Alliance for IoT and Edge Computing Innovation

IoT and Edge Computing impact on Beyond 5G: enabling technologies and challenges

Release 2.0

AIOTI WG Standardisation

14 April 2023

Executive Summary

This report highlights several IoT vertical domain use cases collected by the Alliance for IoT and Edge Computing Innovation (AIOTI) and determines the specific requirements they impose on the underlying (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 (Beyond) 5G technology are as well introduced.

The Release 2.0 version 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, (4) preliminary 6G use cases.

Table of Content

Table of Figures

List of Tables

Abbreviations

3GPP	3rd Generation Partnership Project
2D	Two Dimensional
4G	4th Generation
5G	5th Generation
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
BICMOS	Bipolar Complementary Metal—Oxide-Semiconductor
BLE	Bluetooth Low Energy
BDA	Big Data Analytics
BMS	Building Management System
BVLOS	Beyond Vision Line of Sight
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
C-ITS	Cooperative-Intelligent Transportation System
CPX	Cyber–Physical Systems
CNN	Convolutional Neural Network
CSS	Car Sharing Service
D2X	Device to everything
DT	Digital Twins
DoF	Degree of Freedom
DoS	Denial-of-Service
eMBB	Enhanced Mobile Broadband
EEW	Early Earthquake Warning
EPON	Ethernet Passive Optical Network
ETSI	European Telecommunication Standardisation Institute

ESP32	Espessif Systems Processor 32
FL	Federated Learning
FFT	Fast Fourier Transform
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GSM	Global System for Mobile communications
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
I&M	Inspection & Maintenance
IP	Internet Protocol
IoRT	Internet of Robotic Things
IoT	Internet of Things
ITS	Intelligent Transportation System
LDM	Local Dynamic Map
LOS	Line Of Sight
LP-WAN	Low Power Wide Area Network
LTE	Long Term Evolution
LTE-V2X	LTE Vehicle to Everything
MCU	MicroController Unit
ML	Machine Learning
MEC	Multi-access Edge Computing
mMTC	Machine-Type Communications
MQTT	Message Queuing Telemetry Transport
MUD	Manufacturer Usage Description
NACF	Network Access Control Function
NB-IoT	Narrowband IoT
NoLOS	Non Line of Sight
NFR	Network Function Registry
NFV	Network Function Virtualisation
NoSQL	Not only Structured Query Language
NSSF	Network Slice Selection Function
NTN	Non-Terrestrial Networks
NR	New Radio
OBU	On-Board Unit
OEM	Original Equipment Manufacturer
OGC	Open Geospatial Consortium
OPEX	Operational Expenditure
OPE	Operational Expenditures
OT	Operation Technology
PCF	Policy Control 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
RSU	Road Side Unit
RUL	Residual Useful Life
SAS	Service Alerting System
SCADA	Supervisory Control and Data Acquisition
SMF	Session Management Function
SME	Small Medium Enterprise
SOI	Silicon-On-Insulator
TC	Technical Committee
TCP	Transmission Control Protocol
TIoT	Tactile Internet of Things
TSC	Time Sensitive Communication
TSN	Time-Sensitive-Networking
MEC	Multi-Access Edge Computing
SDO	Standards Developing Organizations
TMC	Traffic Management Center
UAV	Unmanned Aerial Vehicle
UAS	Unmanned Aerial System
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
uRLLC	Ultra-reliable and Low-latency Communications
UPF	User Plane Function
USM	Unified Subscription Management
UTM	Unmanned Traffic Management system
V2V	Vehicle to Vehicle
VR	Virtual Reality
VRU	Vulnerable Road Users
WAVE	Wireless Access in Vehicular Environments
WiMAX	Worldwide Interoperability for Microwave Access
XML	Extensible Markup Language

1. Introduction

As emphasized in reports published by AIOTI, see [AIOTI-IoT-relation-5G], the Internet of Things 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. (Wireless Local Access Network) WLAN, Sigfox®, ZigBee, LoRa Wide Area Network (LoRaWAN), Narrowband-IoT (NB-IoT)) which all have their specific strengths and weaknesses and that are making the Internet of Things somewhat of a "rag rug".

This is where the 5th Generation (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 Network Function Virtualization (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 (Standards Developing Organizations), such as 3rd Generation Partnership Project (3GPP), ISO, ITU-T and IEEE as requirements for automation in vertical domains focusing on critical communications.

The Release 2.0 version 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 NetwoIrdEurope ETP, see: https://www.networldeurope.eu

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. 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 includes usually 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 (www.inlecom.eu) 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. Website: https://piloting-project.eu/.

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).

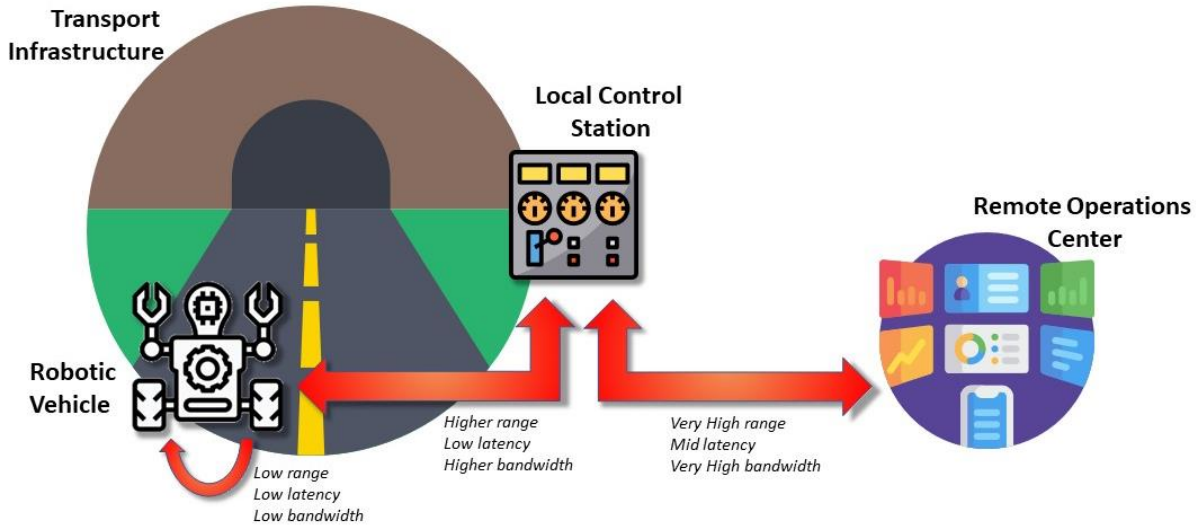
2.1.1.7 Alternative Flow

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?**

Multicell may be required for remote connectivity at 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.

[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.

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.

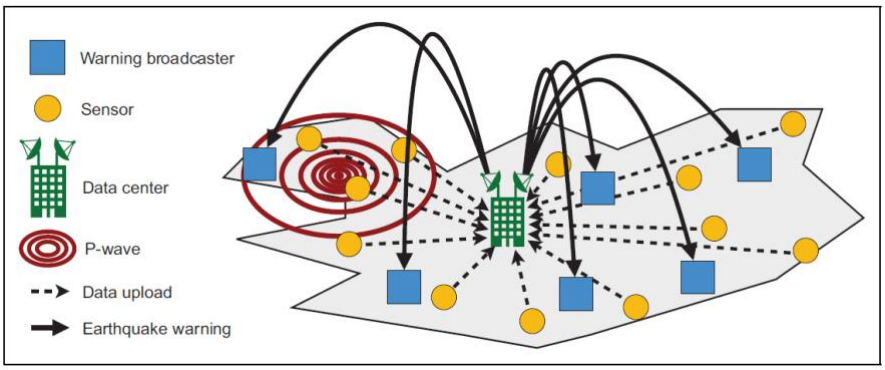


Figure 1: Use case in GeoSciFramework: Early Earthquake Warning (EEW) system

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 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.

[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)

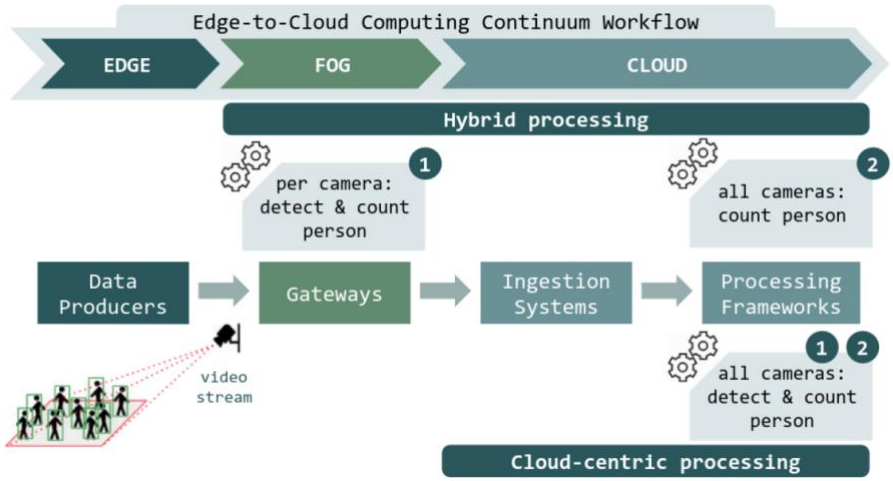


Figure 2: Use case in E2Clab: Smart Surveillance system

2.2.1.2 Source

- GeoSciFramework project (funded by NSR US - https://www.unavco.org/highlights/2019/geosciframework.html).
- Overflow project (funded by ANR France - https://sites.google.com/view/anroverflow/home?authuser=0).
- URBAURAMON project (https://www.uv.es/urbauramon/).

2.2.1.3 Roles and Actors

Actors & Roles in the three use cases

- **Citizens & Vicinity**. People who live (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 starts 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, see 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: This 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.

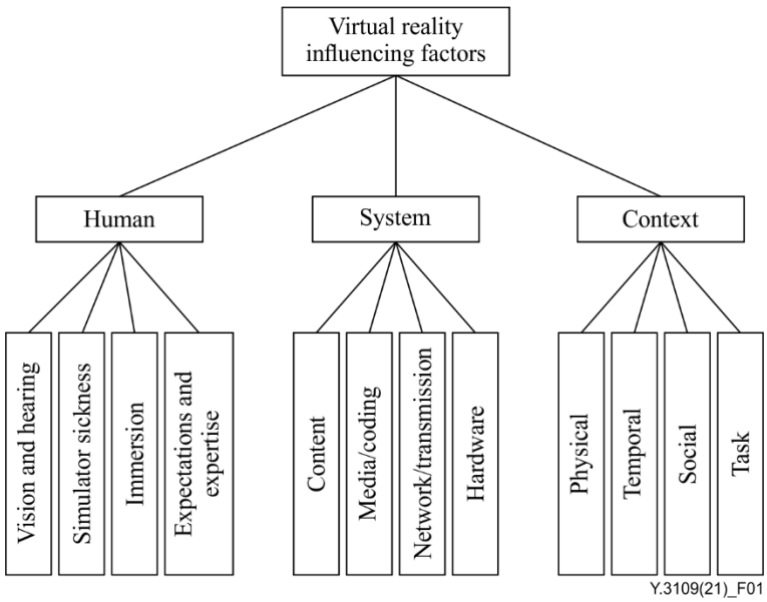


Figure 3: Virtual reality QoE-influencing factor categories, copied from [ITU-T G.1035]

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 (https://www.itu.int/rec/T-REC-Y.3109-202104-I).

