



2.13.8.7 Alternative Flow

2.13.8.8 Post-conditions

2.13.8.9 High Level Illustration



2.13.8.10 Potential Requirements

For this use case similar potential requirements apply similar to the use case: "Drone assisted network performance and coverage monitoring for industrial infrastructures".

2.13.9 AI@EDGE: Edge AI assisted monitoring of linear infrastructures using drones in BVLOS operation

2.13.9.1 Description

The AI@EDGE connect-compute fabric, through the use of AI and Edge Computing combined with 5G, will contribute to the so-called '4.0 Industry' revolution in the industrial sector. In this use case, the use of drones in an industrial environment is investigated as a solution to this digitization process to open new doors towards more efficient solutions for surveying and monitoring of large surface areas.

UC3 aimed to validate drone operations within AI@EDGE enhanced 5G network, incorporating AI and Edge Computing functionalities for automated monitoring of road infrastructures in BVLOS mode.

The major outcomes includes:

integration of systems to enable the flight and operation of drones in 5G networks;

development of AI functions to automate monitoring operations; and

deployment of AI@EDGE repository of AI functions.

These results are supported by:

AI@EDGE technical enablers like distributed and decentralized serverless connect-compute platform and AI-enabling application provisioning, and relevant technologies such as AI Functions for incident detection and 3D modelling;

Edge Computing, by deployment of MEC system for accessing AIFs repository; and

advanced Drones enabling BVLOS operation.

2.13.9.2 Source

Text included in subsections related to the AI@EDGE is copied from Deliverable D2.1 "Use cases, requirements, and preliminary system architecture".

2.13.9.3 Roles and Actors

The different actors involved in the use case scenario are as follows:

Drone operator

Infrastructure concessionaires

Technical staff

Infrastructure users

Drone manufacturer and maintainer

5G vendor for the communication infrastructure stack

IT integrators for the management of the computing infrastructure including specialized hardware and software

Within UC3, the roles of the involved partners are as follows:

AERO: AI@EDGE platform integration, UC3 coordination and development of drone automated monitoring functionalities based on AI and edge computing.

ATOS: in charge of transferring WP3 and WP4 technologies to the development of drone automated monitoring functionalities based on AI and edge computing.

EAB: will contribute to the transfer of WP3 and WP4 technologies; in coordination with its Ericsson Spain branch (ERI-ES), EAB will provide pilot testing facilities through the 5TONIC experimental facility located in Madrid (Spain) [28].

ITL: in charge of integrating HW acceleration features in UC3 experimentations, in coordination with WP5 activities.

2.13.9.4 Pre-conditions

The monitoring of large areas (plots, farms, roads network) through the use of drones is a highly demanded service today, which however suffers from both practical and technical limitations that currently prevent a widespread application.

2.13.9.5 Triggers

One of the most relevant limitations are inefficient communications, both command and control (C2) communications and for remote transmission of images, data or information to be processed in a head-end computing infrastructure.

Table 31: Use case 4 identified risks and envisaged mitigations actions

Use case 3 Identified Risks	Mitigation Actions
Hardware: Weight and size of the physical device associated with the AI@EDGE platform to be integrated onboard allowing an optimal operation. Physical devices associated with the AI@EDGE platform have high power consumption, preventing acceptable flight time.	If the physical device associated with the AI@EDGE platform cannot be integrated onboard (either by weight and size or power consumption) its functions could be, partially or totally, offloaded to a ground station.
Scenario: Stability of radio access connections linked to the status of 5G deployment in the selected area for the use case.	Focus on AI@EDGE platform features that better suit the use case and its technical requirements.
Access to full range of functionalities: Related to network deployment in the selected area: 5G connexion is NSA instead of SA.	If the 5G status on the use case area is not optimal to efficiently perform the operation, repeaters to extend 5G coverage will be deployed.
Equipment on board: Interferences with other drone equipment (controller, GPS satellites, etc).	Pre-checks and damping measures in case of detected interferences or different positioning of the equipment inside the drone.
Connection: Data corruption between the operator and the drone prevents proper control of the last one because of the state of 5G connection.	Automated procedures will be applied until the drone regains connection i.e., intelligent RTL (Return To Launch) function will be fully available.

2.13.9.6 Normal Flow

This UC3 is aiming to expand the AI@EDGE connect-compute fabric border to the drone embedded system, in order to use 5G capabilities to take care of the above-mentioned problems. The drone will be controlled in a BVLOS (Beyond Visual Line of Sight) mode through 5G, to scan industrial infrastructures, to make corresponding 3D modelling, then to identify the different incidents that could exist and to send notifications to the drone operator alerting that an incident has been found. Meanwhile, the information (images, telemetry) is sent in a continuous manner to the central office in order to improve the drone's operator decision-making process.

2.13.9.7 Alternative Flow

2.13.9.8 Post-conditions

The UC3 testbed will be built on top of the 5TONIC laboratory [28]; situated in Madrid (Spain), it is an open research and innovation laboratory focusing on 5G technologies. The testbed specific hardware allows configuring different network topologies of variable size and capacity that will be used to emulate a 5G network. It can provide a NFV infrastructure, 30 mini-PC computers supporting the experimentation with VNFs at smaller scale, as well as the management and orchestration of virtual machines. This setup allows the deployment and/or testing of different NFV/SDN domains, multi-layer control & orchestration, multitenancy NFV/SDN and multi-vendor NFV/SDN. In this section it is explained how the 5TONIC laboratory will be extended for the UC3 testbed and employed to emulate the real scenario.

2.13.9.9 High Level Illustration

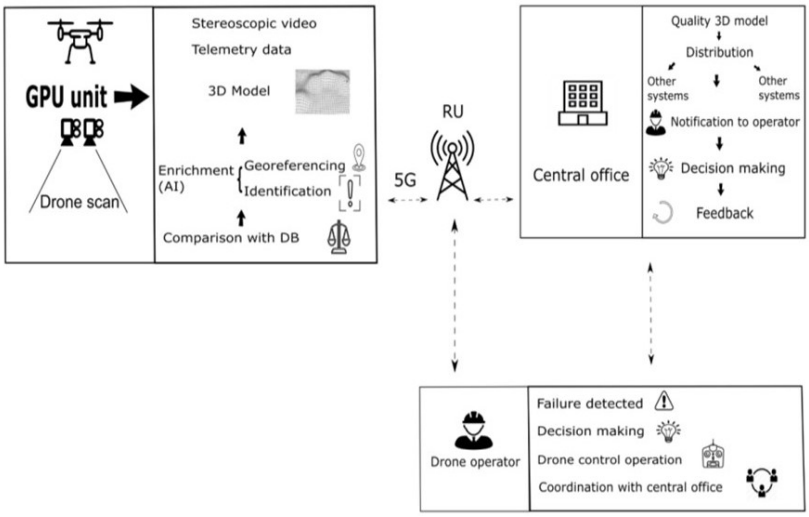


Figure 60: Use case 3 context

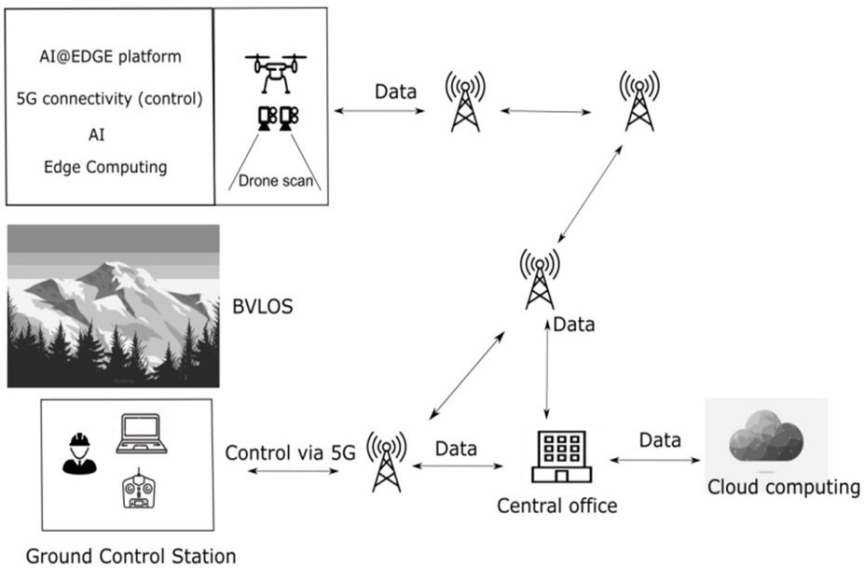


Figure 61: Example of use case 3 scenario

In a reference scenario, depicted in Figure 7, the drone is controlled via 5G in BVLOS mode by the drone operator. The figure describes the path followed by the data highlighting the continuous communication between the drone operator, the drone itself and the control centre. This communication is bidirectional between these three elements in order to coordinate all the actions and take the best decision.

The UC3 architecture, already represented and described in Figure 6 and 7, will leverage on the AI@EDGE fabric features. In particular, the following technological enablers forming the AI@EDGE fabric will be used in this use case:

Distributed and decentralized serverless connect-compute platform.

AI-enabled application provisioning.

Network and service automation platform.

Hardware accelerated serverless platform for AI/ML.

2.13.9.10 Potential Requirements

In this section the UC3 requirements are presented, as grouped in terms of technical features, security and privacy aspects and KPIs.

Security and privacy requirements

Two different security levels can be distinguished:

High: The drone control channel must have the highest security level possible in order to limit radio interferences as much as possible.

Low: The data transmitted (video, datalink) also needs to be protected but it has less importance in terms of security. These levels could correspond to different slices, or even be within a given slice. Privacy: The main restriction founded on this aspect are video-images recorded subject to data protection. These images should be only accessible by the drone operator and central office, so that no external agent can view or use them.

Key Performance Indicators (KPIs)

Four main KPIs are of particular interest for the use case and are detailed in the following.

Environment KPI: Range: geographical reach of at least 20 km (according to the state of 5G technology and deployment at the trials).

Drone operation KPIs:

The latency KPIs sets as 100ms the maximum end-to-end latency budget. It is composed of two components:

Control Signal latency: it should be the lowest possible, and lower than 50 ms based on current awareness on the general system.

Video processing latency: it should be the lowest possible, so that the total end-to end latency budget lays below 100 ms.

A more precise assessment on the acceptable latency budget is needed to possibly update these preliminary figures, which will be done in WP5.

The reliability KPI (tentative metric) is in terms of control signal packet loss which should be lower or equal than 1%. This value is set because control signal must be ensured at all times.

AIF KPI: Mean Average AI Precision in object detection: in the integration of AI-assisted drone framework on the 5G network, detecting incidents through AI analysis processed on-board and at edge-node to generate response action from centralized control station. The metric commonly employed to evaluate the performance of the model for automated detection of incidents in the scenario is the Mean Average Precision (mAP), with an Intersection over Union (IoU) equal to 0.5. This target KPI for the AI@EDGE project, according to the dataset used for the project, will be mAP@.5 >= 0.6 (defining classes as identifiable items such as "persons" or "vehicles") - mAP@.5 refers to the mean average precision at an intersection over union value of 0.5.

2.13.9.11 Radio Specific requirements

Technical requirements Network Bandwidth and Slicing: The required 5G radio bandwidth will be proportional to the video definition and the number of users observing it through the 5G network, in this case the central office and the drone operator.

With respect to slicing, a secure and isolated environment is required to prevent interferences with external operators.

Computing: An edge computing/AI device or system of devices that allows to make an onboard 3D monitoring in real time for the use case application. Video data beamer bit-rate: the video stream bitrate needs a speed of at least 5 Mbps (HD) and it would be great to achieve Full HD or 25 Mbps (Ultra HD).

2.14 Smart Agriculture

2.14.1 COMMECT: Monitoring of Pest Insect Traps

2.14.1.1 Description

Olive tree is a plant native to the Anatolian region, and its main products (olive fruit and olive oil) have been considered important food and commercial products since ancient times. In recent years, with the increasing interest in healthy life and nutrition in the world, the importance of the production and consumption of table olives and olive oil is increasing. Türkiye constitutes a vital gene pool with 93 domestic olive varieties. Modern planting systems, mechanization and digitalization are taking place rapidly in olive farming around the world. On the other hand, Türkiye is not at the same level as developed countries in terms of integrating technology and digitalization into olive farming. The biggest reason for this is the low-income level of olive farming producers and the lack of telecommunication coverage in the countryside. Lack of agriculture knowledge of the olive producer, difficulty accessing digital products, and technological infrastructure can be counted as other reasons. Experts' training of rural people, eliminating the deficiencies and mistakes in traditional olive farming, is expected to positively affect the yield and quality and contribute to Türkiye's economy. Our main intention is to make the right timely decisions to produce higher-yielding quality olives via monitoring the environmental and pest population to better plan their olive orchard activities.

2.14.1.2 Source

Bridging the digital divide and addressing the need of Rural Communities with Cost-effective and Environmental-Friendly Connectivity Solution (COMMECT) HE project

2.14.1.3 Roles and Actors

Olive farmers who undertake the daily work and management of the olive orchard, are mentioned as one group of essential stakeholders. This group is more vulnerable and uninformed about the effects of climate change, disease outbreaks, and economic changes and uncertainties.

Olive processing industrialists in the value chain after olives have been harvested. This group also comprises representatives from cooperatives and olive production unions.

Olive machine producers who produce process machine for table olive and oil olive for the farmers and industrialists.

2.14.1.4 Pre-condition

The main pre-condition is to live with the potential risk of monitoring pest insect traps that could increase the insect population surrounding orchards that do not use these traps.

2.14.1.5 Triggers

The agricultural sector has become increasingly reliant on technological advancements in recent years. The Internet of Things is a new technology expected to boost productivity in farming and agricultural activities, leading to higher yields and lower costs per kilogram of olives. Olive agriculture worldwide rapidly adopts modern planting systems, mechanization, and digitalization.

2.14.1.6 Normal Flow

Commonly, the steps are the follows:

1. Olive fruit fly is the primary pest of olive orchards and causes a significant amount of yield and quality losses. The larvae of olive fruit flies give rise to direct damage.
2. Larvae from the egg eat the fruit flesh by opening galleries around the seed. Its damage in the olive sector is essential since it causes the fruits to decay and the acidity in the olive oil to rise.
3. Pesticides are applied when necessary and on time. This is possible by monitoring the olive fly adults in nature.

4. Spraying should be done before the olive fly becomes harmful by using digital traps to identify the first flies, such that when the number and species of pests exceed a certain threshold.

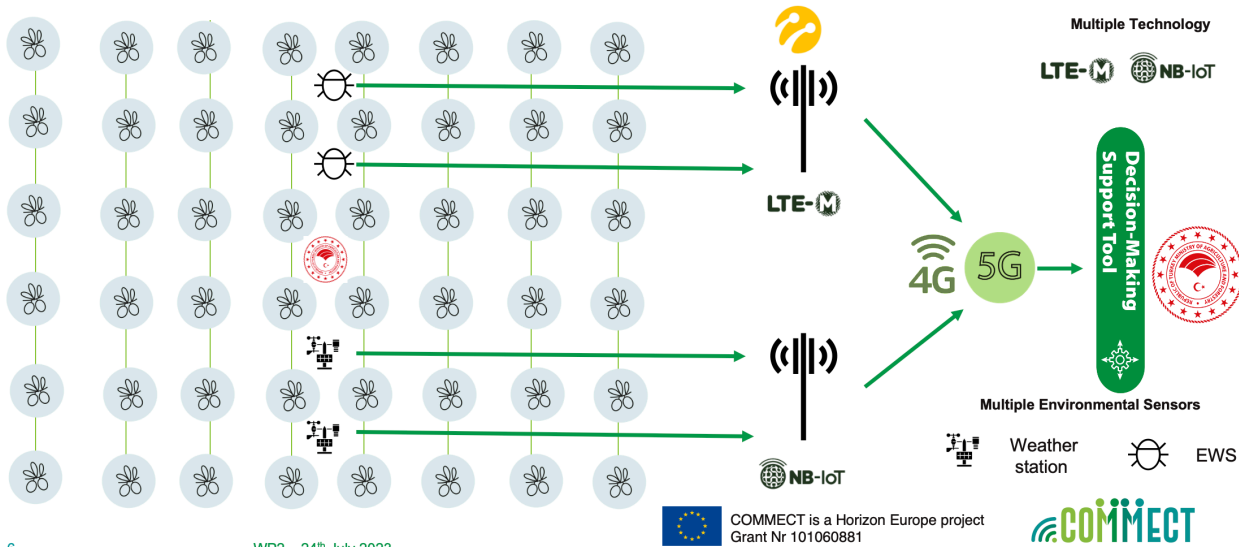
2.14.1.7 Alternative Flow

N/A

2.14.1.8 Post-conditions

Once the risks have been minimized or solved, the olive pest insect traps inform the farmers and industrialists about the population of the insects.

2.14.1.9 High Level Illustration



2.14.1.10 Potential Requirements

The following requirements have been defined for this use case:

Fly Detection Accuracy: potential risk analysis based on olive fruit fly population

Uplink Throughput: uploading of machine vision pest monitoring photo

Power Consumption Decrease: extended battery durability of sensor equipment

2.14.1.11 Radio Specific requirements

Does the radio link crosses public spaces? Or is it constrained to indoor or customer premises?: The base stations give services to the traps and, at the same time, the mobile network operator customers in the region, like rural or suburban areas. The side to side distance is approximately between 5-10 km in rural or suburban areas

Mobility: No mobility is needed

2.14.1.11.2 Bandwidth requirements

Peak data rate: 4 Mbit/s

Average data rate: 2 Mbit/s

Is traffic packet mode or circuit mode? Packet mode

2.14.1.11.3 URLLC requirements

N/A

2.14.1.11.4 Radio regimens requirements

Desired and acceptable radio regimens: Licensed – public mobile.

2.14.1.11.5 Other requirements

UE power consumption

Rechargeable or primary battery? Rechargeable battery

Acceptable battery life: 10 years

Is terminal location required? location accuracy? No, it is not needed.

2.14.2 COMMECT: Securing crops and equipment

2.14.2.1 Description

Use Case titled "Securing Crops and Equipment," is implemented in the context of the COMMECT project and its Living Lab Serbia initiative. It aligns with the increasing demand for digitalization in agriculture focusing on deploying edge ML computing to address challenges in agriculture, such as securing assets from theft, monitoring growth of the crops, and supporting improvement of the overall operational efficiency of agriculture activities in the field.

Implementation of the use case involves several key steps. First, video cameras and edge ML devices are installed in the field, powered by renewable energy sources with battery backup to ensure sustainable operation. These devices are configured and managed remotely, allowing for energy-efficient adjustments and the customization of machine learning models to meet field-specific requirements. Data is then continuously captured and video streams analysed to get insights into the growth of the crops as well as to identify suspicious activities by detecting people and vehicles in the field. , and. The performance of the edge devices is monitored to balance processing power and energy use. Remote management capabilities further enhance the adaptability and reliability of the solution enabling dynamic changes of AI algorithms based on the needs of agricultural operations.

Living Lab Serbia focuses on advancing sustainable agriculture and preserving the natural environment in Gospođinci village, located in the Vojvodina province of northern Serbia. This initiative encompasses five diverse use cases, each addressing critical challenges in rural development. Through these use cases, Living Lab Serbia provides practical demonstrations of how cutting-edge digital technologies can empower local communities, optimize agricultural practices, and protect biodiversity.

2.14.2.2 Source

Bridging the digital divide and addressing the need of Rural Communities with Cost-effective and Environmental-Friendly Connectivity Solution (COMMECT) HE project

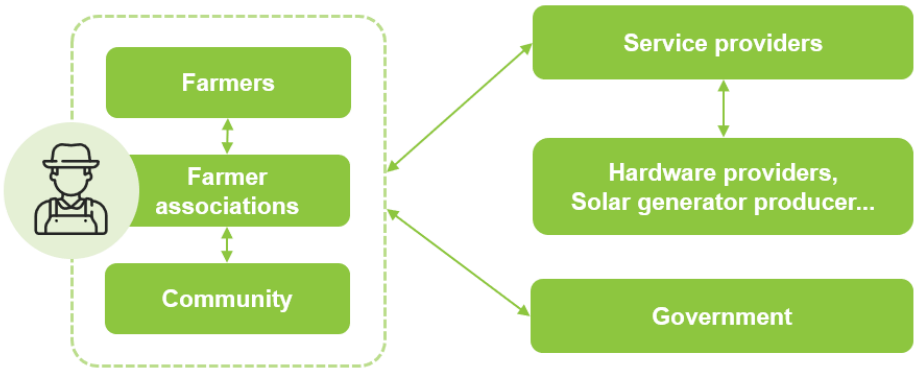
2.14.2.3 Roles and Actors

Use case "Securing crops and equipment" involves several key actors, each playing a vital role in its implementation and success:

Farmers and Farmer Associations are the primary end users and beneficiaries. They adopt improved agricultural practices, integrate digital solutions, and collaborate in data sharing to optimize farming operations.

Companies (e.g., digital service providers, hardware manufacturers, solar trailer producers) are responsible for providing power and network infrastructure along with IoT devices, deploying solutions, and training farmers to use technology effectively. These companies also utilize pilot sites to test and refine their products and services, promote sustainable practices, and foster knowledge exchange and community collaboration.

Local government entities act as policy enablers and regional development supporters. They establish agricultural policies and regulations, attract investments, and encourage sustainable development while working to preserve natural habitats and ecosystems.



2.14.2.4 Pre-conditions

The successful implementation depends on meeting the following conditions:

Technical pre-conditions

Infrastructure readiness: Edge ML devices with sufficient processing power and reliable power supplies must be available to support operations in remote areas.

Connectivity: A stable communication network (e.g., LoRa, 4G/5G, or Wi-Fi) is essential for transmitting alerts and data securely using robust protocols.

Device setup: Cameras must be installed and calibrated to capture accurate video data, covering key monitoring areas.

ML model deployment: Pre-trained ML models optimized for detecting people, vehicles, and audio patterns should be deployed and configured on edge devices.

Non-technical pre-conditions

End-user training: Farmers and users must be trained to operate the system, interpret data, and respond to alerts effectively.

Stakeholder engagement: Collaboration among farmers and technology providers.

2.14.2.5 Triggers

Specific triggers are necessary to initiate actions such as analyses and alerts, based on real-time data processing:

Detection of movement: When people or vehicles are detected in the monitored area, the system analyzes video feeds to identify activity and sends picture with captured object and alert (e.g., SMS or app notification).

Crop monitoring events: Significant changes in crop growth parameters (height, size, or signs of stress) and activity tracking (spraying, plowing, sowing) providing actionable insights for job management.

2.14.2.6 Normal Flow

The typical operation involves seamless data exchange between key components, following these steps:

Continuous data collection: Cameras deployed on edge devices, powered by a mobile solar generator with battery backup, capture real-time video streams from the monitored area.

Real-time data processing: Edge computing devices analyze collected data using ML algorithms, detecting and counting people or vehicles and monitoring crop growth. Each device processes at least two video streams simultaneously.

Event detection: Potential threats or events, such as unauthorized vehicles or theft attempts, are identified by classifying anomalies based on trained ML models.

Communication with IoT Platform: Data is transmitted from the edge devices through switch to a router which forwards data to the IoT platform and agroNET solution via a 4G network.

User notifications: Alerts and insights are sent to farmers via mobile or web applications, providing information on detected events.

Remote monitoring and configuration: configuration of edge devices, updates and changes of ML algorithms, monitoring power consumption, and optimizing battery usage.