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

Actors & Roles

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**.

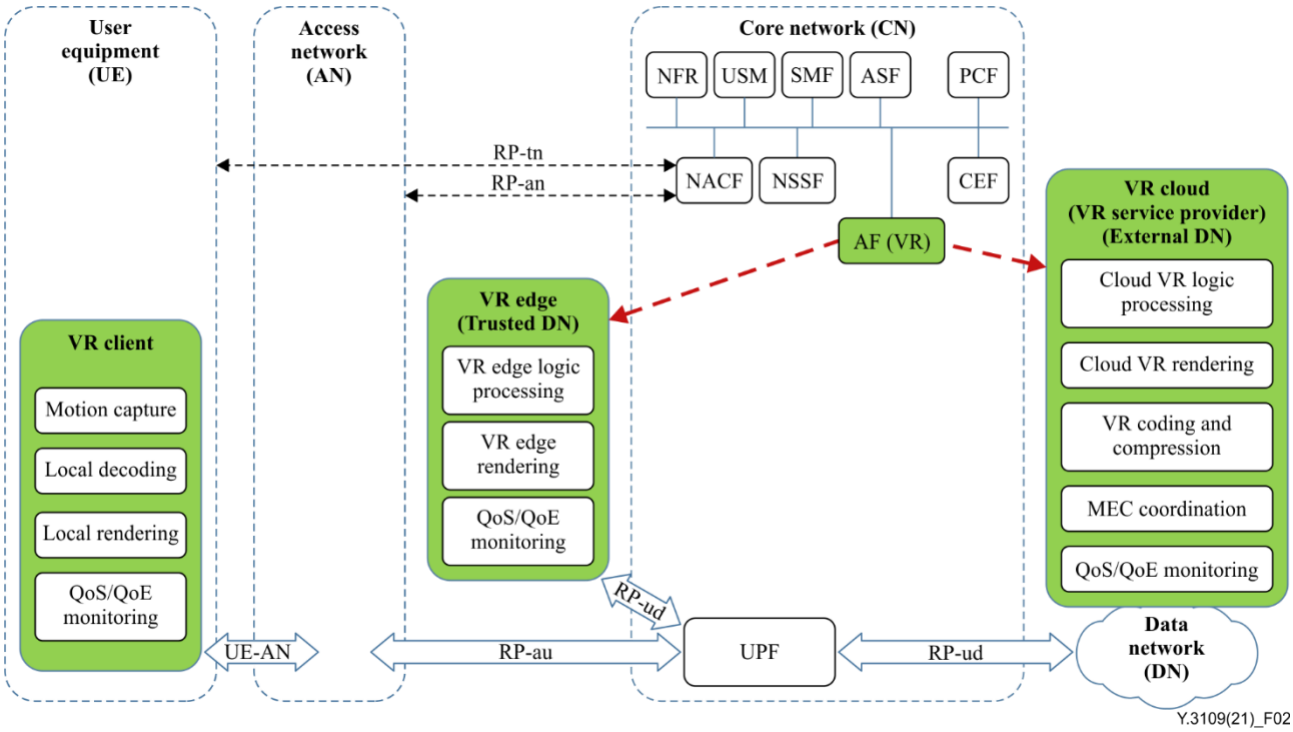


Figure 4: A conceptual architecture of the VR service framework, copied from [ITU-T SG13 Y.3109]

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].

2.2.2.10.1 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 (DT)

2.3.1 Digital Twin (DT) 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 (DTs) 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.

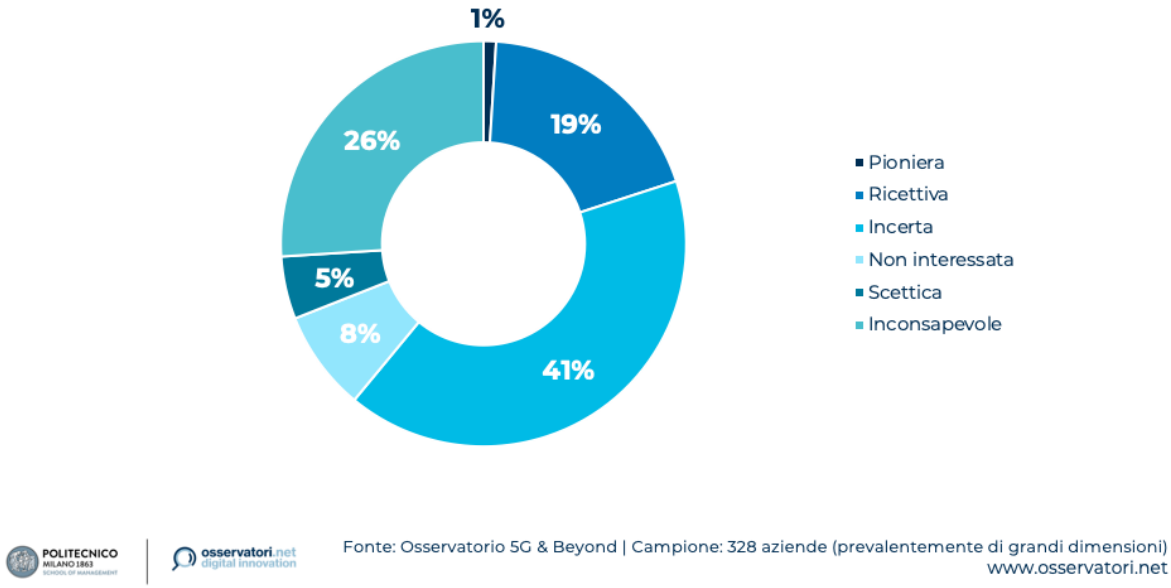


Figure 5: Potential Italian utilizer companies attitude towards 5G

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:

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).

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

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, see Section 3.1.

2.3.1.2 Source

As stated above, use case was executed in the context of the MISE (Italian Ministry of Economical 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

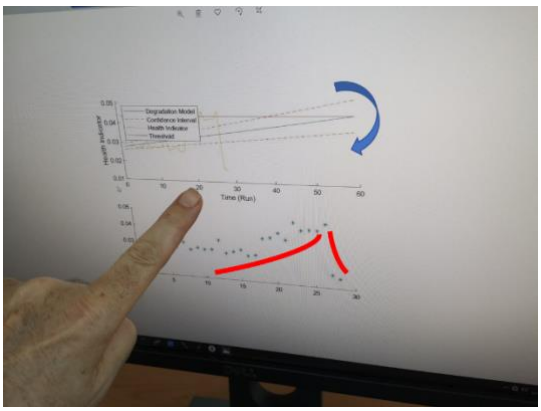
Use case is structured in two distinct flows, both of them leveraging 5G data transmission from sensors to backend and MEC functionalities.

1. Advanced Maintenance Execution System:

a. 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

b. 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)

c. Computed prediction is pushed to mobile devices connected through 5G



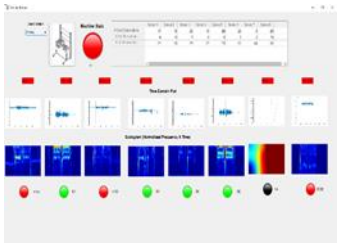
2. Self-Reconfigurable and Adaptive Production:

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

b. 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

c. 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

d. 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

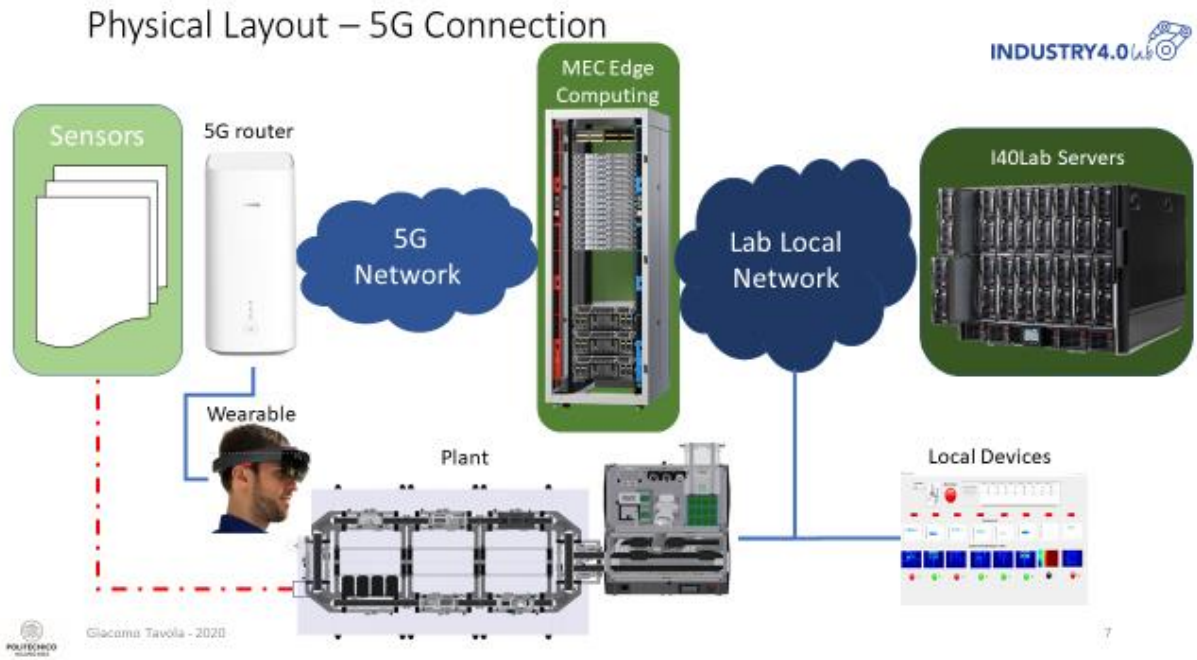


Figure 6: Physical Layout – 5G Connection

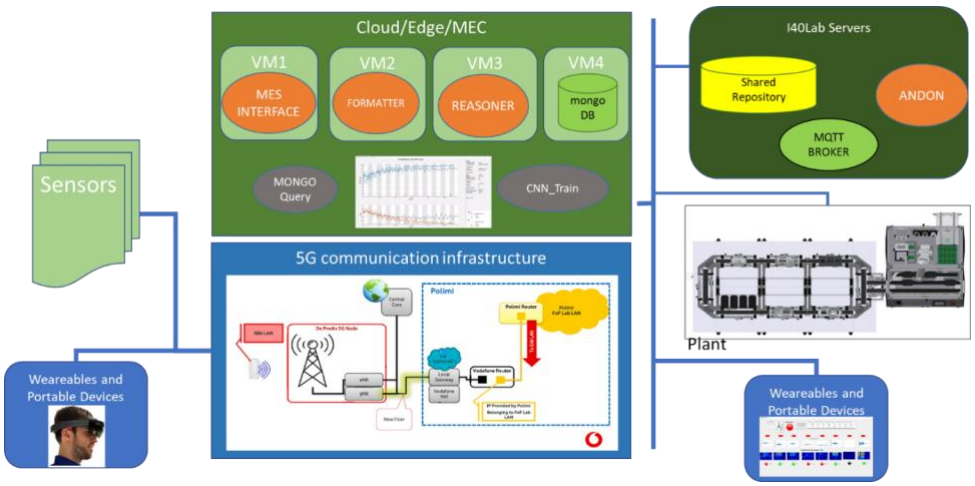


Figure 7: Network & Application Architecture

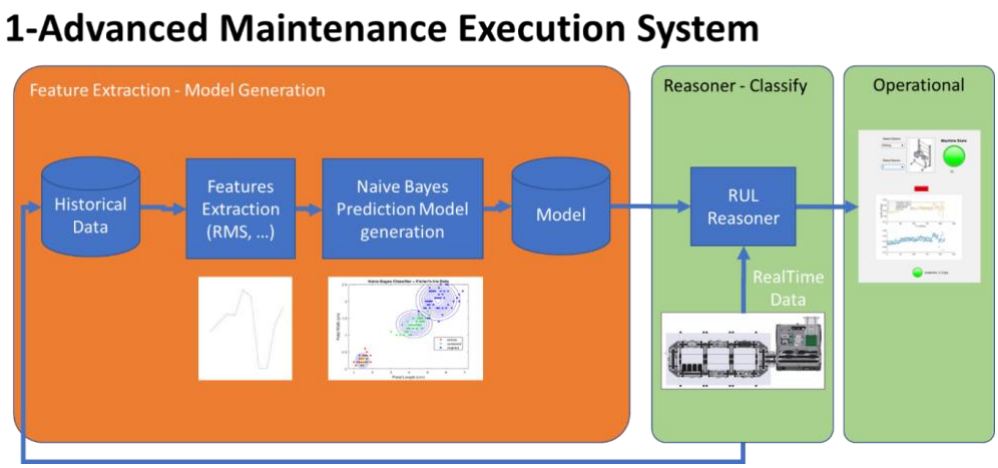


Figure 8: Advanced Maintenance Scenario

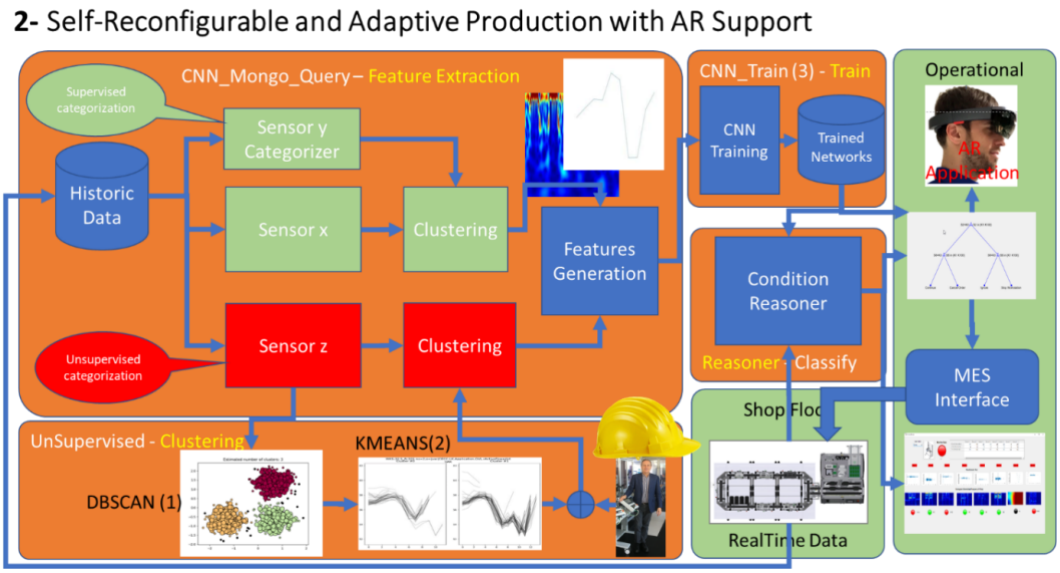


Figure 9: Condition Management and AR Support Scenario

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

2.4 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 (https://www.affordable5g.eu/; https://5g-ppp.eu/affordable5g/; https://cordis.europa.eu/project/id/957317)

2.4.1.3 Roles and Actors

Actors & Roles

- 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

1. The video streaming will be processed in the edge, exploiting its compute resources, to identify danger or emergency events.
2. 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.
3. 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.
4. Besides, the Urban Platform should also be able to access the recorded images that led to the triggering of the alarm.

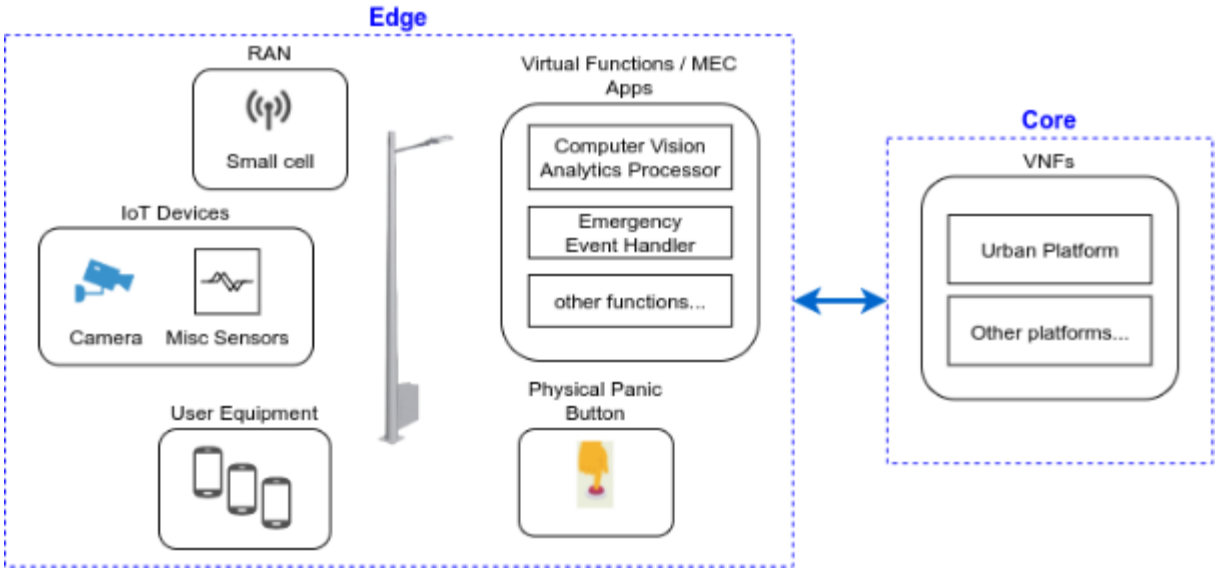
2.4.1.7 Alternative Flow

- 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 website: https://www.braine-project.eu

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 10** 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.

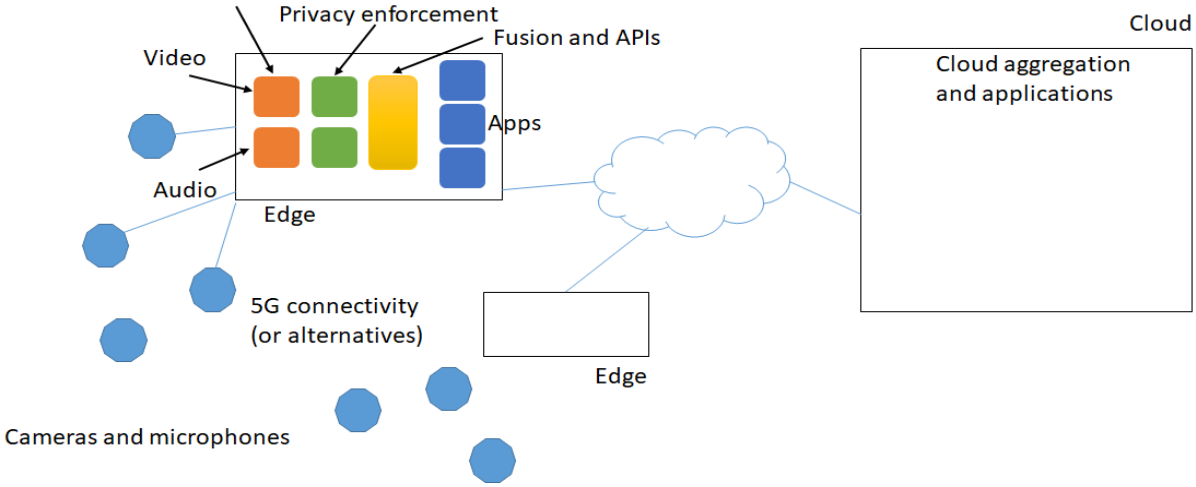


Figure 10 Block Diagram

Each edge node implements the high-level architecture depicted in **Figure 11**. 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.

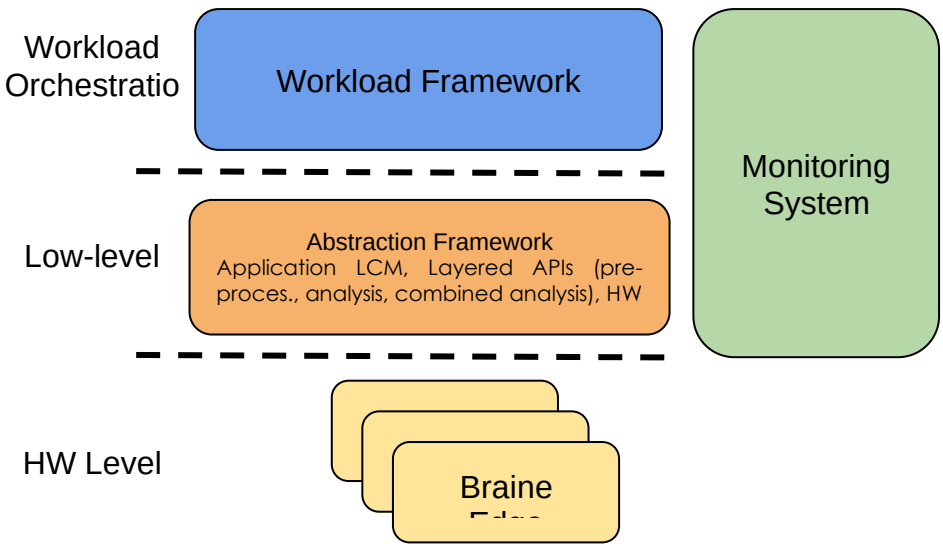


Figure 11 Architecture

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

2.4.11.2 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

2.4.11.3 URLLC requirements

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

Required Reliability 99,9999%
Maximum tolerable jitter: 0.5ms

2.4.11.4 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.