2.14.2.7 Alternative Flow

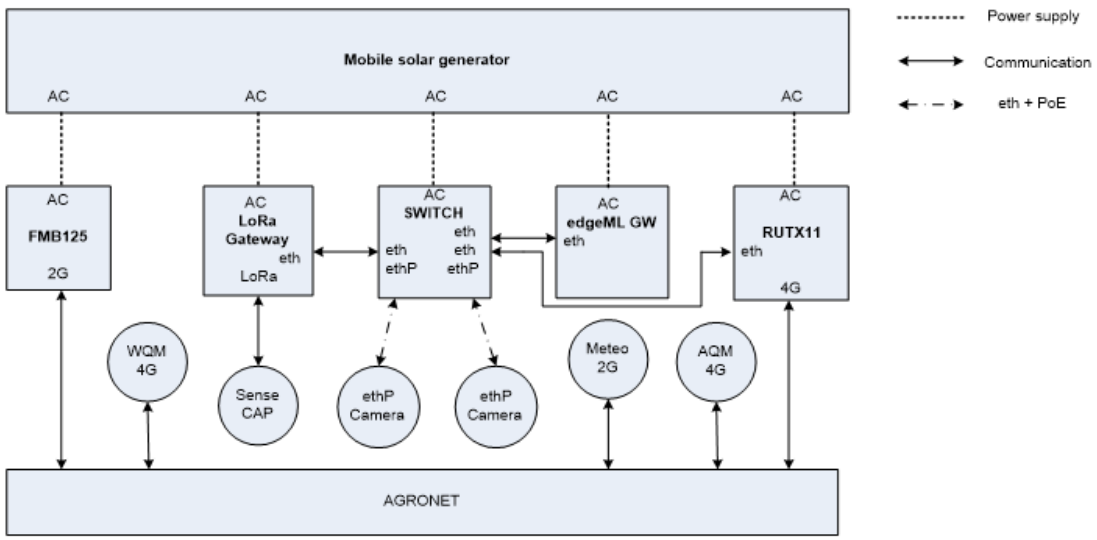
N/A

2.14.2.8 Post-conditions

Once the use case is deployed and the system is fully operational, farmers will have a solution for monitoring and securing crops and equipment. The system will notify farmers when anomalies are detected, sending pictures and relevant data to the agriculture platform for further analysis and action.

2.14.2.9 High Level Illustration

The system architecture integrates this use case with others implemented within the Living Lab, as illustrated in the figure below.



2.14.2.10 Potential Requirements

Technical requirements:

Video processing: The edge computing infrastructure must support real-time processing of video streams. The insights generated can be variable, depending on the needs of particular agricultural operations and deployment context. A minimum of two video streams should be processed simultaneously.
Edge ML remote configuration: power consumption, battery status, and power requirements of active ML algorithms must be monitored. Edge devices should be remotely configurable to optimize power consumption as needed.
The table below summarizes technical requirements for this use case. Table is copied from *Deliverable 1.2 Report on COMMECT requirements and KPIs*.

1. Requirement ID	2. Description	3. Technical Requirement(s)	4. Target Value
R5.8	Edge ML computing infrastructure	Video processing	>=2
R5.9	Power consumption and power requirements monitoring	Edge ML remote configuration	Remote configuration supported and enabled.

Non-functional requirements:

Flexibility: The system must be adaptable to various agricultural environments, crop types, and evolving technology requirements.

Integration capability: The system should seamlessly integrate with existing technologies and digital IoT solutions.

Continuous operation: The system must ensure continuous operation to maintain effective security and crop monitoring functions.

2.14.2.11 Radio Specific requirements

2.14.2.11.1 Radio Coverage

Outdoor radio link

Low power, long-range for sensors in the field

WiFi or cable for video cameras

Mobility is welcome, but not mandatory

2.14.2.11.2 Bandwidth requirements

The solution addressing the use case is designed to maximize the edge processing and minimize the amount of data transferred to cloud. Current 4G connectivity supports well the scenario. However, if edge processing is not used and more remote management required (e.g., remote control of drones monitoring and spraying crops), that increased throughput and minimal latency would be required.

2.14.2.11.3 URLLC requirements

N/A

2.14.2.11.4 Radio regimens requirements

No particular requirements. What is important, is availability of reliable communication network.

2.14.2.11.5 Other requirements

Sensors: long duration battery (at least one season), replaceable or rechargeable.

Edge: rechargeable without interruption.

Ability to automatically determine location of the edge server is preferrable. GPS accuracy. Location of sensors is welcome if it does not significantly impact the battery lifetime.

3. Emerging Topics

This section describes emerging topics that are related to IoT and Edge Computing and can impact the specifications and deployments of 5G. Those emerging topics are:

1. Digital Twin (DT)
2. Deep Edge, Terminal and IoT Device Integration in B5G communication infrastructure
3. Edge, Mobile Edge Computing and Processing
4. Network and Server security for edge and IoT
5. Plug and Play Integrated Satellite and Terrestrial Networks
6. Autonomous and Hyper-connected On-demand Urban Transportation
7. Opportunities for IoT Components and Devices
8. EU legislative framework.

3.1 Digital Twin

It is important to define the meaning of Digital Twin (DTw) concept before proceeding, as it has been interpreted in many ways in the past years. It is important to have a common understanding what are implication of such concept and, more, to properly address possible impact and benefits of this approach considering adoption of 5G.

The Digital Twin in its original form is described as a digital informational construct about a physical system, created as an entity on its own and linked with the physical system in question. One of the first domain it was adopted was in Aerospace Industry, where it was referred as "To address the shortcomings of conventional approaches, a fundamental paradigm shift is needed. This paradigm shift, the Digital Twin, integrates ultra-high fidelity simulation with the vehicles on-board integrated vehicle health management system, maintenance history and all available historical and fleet data to mirror the life of its flying twin and enable unprecedented levels of safety and reliability." [TaQi19].

In such perspective the key aspect referred to DTw is the accurate representation of the structure, the status and the actual behaviour of a physical object in term of collection of relative data. The most relevant aspect is in such way associated to be able to collect in "proper" way enough and with adequate granularity information or in other words Digital Twin in its origin describes a product mirroring its available informational status.

Based on the given definitions of a Digital Twin an evolution took place to represent increased capacity of DTw to provide enriching services based on embedded technologies able to structure, elaborate and forecast the information related to the physical object. So, in manufacturing domain, one new definition can be adopted to better describe this aspects. "The DT consists of a virtual representation of a production system that is able to run on different simulation disciplines that is characterized by the synchronization between the virtual and real system, thanks to sensed data and connected smart devices, mathematical models and real time data elaboration. The topical role within Industry 4.0 manufacturing systems is to exploit these features to forecast and optimize the behaviour of the production system at each life cycle phase in real time." [TaCa19].

A relevant aspect that needs to be considered is now the way the DTw interact with the physical world, in fact we have for sure the need to gather information to "build" the basic content of the digital twin, but other important questions emerge:

1. Data collection is carried out manually or automatically?
2. Data collection is executed only once at the creation of the DTw or carries on for its entire life?
3. Internal representation of the physical object is static or is dynamically updated?
4. Any possible result of DTw elaboration can be "returned" to the Physical object to improve its behaviour (efficiency, safety, duration,) or to a third entity to provide any value?

Before answering in full to these questions, let first focus on the interactions between Physical Object and DTw. We introduce this terminology for DTw, as digital counterparts of physical objects. We consider these definitions: Digital Model, Digital Shadow and Digital Twin strictly speaking, see [Glaes12].

A Digital Model is a digital representation of an existing or planned physical object that does not use any form of automated data exchange between the physical object and the digital object.

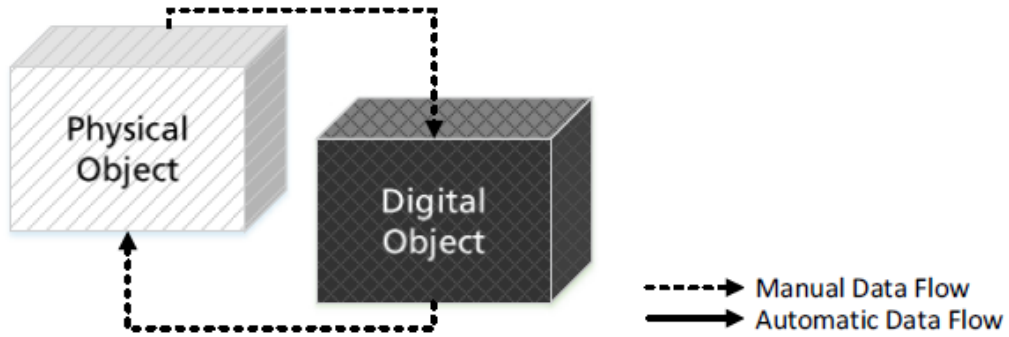


Figure 62: Data Flow in a Digital Model

Based on the definition of a Digital Model, if there further exists an automated one-way data flow between the state of an existing physical object and a digital object, one might refer to such a combination as Digital Shadow.

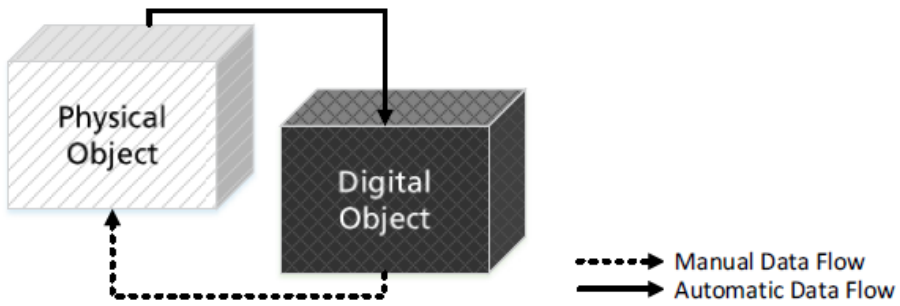


Figure 63: Data Flow in a Digital Shadow

If further, the data flows between an existing physical object and a digital object are fully integrated in both directions, one might refer to it as Digital Twin.

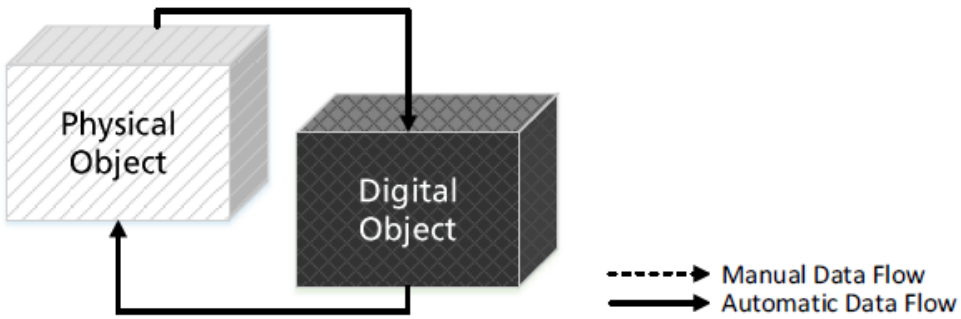


Figure 64: Flow in a Digital Twin

A more structured representation of DTw that encompasses an advanced bi-directional information flow between physical and digital entity and internal capacity able to elaborate and enrich information including capability to provide added value or services.

We can represent it with the following representation in Figure 65, see [GaRo12].

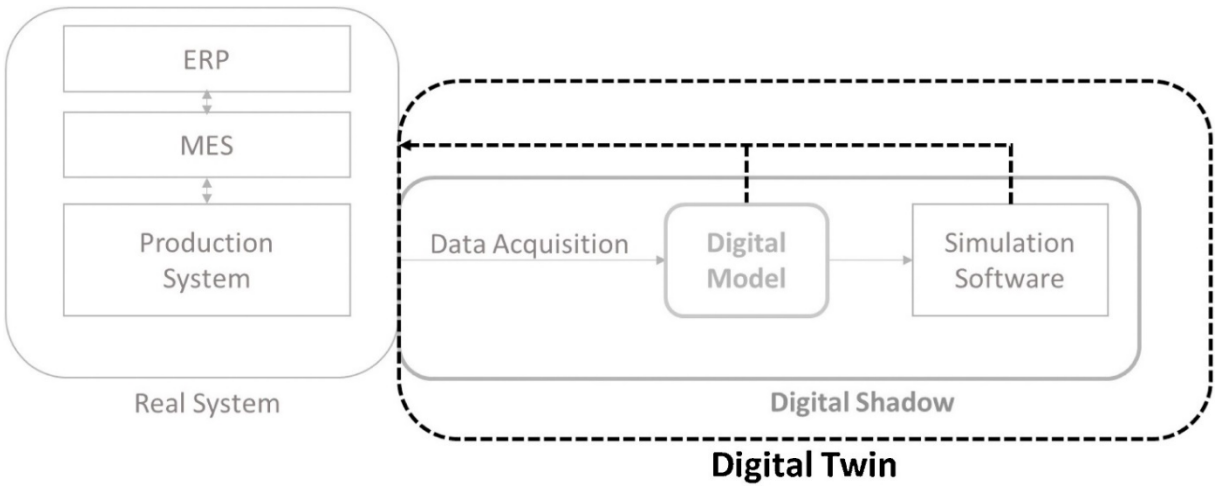


Figure 65: Digital Twin (DT) schema, copied from [GaRo12]

State-of-the-art technologies such as the IoT, Wireless and Mobile Communication, cloud computing, big data analytics, and AI have greatly stimulated the development of smart manufacturing. An important prerequisite for smart manufacturing is cyber–physical integration, which is increasingly being embraced by manufacturers. As the preferred means of such integration, CPS and digital twins have gained extensive attention from researchers and practitioners in industry, see [KrKa18]. The essence of CPS is to add new capabilities to physical systems using computation and communication, which intensively interact with the physical processes and, if needed, is able to involve as part of the process also human operators and/or decision makers, providing added value services all along the lifecycle of the production process and eventually of the product.

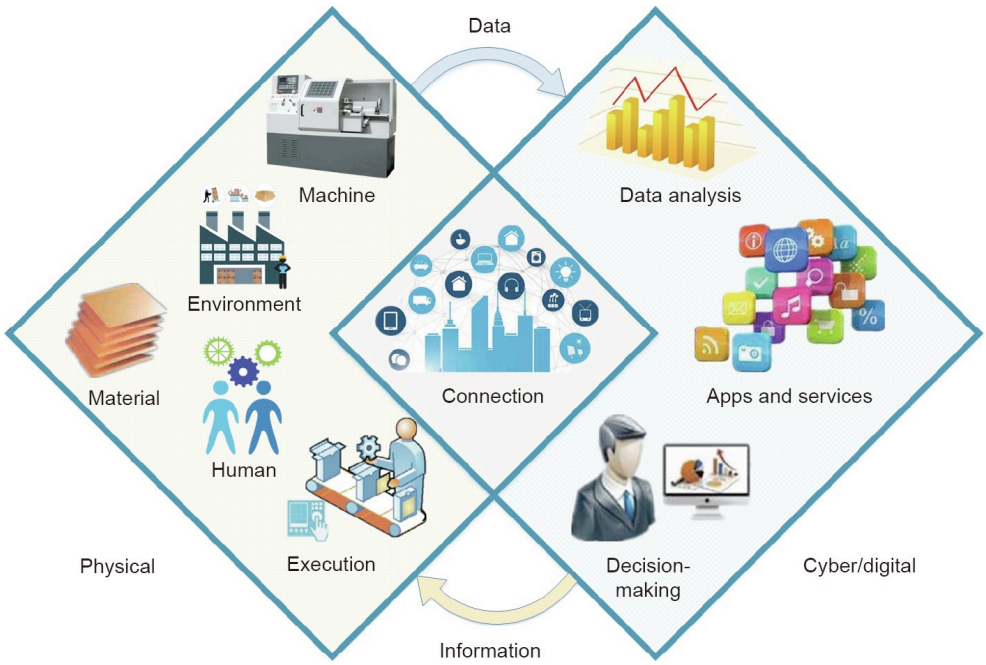


Figure 66: Mapping between physical and cyber/digital worlds, copied from [KrKa18]

CPS Cyber Physical concept as evolution of the Digital Twin is at the base of new paradigm, as Industry 4.0 in Manufacturing, Logistics and Operation. In **Table 32** the differences between the two terms are formalized.

Table 33: Correlation and comparison of CPS and DTs. copied from [KrKa18]

Table 1
Correlation and comparison of CPS and DTs.

Items	CPS	DTs
Origin	Coined by Helen Gill at the NSF around 2006	Presented by Michael Grieves in a presentation on PLM in 2003
Development	Industry 4.0 listed CPS as its core	Not much attention paid to DTs until 2012
Category	Akin to a scientific category	Akin to an engineering category
Composition	The physical world and the cyber world, CPS focus more on powerful 3C capabilities	The physical world and the cyber world, DTs focus more on virtual models
Cyber–physical mapping[a]	One-to-many correspondence	One-to-one correspondence
Core elements	CPS emphasize sensors and actuator	DTs emphasize models and data
Control	Physical assets or processes affecting cyber representation, and cyber representation controlling physical assets or processes	Physical assets or processes affecting cyber representation, and cyber representation controlling physical assets or processes
Hierarchy	The unit level, system level, and SoS level. A smart production line, shop floor or factory are examples of system-level CPS and DTs; a service platform constitutes SoS-level CPS	The unit level, system level, and SoS level. A complex product can also be considered as a system-level DT; an SoS-level DT covers the product life-cycle
Integration with new IT	Be inseparable from new IT	Be inseparable from new IT. A DT is easier and faster to integrate with new IT compared with CPS

[a] Including two directions—cyber to physical and physical to cyber.

Fast development and evolution of DTw and CPS, fostered by research and technology development, require a more structured approach to the description, analysis and eventually implementation. Id doing that we have to consider not only the technical aspects, but also the operational, human and business implications.

The following model provide a comprehensive representation of an incremental implementation of the CPS approach, specifically in the context of an Industry 4.0 environment, see [CiNe19].

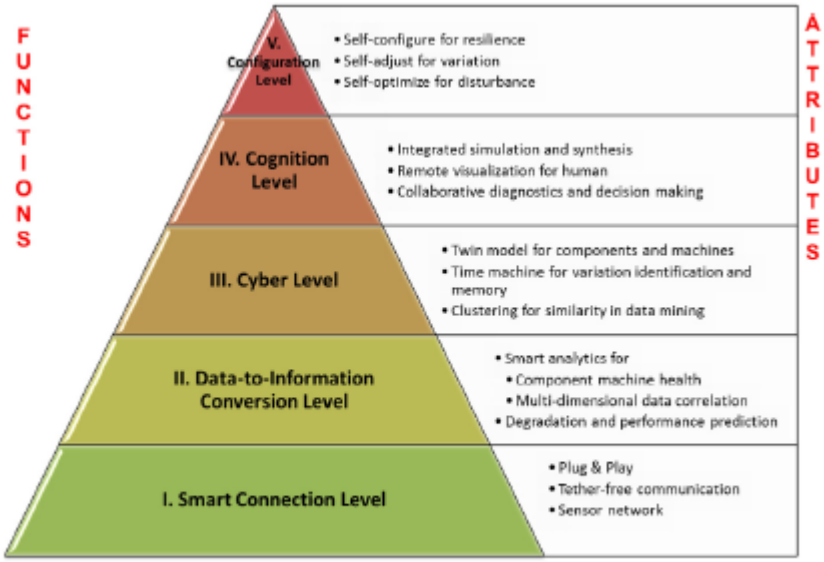


Fig. 1. 5C architecture for implementation of Cyber-Physical System.

Figure 67: 5C Architecture for implementation of Cyber-Physical System, copied from [CiNe19]

For each of the levels it is also possible to identify technological impact as well business and operation impacts, see [CiNe19].

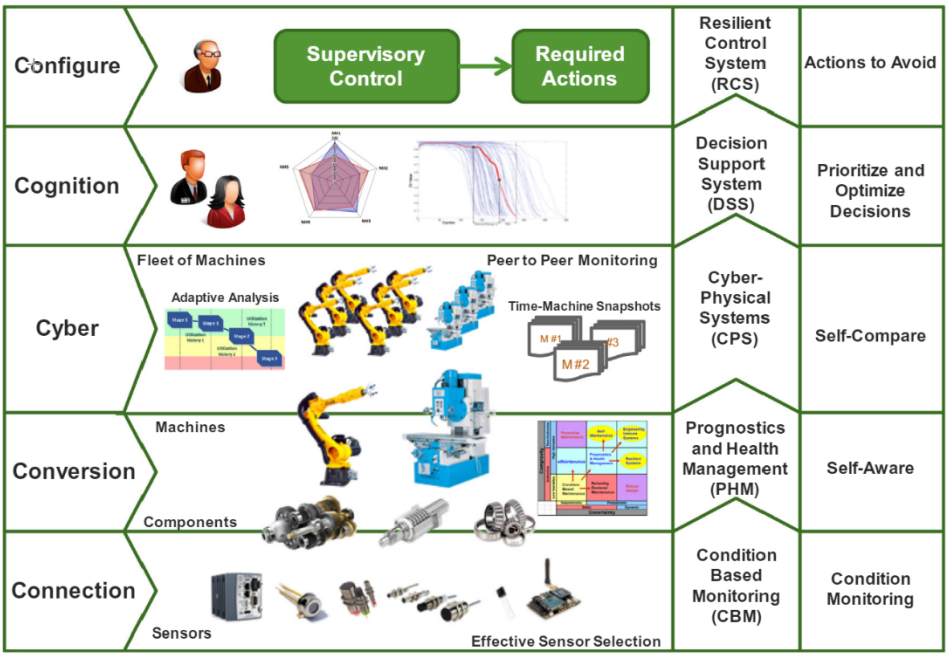


Figure 68: Applications and techniques associated with each level of the SC architecture, from [CiNe19]

It is important to remark how the identified application in order to provide reliable added value services need to satisfy to key attributes, to be connected with a robust, fast and secure way with the field and to adapt the models to the changing situation and configuration in the real world. To such purpose adoption of most advanced technology related to Machine Learning (ML) and generally speaking AI ensure a constant adaptation to changes. At the same way High Performance (HPC) computation capability is needed to execute methods and applications providing the requested services.

Characteristics and requirements for integration of CPS/DTw with a physical environment are summarised below, see [LeBa15]:

1. Ubiquitous connectivity and smart objects: Manufacturing assets should be equipped with smart sensors with the capability of real-time monitoring and data exchange with other elements in the network. These constant data transactions require a secure, reliable, and high-speed platform.
2. Advanced analytics: It is essential to automate the whole process of data pre-processing, perception, analysis, learning, and execution without the need for extensive human interference and manual feature engineering. This process brings self-configure, self-adapt, and self-learning functionalities to the manufacturing systems, which increases productivity, speed, flexibility, and efficiency
3. Cooperative decision making: Data from multiple resources and real-time limitations must be considered to achieve a globally optimal solution. In this process, feasibility, efficiently, and execution plans of different orders are evaluated.
4. Autonomous and rapid model building and updates: Data synchronisation and advanced model mapping between virtual and physical systems guarantee the minimum difference between virtual components and their physical counterparts, which is essential for real-time control, optimisation, forecast, etc.
5. Autonomous disturbance handling and resilience control: Manufacturing systems need to respond to failures autonomously and resiliently in order to prevent catastrophic operational disruptions.

As for the DTw, it is considered to be a new way of managing the industrial IoT. Integrating cloud technologies in DTws holds promise for ensuring the scalability of storage, computation, and communication. BDA, AI, and corresponding algorithms are also seen as important foundations for a DTw. In the exploration of potential DTw applications, new IT and not-IT technologies play a more and more important role, moving from a pure technology perspective towards a holistic approach where many disciplines and skill are required to converge towards a full exploitation of available information. In the following picture it is sketched the DTw/CPS evolution starting for a pure industry related data domain through information elaboration in an IT perspective, but definitively moving towards the broader knowledge domain where not only process/product asset are considered, but also humans are part of the game.

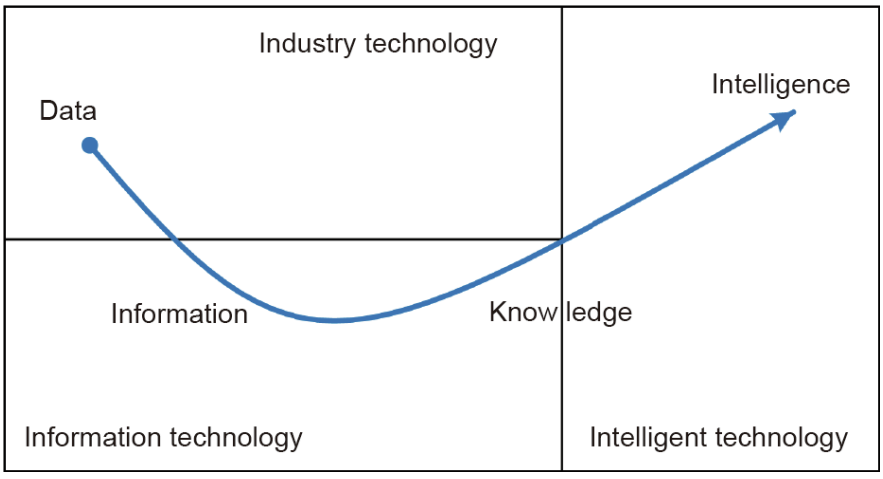


Figure 69: Integration of industrial technology, information technology, and intelligent, copied from [KrKa18]

In such journey 5G technology can play a terrific role, "5G can help support advanced Industry 4.0 strategies by bringing ubiquitous, high speed, reliable, high coverage connectivity to industrial environments and systems " First of all 5G utilizes advanced technologies such as Millimetre Wave and terahertz band, NFV, Wireless Software Defined Network (WSDN), Cloud Radio Access Network (CRAN), and Massive MIMO to provide low latency, high reliability, high transmission rate, high coverage, high security, and scalable networking which can better support the communication demands of future smart manufacturing [LeAz20]. More security mechanism in 5G is addressing some of the concerns for data protection, Frequency Slicing is supporting critical applications requiring specific service level in term of speed and latency, Edge Computing functionality can support distributed computational architecture or Distributed Ledger application. In the following picture a set of functionalities potentially impacted by 5G technology, see [JML20].

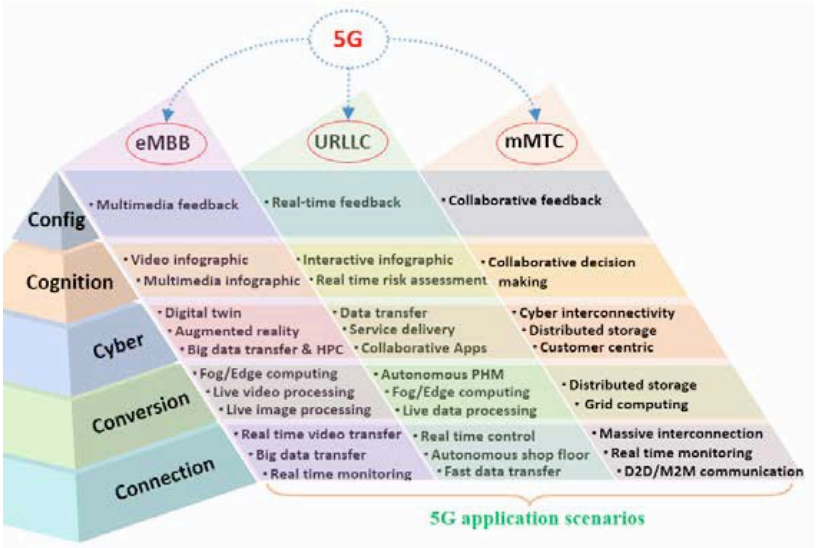


Figure 70: Application Scenarios, copied from [JML20]

3.2 Deep Edge, Terminal and IoT Device Integration in B5G communication infrastructure

This section is related to the Networld2020[13] SNS SRIA [Networld2020-SRIA] and focuses on challenges of the integration of deep edge, terminal and IoT devices in the SNS architecture.

Architecturally, the 'deep edge' with its IoT as well as end user or vertical industry devices is becoming part of the common resource pool, provided as a non-decomposable set of resources by some edge entity, such as an end user, industrial site owner, or a building owner. It is envisioned that tenant-specific resource usage to expand into the deep edge with the same control and data plane considerations and resource management considerations, applying to all those resources. In other words, in principle, we see aspects of controllability of those edge resources to equally apply together with the general programmability for the realization of compute tasks as well as for data and forwarding plane operations through those resources.

However, some edge resources might not directly fit into this vision. For instance, IoT will introduce particular, service-dedicated, possibly intelligent yet resource-constrained components (micro-electronics, battery driven components), which will need a particular consideration for the integration with the rest of the system. Indeed, such IoT components and devices might impose additional requirements on, e.g., volatility and longevity, punctual presence at any moment, persistence, generality, capacities, connectivity, interfaces and APIs from/towards the system. Hence, they might not support direct integration and require particular solutions instead (e.g., gateways or subsystems).

[13] Networld2020 ETP has been renamed to NetwolrdEurope ETP, see: https://www.networldeurope.eu

This section focuses on the following objectives, see (section 4.7 of Networld2020 SNS SRIA [Networld2020-SRIA]):

- Future research will need to develop a suitable common model of system-wide representation akin to 'device drivers' in existing computing platforms.
- Future research will need to address edge-specific constraints through suitable scheduling mechanisms that take those constraints into account, while relying on edge-specific control agents enabling the enforcement of the policies underlying the scheduling solutions
- Through research in this space, future solutions to enable an edge resource market that would allow for auctioning the availability of resources to tenants very much like the bidding for white space on a webpage as we know today, basing all interactions on a trusted, auditable, and accountable basis that caters to the dynamics experienced at the edge.
- This will require research into novel programming models and (e.g., policy) languages that not only support all of these services, applications and deployments but also cater to the expected dynamics of the market itself.
- Research is needed for providing new IoT device management techniques that are adapted to the evolving distributed architectures for IoT systems based on an open device management ecosystem.
- In addition, novel programming models and languages are required to support all of these services, applications and deployments. Research challenges in this area include:
    - delivery model and APIs, with effective use of ultra-dense and diverse wired and wireless networks effective management of billions of devices, ensuring they are suitably configured, running appropriate software, kept up-to-date with security updates and patches, and run only properly authenticated and authorized applications.
    - privacy and data management, and the location of processing and data to match legal and moral restrictions on data distribution, access and processing, will be increasingly important.
    - policy descriptions, rules and constraints will need to be specified in a form that can be enforced by the infrastructure on the services.

3.3 Edge, Mobile Edge Computing and Processing

This section is related to the Networld2020 SNS SRIA [Networld2020-SRIA] and focuses on Edge, Mobile Edge Computing and Processing challenges.

These approaches require responsive network connectivity to allow "things" and humans to touch, feel, manipulate and control objects in real or virtual environments. Edge processing in the architecture is essential for ultra-low latency and reliability, while the AI processing is transferred at the mobile/IoT device. Research challenges in this area cover open distributed edge computing architectures and implementations for IoT and integrated IoT distributed architectures for IT/OT integration, heterogeneous wireless communication and networking in edge computing for IoT, and orchestration techniques for providing compute resources in separate islands. In addition, built-in end-to-end distributed security, trustworthiness and privacy issues in edge computing for IoT are important, as well as federation and cross-platform service supply for IoT.

In addition, distributed service provisioning will extend also even beyond the edge, i.e., to on-premises devices such as Industrial IoT devices, robots, AGVs, connected cars. Novel forms of dynamic resource discovery, management and orchestration are required, allowing service provisioning to exploit on-premises devices as "on-demand" extensions of resources provided from the core or the edge.

In this framework, novel resource control schemes, balancing between autonomy of devices and the overall optimization and control of the network by the operator(s) will be required, thus innovating the existing collaboration models between different network service providers. This will also allow to take in better account users' context, exploiting the typical co-location of users with on-premises devices and, sometimes, their very tight physical bound. In this sense, this approach will allow designing network services in a more user-centric way.

IoT Distributed and Federated Architectures Integrated with 5G architecture and AI: Further research is needed in novel IoT distributed architectures to address the convergence of (low latency) Tactile Internet, edge processing, AI and distributed security based on ledger or other technologies, and the use of multi-access edge computing. Research challenges include serving the specific architectural requirements for distributed intelligence and context awareness at the edge, integration with network architectures, forming a knowledge-centric network for IoT, cross-layer, serving many applications in a heterogeneous networks (including non-functional aspects such as energy consumption) and adaptation of software defined radio and networking technologies in the IoT.

5G and beyond mobile networks will enable unprecedented density of connected devices many of which will create tremendous amounts of data. As an example, an autonomous car is expected to create data at a rate of estimated 5 terabytes per hour. Transferring these raw data to a central cloud for processing is not feasible for (at least) three reasons:

Bandwidth

If the device is connected via LPWAN (e.g. NB-IoT with an uplink peak data rate of 159 kbit/s[14]) the bandwidth is limited and not suitable to transfer large amount of data (e.g. multimedia data).

Network Congestion

With a culminated capacity of the last mile exceeding the capacity of the core network by two orders of magnitude the core is becoming a bottleneck for huge amounts of data to be transferred to the cloud data centres while at the edge there is sufficient capacity available.[15]

Latency

There are applications where latencies beyond the range of hundreds of milliseconds are not acceptable. Multiplayer online gaming is an example which is a driving force in edge development (gamers are paying for latency!). In safety relevant use cases it often is not just a question of "user experience" but a matter of life or death.

Storing (or buffering) raw data locally is often not an alternative either since devices do not have sufficient storage capacity or storage is just too expensive. Taking the example of an autonomous car above and with a current storage price of roughly 20 € per Terabyte to store the raw data of that car would cost 100 € per hour – even without redundancy.

Those restrictions can be overcome by taking content delivery network (CDN) technologies a step further and process data in or near the device by which it is being created (e.g. in a mobile phone or in a surveillance camera). The processing can result in immediate action of an actuator in response to sensor inputs or in condensing data before storing them or sending them to a central cloud. Artificial intelligence comes into play to identify relevant data pattern, but also as a means for network resource optimization and network security. Beyond 5G networks are expected to come with AI already embedded in the network functions[16].

[14] See https://en.wikipedia.org/wiki/Narrowband_IoT

[15] See e.g. https://blogs.akamai.com/kr/2018_Edge_Korea_TomLeighton.pdf or https://www.akamai.com/de/de/about/events/edge-highlights.jsp#edgeworld-2019-tom-leighton-through-the-clouds-a-view-from-the-edge (at ~ 13:00 minutes)

[16] See e.g. https://ieeexplore.ieee.org/document/9430853

When data are being condensed for transfer or storage this must be done in a manner that potentially valuable information is being retained.

Regulatory requirements may also be relevant for data retention (e.g. in autonomous driving). Such handling of data will be important design decisions when developing edge applications.

Developers are facing competing frameworks to make their apps edge-aware – some of which are provided by large cloud providers (e.g. AWS Greengrass, Azure IoT Edge). To avoid another lock-in, users might consider open-source alternatives like ETSI MEC[17], LF Edge[18], Open Edge Computing[19] or OpenStack[20] (just to name a few).

Developers will also have to deal with different levels of edge computing complexity. One dimension of complexity is the edge-awareness of the application. In the case of edge-unaware applications, developers do not have to deal with the edge specifics and the network is responsible to handle client requests transparently in a manner that those are handled by the server instance with optimum network proximity (just like in today's CDNs). On the other hand, edge-aware applications will have to make use of the available edge-resources by exploiting the specific APIs that are exposed by the edge implementation.

A second dimension of complexity is mobility. When the device is mobile, this is uncritical as long as the edge application is running on the device itself ('device edge'). But if for example the processing is done at the base station ('far edge'), the application context needs to be moved from one base station to another as the user is moving through the mobile network. If roaming between different MNOs comes into play, things even get more complex.

As a side effect, to not send data to a central cloud can be seen as a gain in privacy. However, this presupposes that data security is guaranteed in the edge. This, in turn, is not a trivial task, because the attack surface increases enormously and the remote management of the high number of edge devices is a challenge and requires new methods and standards.

Availability can be another benefit of edge computing. Given the edge applications are programmed accordingly they can provide business continuity in situations of loss of network connectivity or downtimes (planned or unplanned) of the cloud data center.

While edge computing will certainly support the goals of the digital transition, we should not forget about the other side of the medal: sustainability and the green transition. On the positive side of the energy equation, edge computing reduces energy-hungry data transfers. On the downside, the intelligence and processing power required at the edge comes at a (energy) cost. Research should be undertaken on how the net carbon footprint of edge computing could be minimized. When the device is energy constrained (e.g. battery driven) other options like energy harvesting could be taken into consideration.

As the talks and discussions in the workshop *IoT and Edge Computing: Future directions for Europe*[21] have shown edge computing is expected to be the first evolutionary step towards a 'computing continuum' reaching from the cloud data centre to the edge device. Cloud federation as investigated by the European Gaia-X project[22] will allow for flexibility when choosing the cloud vendor preventing vendor lock-ins. Moreover, a split of functions that make up a service will allow to run workloads on the device best suited (e.g. due to the availability of specialized processors like DPUs).

[17] https://forge.etsi.org/rep/mec

[18] https://www.lfedge.org/

[19] https://www.openedgecomputing.org/

[20] https://www.openstack.org/use-cases/edge-computing/

[21] Workshop of 11 September 2020 hosted by the NGIoT CSA project and organised together with the European Commission and AIOTI, replay and presentations available at https://www.ngiot.eu/event/iot-and-edge-computing-future-directions-for-europe/

[22] https://www.gaia-x.eu/

"Edge computing represents the first step towards the decentralisation of Cloud computing, bringing the concept of Federated Cloud to its next evolutionary stage."[23]

As a conclusion, the edge computing paradigm is getting track to deal with some of the shortcomings of the central cloud paradigm. Several technical hurdles need to be overcome with respect to deployment, management and securing of billions of edge devices. Standardisation will be required to avoid islands instead of a continuum. For 5G and beyond mobile networks, edge computing will come in quite naturally to fulfil the promises of ultra-reliability and low latency communications (URLLC) and can be expected to become an integral part of future mobile networks.

3.3.1 Functional Splitting: allowing dynamic computing power allocation for signal processing

The purpose of this section is to provide information on systems oriented to deploy computational power allocation on different parts of the so-called continuum computing. According to Balouek et al[24], this concept aims at "realizing a fluid ecosystem where distributed resources and services are programmatically aggregated on demand to support emerging data-driven application workflows".

Usually, data gathering is made directly for simple parameters coming from direct sensors, but other times the information comes in audio or video format and which made it necessary to allocate some computation power in the nodes, in the Edge or sometimes directly in the Cloud (also computation options in the Fog/Mist can be considered). Another way to focus this problem, as in the node the possibilities to allocate high computation power are few, is to split the signal processing procedure in different blocks and assign (manually or automatically) the computing power for each block (or function) to different parts of the system architecture. This assignment can be managed by an orchestrator, assigning task functions according to the computing resources disposal in the architecture.

The functional splitting concept is often applied to the 5G network[25], but with this vision, the concept goes beyond the network functional splitting and can be applied to other fields.

In Noriega et al.[26] and Pastor et al.[27], the authors implemented an Edge computing system by using different Raspberry Pi 3 (Rpi3) nodes in order to carry out a performance evaluation with when computing complex audio signal processing metrics directly on Rpi3 nodes, considered as Edge. In Segura et al.[28], authors focus the same problem from the functional splitting perspective with different options in a 5G architecture, see as well the URBAURAMON project.

Other perspectives to face the problem of the improvement of performance in the computation of the complex parameters with a signal processing strategy are: to use a parallel strategy or to use an Artificial Intelligence strategy (e.g. Convolutional Neural Network (CNN)).

[23] http://www.pledger-project.eu/FederatedCloud_RA_PP_022021.pdf

[24] D Balouek-Thomert, E. Gibert-Renart, A Reza-Zamani, A Simonet, M Parashar, "Towards a computing continuum: Enabling edge-to-cloud integration for data-driven workflows" Journal of High Performance Computing Applications, Vol. 33(6), pp. 1159-1174, 2019. DOI: 10.1177/1094342019877383

[25] D. Harutyunyan and R. Riggio, "Flexible functional split in 5G networks," 2017 13th International Conference on Network and Service Management (CNSM), Tokyo, Japan, 2017, pp. 1-9, doi: 10.23919/CNSM.2017.8255992.

[26] J. E. Noriega-Linares, A. Rodriguez-Mayol, M. Cobos-Serrano, J. Segura-Garcia, F.-C. S., and J. M. Navarro, "A wireless acoustic array system for binaural loudness evaluation in cities," IEEE Sensors Journal, vol. 17, pp. 7043–7052, 2017.

[27] A. Pastor-Aparicio, J. Segura-Garcia, J. Lopez-Ballester, S. Felici-Castell, M. García-Pineda and J. J. Pérez-Solano, "Psychoacoustic Annoyance Implementation With Wireless Acoustic Sensor Networks for Monitoring in Smart Cities," in IEEE Internet of Things Journal, vol. 7, no. 1, pp. 128-136, Jan. 2020, doi: 10.1109/JIOT.2019.2946971.

[28] J. Segura-Garcia, J. M. A. Calero, A. Pastor-Aparicio, R. Marco-Alaez, S. Felici-Castell and Q. Wang, "5G IoT System for Real-Time Psycho-Acoustic Soundscape Monitoring in Smart Cities with Dynamic Computational Offloading to the Edge," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3063520.

In Fayos et al.[29], authors compared a Fog computing system based on different orchestration platforms (i.e. DockerSwarm and Kubernetes) in order to improve performance, for the same complex signal processing problem, with homogeneous and heterogeneous clusters of Small Board Devices. In Salah[30] and El Khafhali et al.[31], the authors focus the efforts in the modelling and provision of the task distribution in the Cloud. In Lopez et al.[32], the authors focused the computing problem by designing a CNN to obtain these parameters and compared its performance with the one of the algorithms in different platforms.

The main challenges associated to the signal processing functional splitting are related to the planned problem and the resources planned in the network (i.e. sampling, windowing, weighting, compression, filtering, etc.). For instance, for audio processing and using ESP32 MCU in the node, we can manage audio sampling, windowing and performing Fourier transform and some other simple operations or functions related to filtering and we can send to the Edge the output information to finish the computing process there. At this point, we need to consider possible delays in the communication but using simple/lightweight protocols (such as MQTT), and using controlled audio/processed chunks, we can obtain affordable delays (i.e. not too high) [5], allowing real-time processing/monitoring. We can also use this procedure for video processing and other temporal related signals but redefining the splitting options to consider the specific problematic of the video processing (e.g. redefining FFT to FFT2D, applying 2D filtering per frame, etc.).

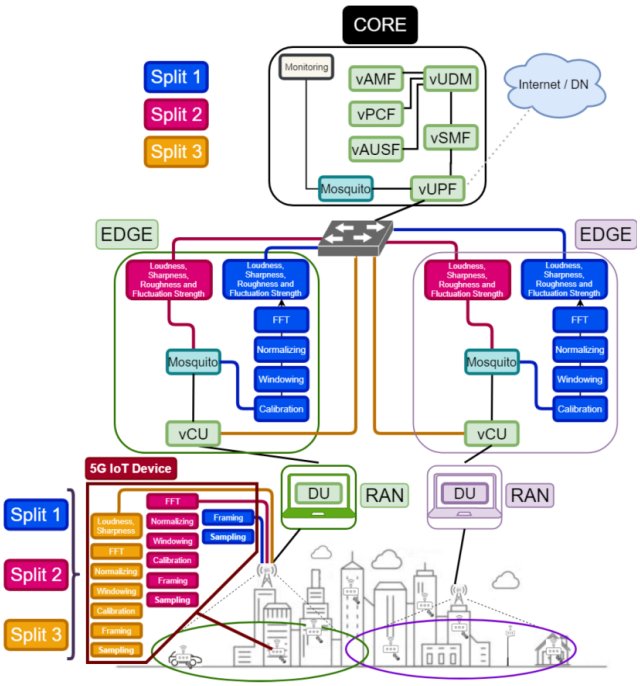


Figure 71: Conceptual diagram of the IoT architecture with different splitting options for the 5G complex metrics calculation system[5]

[29] R. Fayos-Jordan, S. Felici-Castell, J. Segura-Garcia, J. LopezBallester, and M. Cobos, "Performance comparison of container orchestration platforms with low cost devices in the fog, assisting internet of things applications," Journal of Network and Computer Applications, vol. 169, p. 102788, 2020. [Online]. Available: http: //www.sciencedirect.com/science/article/pii/S1084804520302605

[30] K. Salah, "A queueing model to achieve proper elasticity for cloud cluster jobs," in 2013 IEEE Sixth International Conference on Cloud Computing, 2013, pp. 755–761.

[31] S. El Kafhali and K. Salah, "Stochastic modelling and analysis of cloud computing data center," in 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), 2017, pp. 122–126.

[32] J. Lopez-Ballester, A. Pastor-Aparicio, S. Felici-Castell, J. Segura-Garcia, and M. Cobos, "Enabling real-time computation of psychoacoustic parameters in acoustic sensors using convolutional neural networks", " in *IEEE Sensors Journal*, vol. 20, no. 19, pp. 11429-11438, 1 Oct.1, 2020, doi: 10.1109/JSEN.2020.2995779.

The 5G IoT infrastructure designed for the soundscape description within the context of a Smart City, considers the following elements or subsystems: a) the node as a 5G IoT sound monitoring device that has connected sensors and collects information, b) the Radio Access Network (RAN) as the radio interface, c) the Edge where some offloading from the device can be applied to allow energy savings and d) the Core where the information is gathered and processed monitoring. Figure 71 shows a conceptual diagram of these elements with their components, considering the different functional splitting options to compute the metrics for psycho-acoustic soundscape.

The system developed in Balouek et al[1] is an earthquake and tsunami detection and warning global system (by the moment of publication it is deployed in a USA area). Here, the amount of data gathered is huge and the authors propose a ruled-base system for distributing computation loads between Edge and Core and oriented to decentralize the computation, establishing what they call a "virtual slice". This development was made in the context of the GeoSciFramework project (funded by the National Science Foundation).

Another application of this concept is in Rosendo et al[33], where the authors develop a configurable framework for different use cases, but for this project they specify a Smart Surveillance system, achieving very good results in terms of latency and throughput.

In the URBAURAMON project, the main challenges associated to the signal processing functional splitting are related to the planned problem and the resources planned in the network (i.e. sampling, windowing, weighting, compression, filtering, etc.).

In the case of GeoSciFramework project, the proposed architecture is show in Figure 72 is divided in four layers containing the infrastructure layer (which is divided in two components, such as data producers and computing resources), the federation layer (which defines the relations between the infrastructure components, the streaming layer (which stablishes the rules and constraints for the data processing, indexing and discovery from multiple sources in order to achieve real-time processing, to this end a distributed strategy was followed), and the application layer (which is oriented to manage the data consumers, i.e. applications to deal with data production and delivery –by publication/subscription with MQTT-, establishing the workflow management system and the selection of resources).

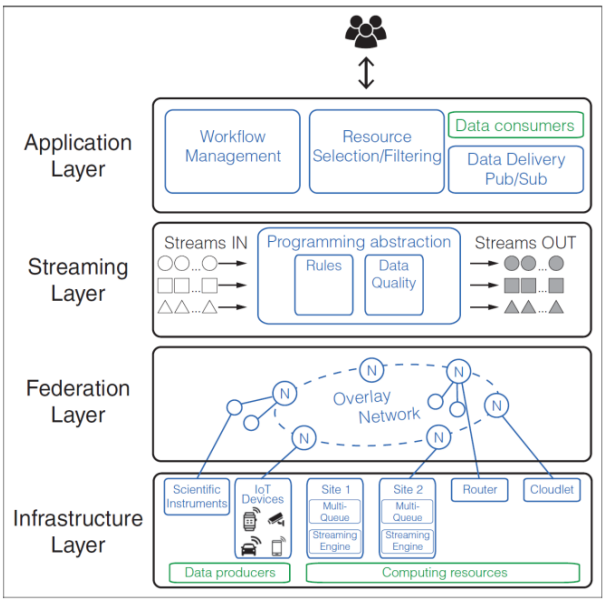


Figure 72: Overall layered architecture of the edge-based data-intensive IoT system.