2.4.11.5 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 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

Actors & Roles

- **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 communicate 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. are 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?

2.6 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 analyzed 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 (https://www.vital5g.eu/wp-content/uploads/2022/05/VITAL5G-D1.1_Report-on-Use-case-requirements-v2.0.pdf)

2.6.1.3 Roles and Actors

Roles relating to/appearing in the Use Case are described in Table **3**.

Table 3: Involved stakeholders and their role

https://www.vital5g.eu/wp-content/uploads/2022/05/VITAL5G-D1.1_Report-on-Use-case-requirements-v2.0.pdf

	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 VITAI-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 12 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.

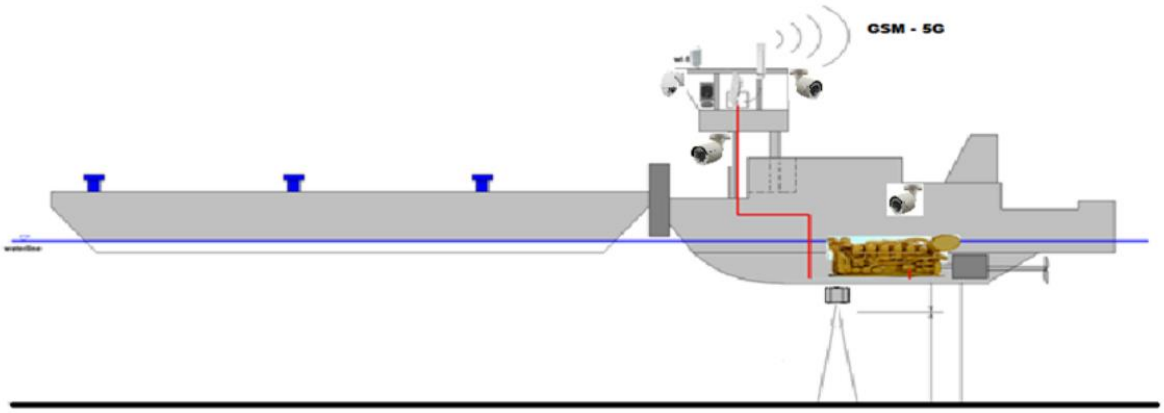


Figure 12: Positioning of hardware and sensors on a ship
(Figure copied from VITAL-5G D1.1 Report on use case requirements, see: https://www.vital5g.eu/wp-content/uploads/2022/05/VITAL5G-D1.1_Report-on-Use-case-requirements-v2.0.pdf, page 42)

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 13**.

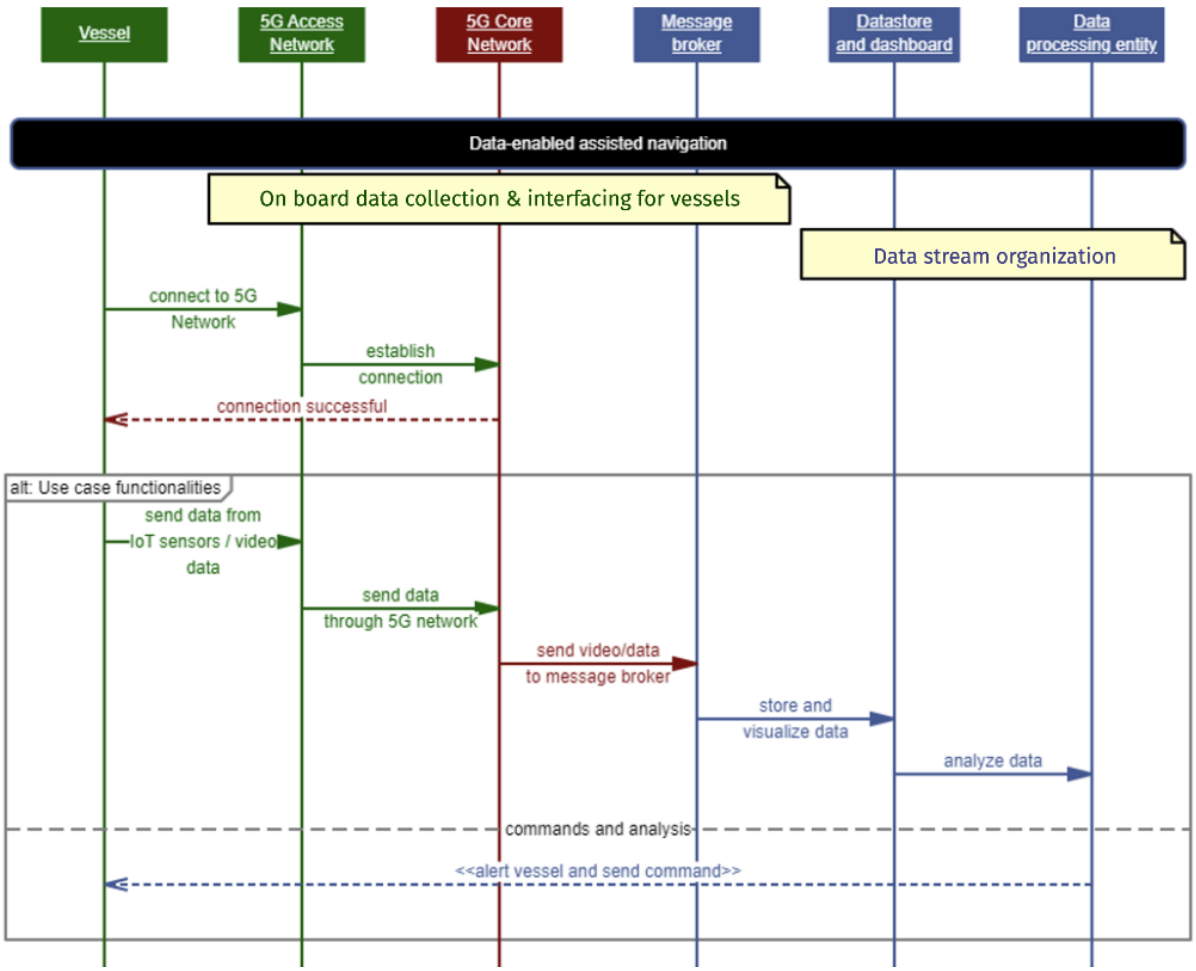


Figure 13: Data-enabled assisted navigation service flow diagram
(Figure copied from VITAL-5G D1.1 Report on use case requirements, see: https://www.vital5g.eu/wp-content/uploads/2022/05/VITAL5G-D1.1_Report-on-Use-case-requirements-v2.0.pdf, page 32)

- **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 14.

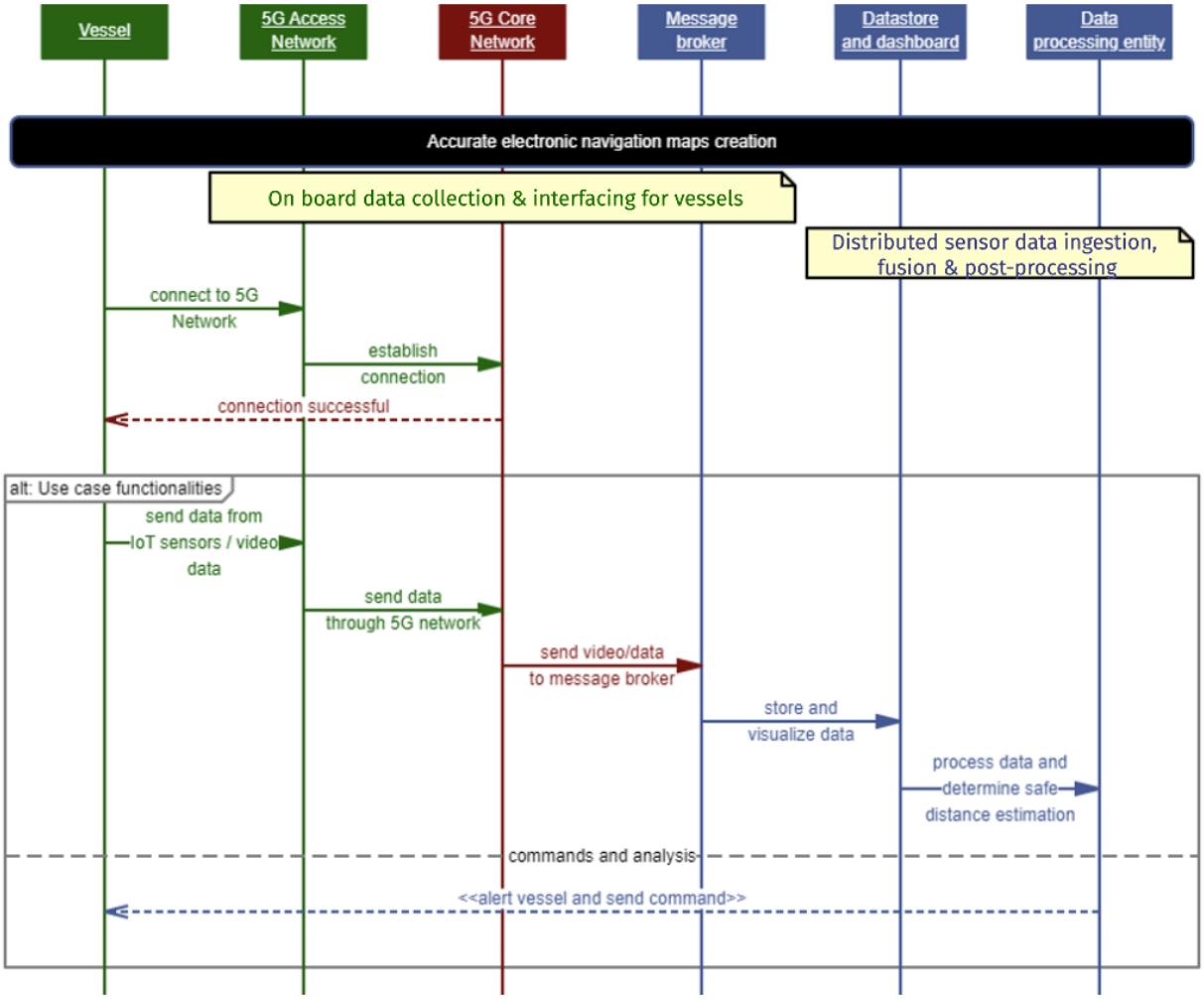


Figure 14: Accurate electronic navigation maps creation service flow diagram
(Figure copied from VITAL-5G D1.1 Report on use case requirements, see: https://www.vital5g.eu/wp-content/uploads/2022/05/VITAL5G-D1.1_Report-on-Use-case-requirements-v2.0.pdf, page 33)

- **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 15.