[33] D. Rosendo, P. Silva, M. Simonin, A. Costan, G. Antoniu. "E2Clab: Exploring the Computing Continuum through Repeatable, Replicable and Reproducible Edge-to-Cloud Experiments". Cluster 2020 - IEEE International Conference on Cluster Computing, Sep 2020, Kobe, Japan. pp.1-11, 10.1109/CLUSTER49012.2020.00028.

The E2Clab/OverFlow project, applied an image processing function in a smart surveillance system for counting persons/detecting a specific person or for free parking space detection[34][35] in a Smart City environment.

Also, the use of artificial intelligence in this environment is possible with the distribution of the computing task force in different places of the 5G environment.

3.4 Network and Server security for IoT and edge Computing

This section is related to the Networld2020 SNS SRIA [Networld2020-SRIA] and focuses on Network and Server security for edge and IoT challenges.

The massive deployment of IoT devices and the emergence of 5G technologies in our daily lives are bringing new data-driven and increasingly autonomous scenarios. The realization of these new services requires efficient and effective management of computing and network resources to deal with huge amounts of data and meet the real-time requirements of such applications. To this end, there is a growing trend for the deployment of computing/network resources at the edge of the network, to interconnect the end devices with cloud infrastructures. This results in the cloud-to-edge-to-device spectrum, which represents a *computing continuum*[36] of resources distributed at different network levels.

This trend toward an increasing interconnectivity requires the adoption of automated mechanisms to detect and react against potential cybersecurity attacks. Indeed, in recent years the convergence between Artificial Intelligence (AI) techniques and the adoption of Software-Defined Networking (SDN) techniques is enabling the development of self-protective IoT systems.

To enhance such systems with the ability of detecting potential security attacks or threats, a crucial aspect is the identification of the intended behaviour of each IoT device composing a system. Indeed, the use of common machine learning (ML) techniques for the so-called intrusion detection systems (IDS) is based on the definition of the devices' intended or "normal" behaviour to train a certain model (e.g., a neural network). Therefore, the identification of potential actions that are not considered as normal behaviour could be used to infer an attack or threat. In 2019, the Manufacturer Usage Description (MUD)[37] was standardized in the scope of the IETF for the definition of network behaviour profiles for IoT devices. In particular, it describes a data model to restrict the communication from/to a certain device, so that manufacturers are enabled to define the intended network behaviour of their devices. Such behavioural profiles are described by using a set of policies or Access Control Lists (ACL) with the endpoints of the intended communication to reduce the attack surface. Furthermore, the standard specification defines an architecture for obtaining MUD files associated to a certain device containing its intended behaviour. The use of the MUD standard has received a significant interest from Standards Developing Organization (SDO), such as the National Institute of Standards and Technology (NIST), which proposes the MUD standard as a key approach to mitigate denial-of-service (DoS) attacks[38] in home and small-business networks[39].

One of the main potential applications derived from the MUD standard is the development of IDS (Intrusion Detection System) to be considered in IoT scenarios. Indeed, such approach has been considered in recent research activities[40].

---

[34] J. Nyambal and R. Klein, "Automated parking space detection using convolutional neural networks," 2017 Pattern Recognition Association of South Africa and Robotics and Mechatronics (PRASA-RobMech), 2017, pp. 1-6, doi: 10.1109/RoboMech.2017.8261114.

[35] G. Amato, F. Carrara, F. Falchi, C. Gennaro and C. Meghini, "Deep learning for decentralized parking lot occupancy detection", Expert Systems with Applications, 72, pp 327-334, 2017. URL: https://github.com/fabiocarrara/deep-parking (Visited on 04/07/2021)

[36] https://ec.europa.eu/digital-single-market/en/news/building-ecosystem-where-iot-edge-and-cloud-converge-towards-computing-continuum

[37] E. Lear, D. Romascanu, and R. Droms, "Manufacturer Usage Description Specification (RFC 8520),", 2019

[38] T. Polk, M. Souppaya, and W. C. Barker, "Mitigating IoT-Based Automated Distributed Threats,", 2017

[39] NIST, "Securing Small-Business and Home Internet of Things Devices:NIST SP 1800-15," 2019

[40] S. Singh, A. Atrey, M. L. Sichitiu, and Y. Viniotis, "Clearerthan MUD: Extending Manufacturer Usage Description (MUD)for Securing IoT Systems," inInternet of Things – ICIOT 2019,V. Issarny, B. Palanisamy, and L.-J. Zhang, Eds.Cham: SpringerInternational Publishing, 2019, vol. 11519, pp. 43–57

In particular, the MUD profiles associated to different IoT devices can be aggregated to build a graph representation of the intended communication in a certain network or system. For example, in a simple approach, graph nodes can be used to represent communication endpoints while edges are used for the interactions between nodes. From the deployment perspective, the use of fog computing could be key to enable an effective detection approach for cybersecurity attacks. Specifically, fog nodes can be used to create a *continuous monitoring* component, so that network traffic of IoT devices can be inspected in real-time. This component could be additionally used to extract the relevant information (i.e., *features*) to be further analysed by an *AI-enabled attack detector*, which is intended to identify potential attacks based on the use of ML techniques. In this context, the use of fog nodes could be used to enable a distributed and cooperative approach for the identification of cybersecurity attacks in IoT-enabled scenarios by performing the tasks associated to network traffic monitoring and attack detection.

Indeed, an important limitation of current approaches to the application of ML techniques for the detection of attacks in IoT, is that they are based on centralized architectures in which a single entity obtains data from the end devices to train a certain model.

This represents a major problem in IoT scenarios, due to the amount and sensitivity of the data that such devices can generate. To address such issue, the use of *federated learning* (FL) is characterized by a collaborative learning process, in which a set of client devices are managed by a central coordinator[41]. However, client devices do not share their data with the coordinator, but only partial updates of the global model that are aggregated by such entity. In each round of training, the coordinator sends information on the current model that is updated by clients through local calculations. This process could foster the compliance of GDPR basic principles. Furthermore, end devices can obtain a more comprehensive overview of the network behaviour since each device obtain information from the other devices in the network.

However, the application of FL in the IoT ecosystem still has to cope with significant challenges related to scalability, heterogeneity and practical aspects, because of the resource constraints associated to certain IoT devices[42]. One of the well-known issues of FL is related to the coordinator, which could represent a single point of failure of an FL scenario that could rise the possibility of *poisoning attacks*. Furthermore, poisoning attacks could be also launched by malicious devices by generating false date during the training process. In particular, an attacker could send forged model updates to the coordinator. Therefore, there is a need to ensure only legitimate and authorized devices are enabled to participate in the training process. For this purpose, the use of MUD profiles could be considered, so that only MUD-compliant devices participate during the process[43].

Furthermore, the use of lightweight authentication and identity management schemes for IoT devices is essential to mitigate such attacks. In addition, recent proposals have considered the use of blockchain technology[44], which consists of an immutable transaction and tamper-proof ledger. Thus, instead of sharing the model updates directly with the coordinator, the use of blockchain is proposed to share the global model updates, in order to avoid issues associated to the centralized coordinator entity.

However, the realization and deployment of such ecosystem still needs to be further investigated in the next future to come up with an AI-enabled and automated approach for an effective security attacks detection and mitigation for IoT scenarios.

---

[41] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions, "IEEE Signal Processing Magazine", vol. 37, no. 3, pp. 50–60, 2020.

[42] Imteaj, A., Thakker, U., Wang, S., Li, J., & Amini, M. H. (2020). Federated learning for resource-constrained iot devices: Panoramas and state-of-the-art. arXiv preprint arXiv:2002.10610.

[43] Feraudo, A., Yadav, P., Safronov, V., Popescu, D. A., Mortier, R., Wang, S., ... & Crowcroft, J. (2020, April). CoLearn: Enabling federated learning in MUD-compliant IoT edge networks. In Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking (pp. 25-30).

[44] Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2019). Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Transactions on Industrial Informatics, 16(6), 4177-4186.

3.5 Plug and Play Integrated Satellite and Terrestrial Networks

This section is related to the Networld2020 SNS SRIA [Networld2020-SRIA] and focuses on Plug and Play Integrated Satellite and Terrestrial Networks challenges.

Satellite universal coverage, multicasting, and broadcasting capabilities provide enhanced connectivity options and seamless user experience when integrated with the overall 5G system. Satellite systems provide large-scale global connections of services where terrestrial coverage is not available. With an integrated 5G/satellite architecture a truly universal coverage can be achieved [LiGe19]. As IoT density decreases, demands for connectivity change from urban to rural areas, reducing demands on a network, see **Figure 73**.

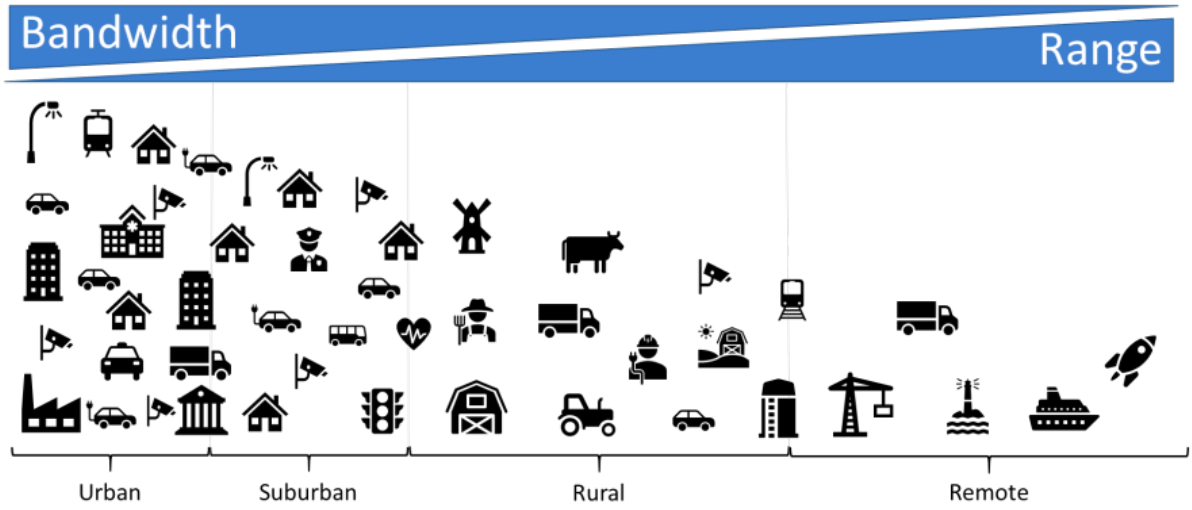


Figure 73: 5G/Satellite Coverage

Traditional Mobile Sat Systems (MSS) like Inmarsat, Thuraya, Iridium, Globalstar have been dominant in the M2M/IoT market, using their L-band spectrum with a focus on mobile and maritime applications. In the last 10 years they realised 3.5 - 4 million satellite IoT terminals in the field. With the availability of Ku-band and Ka-band satellite connections provides higher through-put to meet the demand on of the IoT sector such as fixed satellite systems like Eutelsat, Intelsat or Asiasat. Their higher bandwidths provide backhaul services connecting terrestrial local area IoT networks (e.g., NB-IoT, Lora, WiFi, BT) from high density sensor networks to the internet, see [Satell-market].

New satellite players take advantage of the new cubesat technology (using a range of UHF, VHF, S-band, and Ku-band services) to bring down their service costs, while the Low Earth Orbit allows the use of low power modems to connect the ground sensors, see [KoLa20].

Nanosatellites are defined as any satellite weighting less than 10 kilograms. They all are based on the standard CubeSat unit, namely a cube-shaped structure measuring 10x10x10 cm with a mass of somewhere between 1 kg and 1.33 kg. This unit is known as 1U. As the number Internet of Things (IoT) devices and Machine-to-Machine (M2M) communications increases at an exponential right rate. No communications system can provide end to end connectivity and satellite systems create the opportunity to provide extended coverage, see [NASA-cubesats].

Companies such as Astrocast, Myrioata, Lacuna, Kineis, Kepler Communications, Swarm technologies and Hiber provide service features, low cost, low power, low latency, makes them well suited for Direct-To-Satellite services.

For satellite systems to integrate with 5G networks the architecture will need to address a number of specific issues namely, see e.g., [ISTINCT]:

- Diversification of the spectrum usage across multiple technologies
- Edge networks to reduce the impact of the backhaul in the end-to-end system
- Adapted data path protocols to massive communication environments

- Application protocols adaptation through the virtualization environment
- Addressing the M2M communication needs in an efficient manner
- Participation within the main standardization organizations: 3GPP, ETSI NFV,ETSI MEC, IETF, ONF

3.5.1 Satellite connectivity for global IoT coverage

Today, there are 1.7 billion cellular IoT devices active worldwide. By 2026, there will be 5.9 billion according to Ericsson [Ericsson20], an increase of nearly 350%. Given this tremendous growth, it is clear that the ability to connect diverse IoT device types, with different needs, at massive scale and with global coverage, is urgently needed.

Mobile network coverage is mostly focused on areas with mid to high population density. Areas with low density of population are underserved because of the small or null return on investment required to cover such regions. Currently only 30% of the Earth's landmass, or 10% of the Earth surface has mobile network coverage.

IoT applications such as vehicle monitoring, asset tracking, agricultural sensors and infrastructure monitoring cannot be deployed or used where there is no terrestrial network. Therefore, benefits provided by IoT applications cannot currently be achieved in large portions of the Earth surface.

The capability of satellites to provide global coverage makes them an excellent choice to address the lack of coverage in low populated, isolated and remote areas. The combination of satellite communications together with 3GPP standards offer the possibility to integrate terrestrial and non-terrestrial networks in an easy and simple way.

There are already satellites today that offer global connectivity services for IoT but the communication protocols used are not standard, which requires the development of dedicated terminals, and are typically dedicated to specific vertical solutions. Also, current satellite solutions do not integrate with existing IoT terrestrial networks and, finally, its cost does not meet the price points required for massive IoT deployment.

The market today is demanding standard solutions based on roaming, such as 5G, which are interoperable with terrestrial networks, avoid vendor chipset and service provider lock-in, benefit from massive scale deployment and chipset manufacturers diversity. These requirements provide the lowest cost solution on chipset and service costs, reduce dependencies on manufacturers and service providers and protect investments on sensors. Combining terrestrial and satellite networks under 5G makes it possible to ensure seamless connectivity using the best available network at any time, see **Figure 74**.

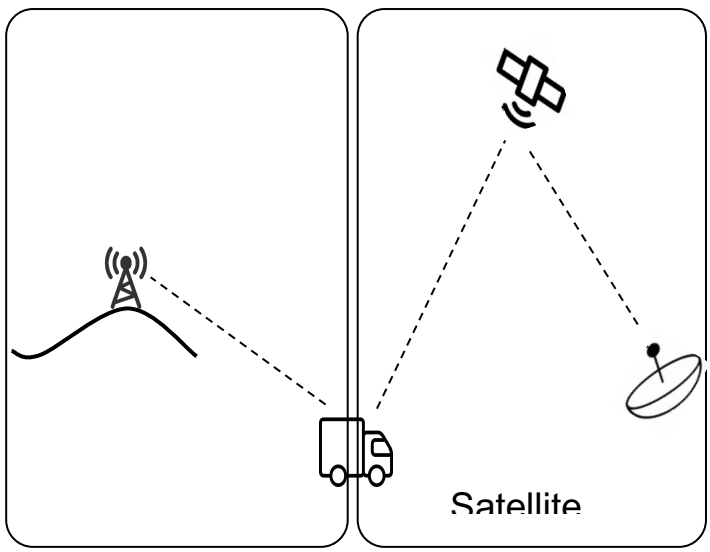


Figure 74: Integrated terrestrial and satellite IoT networks

3.5.2 Evolution to 5G IoT over satellite

While traditionally satellite and terrestrial standardization have been separate processes from each other, the satellite communications industry is nowadays strongly involved in the 5G standardization process led by 3GPP in a quest towards achieving a higher layer operational integration and high degree of radio interface commonality between non-terrestrial networks (NTN) and 5G radio access technologies. Studies on satellite access began in 3GPP a few years ago in the context of Rel. 14 and Rel. 17, to be finalized by mid-2022, will be the first version to support 3GPP standards running over non-terrestrial networks. Specifically, Rel-17 is expected to come with an adaptation of the 5G New Radio (NR) protocol for NTN (this work is already at normative phase, after completion of the study phase) as well as adaptation of the NB-IoT and eMTC protocols for NTN (this work is at study phase).

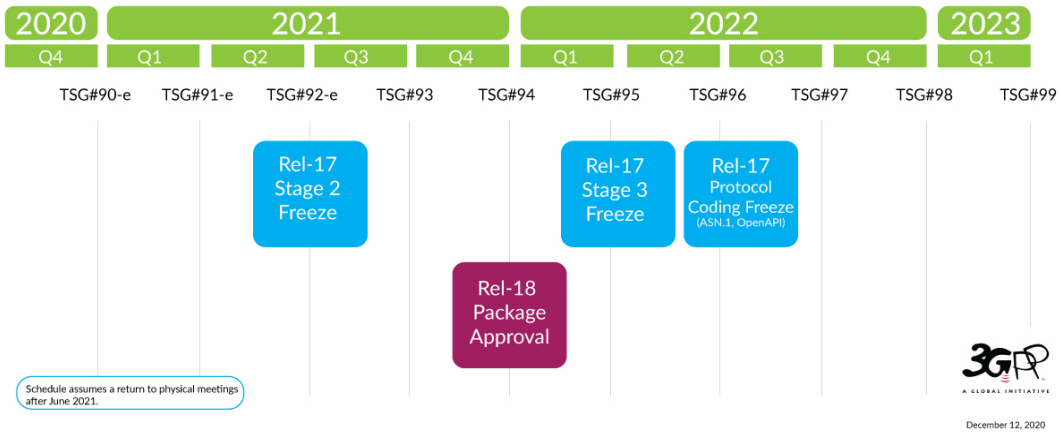


Figure 75: 3GPP Release 17 timeline, copied from 3GPP

Today it is not clear whether Release 17 study phase of IoT over NTN will be moved to normative phase in 3GPP RAN plenary meeting TSG#92-e that will take place in June 2021 for a deployment timeframe for Rel-17 and IoT services over satellite around 2023-24. The following opportunities to provide input on the 3GPP SA1 group, focusing on services, will be in S1-94 in May/July and S1-95 in August, which will address services for Release 18, see **Figure 75.**

3.5.3 IoT devices

3GPP current study items plan that IoT devices will support both terrestrial and non-terrestrial networks on the same device for integrated and seamless connectivity. This makes it possible for the device to select the best and most cost-effective network at any given time. By having a single chipset capable of connecting to mobile and satellite networks it is not necessary to implement two different RF chains that increase complexity and cost of the IoT device. Moreover, the chipset can benefit from the economies of scale provided by all mobile and satellite IoT devices using the same chipset. Typically, the terrestrial network will be used when there is coverage and the device will roam into the satellite network when there is no mobile terrestrial network available.

Testing performed by Mediatek and Inmarsat in August 2020 [3GPP-TSG-RAN89E] show that IoT Satellite communication could be possible with current NB-IoT chipsets. If this is confirmed then existing IoT devices using NB-IoT could use satellite connectivity without having to modify or replace its current hardware just with a firmware update. The firmware update would support the waveform required to cope with the impairments of the satellite connection providing backward compatibility, while switching from one network to the other will be supported by already existing 3GPP roaming support.

Satellites providing 5G IoT connectivity may use transparent or regenerative payloads in the satellite. LEO satellites will tend to use regenerative payloads because of the discontinuous connectivity to the core and the needs of 5G to establish connections with the terminals/IoT devices. GEO satellites can use either transparent or regenerative payload on the satellites as they have the possibility to connect to a base station on the ground for signalling.

3.5.4 IoT communication satellites

Traditionally satellite communications have been delivered by Geostationary satellites. Advances in space technology have opened the possibilities for LEO, Low Earth Orbit, satellites to also provide communication services. For this reason, there will be several options for IoT satellite services and its selection will depend on the requirements of the IoT application such as bandwidth, delay tolerance and service continuity.

In contrast with services designed to provide high data rates and continuous service, which are likely to require dense constellations (e.g. in the order of hundreds or more) of high-capacity satellites, NB-IoT solutions with sparse LEO constellations (e.g. in the order of tens of satellites) of CubeSats or similar platforms are anticipated to be a compelling approach to address the needs of many IoT and M2M applications. In particular, there is a wide range of delay-tolerant IoT/M2M applications that do not require continuous service coverage and that generate short, infrequent messages that can be properly addressed with such solutions. For example, in smart agriculture applications, small messages, few messages per day, large delays are not a service problem and can be perfectly achieved by a satellite network not offering continuous coverage. More examples are maritime use cases for non-critical asset tracking where today a data logger is already used, livestock monitoring during pasture in rural areas, and in general any non-critical asset tracking, environmental monitoring and infrastructure monitoring.

Satellite constellations based on CubeSat technology can benefit from low complexity and cost-effective solutions to offer the IoT services, and its required infrastructure, being discussed in this report. Together with the increase of launch opportunities due to new launchers being available and its reusability, this new model, sometimes referred as the New Space model, has greatly increased the number of satellites being built, launched and deployed.

With the increased number of satellites and satellite constellations being deployed at the moment, it is imperative that the satellite design includes its deorbit once its mission has finished in order to minimize the space debris. Satellites must follow ISO 24113:2019 Space Systems-Space Debris Mitigation Requirements [ISO 2413] and ESA Space Debris Mitigation Compliance Verification Guidelines ESSB-HB-U-002 [ESA ESSB HB –U 002].

3.6 Autonomous and Hyper-connected On-demand Urban Transportation

The transportation domain is ongoing an evolution towards increasing levels of connectivity and automatism. This is the so-called Collaborative, Connected and Automate Mobility (CCAM) paradigm[45]. In this evolution, vehicles will be increasingly connected through different wireless standards like ITS G5 and LTE-V2X but they will also benefit by increasing level of automatism[46]. While the possibility of having fully automated vehicles (level 5 of the J3016 standard)[47] may still take considerable time to happen, levels 2, 3 and 4 are more near deployment in the market or they are already deployed in the market[48]. There are considerable expectations for these new technologies and many studies and reports have identified a number of key benefits for the deployment of these technologies from the obvious and primary benefit to improve the safety conditions in the road to improvement in traffic management, improve compliance to regulation and so on.

The connectivity trend and the automated vehicle trend have evolved from different origins as the first (connectivity) trend is focused on providing connectivity to the vehicle for a variety of applications including safety while the second (automated vehicle) trend is focused on applying artificial intelligence to the processing and analysis of the data originating from the sensors to improve the awareness of the vehicle intelligence.

---

[45] Alonso Raposo, M., Grosso, M., Després, J., Fernández Macías, E., Galassi, C., Krasenbrink, A., ... & Ciuffo, B. (2018). An analysis of possible socio-economic effects of a Cooperative, Connected and Automated Mobility (CCAM) in Europe. European Union.

[46] Weber, R., Misener, J., & Park, V. (2019, May). C-V2X-A Communication Technology for Cooperative, Connected and Automated Mobility. In Mobile Communication-Technologies and Applications; 24. ITG-Symposium (pp. 1-6). VDE.

[47] SAE, S. (2014). J3016 standard: taxonomy and definitions for terms related to on-road motor vehicle automated driving systems.

[48] Yang, CY David, Kaan Ozbay, and Xuegang Ban. "Developments in connected and automated vehicles." (2017): 251-254.

There is a logical link between the two trends because the connectivity technologies can provide useful information to the automated vehicles for different levels of automation, so that it is an additional input to the artificial intelligence component in the vehicle[49].

There are two main connectivity technologies: short range communications which provides fast communication between vehicles (V2V) and vehicles to infrastructure (V2I) and long-range communication (e.g., 3GPP) where the vehicle can be both the source of information to back-end offices for various applications (e.g., traffic management) but it can also be a recipient of information (e.g., weather conditions). V2X has been traditionally designed using the 802.11p standard[50] while long range communication can be provided by cellular networks. On the other side, there are ongoing discussions on the possibility that 3GPP can also be used for V2X using Device 2 Device (D2D) protocols.