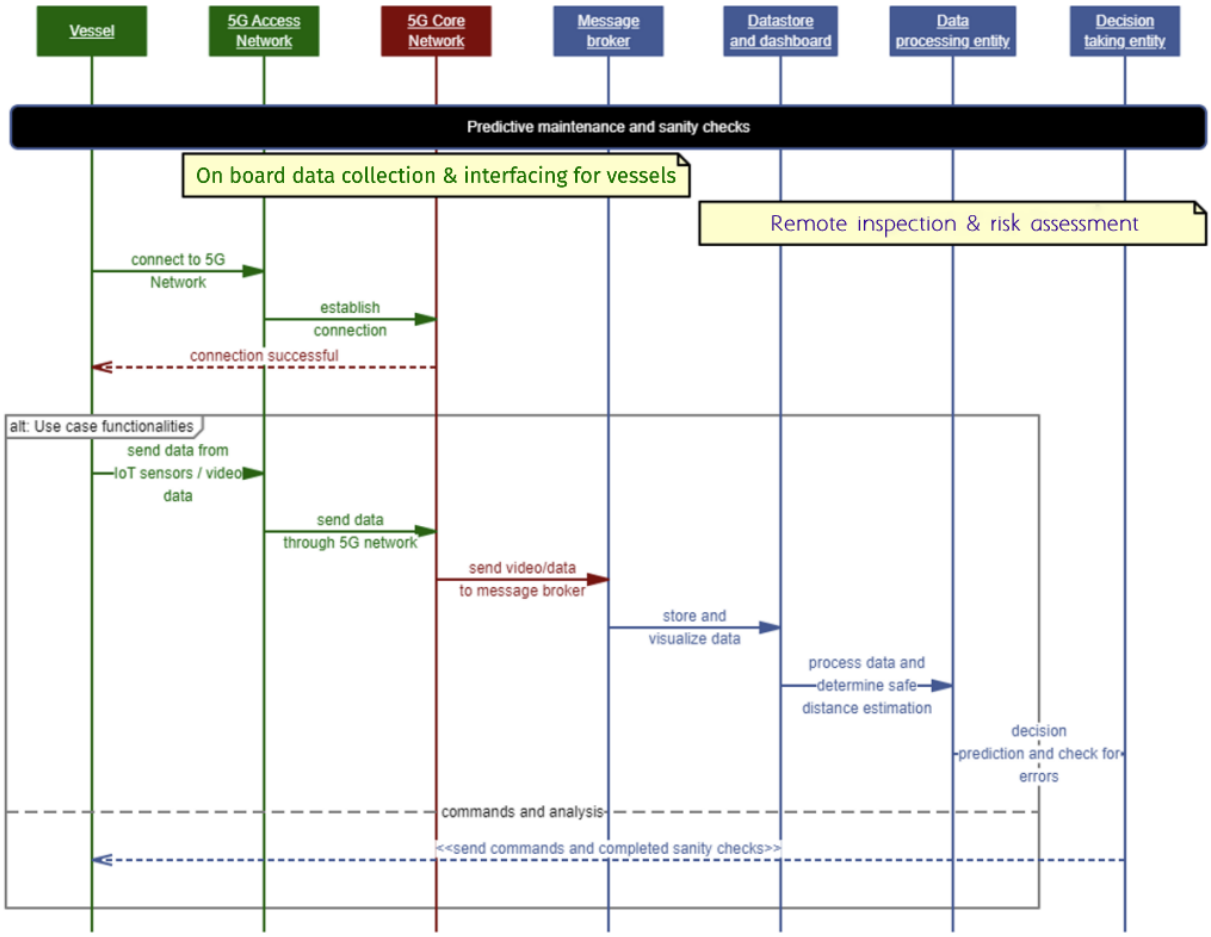


Figure 15: Predictive maintenance and sanity checks service flow diagram

(Figure copied from VITAL-5G D1.1 Report on use case requirements, see: https://www.vital5g.eu/wp-content/uploads/2022/05/VITAL5G-D1.1_Report-on-Use-case-requirements-v2.0.pdf, 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

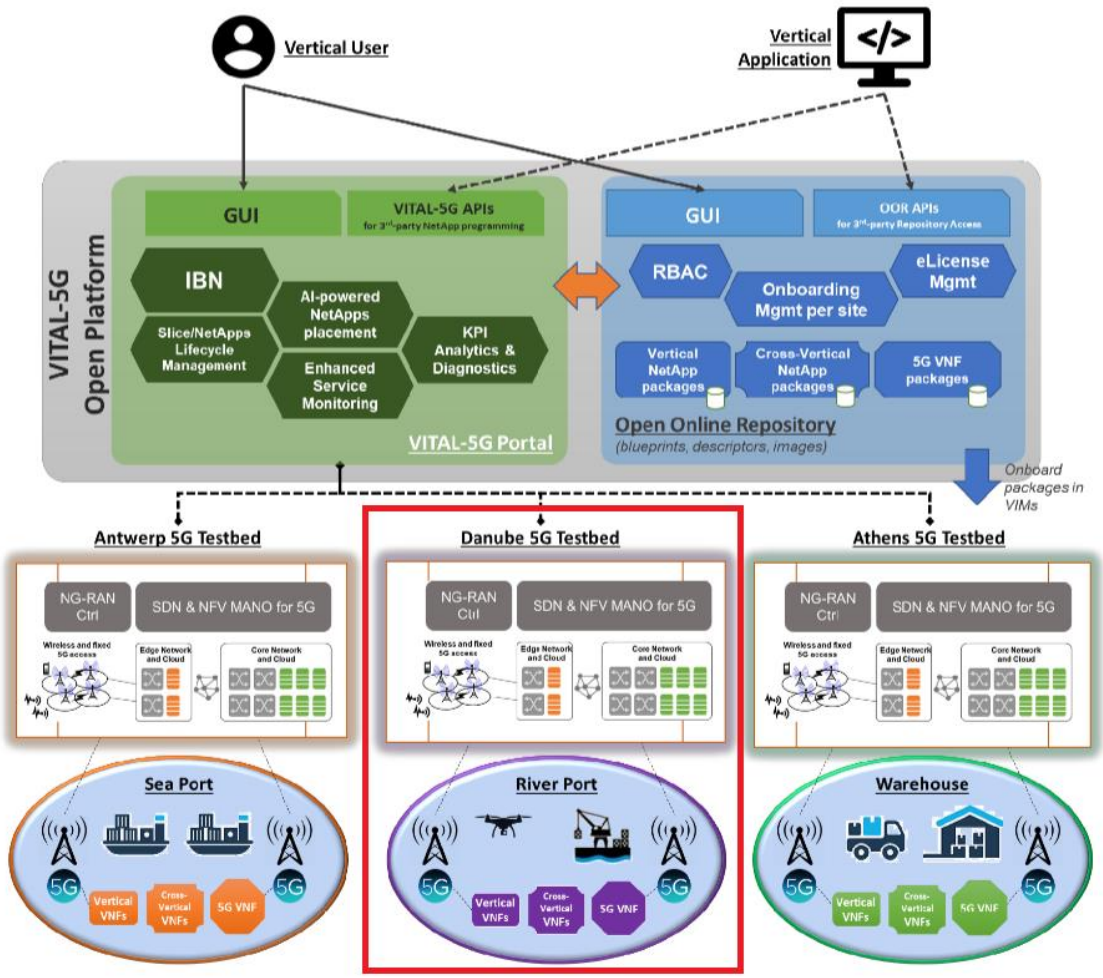


Figure 16: High-level architecture of the VITAL-5G system

(Figure copied from VITAL-5G D1.2 System Specifications and Architecture, see: https://www.vital5g.eu/wp-content/uploads/2022/01/VITAL5G-D1.2-5G-system-specifications-and-architecture_Final.pdf, 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 17**;
- 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.

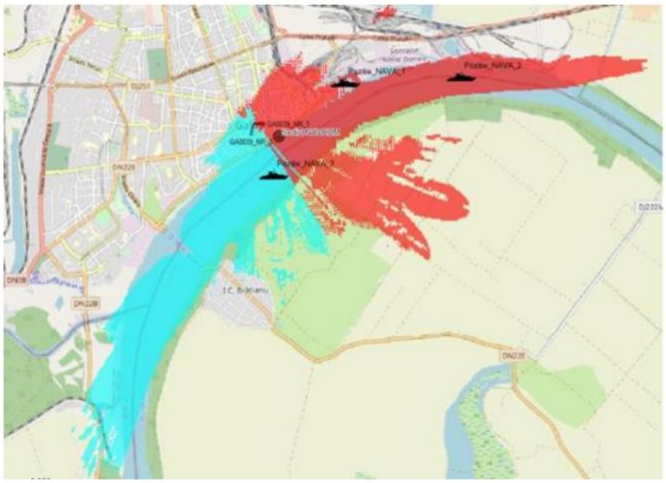


Figure 17: 5G Galati site coverage simulation map with the Use Case interest area representation

(Figure copied from VITAL-5G D3.1 Report on VITAL-5G infrastructure upgrades & extensions, see: https://www.vital5g.eu/wp-content/uploads/2022/04/VITAL-5G_D3.1-Report-on-VITAL-5G-infrastructure-upgrades-extensions_v1.0.pdf, 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 4** - **Table 7** as KPIs for latency, throughput, availability, dependability, and connectivity.

Table 4: 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 5: 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 6: 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 – 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	

Table 7: 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 – 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	

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 (www.inlecom.eu). 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 (https://www.chariotproject.eu/)

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

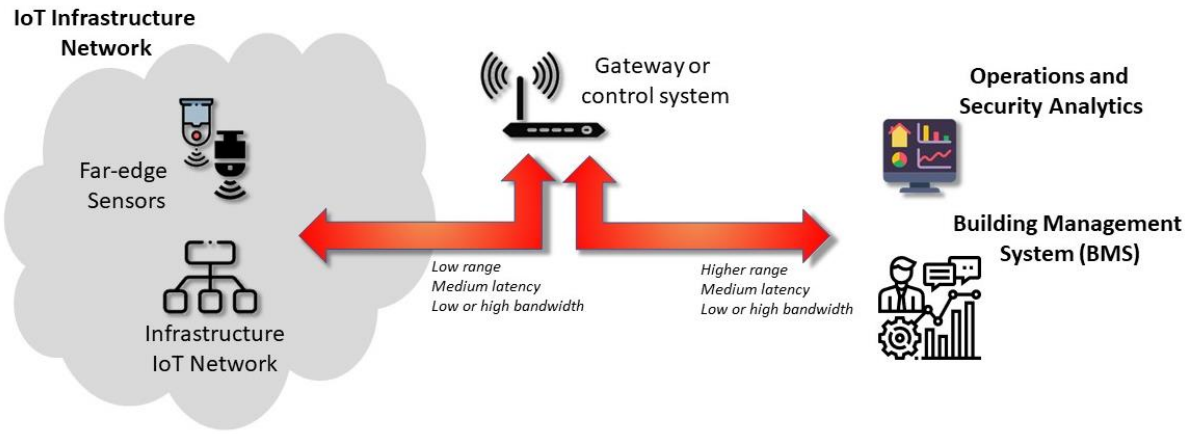
2.7.1.7 Alternative Flow

- 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 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 analyzed 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 (https://www.auroral.eu/#/p-pilots).