For example, in USA, 3GPP has also been proposed for V2X communication leading to a possible coexistence of the two technologies at least in some geopolitical areas (e.g., USA)[51]. Additional details on the debate on ETSI ITS G5 versus 3GPP LTE-V2X can also be found in section 3.2 of the AIOTI report "IoT Relation and Impact on 5G"[52]. The security (authentication and integrity) of V2X has been designed and described in ETSI and IEEE standards[53] and they may rely on a Public Key Infrastructure (PKI).

The security of cellular networks for long range communication can be based on the authentication, integrity and encryption already described in the 3GPP standards even if it was designed for a different use case.

Automation technologies include the artificial intelligence component, which is used both for a) data analysis of the data originating from the sensor (e.g., camera, LIDAR, inertial measurement units) and b) composing the awareness context of the vehicle and c) taking a decision on the action to take (e.g., avoid a pedestrian).

Beyond the technologies underlying these trends, we also investigate here the potential impacts (e.g., societal) and the potential applications of the combined connectivity and automated concepts, otherwise called CCAM (Cooperative, connected and automated mobility).

At the highest level of automation (level 5 in J3016), the concept of vehicles sharing have been proposed by various sources. In this concept, the vehicle is not owned and driven (for automation levels below 5) by a single proprietary but it can be shared among different users, thus leading to a new economy model where ownership is replaced by pay-by-use.

The emergency of such sharing models can be applied not only to passenger's vehicles but also to commercial vehicles and to public transportation where the vehicles will be owned by the government. Such sharing models poses new challenges not only because they can be economically disruptive (businesses may disappear) but they can also generate great risks from a privacy and security point of view. From a privacy point of view, it is imperative that the data on the passengers is not disclosed or accessible to un-authorized party. From a security point of view, it is necessary that shared automated vehicles cannot be compromised and used for criminal activities[54].

[49] Tong, W., Hussain, A., Bo, W. X., & Maharjan, S. (2019). Artificial intelligence for vehicle-to-everything: A survey. IEEE Access, 7, 10823-10843.

[50] Jiang, D., & Delgrossi, L. (2008, May). IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. In VTC Spring 2008-IEEE Vehicular Technology Conference (pp. 2036-2040). IEEE.

[51] Bey, T., & Tewolde, G. (2019, January). Evaluation of DSRC and LTE for V2X. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1032-1035). IEEE.

[52] AIOTI Report. IoT Relation and Impact on 5G. Release 3.0. https://aioti.eu/wp-content/uploads/2020/05/AIOTI-IoT-relation-and-impact-on-5G-R3-Published.pdf

[53] Fernandes, Bruno, João Rufino, Muhammad Alam, and Joaquim Ferreira. "Implementation and analysis of IEEE and ETSI security standards for vehicular communications." Mobile Networks and Applications 23, no. 3 (2018): 469-478.

[54] De La Torre, G., Rad, P., & Choo, K. K. R. (2020). Driverless vehicle security: Challenges and future research opportunities. Future Generation Computer Systems, 108, 1092-1111.

The recent terrorist attacks where commercial vehicle was used to kill pedestrians[55] could be replicated with a shared vehicle driven remotely or with a driving plan inserted in the automated vehicle driving engine by a terrorist or a criminal.

Then, for these reasons or other reasons, it is possible that shared vehicles will be submitted to stringent type approval processes even more than conventional vehicles. The integration of shared commercial vehicles with other means of transportation would also improve the efficiency of the supply chain as the so called "last mile" delivery can be automated through this concept.

Apart from the driverless vehicles (i.e., level 5) the lowest levels of automation can still generate new applications which would greatly benefit the road transportation sector. We can identify just few of them. The presence of sensors in the vehicle and artificial intelligence components can be used to support more sophisticated applications of traffic management where the data from sensors is conveyed to back-end traffic management applications where the traffic conditions (e.g., traffic signs, urban public transport) can be made more efficient on the basis of the real-time received data. In addition, vehicles equipped with inertial measurement units can provide real-time information on the conditions of the road surface for road maintenance purpose or to improve safety (e.g., slippery conditions due to rain can be analysed and communicated to other vehicles in the region). In another example, the findings from the artificial intelligence components of the vehicle (e.g., optimal weights of the deep learning algorithms) can be shared among the AI component of the vehicles to improve driving efficiency.

For example, the poor lighting or surface conditions in a specific urban area can be mitigated by making the Artificial Intelligence (AI) components of different vehicles travelling in the area to share the model parameters through federated learning[56]. As in other contexts, it is important that the integrity of the exchanged data is protected because false data can compromise the functioning of the AI components and therefore the safety of passengers and pedestrians.

Finally, we would like to highlight that the emergency of CCAM would require complex data management and analysis systems and infrastructures as the amount of data originating from the vehicles can be massive. We also note that the tracking of the history of the vehicles is particularly important for maintenance purposes or for compliance to regulations because of the long lifetime of the vehicles. Then, technologies like the Blockchain with its properties of decentralization, transparency, and immutability can be quite beneficial in this context[57].

3.7 Opportunities for IoT Components and Devices

This section is related to the Networld2020 SNS SRIA [Networld2020-SRIA] and focuses on Opportunities for IoT Components and Devices challenges.

Deploying and managing a large set of distributed devices with constrained capabilities is a complex task. Moreover, updating and maintaining devices deployed in the field is critical to keep the functionality and the security of the IoT systems. To achieve the full functionality expected of an IoT system, research should be done in advanced network reorganization and dynamic function reassignment. Research is needed for providing new IoT device management techniques that are adapted to the evolving distributed architectures for IoT systems based on an open device management ecosystem in a high threat landscape.

Components (micro-electronic components) and devices mainly for IoT and vertical sector applications are essential elements of future secure and trusted networks and to support the digital autonomy of Europe.

[55] https://www.history.com/this-day-in-history/2016-nice-terrorist-attacks

[56] Chai, H., Leng, S., Chen, Y., & Zhang, K. (2020). A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles. IEEE Transactions on Intelligent Transportation Systems.

[57] Baldini, G., Hernández-Ramos, J. L., Steri, G., Neisse, R., & Fovino, I. N. (2020). A Review on the Application of Distributed Ledgers in the Evolution of Road Transport. IEEE Internet Computing, 24(6), 27-36.

With respect to the increasing demand and expectation of secure and trusted networks, especially for critical infrastructures, there should be European providers for such devices as an additional source to latest technologies to complement the European value chain and mitigate the existing gaps.

3.7.1 Approach for components

European semiconductor players are stronger in IoT and secured solutions, while mass-market oriented market are dominated by US or Asian players. For European industry to capture new business opportunities associated with our connected world, it is crucial to support European technological leadership in connectivity supporting digitisation based on IoT and Systems of Systems technologies.

Increasingly, software applications will run as services on distributed systems of systems involving networks with a diversity of resource restrictions.

It is important to create the conditions to enable the ecosystem required to develop an innovative connectivity system leveraging both heterogeneous integration schemes (such as servers, edge device) and derivative semiconductor processes already available in Europe.

Smart services, enabled by smart devices themselves enabled by components introducing an increasing level of "smartness", will be used in a variety of application fields, being more user-friendly, interacting with each other as well as with the outside world and being reliable, robust and secure, miniaturised, networked, predictive, able to learn and often autonomous. They will be integrated with existing equipment and infrastructure - often by retrofit.

Enabling factors will be: Interoperability with existing systems, self- and re-configurability, scalability, ease of deployment, security, sustainability, and reliability, will be customised to the application scenario.

Related to technological game changers in 5G network infrastructure, Europe strengths are RF SOI and BICMOS technologies for cost-effective GaAs replacement, FD-SOI for integrated mixed signal System on Chip.

The 5G technologies and beyond utilise the sub-6 GHz band and the spectrum above 24 GHz heading to millimetre-wave technology moving towards 300 GHz and Terahertz frequencies for 6G technologies.

The design of electronic components and systems to provide the 5G and beyond connectivity have to take into account the new semiconductor processes for high-speed, high-efficiency compound semiconductor devices considering the significant increases in the density of wireless base stations, wireless backhaul at millimetre wave frequencies, increased transport data rates on wired networks, millimetre wave radios in 5G equipment and multi-frequency/multi-protocol IoT intelligent nodes to support higher data rates, more devices on the network, steerable beams resulting from massive MIMO antennas, low power consumption and high energy efficiency.

It is expected that the mobile and intelligent IoT devices to provide edge computing capabilities and intelligent connectivity using multi-frequency/multi-protocol communications technologies. Cellular IoT devices covering higher frequencies need to integrate microwave and analogue front-end technology and millimetre wave monolithic integrated circuits (MMIC).

The development of 5G technologies and beyond requires semiconductor technologies that are used for RF devices, base stations, pico-cells, power amplifiers to cover the full range of frequencies required. Horizon Europe partnerships Smart Network and Services JU (SNS JU) and Chips JU have to address the development of III-V semiconductors-based GaAs, GaN, InGaAs, SiC semiconductor technologies to implement new components, devices and systems to have the edge in efficiency and power usage needed for base stations.

The new devices for 5G technologies and beyond need to combine RF, low operating power, thermally and energy-efficient, small form factor and heterogeneous integration of different functions. These new requirements push for creating new components based on multi-chip modules and Silicon in Package (SiP) and various technologies that combine the capabilities of silicon CMOS with III-V semiconductors.

The focus for new 5G and beyond connectivity IoT devices is on providing new components including hybrid electronic circuits able to operate with better stability, less noise, providing increase functionality, complexity, and performance. The new functionalities include stronger security mechanisms and algorithms integrated into the devices and components and designed for easy implementation of end-to-end security at the application level.

Activities need to be aligned with the Chips JU to develop 150 mm and beyond wafers for III-V semiconductors on Silicon to provide the components for 5G and beyond wireless cellular networks and devices for providing optimum use of available bandwidth for millimetre-wave and higher frequencies.

Components must be designed to meet the security requirements of critical infrastructure as required on high level by the NIS directive[58], Cybersecurity Resilience Act[59] and the US Executive Order on Improving the Nation's Cybersecurity[60].

ENISA has published several best practices documents on IoT security and securing the IoT supply chain[61][62][63], as well as other organizations such as NIST[64][65] and GSMA[66] Specific to 5G networks the EU Cybersecurity Act will mandate certifications for specific components in 5G networks[67], particularly on the network level but users of 5G IoT networks are expected to require string security functions to enable the vertical applications. For components this means that they must include technology enabling high security such as cryptographic hardware, secure updates and a secure component supply chain from cradle to grave. There is an opportunity in being able to early on supply the security needed by future networks and applications.

SNS JU will not directly be involved in component research, development and design. However, the research and development in the SNS JU will enable other initiatives to provide the know-how and later the design and production of communication and computing components.

These activities will help to facilitate the re-launch of the micro-electronics industry in the ICT domain in Europe by means of cooperation with the Chips JU by promoting the development of European added value embedded solutions for innovative and secure applications. SNS JUs will develop the communication know-how and IPRs and will provide algorithms to the micro-electronics industry, which will be dealing with the design and production. With this approach ongoing activities in the Chips JU can be leveraged. From the SNS JUs perspective that could be a fabless approach. A joint effort of different Partnerships under Horizon Europe will involve the appropriate expertise from different communities.

3.7.2 Approach for devices

Devices and especially end devices for IoT and vertical applications including critical infrastructures are an essential part of future networks. In addition to components, they also must fulfil a high security level.

[58] NIS Directive, https://digital-strategy.ec.europa.eu/en/policies/nis-directive

[59] Cybersecurity Resilience Act, https://www.chips-ju.europa.eu/

[60] Executive Order on Improving the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[61] ENISA Guidelines for Securing the Internet of Things, https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[62] ENISA Good Practices for Security of IoT, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

[63] ENISA Baseline Security Recommendations for IoT, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[64] NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline, https://csrc.nist.gov/publications/detail/nistir/8259a/final

[65] NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers, https://csrc.nist.gov/publications/detail/nistir/8259/final

[66] GSMA IoT Security Guidelines and Assessment, https://www.gsma.com/iot/iot-security/iot-security-guidelines/

[67] Securing EU's Vision on 5G: Cybersecurity Certification, https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

The SNS JU is enable and validate, among others, specialised devices for IoT and sensor systems especially for vertical sectors by leveraging system on chip activities and specifying the way they communicate in the network/systems as well as controlling them and integrating them in their operational systems in vertical (and as well cross- vertical) application domains by means of cooperation with the Chips JU and leveraging AIOTI activities.

System on chip activities can be leveraged for such industrial device activities. The close cooperation between vertical sectors and the ICT industry in Europe will support the development of entire communication and networking solutions in Europe. These activities offer opportunities for start-ups to design communication modem chips and other components devised for many vertical applications.

Devices must be designed with a security first approach, considering the whole life cycle of devices. Especially for critical infrastructure this will be mandated early on but these requirements will also affect other devices as the threat landscape continues to evolve, expanding on the opportunity. For devices this means that manufacturers must adopt a holistic view on supply chain security including all components that go into the device. The device must contain enough security functionality to enable the user to adopt zero trust and zero touch architectures and paradigms including verifying the supply chain, secure deployment of devices and secure life cycle management of devices over the whole device lifecycle, including potential ability to upgrade to future post quantum cryptographic algorithms.

3.7.3 Requirements for IoT devices

Devices with IoT gateway capabilities in support of different IoT connectivity modes, both at local and public network level. In particular for each supported vertical industrial domain and as well cross vertical industry domains:

- requirements will be derived on which software and hardware capabilities and characteristics these multi-modal IoT devices and network elements should support, when integrated and used into the 5G and beyond 5G network infrastructures. Considering that these IoT devices support e.g., wireless technologies that are non-5G and beyond 5G radio technologies, such as Bluetooth, Wi-Fi, ZigBee, LoRa, Sigfox.
- integration and evaluation activities of these multi-modal IoT devices and network elements in the 5G and beyond 5G network infrastructures will be planned and executed.
- Hardware requirements for IoT Devices:
  - Requirements applied for each supported vertical industry domain and as well cross vertical industry domains when integrated and used into the 5G and beyond 5G network infrastructures.
  - At least three different frequency bands for sub-1 GHz, (700 MHz), 1 - 6 GHz (3.4 - 3.8 GHz), and millimetre-wave (above 24 GHz) and integrate multiple protocols in addition to cellular ones.
  - Functional and non-functional requirements, such as high data capacity, highest levels of reliability (connectivity), fast reaction times (low latency), sensing/actuating, processing and storage capabilities; low power consumption.
  - Strong security functionality with hardware cryptographic security modules, initial device identities and upgradable cryptographic algorithms.

3.8 EU legislative framework

Many of the gaps identified for the coverage of remote areas, or with very little population density are still not properly addressed today, where no public network coverage is available. This requires the need to create new technological solutions, where you can combine resources from different suppliers. One of the options could be linked to the use of equipment in the fields, which could be used as relays to reach an area covered by a tower. However, the implementation of such solutions should not modify the behaviour of the integrity of such equipment.

Many conformity assessments for safety and security are today supported by the Original Equipment Manufacturer (OEM) to validate the compliance of an equipment to get the CE marking and homologations or certifications. These requirements are applied on equipment used in the fields and/or potentially used on a public network.

The use of the European and international standards is needed to allow proper risk assessments under the future regulation for machineries replacing the current Machinery Directive (2006/42/EC). Integrating new technologies (IoT devices, AI/ML, cyber-security, autonomous features, etc.) into the Essential Health and Safety Requirements, while maintaining high levels of safety and security, and protecting the OEM against potential litigations, is challenging. This comes to the proposal of a valid business case to engage OEM in standard developments with a good legislation. The ultimate goal is to protect the end user while mitigating the risk of misuse of the equipment.

With the connectivity of such equipment, the OEM sometimes can hardly differentiate which legislation is on top of the other, when he reviews the Radio Equipment Directive, the Electro-Magnetic Compatibility directive, and the Machinery Directive. This is the reason why the technical specifications to implement such relays will determine a hierarchy and include the compliance to these European legislations to address these risks at the same time.

Part of these requirements includes privacy and trust in the data transferred. The data governance is not part of the scope and the solution to develop is to provide the access to an area covered by a telco provider through the relays supported by the equipment in the fields.

The requirements mandated in the new EU legislation such as Cybersecurity Resilience Act and AI Act[68] also need to be taken into account.

[68] AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689&qid=1734865191801

4. Conclusions and Recommendations

It is expected that 5G and beyond 5G systems will extend mobile communication services beyond mobile telephony, mobile broadband, and massive machine-type communication into new application domains, so-called vertical domains.

[AIOTI-IoT-relation-5G] highlighted specific IoT vertical domain use cases and determined the specific requirements they impose on the network infrastructure. This report highlights additional IoT and Edge Computing vertical domain use cases collected by AIOTI and determines the specific requirements they impose on the underlying 5G and Beyond 5G network infrastructure. These use cases and requirements can be used by Standards Developing Organizations (SDOs), such as 3GPP, ITU-T, ISO and IEEE as requirements for automation in vertical domains focusing on critical communications. In addition to these use cases also emerging topics in the area of 5G/6G technology are as well introduced.

In particular, this report lists first relevant IoT and edge computing use cases and their possible requirements on an underlying 5G/6G communication infrastructure.

The Release 2.0 of this report included 6 additional use cases in the areas of: (1) use of drones, (2) 5G cloud-RAN, (3) Health-Critical Remote Operations, (4) preliminary 6G use cases. Secondly, emerging topics in the context of the Beyond 5G communication infrastructure, relevant for IoT and edge computing use cases are identified.

The Release 3.0 of this report includes 6 additional use cases as well in the area of Edge-Cloud Orchestration in Section 2.13.

In this Release 4.0 of this report 14 additional use cases in various areas are included.

4.1 Requirements

By analysing the requirements that are derived from the presented use cases as described in the Section 2, it can be concluded that for these use cases the requirements listed in [Networld2020-SRIA] report, see Annex III as well are covering the needs that each of these use cases impose on the underlying 5G/6G infrastructure.

In particular, requirements are identified by these use cases added in this Release 4 of the report:

2.3 Digital Twin (DT)

2.3.2 EVOLVED-5G: "Efficiency in FoF Operations with Novel Predictive Maintenance applied on Digital Factory Twin

Requirements:

THE EVOLVED-5G PLATFORMS The EVOLVED-5G project makes use of two different platforms located in Athens (composed by two sites: NCSR Demokritos and Cosmote) and Málaga. The two platforms provide 5G capabilities and cloud infrastructures where Open5Genesis framework for the coordination of the experiments is deployed.

The two platforms provide support for the execution of the Validation and Certification processes, by making available their containerization environments for the deployment of the Network Applications, as well as a real 5G network that Verticals can use for the execution of additional tests more related to the specific functionality of each particular Network App.

The Athens platform is comprised of two testbeds, NCSRD and COSMOTE, which are interconnected through a 10G direct fiber link. For platform assessment, the two sites act as independent full 5G SA solutions that are evaluated using the Open5Genesis experimentation framework, which dictates the lifecycle of the experiments. As shown in Figure 1, Open5Genesis is hosted at NCSRD's premises and manages and orchestrates all the experiments.

The first 5G SA network is based on the ATHONET 5G SA Core and ERICSSON BBU/RRU/RAN which is deployed at the COSMOTE campus. The second 5G SA network is deployed at the NCSRD campus and is based on the Amarisoft 5G solution.

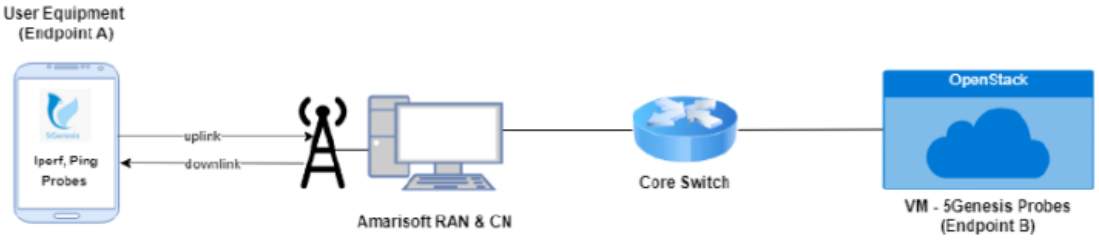


Figure 76: NCSRD site testbed setup

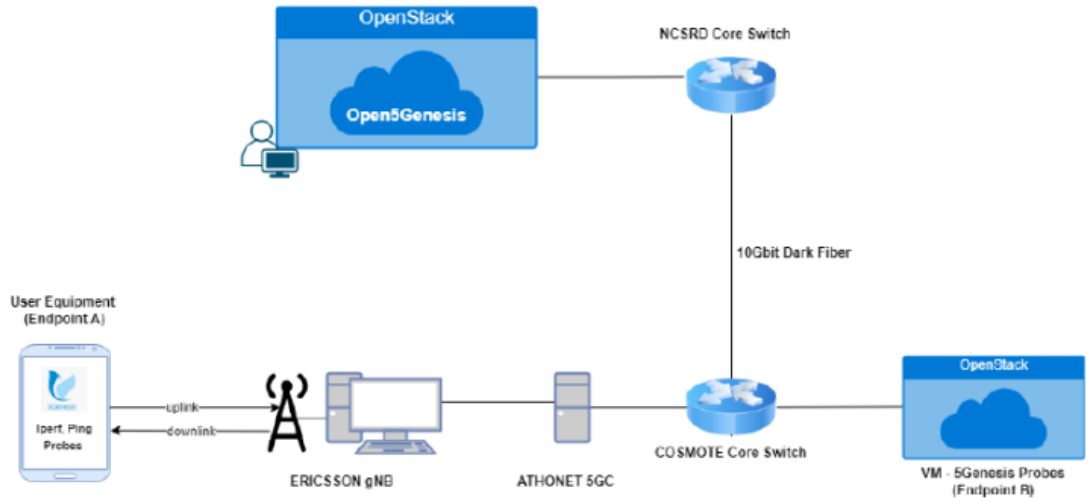


Figure 77: COSMOTE - NCSRD sites testbed setup

The framework is composed of three layers:

Management and Orchestration (MANO) layer: Handles virtualization, network slices, and virtual resources management.

Coordination layer: Responsible for the overall coordination of the experiments, including experiments' life cycle management, KPIs monitoring, and analytic results presentation.

Infrastructure layer: Handles user traffic providing 5G network connectivity.

Throughput measurements

Amarisoft/NCSRD Downlink Mean Throughput: 331.3 Mbps

Athonet-Ericsson/COSMOTE Downlink Mean Throughput: 905.73 Mbps

Amarisoft/NCSRD Uplink Mean Throughput: 48.49 Mbps, best: 214.18 Mbps

Athonet-Ericsson/COSMOTE Uplink Mean Throughput: 67.58 Mbps

Latency measurements

Amarisoft/NCSRD Mean RTT: 28.69 ms, Lowest: 9.99 ms

Athonet-Ericsson/COSMOTE Mean RTT: 15.78 ms

2.5 Autonomous Urban Transportation

2.5.2 5G-VICTORI: UC #1.1: Enhanced Mobile Broadband under High Speed Mobility

Requirements:

The 5G-VICTORI track-to-train communication is using a heterogeneous wireless network, consisting of sub-6GHz technologies, through IEEE 802.11ax devices, and V-Band 60 GHz mmWave links. The resource heterogeneity will assist in exploring the diversity that accessing different spectrum provides, allowing the setup of robust track-to-train communication links.

Table 34: UC # 1.1 Requirements foreseen in FRMCS and 5G landscape

UC # 1.1: Enhanced Mobile Broadband Under High Speed Mobility Vertical: Transportation – Rail			Services			
			Future Train operation services (URLLC)	Critical (CCTV)	Other Passenger Services (eMBB)	MCPTT
UC Requirement - KPI		Units				
1	Latency (min. between user service end-points)	ms	20-100 ms	100 ms	Non Critical	20 ms
2	User Datarate (Max.)	Mbps	100 kbps	10-15 Mbps (Uplink)	~10 Mbps / passenger	100 kbps
3	Reliability (%) - Min/MAX	%	99.9999% (SIL4)	99.9999% (SIL 4)	Not Critical	99.99% (SIL2)
4	Availability (%) - Min/MAX	%	99.9999% (SIL4)	99.9999% (SIL 4)	Not Critical	99.99% (SIL2)
5	Mobility	km/h	50-150 km/h	50-150 km/h	50-150 km/h	50-150 km/h
6	Traffic Density (Traffic demand per specific area)	Mbps / area surface	Non Critical	150 Mbps	max. 1-2 Gbps, assuming 5-10 Mbps/ passenger @ train or station, Total: 100-300 passengers in a cell coverage area, ~max. ave. 1-2 Gbps	Non Critical
7	Device Density (#Devices per specific area)	Devices/ area surface		(non-critical) 2CCTV cameras / train, 5 trains in area of coverage	100-300 passengers/ users per cell coverage area	5 trains in area of coverage
8	Location Accuracy	m	1 m			
Additional Requirements						
9	Packet Loss Ratio	Num	10^{-6}	0.005	Non Critical	10^{-6}
10	Bit Error Rate		Mission critical	Mission critical	Non Critical	Critical
11	Security (Y/N) ("Carrier Grade")	Y/N	Y	Y	Y	Y
12	Type of Device		IoT devices/ Cameras/ Gateways	CCTV Cameras	Smartphones	KCC clients/ UEs
13	Type of Connection (i.e. Ethernet, WLAN, Zigbee)		5G/NB-IoT/Wi-Fi	5G/Wi-Fi	5G/Wi-Fi	5G/Wi-Fi
14	Battery Lifetime		Non Critical	Non Critical	Non Critical	Non Critical

Table 35: UC # 1.3 Network Characteristics Requirements and KPIs

Req ID [U/F-TYPE-RQ#]	Description [Descriptive text]	Priority [H/M/L]	KPIs and Parameters [to be measured]
F-PE-3201	The Rail Critical Services and other on-board vertical services, using the same 5G air-interface frequency spectrum band 3.8 GHz and the same 5G CPE gateway, **shall** show good performance isolation between the different vertical services, using slicing and QoS.	H	Check isolation between different vertical services using the same 5G air-interface spectrum band.
F-PE-3202	The onboard 5G Customer Premises Equipment (CPE) modem **shall** supports doppler up to at least a train speed of 100 km/h. The reason is to make the 5G connectivity periods longer than what a non-doppler capable modem offers (5G connectivity only when the train stands still).	M	Check that the onboard CPE can connect to the 5G cellular network at a train speed of at least 100 km/h and convey data between onboard and office.
F-PE-3203	The Rail Signaling traffic that are used for the 5G demo purposes onboard the train **shall** have access to a 5G cellular network bitrate between the train and office of around 200 kbps.	M	Check that rail traffic signaling can use a bitrate of around 200 kbps over the 5G cellular network.
F-PE-3241	The HD CCTV cameras that are used for the 5G demo purposes onboard the train **shall** each have access to a 5G cellular network bitrate between the train and office of around 5 Mbps, i.e. 10 Mbps for two HD CCTV cameras.	M	Check that each onboard HD CCTV camera can use around 5 Mbps over the 5G cellular network.

Radio Specific requirements

Radio Coverage

Radio cell range

Does the radio link crosses public spaces? Or is it constrained to indoor or customer premises?

Sub-6 GHz units demonstrated very high coverage (close to 1 km outside the target area of coverage) without LoS. This feature would render them a fit solution for the cases where the terrain only provides nLoS links.

mmWave was able to connect up to 75 m away from the nodes

The coverage is constrained to private places (the railway track) in Patras

Is Multicell required?

Is handover required? Seamless? Tolerable impact in delay and jitter?

Handover or mobility management is required for the connectivity in the track to train communication between Sub-6 and mmWave nodes that are deployed along the rail track.

The mobility management framework needs to cope with handovers in the same technology (change in the association of the onboard mmWave unit **T1**/**T2**), as well as changes across different technologies (handover between different stanchions). The mobility management framework is programming dynamically the flows in the P4 software switches either on the train, or the operation room, so as traffic entering/exiting the track-to-train network is always depicted in the same manner at the two endpoints. To this aim, the flows are set to mangle packet headers (MAC and IP layer) as they go through the switch, and the output port for the ingress/egress traffic is determined by each flow.

Cross-technology handover: Instantaneous losses (lasting less than 500 ms) for packets currently in transit to the network.

Bandwidth requirements

Sub-6 the most stable setup (and given the mobility of the train) was achieved with the 3x3 MIMO setup for the 802.11ac cards, allowing effective throughput when using a static setup of up to 550 Mbps. Throughput of up to 900 Mbps was observed in the 4x4 MIMO setup, but in a highly unstable manner, and hence the 3x3 setup was used.

Towards being able to achieve higher Modulation and Coding Schemes (MCS) in higher distances, directional panel antennas were used and mounted on the stanchions. The antennas were configurable for their sector size to 60, 90 or 120 degrees (and respective gains of 21, 20 and 19 dBi). Through extensive testing, the 90-degree configuration yielded the highest throughput in higher distances and was selected for the final demonstration.

mmWave (60 GHz)

The mmWave nodes are COTS 60-GHz 802.11ad-compliant devices (Mikrotik wAP 60Gx3). They utilize Qualcomm QCA6335 chip for digital signal processing, supporting up to MCS8 according to the IEEE802.11ad standard. The radio-frequency (RF) front-end is based on Qualcomm's QCA631 chip with three 6x6 phased-array antennas supporting beam steering in 2D. With three sectors, the modules are capable of 180° coverage in azimuth. However, a **net data rate of 1 Gbps** is possible because of 1 GbE connection.

Is traffic packet mode or circuit mode?

The traffic is packet mode.

Radio regimens requirements

Desired and acceptable radio regimens

Unlicensed schemes due to the use of ISM bands at both Sub-6 and mmWave (60 GHz unlicensed)

Other requirements

Is terminal location required? location accuracy?

Onboard 5G Network demonstrating the connectivity within the onboard network and the connectivity between the onboard (standalone) network to the 5G-VINNI facility (control room) while the multi-technology (Sub-6 GHz and mmWave) backhaul network is operational.

5G UEs are laptop with Quectel RM500Q-GL modem and **Google Pixel 6 phone** for connecting to the 5G network onboard the train.

static testing:

5G-NR throughput test: peaking at 109Mbps for SISO configuration, for 2x2

MIMO up to 230Mbps were observed, RTT=~ 14ms

Mobility Testing:

5G-NR throughput test: variations between 50-109Mbps, RTT depending on the technology backhaul (mmWave backhaul RTT=~ 14ms, Sub-6 GHz RTT=~ 14 – 25 ms)

2.5.3 5GMETA: Driving Safety & Awareness

Requirements:

Table 8 shows the list of KPIs of UC3 with a general description and their target values.

Table 36: KPIs for Use case: Driving Safety & Awareness

Evaluation metric	Description	Target values
Latency	End-to-end latency between misbehaving vehicle and MEC/Cloud services. Low latency is required for road safety	< 100 ms
Reliability	Communication reliability between misbehaving vehicle and MEC/Cloud services. High reliability is required for road safety	> 99.9%
Misbehaviour Detection latency	Time needed for detecting driving misbehaviour starting from the moment when all needed data are available	< 200 ms
Misbehaviour Response latency for ETSI Basic Services	Time needed to alert surrounding vehicles from the moment when all needed data are available	< 100 ms

2.7 Critical Infrastructure support applications

2.7.3 ERATOSTHENES: Smart Health

Requirements:

A number of functional requirements for Pilot 2:

Consistent representation of trust relationships in personalized health devices

Assignment of trust score measurement to every device

Automatic deployment and update of software

End to End Cryptography

A number of non-functional requirements for Pilot 2:

Increase the average speed of software updates

Accuracy on detecting attacks and/or anomalies

Reduction of checking time of context condition for emergency situations

Radio Specific requirements

Only preliminary information is provided.

Radio Coverage

Radio cell range

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

Radio link crosses public spaces

Required scope of the multicell arrangement:

Global

Mobility: maximum relative speed of UE/FP peers

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

Special coverage needs

Healthcare

Bandwidth requirements

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

URLLC requirements

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

Radio regimens requirements

Desired and acceptable radio regimens

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

Other requirements

Requirements related to monitoring metrics of the gateway such as the OS-version, connectivity issues related to Internet speed, CPU usage, memory usage

Protection of personal identifiable information based on GDPR

2.7.4 ERATOSTHENES: Connected Vehicles

Requirements:

Functional Requirements

Integration of Advanced driver-assistance systems Platform Tool client with ERATOSTHENEES modules

Reliable and scalable communication of ERATOSTHENES server to support the Distributed Ledger Technology (DLT)

Reliable integration of ERATOSTHENES sub modules with its clients counterpart (e.g., Self-sovereign Identity (SSI) Management module.

Reliable integration of Trust Management Broker (TMB) in ERATOSTHENES server, which acts as a communicator between the IDAPT client modules and the trust modules in the Domain (e.g., Trust Management and Risk Assessment (TMRA), Manufacturer Usage Description (MUD) management, Cyber Threat Intelligence Sharing Agent (CTISA), and Intrusion Detection System (IDS) modules) .

The system should be able to detect and respond (e.g. mitigate) to attacks.

Non-Functional Requirements

Reliable communication between the emergency bodies due to the information nature.

Secure and Privacy-Preserving Information Sharing

Efficient resource utilization (device/network)

Radio Specific requirements

Radio Coverage: Not applicable

Expected maximum and typical radio range:

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

Radio link crosses public spaces

Required scope of the multicell arrangement:

Global

Is handover required?

Mobility: maximum relative speed of UE/FP peers

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

Special coverage needs

Transportation

Bandwidth requirements

Network load (kb/s): To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

URLLC requirements

Required Latency, reliability and Maximum tolerable jitter:

To be performed when in the full use case environment with final versions of ERATOSTHENES modules.

Radio regimens requirements

Desired and acceptable radio regimens:

To be performed when in the full use case environment with final versions of ERATOSTHENES modules

Other requirements

To be performed when in the full use case environment with final versions of ERATOSTHES modules.

CPU usage (%)

Time between first message send/receive

Time between message receive/ present on HMI

Time for any message (not just first)

Total time for message through system (ms)

Timely response to attacks (detailed fully in trials plan)

2.8 Smart Manufacturing and Automation

2.8.3 5G-VICTORI: UC #2: Factories of the Future

Requirements:

The service performance requirements for the main communication services categories foreseen in the forthcoming smart factory/ digital utilities and 5G landscape are summarised in **Table 14.**

Table 37: UC # 2 Key UCs requirements and KPIs

Vertical: Smart Factory			UC # 2 – Digitization of Power Plants		
			Monitoring & Alerting Services (URLLC)	Maintenance Services (mMTC)	CCTV(as eMBB type of service)
UC Requirement - KPI		Units			
1	Latency (min. between user service end-points)	ms	10 ms	Not Critical	100-150 ms
2	User Datarate (Max.)	Mbps	0.1 Mbps (per device)	1-100 kbps (per sensor)	10-15 Mbps (Uplink, per HD/4k camera)
3	Reliability (%) - Min/MAX	%	> 99.9999999% (SIL 7)	>99%	99.9999 % (SIL 4)
4	Availability (%) - Min/MAX	%	> 99.9999999% (SIL 7)	>99%	99.9999 % (SIL 4)
5	Mobility	km/h	0 km/h	0 km/h	0 km/h
6	Traffic Density (Traffic demand per specific area)	Mbps/ area surface	Low, not critical 1000 Mbps/ 2000 m^2	Low, not critical 1000 Mbps/ 2000 m^2	20-100 Mbps / 2000 m^2
7	Device Density (#Devices per specific area)	Devices/ area surface	Low, not critical 100 Dev over 2000 m^2	100 Dev over 2000 m^2	Low, not critical 20 cameras/ 2000 m^2
8	Location Accuracy	m	non critical because the deployment is static thus the sensors' location is already known	non critical because the deployment is static thus the sensors' location is already known	non critical because the deployment is static thus the sensors' location is already known
Additional Requirements					
9	Packet Loss Ratio	Num	10^{-9}	10^{-6}	0.005
10	Bit Error Rate		Mission critical		Mission critical
11	Security (Y/N) ("Carrier Grade")	Y/N	Y	Y	Y
12	Type of Device		IoT devices/ Cameras/ Gateways	IoT devices/ Gateways	CCTV Cameras (possibly FHD/4K)
13	Type of Connection (i.e. Ethernet, WLAN, Zigbee)		5G/NB-IoT/Wi-Fi	5G/NB-IoT/Wi-Fi	5G/Wi-Fi
14	Battery Lifetime		Non Critical	up to 10 years	Non Critical
15	User Datarate (Max.)	Mbps/ sampling point	Non Critical	2-10 Mbps	Non Critical

Table 38: UC # 2 Network functional requirements and KPIs

Req.ID [U/F-Type-RQ#]	Description [Descriptive text]	Priority [H/M/L]	KPIs and Parameters [to be measured]
S-FU-5301	**Air Interface – Access Network** Towards delivering the required network coverage for the specific devices, it is needed to design and develop antennas operating at 5G/ Wi-Fi & NB-IoT frequency bands.	H	• Antenna operation at 5G, Wi-Fi and/or NB-IoT support.
S-FU-5302	**Distributed Pools of (Compute/Network) Resources** Towards achieving the stringent QoS targets as well as efficient resource utilisation, it is necessary to enable instantiation of network, compute and storage resources optimally selected from a common resource pool that is physically distributed. This requires that the deployment is based on distributed (at different geographical locations, e.g. in the notion of edge computing) pools of resources (i.e. DCs) where the allocation is based on specific QoS and resources requirements.	H	• Capability for instantiation of network and compute resources for a specific service over geographically distributed pools of resources. It shall be possible to use various Edge and Core DCs to host different parts of the Power Plants Monitoring and Preventive Maintenance Applications. • Monitoring of distributed resources pools from a common platform.
S-FU-5303	**Multi-Tenancy** The 5G facility needs to support simultaneously multiple tenants and multiple services, with various QoS, requirements, etc., over a single infrastructure. Since it can be possible that different departments make use and have access rights to different monitoring and maintenance applications/ information over the same ADMIE facility (e.g. one department can control the CCTV cameras, and another one can be in charge of monitoring the cable status), it shall be possible from the 5G facility to allow the creation of multiple tenants for this scenario.	H	• Delivery of services with the requested QoS to multiple tenants over a single network deployment.

2.8.3.11 Radio Specific requirements

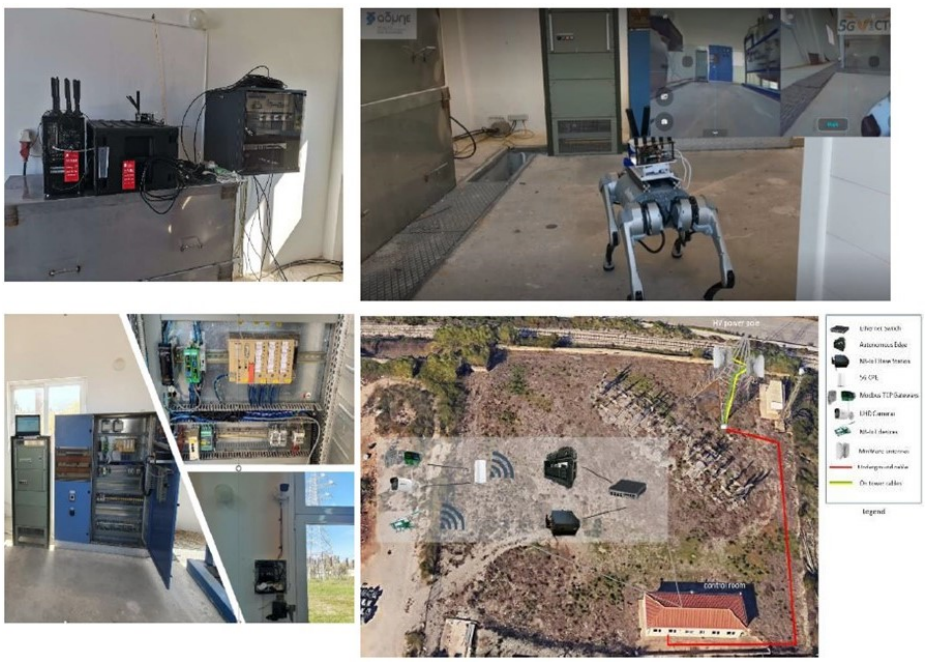


Figure 78: a) 5G network deployed at ADMIE facility for Patras trials, b) robotic camera for the high voltage environment with live streaming over 5G, c) various interconnected sensors at the high voltage facility

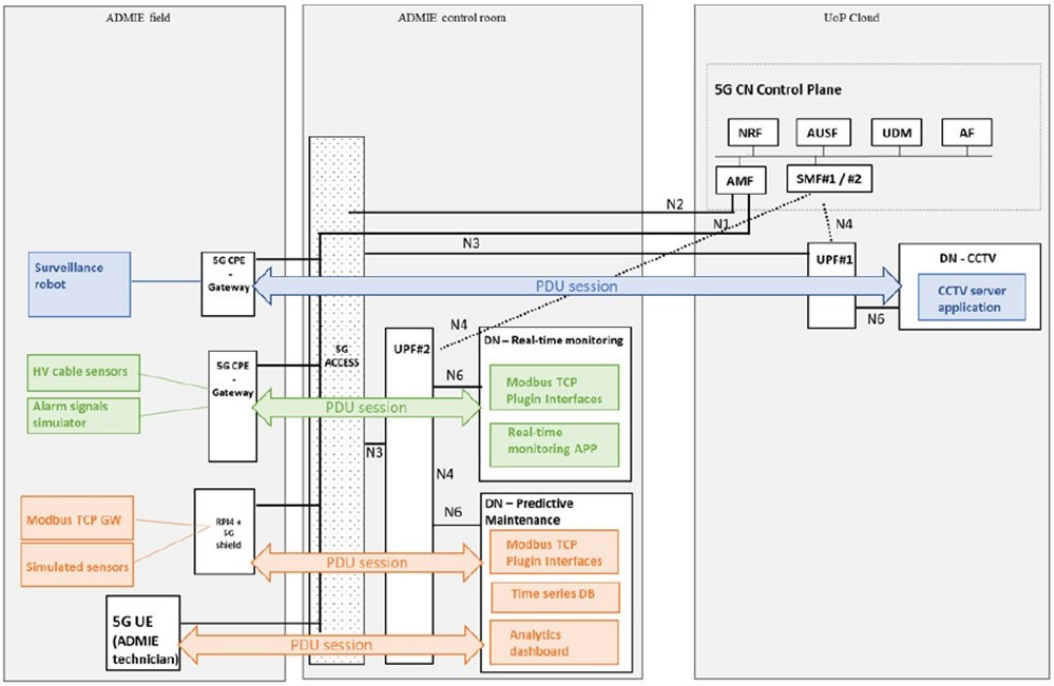


Figure 79: High-level architecture of UC #2

CCTV monitoring of facilities over 5G provides live video feed when technical personnel is present or an event occurs, while not compromising other Industry 4.0 applications running in the background. For the demonstration of this service, two UHD CCTV cameras are installed inside the HV cable control room and a third robotic camera is used inside the Smart Factory facility. The purpose of the Facility CCTV Monitoring service on high-level is the following:

Provide network slice customized for CCTV monitoring.

Demonstrate that CCTV Streaming is conveyed over 5G with the required characteristics, regardless of other services and background traffic.

Table 39: High-Level 5G Deployment Scenario UC #2

Scenario Description Template – Lab		
Radio access technology (RAT)	5G VINNI _3 (AW2S)	5G VINNI_4 (Callbox Classic)
Standalone / Non-Standalone (if applicable)	SA	SA
Cell Power	33 dBm	20 dBm
Frequency band:	n78	n78
Maximum bandwidth per component carrier	100 MHz	50 MHz
Sub-carrier spacing	30 KHz	30 KHz
Number of component carriers	n/a	n/a
Cyclic Prefix	n/a	n/a
Massive MIMO	n/a	n/a
Multiple-Input Multiple-Output (MIMO) schemes (codeword and number of layers)	4x4 MIMO	2x2 MIMO
Modulation schemes	Downlink: 256 QAM Uplink : 256 QAM	Downlink: 256QAM Uplink: 256QAM
Duplex mode	TDD	TDD
TDD uplink/downlink pattern	7 Down / 2 Up timeslots	7 Down / 2 Up timeslots
Contention based random access procedure/contention free	n/a	n/a
User location and speed	n/a	n/a
Background traffic	n/a	n/a
Computational resources available	n/a	n/a

Table 40: CCTV services report from tests done at the Field Demo in Patras

Field	Description
Test Case ID	**EDCv01**
Facility, Site	5G-VINNI, ADMIE site
Description	This test case demonstrated the provisioning of a CCTV network slice for critical assets monitoring over a private 5G network, where the CCTV equipment are connected over the mmWave backhaul to the UoP cloud (e.g. ADMIE offices) where the Open5GS Core Network and facility CCTV monitoring service were instantiated.
Executed by	Partner: ADMIE, ICOM, UoP
Purpose	Smart CCTV surveillance services for industrial environments over 5G
Scenario	**EDCv01**
Slice Configuration	CCTV slice
Components involved	MEC server (Autonomous Edge + gNB) CCTV camera Mobile surveillance robot with 5G connectivity Network switch mmWave 10Gbit Link UoP DC
KPIs collected (Metrics collected)	CCTV camera datarate, mobile surveillance robot camera datarate, CCTV streaming latency, CCTV maximum packet loss ratio
Tools involved	wireshark
Results and KPIs **Primary** **Complementary**	Video streaming latency: Min = 0.9 s/ avg = 2.32 s / max latency = 5.01 s (including application processing overhead) CCTV camera datarate: Min = 6.5 Mbps / avg = 9.33 Mbps / max bitrate usage = 12.78 Mbps 5G-enabled mobile surveillance robot camera datarate: Min = 0.4 Mbps / avg = 1.5 Mbps / max bitrate usage = 2.5 Mbps Aggregated datarate: Min = 7.3 Mbps / avg = 11.03 Mbps / max bitrate usage = 15 Mbps
Target metric/KPI and verification (pass/fail)	Seamless provisioning with no interruption time achieved, throughput expected results achieved

Radio Coverage

Radio cell range

Specification of expected maximum and typical radio ranges (indicate if LOS/NoLOS)

10000 m2 with multipath

Does the radio link crosses public spaces? Or is it constrained to indoor or customer premises?