HUAWEI & NOVA-WIND PRESENT AN INNOVATIVE FIRE DETECTION PILOT SOLUTION USING 5G, ARTIFICIAL INTELLIGENCE AND DRONE TECHNOLOGY, see: https://huawei.eu/press-release/huawei-nova-wind-present-innovative-fire-detection-pilot-solution-using-5g-artificial

H2020 – ICT- 2020 VITAL-5G: "Vertical Innovations in Transport And Logistics over 5G experimentation facilities" European project (https://www.vital5g.eu/wp-content/uploads/2022/05/VITAL5G-D1.1_Report-on-Use-case-requirements-v2.0.pdf)

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 18.

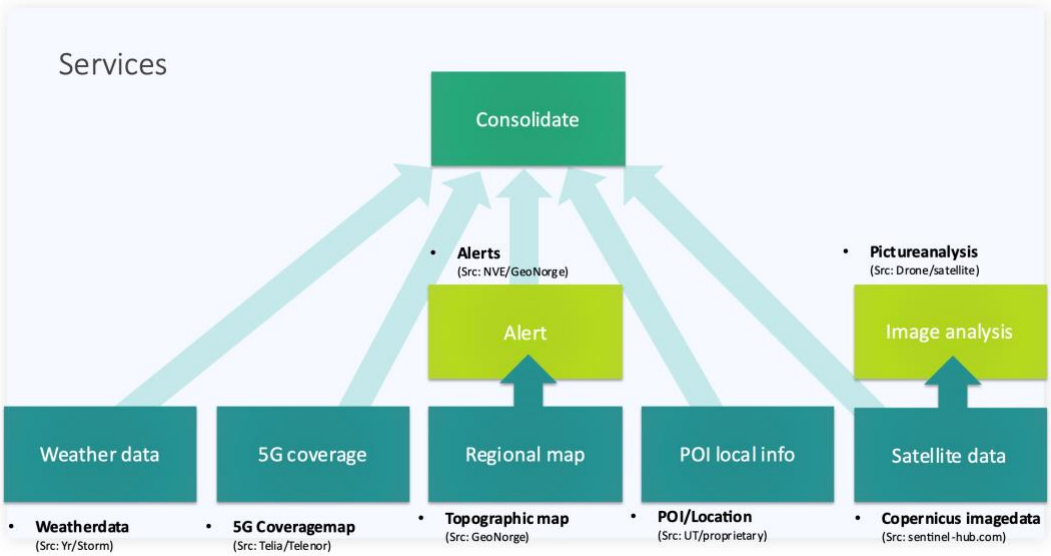


Figure 18: Examples of AURORAL services

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 19.

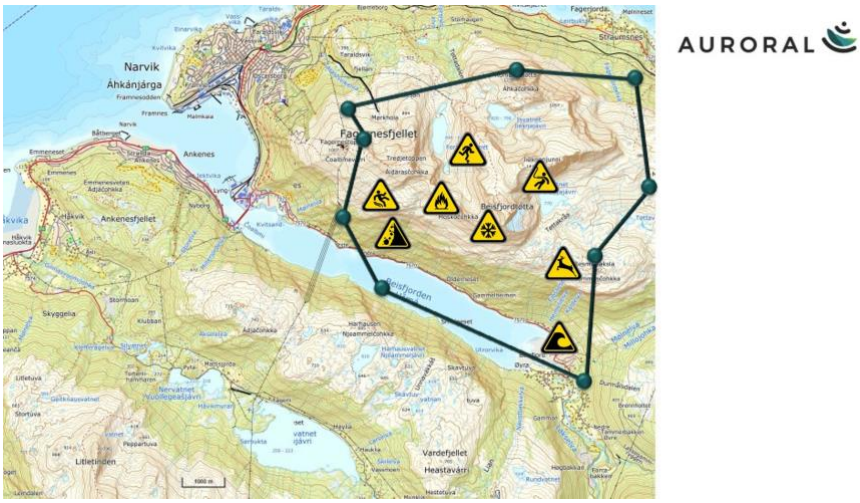


Figure 19: AURORAL coverage area of rescue

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.

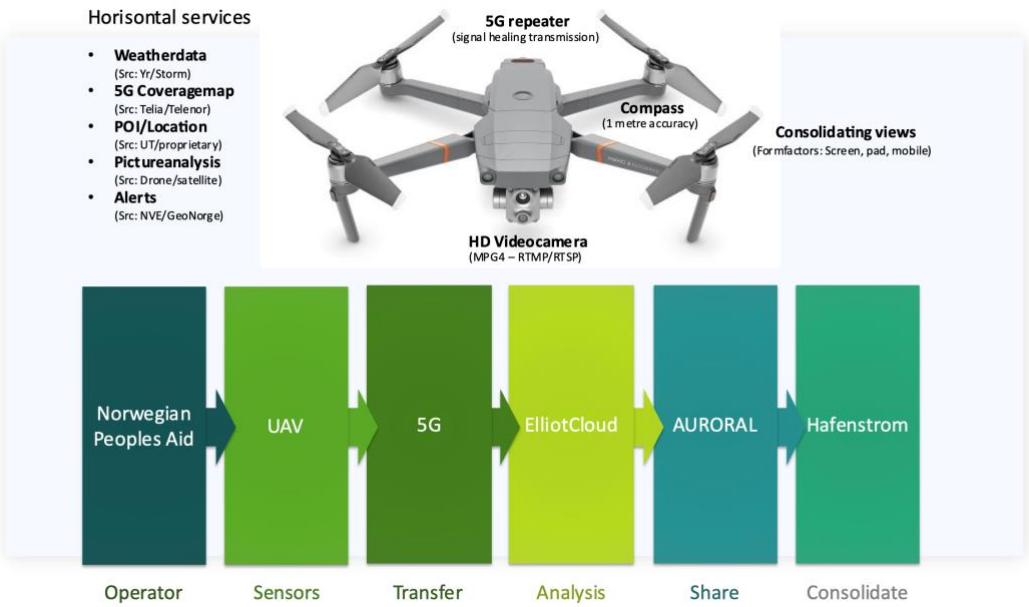


Figure 20: Normal Flow of operation

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 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 13**.

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 21 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 16**.

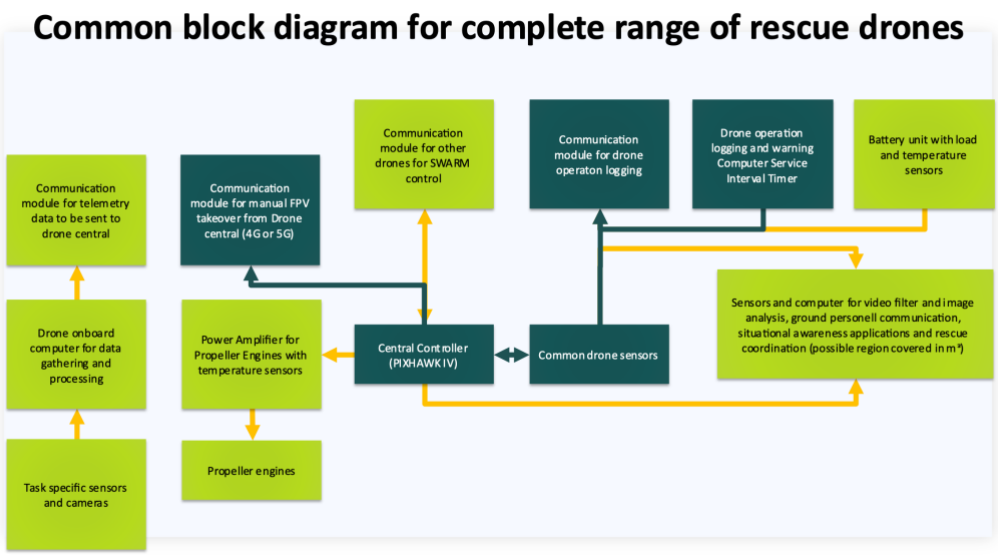


Figure 21: Complete block diagram for complete range of rescue drones

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 prioriterisation		
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		

2.8 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 22 (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.

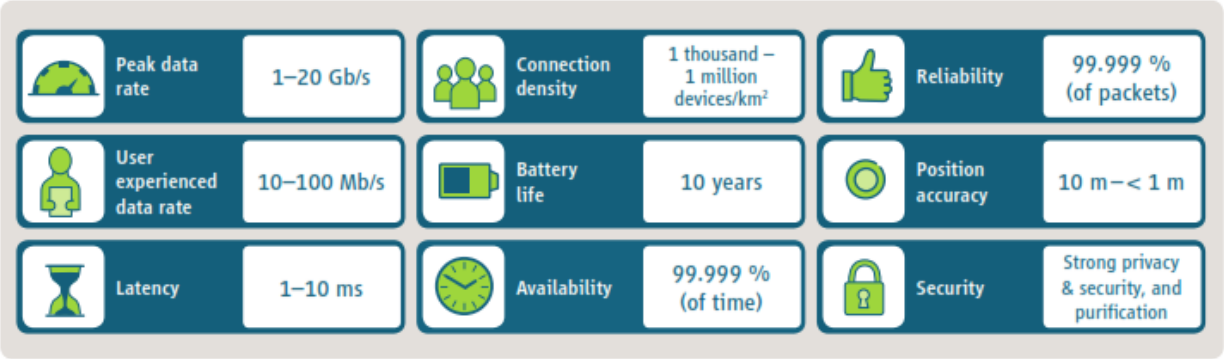


Figure 22: Selected target key performance indicators of 5G according to ITU-R (cf. [ITU-R M.2410-0])

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 (3rd Generation Partnership Project, www.3gpp.org) organization 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 23 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.

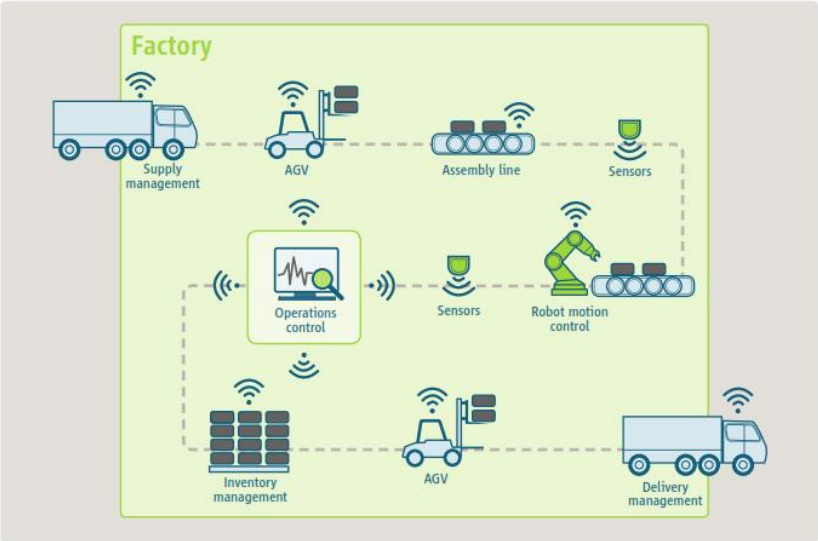


Figure 23: Exemplary application areas of 5G in the factory of the future

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 24, 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).