Constrained to an outdoor private area

Bandwidth requirements

CCTV camera data rate: Min = 6.5 Mbps / avg = 9.33 Mbps / max bitrate usage = 12.78 Mbps

5G-enabled mobile surveillance robot camera data rate: Min = 0.4 Mbps / avg = 1.5 Mbps / max bitrate usage = 2.5 Mbps

Aggregated data rate: Min = 7.3 Mbps / avg = 11.03 Mbps / max bitrate usage = 15 Mbps

2.9 Service Trust and Liability Management

2.9.2 5G COMPLETE: Example: UC#4: Advanced Surveillance/Physical Security Service Requirements:

Table 41: Enhanced Security

VU-OTH-20	Enhanced Security
Priority	Essential
Description	Enhanced security is required at the distributed pools of compute resources in order to ensure that the application components and software/data repositories are not compromised by malicious parties.
Success Criteria	Success Criteria: • Security is ensured at compute resources domain.
Use Case	UC#4

Table 42: High availability of Vertical Service

VU-OTH-21	High Availability of Vertical Service
Priority	Essential
Description	High Availability of the Vertical Service is needed.
Success Criteria	Success Criteria: • Ensuring 99.99%-99.9999%availability for 24x7 monitoring.
Use Case	UC#4

Table 43: Lifecycle management of Vertical Services

VU-PERF-19	Low Processing Delay
Priority	Essential
Description	Low processing latency is needed for specific functionalities (e.g. object detection/classification at high FPS (Frames per Second) from multiple cameras simultaneously).
Success Criteria	Success Criteria: • To simultaneously process all cameras' high FPS stream without delay (with respect to the real-time content).
Use Case	UC#4

Bandwidth requirements

Table 44: Low delay/latency

VU-PERF-17	Low Delay/Latency
Priority	Essential
Description	Low Delay/Latency is required between the cameras and the processing unit (i.e. MEC), which is critical for the real-time dispatching of object-tracking related commands (to be executed by the camera).
KPIs	KPI: <20ms
Use Case	UC#4

Table 45: High bandwidth

VU-PERF-18	High Bandwidth
Priority	Essential
Description	High Bandwidth is required to provide the capacity needed for a high number of cameras served from a specific FWA node (for live streaming, object tracking, etc.).
KPIs	KPI: > 8 Mbps per camera (depending on cameras' capabilities)
Use Case	UC#4

URLLC requirements

VU-OTH-21	High Availability of Vertical Service
Priority	Essential
Description	High Availability of the Vertical Service is needed.
Success Criteria	Success Criteria: • Ensuring 99.99%-99.9999%availability for 24x7 monitoring.
Use Case	UC#4

2.11 Preliminary 6G use cases

2.11.2 RISE-6G: Control for RIS-based localisation and sensing

Requirements:

Radio Specific requirements

In the context of radio systems, localisation (synonym: positioning) is the process of determining the 2D or 3D location of a connected device (a user equipment (UE)), based on uplink (UL) or downlink (DL) measurements with respect to several base stations (BSs) [PRL+18]. The measurements are performed based on the reception of dedicated pilot signals and can be of the forms described in

Table 23. Observe that a combination of angle and delay measurements can be used for UE localisation and that different measurement combinations put different requirements on both the number of BSs as well as on their mutual synchronisation. For this latter reason, pure ToA measurements with a UE synchronized to a BS is impractical in real scenarios, since even small synchronisation errors lead to large localisation errors (e.g., 10 ns clock error corresponds to 3 meters error). Examples of two different measurement for localisation are shown in **Figure 44.**

Table 46: Localisation measurements and requirements for 3D positioning

Measurement	UL or DL	Number of BSs needed	Comment
Time-of-arrival (ToA) of the first path	Either	3	BSs should be synchronized with the UE
Time-difference-of-arrival (TDoA), derived from several ToA measurements	Either	4	BSs should be mutually synchro-nized
Round-trip-time (RTT), derived from several ToA measurements	Both	3	No synchronisation needed
Angle-of-arrival (AoA) at the BS	UL	2	Requires planar arrays at each BS
Angle-of-departure (AoD) from the BS	DL	2	Requires planar arrays at each BS
TDoA+UL-AoA	UL	2	BSs should be mutually synchro-nized
RTT+ UL-AoA	Both	1	No synchronisation needed

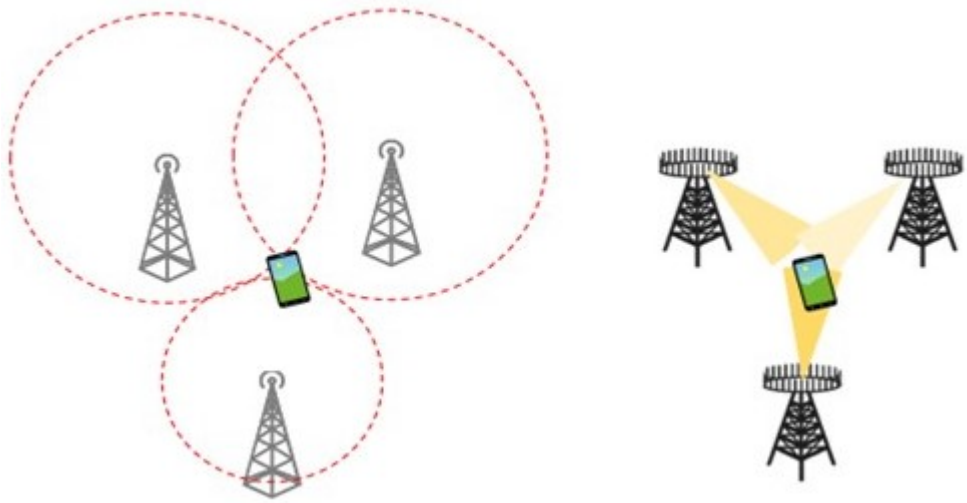


Figure 80: Example of RTT-based localisation (left), constraining the UE on the intersection of circles (2D) or spheres (3D); and localisation based on DL-AoD measurements (right), constraining the user within a sector of each BS

Bandwidth requirements

The amount of available bandwidth is directly related to delay resolution and thus to multipath suppression (in particular, two paths can be resolved if their delay difference is at least 1 over the bandwidth). If strong signal paths are present, say, 10 meters after the direct path, then a bandwidth of around 30 MHz is needed to resolve this secondary path. For that reason, a large bandwidth is important for accurate localisation in cluttered environments.

Other requirements

Transmission power: the accuracy of delay and angle measurements depends on the received signal-to-noise ratio (SNR), which is itself proportional to the transmission power. Hence, higher transmit powers lead to more accurate localisation, provided multipath can be resolved. Since localisation depends on pilot signals, an increase in SNR can also be achieved through longer transmission times.

Number of antennas: similar to bandwidth being related to delay resolution, so is the number of antennas proportional to angle resolution (the relation for a linear array is that two paths with angle difference (in radians) beyond 2/(number of antennas) can be resolved). Hence, a larger array of half-wavelength spaced elements leads to improved angular resolution.

Signal processing and hardware limitation: depending on the computational capacity and knowledge regarding the utilized beams, the delay and angle estimation performance can be improved. Moreover, hardware and calibration errors (e.g., synchronisation errors) significantly affect localisation performance, leading to a significant gap between theory and practice.

2.12. Drones

2.12.3 5G-INDUCE: Drone assisted network performance and coverage monitoring for industrial infrastructures

Requirements:

B5G/6G, a major driving force behind the vision of 6G, involves the deployment of connected and autonomous vehicle systems (CAVs) and drone communications. Research efforts in the field of CAV and drone-based communication systems have been steadily increasing in both academia and industry, targeting strict requirements, especially ultra-low latency and unprecedented communication reliability. As the industry is shifting towards wireless, real-time and high-throughput networking, drone base stations are envisaged to constitute pivotal assets. Table 28 showcases the main differences between 5G and 6G networks and the main improvements with regard to their core attributes.

Table 47: Mapping of functional to non-functional requirements

List of 5G-INDUCE **Functional** requirements	Prevailing **Non-functional** Requirements (ISO/IEC 25010)							
	Functional Suitability	Performance Efficiency	Compatibility	Usability	Reliability	Security	Maintainability	Portability
GPR.A (Generic platform impl.)	○	○	○	○	○	○	○	○
GPR.B (Generic OSS implementation)	○	○	●		○			
GPR.C (Generic NAO implementation)	○	○		○	○			
GPR.D (User Interfacing and sharing)	○			●		●	○	○
GPR.E (Security capabilities)	○		○		●	●		
GPR.F (Generic services' use cases)	●					○	○	●
GPR.G (Data processing and regulations)	○		●			○		
MSR.A (End user NAO interface)	○			●		○	○	
MSR.B (NAO)	○	○		○	○			
MSR.C (NAO-OSS Interface)	○		○					○
MSR.D (OSS)	○	●	○		○			
MSR.E (OSS-Network Orch. interface)	○		●				○	○
MSR.F (Network Orchestrator)	○	○	○		○			○

Table 48: Comparison of 5G and 6G attributes

2.13 Edge-Cloud Orchestration

2.13.7 5G COMPLETE: UC#3: 5G Wireless Transport services with MEC capability provided to Nos

Requirements:

Radio Specific requirements

Bandwidth requirements

Table 49: High-bandwidth wireless transport network links

P-PERF-12	High-bandwidth wireless transport network links
Priority	Essential
Description	High bandwidth wireless transport network links are required in order to meet the NO high datarate requirements. Optical network can provide scalable solutions for very high datarates at the transport network segments. At the same time, wireless transport network solutions are needed in order to address numerous infrastructure deployment challenges faced by the Infrastructure Provider and NO. Datarates of up to 2Gbps to dedicated last-mile transport links (potentially providing connectivity to gNBs and high datarate Wireless Access Points, e.g. WiFi6) are required to serve the cumulative datarate requirements at the access network nodes' level. Even higher transport network data rates are needed at the transport network segments where transport links are aggregated. 1st level aggregation of at least 4 last-mile transport links is common in network deployments.
KPIs	KPIs: • Capability of last mile transport network links to provide 2Gbps transport capacity. • Capability of transport network to perform 1st level aggregation of at least 4 last mile transport network links.
Use Case	UC#3

Table 50: Resilience

P-OTH-13	Resilience
Success Criteria	Success Criteria: • Demonstrate 5G wireless transport network deployments and functionalities in support of the required resilience.
Use Case	UC#3

2.13.8 5G-INDUCE: ML-Supported Edge Analytics for Predictive Maintenance

Requirements:

For this use case similar potential requirements apply similar to the use case: "Drone assisted network performance and coverage monitoring for industrial infrastructures".

2.13.9 AI@EDGE: Edge AI assisted monitoring of linear infrastructures using drones in BVLOS operation

Requirements:

Security and privacy requirements

Two different security levels can be distinguished:

High: The drone control channel must have the highest security level possible in order to limit radio interferences as much as possible.

Low: The data transmitted (video, datalink) also needs to be protected but it has less importance in terms of security. These levels could correspond to different slices, or even be within a given slice. Privacy: The main restriction founded on this aspect are video-images recorded subject to data protection. These images should be only accessible by the drone operator and central office, so that no external agent can view or use them.

Key Performance Indicators (KPIs)

Four main KPIs are of particular interest for the use case and are detailed in the following.

Environment KPI: Range: geographical reach of at least 20 km (according to the state of 5G technology and deployment at the trials).

Drone operation KPIs:

The latency KPIs sets as 100ms the maximum end-to-end latency budget. It is composed of two components:

Control Signal latency: it should be the lowest possible, and lower than 50 ms based on current awareness on the general system.

Video processing latency: it should be the lowest possible, so that the total end-to end latency budget lays below 100 ms.

A more precise assessment on the acceptable latency budget is needed to possibly update these preliminary figures, which will be done in WP5.

The reliability KPI (tentative metric) is in terms of control signal packet loss which should be lower or equal than 1%. This value is set because control signal must be ensured at all times.

AIF KPI: Mean Average AI Precision in object detection: in the integration of AI-assisted drone framework on the 5G network, detecting incidents through AI analysis processed on-board and at edge-node to generate response action from centralized control station. The metric commonly employed to evaluate the performance of the model for automated detection of incidents in the scenario is the Mean Average Precision (mAP), with an Intersection over Union (IoU) equal to 0.5. This target KPI for the AI@EDGE project, according to the dataset used for the project, will be mAP@.5 >= 0.6 (defining classes as identifiable items such as "persons" or "vehicles") - mAP@.5 refers to the mean average precision at an intersection over union value of 0.5.

Radio Specific requirements

Technical requirements Network Bandwidth and Slicing: The required 5G radio bandwidth will be proportional to the video definition and the number of users observing it through the 5G network, in this case the central office and the drone operator.

With respect to slicing, a secure and isolated environment is required to prevent interferences with external operators.

Computing: An edge computing/AI device or system of devices that allows to make an onboard 3D monitoring in real time for the use case application. Video data beamer bit-rate: the video stream bitrate needs a speed of at least 5 Mbps (HD) and it would be great to achieve Full HD or 25 Mbps (Ultra HD).

2.14 Smart Agriculture

2.14.1 COMMECT: Monitoring of Pest Insect Traps

Requirements:

The following requirements have been defined for this use case:

Fly Detection Accuracy: potential risk analysis based on olive fruit fly population

Uplink Throughput: uploading of machine vision pest monitoring photo

Power Consumption Decrease: extended battery durability of sensor equipment

Radio Specific requirements

Does the radio link crosses public spaces? Or is it constrained to indoor or customer premises?: The base stations give services to the traps and, at the same time, the mobile network operator customers in the region, like rural or suburban areas. The side to side distance is approximately between 5-10 km in rural or suburban areas

Mobility: No mobility is needed

Bandwidth requirements

Peak data rate: 4 Mbit/s

Average data rate: 2 Mbit/s

Is traffic packet mode or circuit mode? Packet mode

URLLC requirements

N/A

2.14.1.11.5 Radio regimens requirements

Desired and acceptable radio regimens: Licensed – public mobile.

Other requirements

UE power consumption

Rechargeable or primary battery? Rechargeable battery

Acceptable battery life: 10 years

Is terminal location required? location accuracy? No, it is not needed.

2.14.2 COMMECT: Securing crops and equipment

Requirements:

Technical requirements:

Video processing: The edge computing infrastructure must support real-time processing of video streams. The insights generated can be variable, depending on the needs of particular agricultural operations and deployment context. A minimum of two video streams should be processed simultaneously.
Edge ML remote configuration: power consumption, battery status, and power requirements of active ML algorithms must be monitored. Edge devices should be remotely configurable to optimize power consumption as needed.
The table below summarizes technical requirements for this use case. Table is copied from *Deliverable 1.2 Report on COMMECT requirements and KPIs*.

Requirement 5. ID	6. Description	7. Technical Requirement(s)	8. Target Value
R5.8	Edge ML computing infrastructure	Video processing	>=2
R5.9	Power consumption and power requirements monitoring	Edge ML remote configuration	Remote configuration supported and enabled.

Non-functional requirements:

Flexibility: The system must be adaptable to various agricultural environments, crop types, and evolving technology requirements.

Integration capability: The system should seamlessly integrate with existing technologies and digital IoT solutions.

Continuous operation: The system must ensure continuous operation to maintain effective security and crop monitoring functions.

Radio Specific requirements

Radio Coverage

Outdoor radio link

Low power, long-range for sensors in the field

WiFi or cable for video cameras

Mobility is welcome, but not mandatory

Bandwidth requirements

The solution addressing the use case is designed to maximize the edge processing and minimize the amount of data transferred to cloud. Current 4G connectivity supports well the scenario. However, if edge processing is not used and more remote management required (e.g., remote control of drones monitoring and spraying crops), that increased throughput and minimal latency would be required.

URLLC requirements

N/A

Radio regimens requirements

No particular requirements. What is important, is availability of reliable communication network.

Other requirements

Sensors: long duration battery (at least one season), replaceable or rechargeable.

Edge: rechargeable without interruption.

Ability to automatically determine location of the edge server is preferrable. GPS accuracy. Location of sensors is welcome if it does not significantly impact the battery lifetime.

4.2. Emerging Topics

The following emerging topics that are related to IoT and Edge Computing that can impact the specifications and deployments of beyond 5G communication infrastructure, are identified:

1. Digital Twin (DT)
2. Deep Edge, Terminal and IoT Device Integration in B5G communication infrastructure
3. Edge, Mobile Edge Computing and Processing
4. Network and Server security for edge and IoT
5. Plug and Play Integrated Satellite and Terrestrial Networks
6. Autonomous and Hyper-connected On-demand Urban Transportation
7. Opportunities for IoT Components and Devices
8. EU legislative framework

For each of these emerging topics an overview and as well challenges are identified and briefly explained in Chapter 3.

ANNEX I Reference

AIOTI-IoT-relation-5G] "IoT Relation and Impact on 5G", AIOTI, Release 3.0, April 2020, to retrieved via (accessed on 23 July 2021): https://aioti.eu/wp-content/uploads/2020/05/AIOTI-IoT-relation-and-impact-on-5G-R3-Published.pdf

[3GPP-TSG-RAN89E] 3GPP TSG RAN#89E, RP-201702: https://www.3gpp.org/ftp/TSG_RAN/TSG_RAN/TSGR_89e/Docs/RP-201702.zip

[5GPPP-Vision] 5G Vision, The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services, 5GPPP, February 2015, to be retrieved via: https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf

[3GPP TR 22.804] 3GPP TR 22.804, "Study on Communication for Automation in Vertical domains", Online: http://www.3gpp.org/DynaReport/22804.htm, 2018.

[5GPPP-verticals] 5G-PPP, "5G Empowering Vertical Industries," 02 2016. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2016/02/BROCHURE_5PPP_BAT2_PL.pdf.

[b-3GPP TR 26.918] Technical Report 3GPP TR 26.918 V16.0.0 (2018), 3rd Generation Partnership Project; Technical specification group services and system aspects; Virtual reality (VR) media services over 3GPP (Release 16).

[b-ETSI TR 126 928] "Extended Reality (XR) in 5G", 3GPP TR 26.928 version 16.1.0 Release 16, Jan 2021, to be retrieved via: https://www.etsi.org/deliver/etsi_tr/126900_126999/126928/16.01.00_60/tr_126928v160100p.pdf

[CiNe19] C. Cimino, E. Negri, L. Fumagalli, "Review of Digital Twin applications in manufacturing", Computers in Industry, 2019, 113, p.103130.

[Glaes12] E. S. D. Glaessgen, "The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles," in 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference - Special Session on the Digital Twin, Honolulu, HI, 2012.

[GaRo12] M. Garetti, P. Rosa, S. Terzi, „Life Cycle Simulation for the design of Product–Service Systems," Computers in Industry,, Elsevier, pp. 361-369, 2012.

[ErLi17] Ericsson and Arthur D. Little, "The 5G business potential", second edition, October 2017.

[ESA ESSB HB –U 002] ESA Space Debris Mitigation Compliance Verification Guidelines ESSB-HB-U-002: https://copernicus-masters.com/wp-content/uploads/2017/03/ESSB-HB-U-002-Issue119February20151.pdf

[Ericsson20] Ericsson Mobility Report: https://www.ericsson.com/4adc87/assets/local/mobility-report/documents/2020/november-2020-ericsson-mobility-report.pdf [ISO 2413] ISO 24113:2019 Space Systems-Space Debris Mitigation Requirements: https://www.iso.org/standard/72383.html

[Evans11] D. Evans, "The Internet of Things: How the Next Evolution of the Internet is Changing Everything," [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[ISTINCT] Reference: Assessing satellite-terrestrial integration opportunities in the 5G environment: European Space Agency ARTES 1 Project "INSTINCT: Scenarios for Integration of Satellite Components in Future Networks' Contract No.: 4000110994/14/NL/AD

[ITU-T Y.3106] Recommendation ITU-T Y.3106 (2019), Quality of service functional requirements for the IMT-2020 network.

[ITU-T Y.3107] Recommendation ITU-T Y.3107 (2019), Functional architecture for QoS assurance management in the IMT-2020 network.

[ITU-T G.1035] Recommendation ITU-T G.1035 (2020), Influencing factors on quality of experience for virtual reality services.

[ITU-T Y.3102] Recommendation ITU-T Y.3102 (2018), Framework of the IMT-2020 network.

[ITU-T Y.3104] Recommendation ITU-T Y.3104 (2018), Architecture of the IMT-2020 network.

[ITU-T SG13 Y.3109] ITU-T SG13 Y.3109 (formerly Y.qos-ec-vr-req) "Quality of service assurance-related requirements and framework for virtual reality delivery using mobile edge computing supported by IMT-2020", published in April 2021 (https://www.itu.int/rec/T-REC-Y.3109-202104-I).

[ITU-T H.264] Recommendation ITU-T H.264 (2019), Advanced video coding for generic audiovisual services.

[ITU-T H.265] Recommendation ITU-T H.265 (2019), High efficiency video coding.

[ITU-T H.266] Recommendation ITU-T H.266 (2020), Versatile video coding.

[ITU-T E.860] Recommendation ITU-T E.860 (2002), Framework of a service level agreement.

[ITU-T SG13 Y.3109] ITU-T SG13 Y.3109 (formerly Y.qos-ec-vr-req) "Quality of service assurance-related requirements and framework for virtual reality delivery using mobile edge computing supported by IMT-2020", published in April 2021 (https://www.itu.int/rec/T-REC-Y.3109-202104-I).

[ISO/IEC TR 22417:2017] "Information technology — Internet of things (IoT) use cases", ISO/IEC TR 22417, November, 2017, see: https://www.iso.org/standard/73148.html

[ITU-R M.2410-0] International Telecommunications Union Radiocommunication Sector (ITU-R), "Minimum requirements related to technical performance for IMT-2020 radio interface(s)", Report ITU-R M.2410-0 (11/2017), November 2017, Online: https://www.itu.int/pub/R-REP-M.2410-2017.

[JML20] J. &. A. M. &. M. M. Lee, "5G and Smart Manufacturing," 2020.

[KaWa13] H. Kagermann, W. Wahlster and J. Helbig (Eds.), "Recommendations for implementing the strategic initiative Industrie 4.0: Final report of the Industrie 4.0 Working Group", 2013.

[KrKa18] W. Kritzinger, M. Karner, G. Traar, J.Henjes, W. Sihn „Digital Twin in manufacturing: A categorical literature review and classification," IFAC-PapersOnLine., 51 (2018), pp. 1016-1022, 2018.

[KoLa20] Kodheli, O., Lagunas, E., Maturo, N., Sharma, S.K., Shankar, B., Montoya, J.F.M., Duncan, J.C.M., Spano, D., Chatzinotas, S., Kisseleff, S. and Querol, J., 2020. Satellite communications in the new space era: A survey and future challenges. IEEE Communications Surveys & Tutorials.

[LeBa15] J. Lee, B. Bagheri, and H.-A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems, Manufacturing Letters", vol. 3, 2015, pp. 18-23.

[LeAz20] Jay Lee, Moslem Azamfar, Jaskaran Singh, Shahin Siahpour, "Integration of digital twin and deep learning in cyber-physical systems: towards smart manufacturing", IET Collab. Intell. Manuf., 2020, Vol. 2 Iss. 1, pp. 34-36

[LiGe19] Liolis, K., Geurtz, A., Sperber, R., Schulz, D., Watts, S., Poziopoulou, G., Evans, B., Wang, N., Vidal, O., Tiomela Jou, B. and Fitch, M., 2019. Use cases and scenarios of 5G integrated satellite-terrestrial networks for enhanced mobile broadband: The SaT5G approach. International Journal of Satellite Communications and Networking, 37(2), pp.91-112.

[MuBo22] M. Mukhiddinov, A. Bobomirzaevich Abdusalomov, J. Cho, "A Wildfire Smoke Detection System Using Unmanned Aerial Vehicle Images Based on the Optimized YOLOv5", Special Issue Advanced Computational Intelligence for Object Detection, Feature Extraction and Recognition in Smart Sensor Environments 2022-2023), 1 December 2022

[NASA-cubesats] https://www.nasa.gov/mission_pages/cubesats/overview

[Networld2020-SRIA] "Smart Networks in the context of NGI", SNS SRIA, Networld2020, September 2020, https://bscw.5g-ppp.eu/pub/bscw.cgi/d367342/Networld2020%20SRIA%202020%20Final%20Version%202.2%20.pdf

[Siemens2016] Siemens AG, "5G communication networks: Vertical industry requirements," 11 2016, to be retrieved via (accessed on 23 July 2021): http://www.virtuwind.eu/_docs/Siemens_PositionPaper_5G_2016.pdf.

[Satell-market] http://satellitemarkets.com/satellite-iot-game-changer-industry

[SiBa23] Radheshyam Singh, Kalpit Dilip Ballal, Michael Stübert Berger, Lars Dittmann, "Overview of Drone Communication Requirements in 5G", Lecture Notes in Computer Science book series (LNCS,volume 13533), 01 January 2023.

[TaQi19] F. Tao, Q. Qi, L. Wang, AYC. Nee, „Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison," Engineering. 5. , pp. 653-661, 2019.

[TaCa19] G. Tavola, A. Caielli and M. Taisch, "An "Additive" Architecture for Industry 4.0 Transition of Existing Production Systems," in STUDIES IN COMPUTATIONAL INTELLIGENCE, Springer, 2019, pp. 258-269.