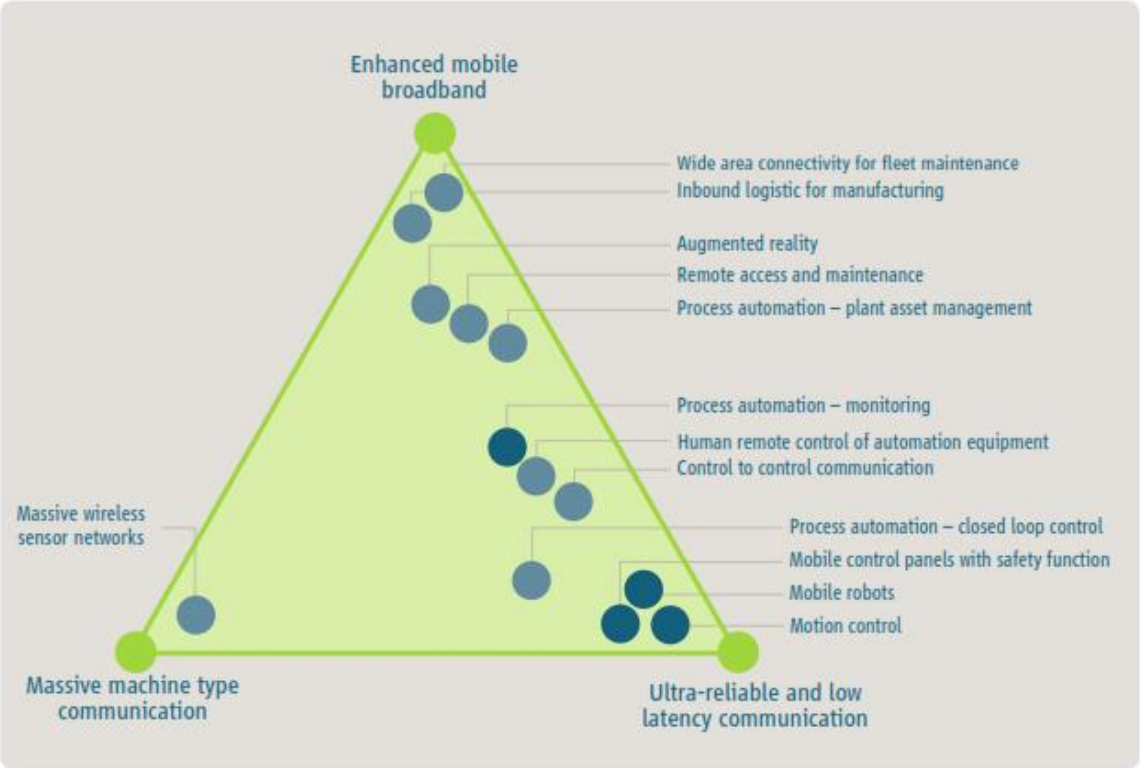


Figure 24: Overview of selected industrial use cases and arrangement according to their basic service requirements

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, Lyoner Straße 9, 60528 Frankfurt am Main, Germany (https://5g-acia.org/wp-content/uploads/2021/05/5G-ACIA_Exposure_of_5G-Capabilities_for_Connected_Industries_and_Automation_Applications_single-pages.pdf)
- References Highlight_Issue_2_FLIP_BOOK_3GPP_March 2021, page 4-5 (https://www.3gpp.org/ftp/Information/Highlights/2021_Issue02/mobile/index.html)

2.8.1.3 Roles and Actors

Actors & Roles

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 25.

- 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.

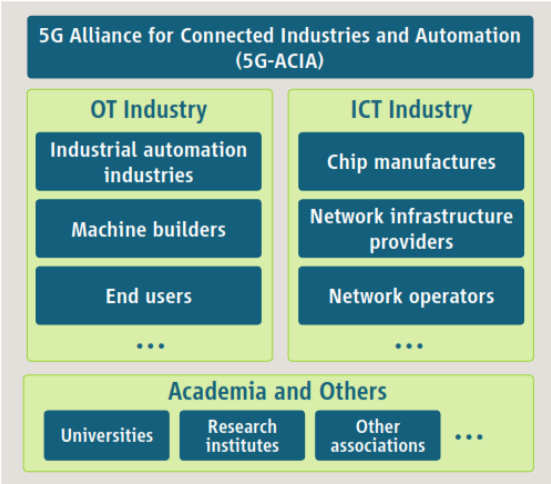


Figure 25: Overview of selected main stakeholder groups participating in 5G-ACIA

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 27. 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 26 shows the roadmap for the 3GPP standardization of Releases 16, 17 and 18 (Source: Puneet Jain, 3GPP Working Group Chair SA2)

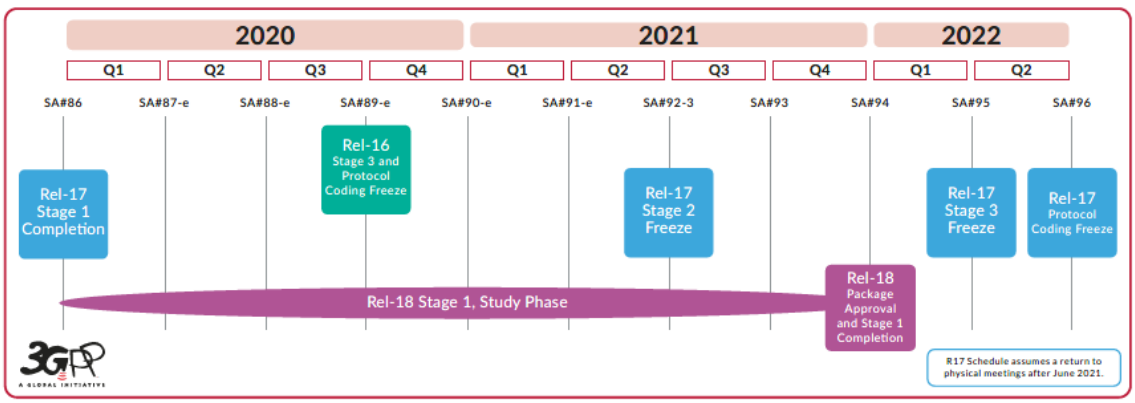


Figure 26: Overview of selected main stakeholder groups participating in 5G-ACIA

2.8.1.9 High Level Illustration

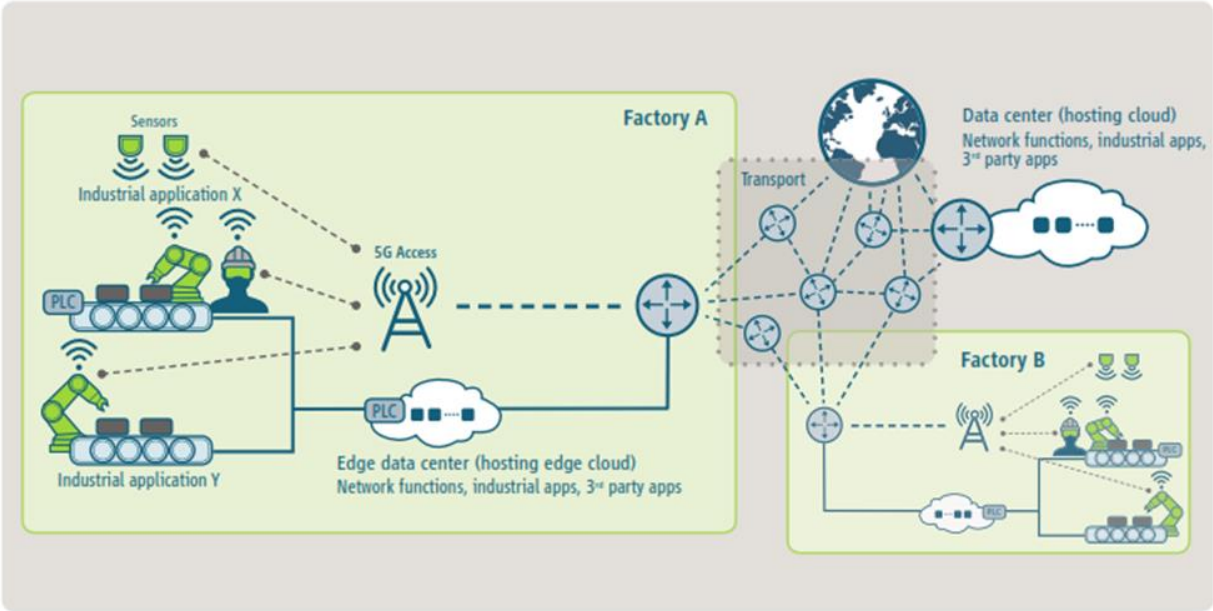


Figure 27: 5G-enabled smart factory scenario

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 24) 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 22 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: https://www.5g-acia.org/publications/.

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, started 2020 (site under development – end Sep conclusion of the site expected September 2021)

Interim information in a company: Critical Manufacturing - Augmanity

2.8.2.3 Roles and Actors (more details are provided in Annex I)

Actors & Roles

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

2.8.2.4 Pre-conditions

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

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

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.

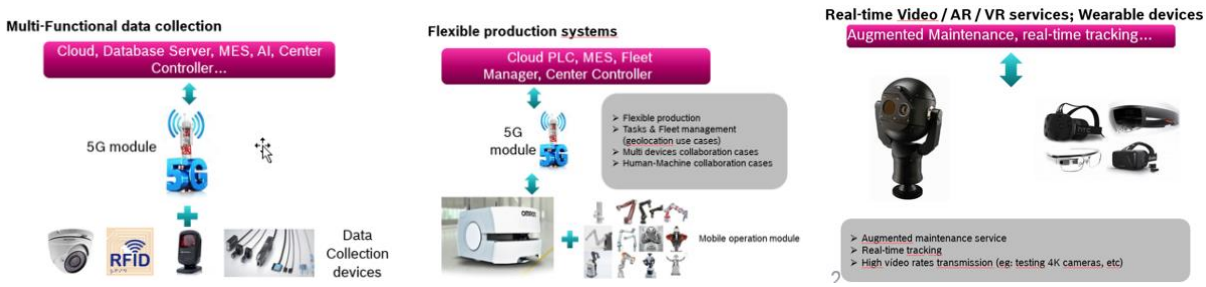
2.8.2.7 Alternative Flow

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.

2.9 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

[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

INSPIRE-5Gplus H2020 European project
(https://www.inspire-5gplus.eu; https://cordis.europa.eu/project/rcn/210216_en.html).

2.9.1.3 Roles and Actors (more details are provided in Annex 1)

Actors & Roles

- **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.).