ANNEX II Template used for Use Case description

X. Use Case (title)

X.1 Description

- Provide motivation of having this use case, e.g., is it currently applied and successful; what are the business drivers, e.g., several stakeholder types will participate and profit from this use case
- Provide on a high level, the operation of the use case, i.e., which sequence of steps are used in this operation?

X.2 Source

- Provide reference to project, SDO, alliance, etc.

X.3 Roles and Actors

- Roles: Roles relating to/appearing in the use case
    - Roles and responsibilities in this use case, e.g., end user, vertical industry, Communication Network supplier/provider/operator, IoT device manufacturer, IoT platform provider, Insurance company, etc.
    - Relationships between roles
- Actors: Which are the actors with respect to played roles
- A detailed definition of the Roles and Actors is provided in [7].

X.4 Pre-conditions

- What are the pre-conditions that must be valid (be in place) before the use case can become operational

X.5 Triggers

- What are the triggers used by this use case

X.6 Normal Flow

- What is the normal flow of exchanged data between the key entities used in this use case: devices, IoT platform, infrastructure, pedestrians, vehicles, etc?

X.7 Alternative Flow

- Is there an alternative flow

X.8 Post-conditions

- What happens after the use case is completed

X.9 High Level Illustration

- High level figure/picture that shows the main entities used in the use case and if possible, their interaction on a high level of abstraction

X.10 Potential Requirements

This section should provide the potential requirements and in particular the requirements imposed towards the underlying communication technology

These requirements can be split in:

- Functional requirements

  (to possibly consider them – but not limited to – with respect to the identified functions/capabilities)

- Non-functional requirements – possible consideration includes:
  - Flexibility
  - Scalability
  - Interoperability
  - Reliability
  - Safety
  - Security and privacy
  - Trust

As example of the format of such requirements is provided in Annex III and Annex IV.

X.11 Radio Specific requirements

X.11.1 Radio Coverage

- Radio cell range

Specification of expected maximum and typical radio ranges (indicate if LOS/NoLOS)

- Does the radio link crosses public spaces? Or is it constrained to indoor or customer premises?
- Is Multicell required?

(If YES, specify the required scope of the multicell arrangement. I.e. "building", "city", "global")

- Is handover required? Seamless? Tolerable impact in delay and jitter?
- Mobility: maximum relative speed of UE/FP peers
- Special coverage needs: i.e., maritime, aerial

X.11.2 Bandwidth requirements

- Peak data rate
- Average data rate
- Is traffic packet mode or circuit mode?
    - If circuit mode, is isochronicity required?

X.11.3 URLLC requirements

- Required Latency

(specify if it is one way or roundtrip)

- Required Reliability

(i.e., 99,99999%)

- Maximum tolerable jitter

X.11.4 Radio regimens requirements

- Desired and acceptable radio regimens (describe the desired and acceptable radio regimens

(i.e.: licensed - public mobile, licensed – specific license, license-exempt)

X.11.5 Other requirements

- UE power consumption
    - Rechargeable or primary battery?
    - Acceptable battery life
- Is terminal location required? location accuracy?

ANNEX III KPIs defined in Networld2020[69] (SNS) Strategic and Research Innovation Agenda (SRIA) 2021 – 2027

Selected KPIs Forecast for Terrestrial Radio Communications during the short, medium, and long -term evolution of 5G NR.

Target KPI	5G NR (Rel.16) 2020	Short-term Evo ~2025	Medium-term Evo ~2028	Long-term Evo ~2030
Spectrum	<52.6 GHz	<150 GHz	<300 GHz	<500 GHz
Bandwidth	<0.5 GHz	<2.5 GHz	<5 GHz	<10 GHz
Peak Data Rate	DL: >20 Gbps UL: >10 Gbps	DL: >100 Gbps UL: >50 Gbps	DL: >200 Gbps UL: >100 Gbps	DL: >400 Gbps UL: >200 Gbps
User Data Rate	DL: >100 Mbps UL: >50 Mbps	DL: >500 Mbps UL: >250 Mbps	DL: >1 Gbps UL: >0.5 Gbps	DL:>2 Gbps UL: >1 Gbps
Density	>1 device/sqm	>1.5 device/sqm	>2 device/sqm	>5 device/sqm
Reliability [BLER]	URLLC: >1-10^{-5}	>1-10^{-6}	>1-10^{-7}	>1-10^{-8}
U-Plane Latency	URLLC: <1 ms	<0.5 ms	<0.2 ms	<0.1 ms
C-Plane Latency	<20 ms	<10 ms	<4 ms	<2 ms
Energy Efficiency (Network/Terminal)	Qualitative	>30 % gain vs IMT-2020	>70 % gain vs IMT-2020	>100% gain vs IMT-2020
Mobility	<500 Km/h	<500 Km/h	<500 Km/h	<1000 Km/h
Positioning accuracy	NA (<1 m)	<30 cm	<10 cm	<1 cm

(Table copied from [Networld2020-SRIA] - Networld 2020 (SNS) Strategic and Research Innovation Agenda (SRIA) 2021 – 2027, see: https://bscw.5g-ppp.eu/pub/bscw.cgi/d367342/Networld2020%20SRIA%202020%20Final%20Version%202.2%20.pdf)

[69] Networld2020 ETP has been renamed to NetwolrdEurope ETP, see: https://www.networldeurope.eu

Selected KPIs Forecast for Satellite Radio Communications during the short, medium, and long-term evolution of 5G NR

KPI	Short Term Evo	Medium-Term Evo	Long-Term Evo
Minimization of unmet capacity[1]	<0.1.%	<0.05%	<0.01%
Maximization of satellite resource utilization[2]	>99%	>99.9%	>99.99%
Time to reallocate satellite resources[3]	<1 min	<5 sec	<1 sec
Solving and detecting time of satellite operation incidents	<10 min	<5min	< 1 min
Energy Reduction using adaptive intersegment links	>50%	>80%	>90%
Connectivity gain for converged satellite cloud scenarios[4]	>100%	>150%	>200%
Reduction of required manual intervention[5]	>50%	>80%	>90%
Widespread IoT coverage [6]	> 50%	>99%	> 99.9%
Reliability (perceived zero downtime)[7]	>50%	>99%	>99.9%
Experienced data rate (Broadband)	DL: >50 Mbit/s UL: >25 Mbit/s	DL: >500 Mbit/s UL: > 250 Mbit/s	DL: >1.0 Gbit/s UL: >0.5 Gbit/s
Area traffic capacity (Broadband)	DL: >75 Mbit/s/km2 UL: >37 Mbit/s/km2	DL: >750 Mbit/s/km2 UL: >370 Mbit/s/km2	DL: >1.5 Gbit/s/km2 UL: >0.75 Gbit/s/km2
Experienced data rate (NB-IoT)	DL: >2 Kbit/s UL: >10 Kbit/s	DL: >20 Kbit/s UL: >100 Kbit/s	DL: >40 Kbit/s UL: >200 Kbit/s
Area traffic capacity (NB-IoT)	DL: >8 Kbit/s UL: >40 Kbit/s	DL: >80 Kbit/s UL: >400 Kbit/s	DL: >160Kbit/s/km2 UL: >800Kbit/s/km2

[1] User demand that is not satisfied

[2] Used satellite resources such as power, bandwidth, etc

[3] Allocation of satellite resources such as power, spectrum, beampattern given a change in the demand

[4] Increase in successful connections

[5] Reduction with respect to today manual intervention

[6] Gain with respect to 2020 wireless area capacity

[7] % of total operation time

(Table copied from [Networld2020-SRIA] - Networld 2020 (SNS) Strategic and Research Innovation Agenda (SRIA) 2021 – 2027, see: https://bscw.5g-ppp.eu/pub/bscw.cgi/d367342/Networld2020%20SRIA%202020%20Final%20Version%202.2%20.pdf)

The optical community is proposing the following key performance indicators

	Target KPI	Current 2020	Short-term Evo ~2025	Mid-term Evo ~2028	Long-term Evo ~2030
Metro/Core	Spectrum[1]	5THz	15THz	30THz	50THz
	Port speed[2]	400Gb/s	1.6Tb/s	3.2Tb/s	6.4Tb/s
	Bandwidth[3]	<75GHz	<300GHz	<600GHz	<1200GHz
	Line capacity[4]	25Tb/s	200Tb/s	600Tb/s	1.5Pb/s
	Node capacity[5]	150Tb/s	1.2Pb/s	3.6Pb/s	9Pb/s
Access	PON speeds	10Gb/s	50Gb/s	100Gb/s	>200Gb/s
	User data rate[6] (consumer)	100Mb/s	~1Gb/s	>2.5Gb/s	>5Gb/s
	User data rate[6] (business)	1Gb/s	~10Gb/s	>25Gb/s	>50Gb/s
	Latency[7]	<1ms	<100µs	<10µs	<1µs
	Power consumption[8]	100% (baseline)	40%	30%	20%
	Service provisioning	Hour	Min	Second	Sub-second
	Network operations	Operator-controlled, reactive	Intent-based, proactive	Self-diagnosing	Self-optimizing

[1] 25% CAGR, in line with conservative traffic predictions

[2] Extrapolation of Ethernet roadmap

[3] Using 400G DP-16QAM as baseline

[4] 50% CAGR, in line with internet content provider traffic predictions. Assumes exploitation of frequency and space domain.

[5] Based on degree 4 node with 50% local add/drop

[6] 50% CAGR based on Nielsen's law

[7] Excluding propagation delay

[8] 15% reduction per Gb/s p.a., extrapolated from past transponder data

(Table copied from [Networld2020-SRIA] - Networld 2020 (SNS) Strategic and Research Innovation Agenda (SRIA) 2021 – 2027, see: https://bscw.5g-ppp.eu/pub/bscw.cgi/d367342/Networld2020%20SRIA%202020%20Final%20Version%202.2%20.pdf)

With respect to the system architecture and networking the following metrics are proposed:

- Runtime Service Scheduling efficiency increase compared to overprovisioning (for a service requiring 99.999% or higher success rates and under typical traffic arrival conditions)

Short term	Medium term	Long term
2x in single tenant environments	10x in single tenant	At least 10x in multitenant environments

(Table copied from [Networld2020-SRIA] - Networld 2020 (SNS) Strategic and Research Innovation Agenda (SRIA) 2021 – 2027, see: https://bscw.5g-ppp.eu/pub/bscw.cgi/d367342/Networld2020%20SRIA%202020%20Final%20Version%202.2%20.pdf)

This includes aspects as path stretch ((ratio between the average control plane path and the average physical node distance) and resource overhead (services being provided by the network resources versus maximum capacity of those resources).

- Time required for runtime conflict resolution when applying resource efficiency methods, that is the increase in multiplexing desired when compared to independent exclusive allocations and the time that is required to settle all the conflicts that may exist.

Short term	Medium term	Long term
2x for multiple concurrent, overlapping allocations	10x for multiple concurrent, overlapping allocations	At least 10x with critical guarantees

(Table copied from [Networld2020-SRIA] - Networld 2020 (SNS) Strategic and Research Innovation Agenda (SRIA) 2021 – 2027, see: https://bscw.5g-ppp.eu/pub/bscw.cgi/d367342/Networld2020%20SRIA%202020%20Final%20Version%202.2%20.pdf)

- In terms of network-resources collection (network garbage collection), in the sense of recovering resources that are not being used anymore, we expect:

Short term	Medium term	Long term
Feasible, additional recovery process off-line	Feasible, running with the resource allocation	Optimal, on resource allocation actions

(Table copied from [Networld2020-SRIA] - Networld 2020 (SNS) Strategic and Research Innovation Agenda (SRIA) 2021 – 2027, see: https://bscw.5g-ppp.eu/pub/bscw.cgi/d367342/Networld2020%20SRIA%202020%20Final%20Version%202.2%20.pdf)

- Features of the pervasive resource control, in terms of autonomic functions.

	Short term	Medium term	Long term
Configuration	Only a minimal initial pre-configuration (only domain name + security association data, e.g. private/public key)	No human intervention	No human intervention across different domains
Scalability	High, large number of nodes	Very High, any number of nodes, densities	Very High, any number of nodes, densities and complexity
Bootstrapping	Reduced time to 70%	Reduced time to 40%	Reduced time to 10%
Convergence time of the control plane	Time reduced to 70%	Time reduced to 40%	Time reduced to 10%
Signalling overhead in reconfiguration	Reduced to 90%	Reduced to 75%	Reduced to 75% in multitenant environments

(Table copied from [Networld2020-SRIA] - Networld 2020 (SNS) Strategic and Research Innovation Agenda (SRIA) 2021 – 2027, see: https://bscw.5g-ppp.eu/pub/bscw.cgi/d367342/Networld2020%20SRIA%202020%20Final%20Version%202.2%20.pdf)

- In terms of network-suitable AI, it is expected:

Short term	Medium term	Long term
Adaptation of current centric-implementation AI models	Fully distributed AI algorithms at the network	distributed AI supporting and serving several models at the same time

(Table copied from [Networld2020-SRIA] - Networld 2020 (SNS) Strategic and Research Innovation Agenda (SRIA) 2021 – 2027, see: https://bscw.5g-ppp.eu/pub/bscw.cgi/d367342/Networld2020%20SRIA%202020%20Final%20Version%202.2%20.pdf)

In security domain, being a mandatory condition for numerous objectives, security is de facto a pre-requisite for the ongoing Digitalization of our societies. Building trust is combination of awareness, understanding and obviously provision of the right solutions with the right level of security. The ambitious objectives listed below aims at being representative of this combination:

- Towards access to real time Cyber Threat Intelligence information (attacks/threats and vulnerabilities), risk Analysis tools and Services enabling 100% of awareness and level-based appropriate protection counter-measure deployment.

Shor term	Medium term	Long term
Federated, consolidated, common basis across CERTs (CSIRT network, NIS directive application)	CTI platforms (including openCTI) and tools for State-of-The-Art sanitization	100% of qualified threats knowledge and appropriate counter measures made accessible

(Table copied from [Networld2020-SRIA] - Networld 2020 (SNS) Strategic and Research Innovation Agenda (SRIA) 2021 – 2027, see: https://bscw.5g-ppp.eu/pub/bscw.cgi/d367342/Networld2020%20SRIA%202020%20Final%20Version%202.2%20.pdf)

- Trust in ICT infrastructure through systematic Exposure of cybersecurity levels 100% compliant with European-legal basis (certification, Security Service Level attributes, GDPR/EU strategy for Data,...)

Short term	Medium term	Long term
5G systems & services certification frameworks, Basic security level exposure with generic security attributes defined	Methodologies and tools for composition and time evolution of certified perimeters (systems & services)	Evolutive approach for data and disruptive technologies

(Table copied from [Networld2020-SRIA] - Networld 2020 (SNS) Strategic and Research Innovation Agenda (SRIA) 2021 – 2027, see: https://bscw.5g-ppp.eu/pub/bscw.cgi/d367342/Networld2020%20SRIA%202020%20Final%20Version%202.2%20.pdf)

- Compliance with highly critical applications and essential services requirements leading to sovereign solutions able to provide 100% availability of services for verticals

Short term	Medium term	Long term
Local, private implementation for limited set of verticals	End-to-End hybrid implementation for most of verticals	High grade support with technology, system and solution independence

(Table copied from [Networld2020-SRIA] - Networld 2020 (SNS) Strategic and Research Innovation Agenda (SRIA) 2021 – 2027, see: https://bscw.5g-ppp.eu/pub/bscw.cgi/d367342/Networld2020%20SRIA%202020%20Final%20Version%202.2%20.pdf)

- Improve attack detection & response mean time of Cybersecurity incidents including zero % unprotected data leakage

Short term	Medium term	Long term
Benchmark strategy including data set and models	Monitoring and attack detection EU-wide strategy	Data protection strategy with response time and robustness outperforming attackers capabilities

(Table copied from [Networld2020-SRIA] - Networld 2020 (SNS) Strategic and Research Innovation Agenda (SRIA) 2021 – 2027, see: https://bscw.5g-ppp.eu/pub/bscw.cgi/d367342/Networld2020%20SRIA%202020%20Final%20Version%202.2%20.pdf)

Annex IV Siemens White Paper "5G communication networks: Vertical industry requirements"

In [Siemens2016], several 5G requirements were derived by Siemens based on their studies on vertical application domains, such as Smart City, Smart Mobility, Smart Manufacturing, Smart Energy and Smart Building.

Table 20 shows a consolidated view of the 5G requirements, while Table 21provides more details on the 5G requirements coming from verticals.

Table 20: 5G promises vs. Vertical requirements, copied from [Siemens2016] with courtesy of Siemens

Category	Requirement	Explicit 5G promises (according to [1], Figure 2)	Consolidated requirements from verticals - Siemens view
Industry-grade Service Quality	Realtime capability – Latency	5 ms (e2e)	1 ms (local) 5 ms (long distance)
	Realtime capability —Jitter	-	1us (local)
	Bandwidth	Peak data 10 Gbps Mobile data volume 10 TB/s/km² Number of devices: 1 mio/km²	kbps ... 10Gbps
	Time period of information loss during failures	-	none (seamless failover)
	Availability/coverage	-	ubiquitous
	Range (distance between communication neighbors)	-	0,1 m ... 200 km
	Reliability (minimum uptime per year [%])	99,999%	99,9999%
	Mobility	500km/h	500km/h
	Outdoor terminal location accuracy	<1m	0,1 m
	Multi-tenant support	yes (Network Slices)	yes
Operation and maintenance	Non-standard operating conditions	Energy consumption reduced by factor 10	• Battery powered devices with >10years lifetime • Harsh environments (weather, vibrations, heat, dust, hazardous gases, etc.)
	Ease of use	-	• Communication services approach • Plug and play device (sensor, actuator, controller) integration
	SLA Tooling	-	Service Level Agreement (SLA) monitoring and management tools for provider and consumer
	Service deployment time (time between service request and service realization)	90 min	hours
	Private 5G infrastructures	-	yes
Non-technical	Scalability: Number of devices per km²	10^6	10^5
	Globally harmonized definition of Service Qualities	-	yes
	Technology availability	-	>20 years
	Globally simplified certification of ICT components	-	Yes
Assured Guarantees		-	mandatory

Table 21: 5G promises vs. Vertical requirements (details), copied from [Siemens2016] with courtesy of Siemens

Category	Requirement	Explicit 5G promises (according to [1], Figure 2)	Siemens demand	Smart City	Smart Mobility	Smart Manufacturing		Smart Energy			Smart Building
						Process	Discrete	Low Voltage	Medium Voltage	High Voltage	
Industry-grade Service Quality	Realtime capability – Latency	5 ms (e2e)	1 ms (local) 5 ms (long distance)	-	1ms (local) 10 ms (long distance)	20ms (local) 1s (long distance)	1ms (local) 20ms (long distance)	-	25ms	5ms (long distance)	100ms
	Realtime capability -- Jitter	-	1us (local)	-	-	20ms	1us	-	25ms	1ms	-
	Bandwidth	Peak data 10 Gbps Mobile data volume 10 TB/s/km^2 Number of devices: 1 mio/km^2	kbps ... 10Gbps	kbps (sensors) ... Mbps (video supervision) ... 10 Gbps (data centers)	10 Mbps ... 1 Gbps	100 kbit/s (automaton stream) ... 100 Mbps (remote access, video supervision)	100 kbit/s (automaton stream) ... 100 Mbps (remote access, video supervision)	1 kbps per subscriber	5 Mbps per secondary substation	1Gbps along power lines	100 kbit/s (automaton stream) ... 100 Mbps (remote access, video supervision)
	Time period of information loss during failures	-	none (seamless failover)	1s	100 ms	100 ms	none (seamless failover)	minutes	25ms	none (seamless failover)	100 ms
	Availability/ coverage	-	Ubiquitous	City-level	Ubiquitous	Industrial Plant Areas	Industrial Plant Areas	Ubiquitous	Ubiquitous	Ubiquitous	City-level
	Range (distance between communication neighbors)	-	0,1 m ... 200 km	10 km	1 km (cars) ... 10 km (trains)	0,1m ... 10 km	0,1 m ... 100 m	10 km	20 km	200 km	100m
	Reliability (minimum uptime per year [%])	99,999%	100%	99,9%	100%	100%	100%	98%	99,9%	100%	99,9%
	Mobility	500km/h	500km/h	100km/h	500km/h	50km/h	50km/h	5km/h	-	-	5km/h
	Outdoor terminal location accuracy	<1m	0,1 m	1 m	0,1 m	0,1 m	0,1 m	10 m	10 m	-	0,1 m
	Multi-tenant support	yes (Network Slices)	yes								
Operation and maintenance	Non-standard operating conditions	Energy consumption reduced by factor 10	• Battery powered devices with >10years lifetime • Harsh environments (weather, vibrations, heat, dust, hazardous gases, etc.)								
	Ease of use	-	• Communication Services approach • Plug and Play Device (Sensor, Actuator, Controller) integration								
	SLA Tooling	-	Service Level Agreement (SLA) monitoring and management tools for provider and consumer								
	Service deployment time (time between service request and service realization)	90 min	hours								
	private 5G infrastructures	-	yes	-	yes	yes	yes	-	optional	yes	optional
Non-technical	Scalability: Number of devices per km^2	10^6	10^5	10^5	10^4	10^5 (high density of devices)	10^5 (high density of devices)	10^4	10^3	10^3	10^5
	Globally harmonized definition of Service Qualities	-	yes	-	yes	yes (for long distance)	yes (for long distance)	-	yes	yes	-
	Technology availability	-	>20 years								
	Globally simplified certification of ICT components	-	Yes								
Assured Guarantees		-	Mandatory	Relaxed	Mandatory	Mandatory	Mandatory	Relaxed	Mandatory	Mandatory	Relaxed

Contributors

The document was written by several participants of the AIOTI WG Standardisation.

Editor:

Georgios Karagiannis, Huawei

Reviewer:

Damir Filipovic, AIOTI, Secretary General

Main Contributors:

Agnia Codreanu (BEIA)
Antonio Kung (Trialog)
Antonio Skarmeta (University of Murcia)
Arne J. Berre (Sintef)
Artur Krukowski (RFSAT)
Asbjørn Hovstø (Hafenstrom)
Christian Kloch (Force Technology)
Christophe Gossard (John Deere)
Damir Filipovic (AIOTI Secretary General)
Erwin Schoitsch (Austrian Institute of Technology - AIT)
Flemming Sveen (Hafenstrom)
George Suciu (BEIA)
Georgios Karagiannis (Huawei)
Giacomo Tavola (Politecnico di Milano)
Gianmarco Baldini (EC JRC)
Izzet Saglam (Turkcell)
Jaume Segura (Universitat de València)
Joao Peixoto (Ubiwhere)
Jose Luis Hernandez (EC JRC)
Kevin McDonnell (Huawei)
Konstantinos Loupos (INLECOM)
Konstantinos Ntafloukas (INLECOM)
Krzysztof Piotrowski (IHP-Microelectronics)
Lavinia Ana Petrache (BEIA)
Marco Carugi (Huawei)
Mari-Anais Sachian (BEIA)
Maria Niculae (BEIA)
Natalie Samovich (Enercoutim)
Nemanja Mišić (DunavNET)
Nikos Giannakakos (UniSystems)
Ranga Rao Venkatesha Prasad (Technical University Delft)
Rui Aguiar (University of Aveiro)
Rute Sofia (fortiss)
Sean McGrath (University of Limerick)
Srđan Krčo (DunavNET)
Thomas Klein (IBM)
Toon Norp (TNO)
Valentina Peniche (AIOTI)
Vasileios Karagiannis (Austrian Institute of Technology - AIT)
Zbigniew Kopertowski (Orange)

Acknowledgements

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating AI, IoT and Edge Continuum Innovation in Europe, bringing together small and large companies, academia, researchers, policy makers, end-users and representatives of society in an end-to-end approach. We strive to leverage, share and promote best practices in the AI, IoT and Edge Continuum ecosystems, be a one-stop point of information to our members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of the AI, IoT and Edge Continuum Innovation in society. AIOTI contributions goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation by creating joint research roadmaps, defining policies and driving convergence of standards and interoperability.