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:

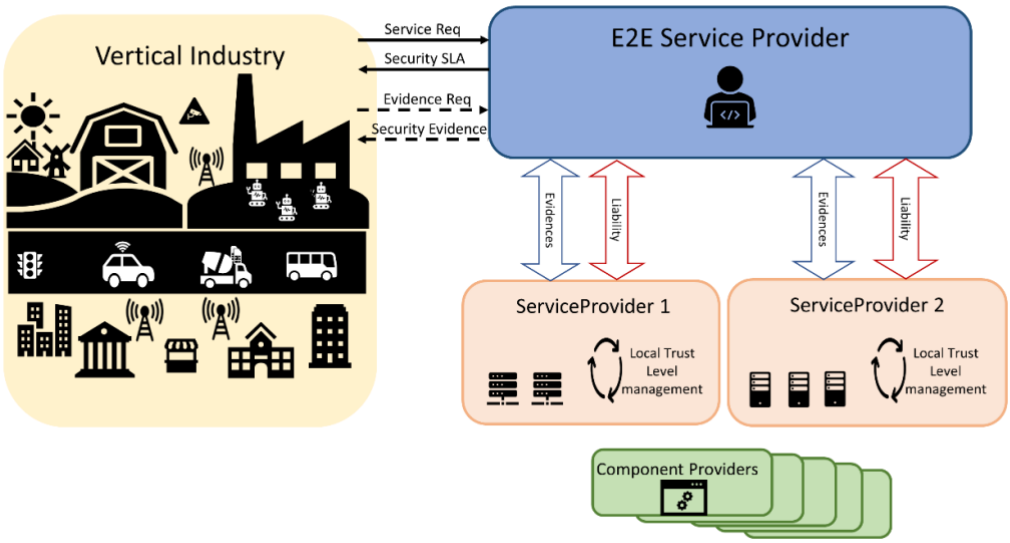
1. The evidence of the occurred problem is collected and root cause of the problem is investigated.
2. E2E Service Provider uses agreed Stakeholder Responsibility, Accountability and Liability descriptor to identify responsible parties based on the root cause.
3. The problem is mitigated based on the 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

<u>*Non-Functional Requirements.*</u>

- 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.

2.10 5G cloud-RAN

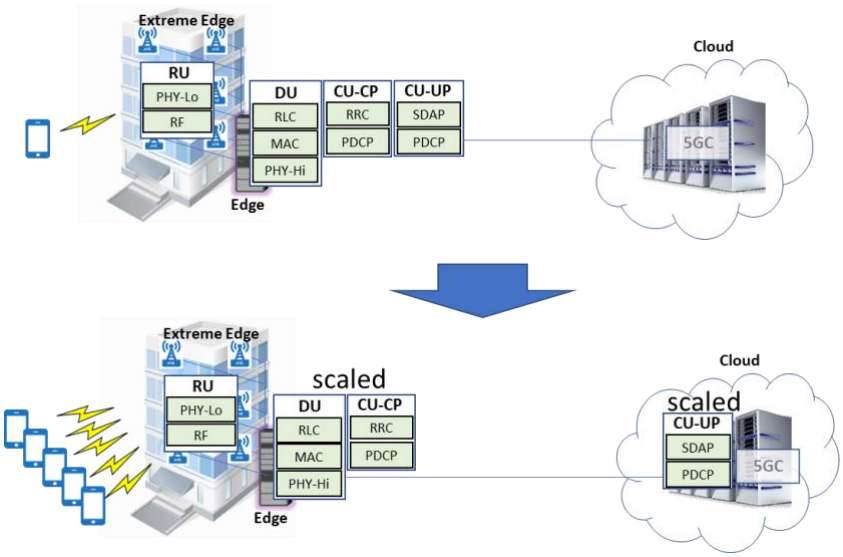
2.10.1 Virtualized base station for 5G cloud-RAN

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
(https://www.morphemic.cloud/ ; https://cordis.europa.eu/project/id/871643).

2.10.1.3 Roles and Actors (more details are provided in Annex I)

Actors & Roles

- **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:

5. Cloud-RAN is being modelled in the CAMEL modelling language which can be then processed by MORPHEMIC platform,
6. Cloud RAN is being deployed at the Edge and becomes operational. This step can be called a 'deployment' phase,
7. Due to the influx of the users, MORPHEMIC recognizes the need to scale the cloud-RAN,
8. 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,

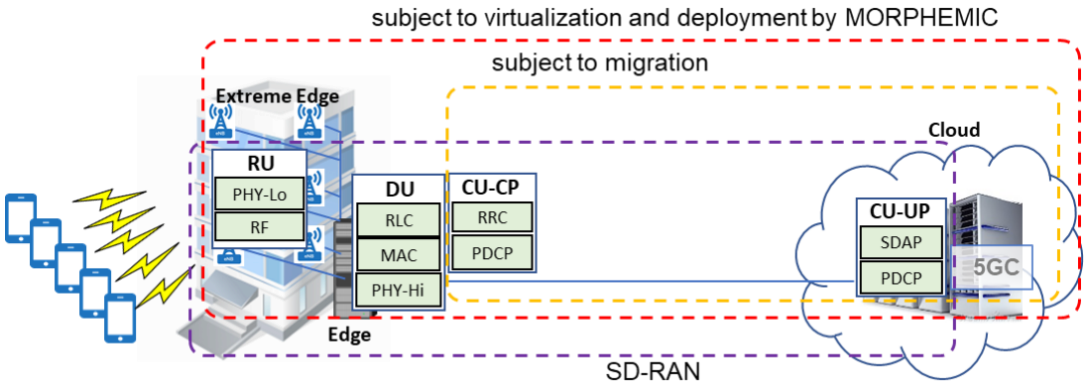
2.10.1.7 Alternative Flow

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**

  (specify if it is one way or roundtrip)

  50 ms one way for Control Plane.

  50 ms one way for User Plane.

- **Required Reliability**

  (I.e 99,99999%)

  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): https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5dc8b611b&appId=PPGMS

2.11.1.1 Description

Hexa-X describes several families of 6G based use cases, see the summary in Figure 28. More details are described below.

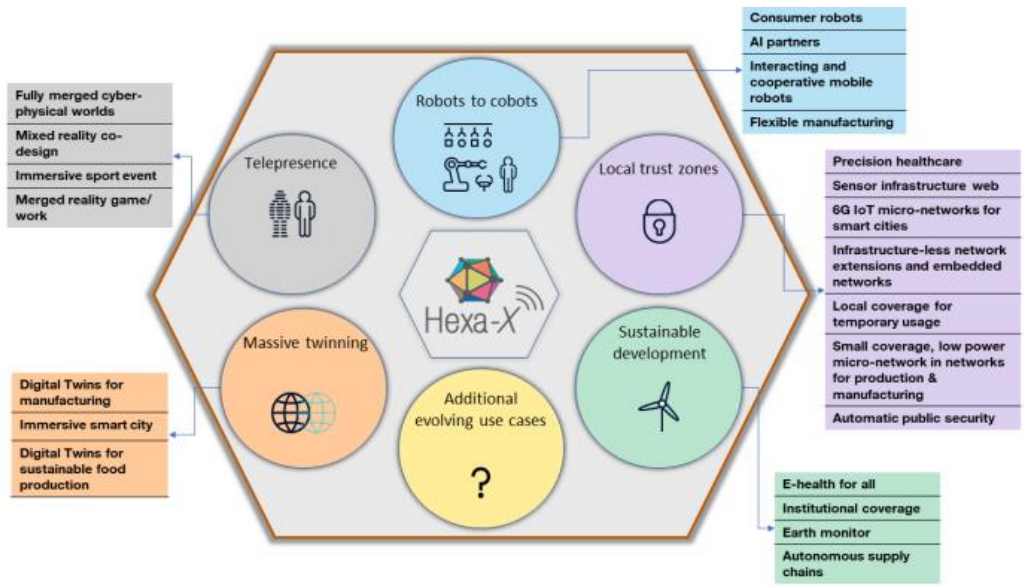


Figure 28: Summary of Hexa-X use case families and use case, source: EC

https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5dc8b611b&appId=PPGMS

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, defense 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:

(a) Managing infrastructure resources.

(b) New products need to be designed and automatically be linked to their DT

(c) 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.

(d) 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 immersive 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", see: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5dc8b611b&appId=PPGMS

2.11.1.3 Roles and Actors

Actors & Roles

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 29 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.

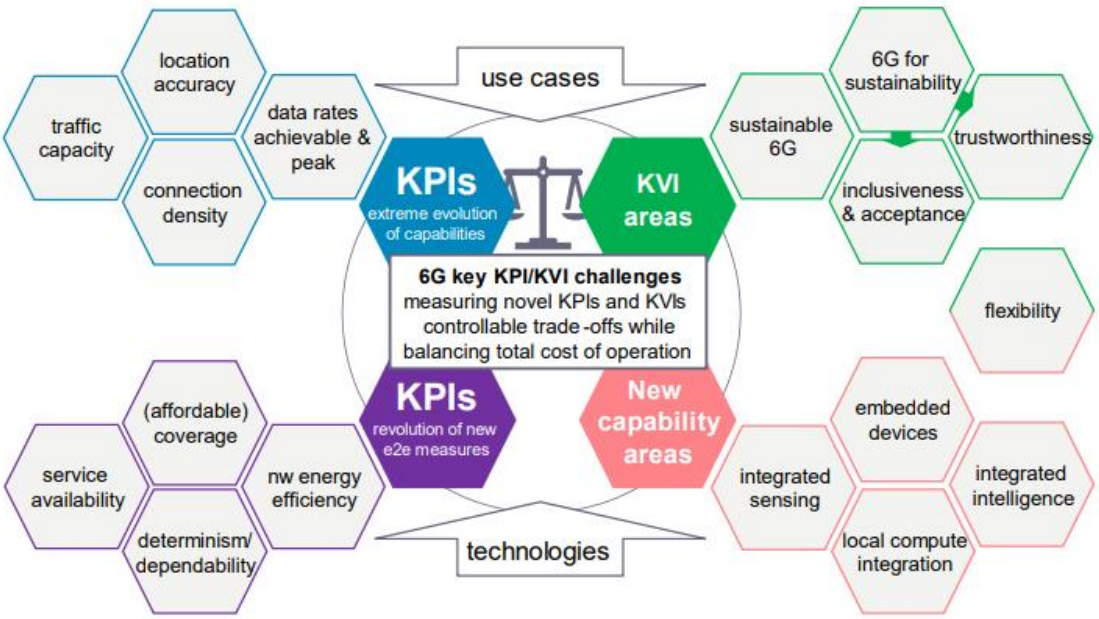


Figure 29: Clustering of Hexa-X Key Performance Indicators s and Key Value Indicators, copied from

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.

2.12 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:

1. In the first variant, 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.

2. 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.

3. 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

https://5gdrones.eu/

2.12.1.3. Roles and Actors (more details are provided in Annex 1)

- **Users -** People who connect during events in the crowd.
- **Drone operator**
- **Telecom operator** – to provide connectivity services

2.12.1.4. Pre-conditions

(A) Preparation stage: In addition to the common preparation stage steps mentioned in Section 3.3.11, this scenario will have the following additional steps:

i. Provide a portable setup comprised of UAVs, small 5G cells, other communication equipment and application servers necessary to support the broadcast and connectivity requirements..

ii. Deploy UAV operator software pilots to application servers provided in the test facility's portable setup.

X.5 Triggers

None

2.12.1.5. Normal Flow

(B) Preliminary flight stage

(C) 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.

2.12.1.6. Post-conditions

(D) Analysis & reporting.

2.12.1.7. High Level Illustration

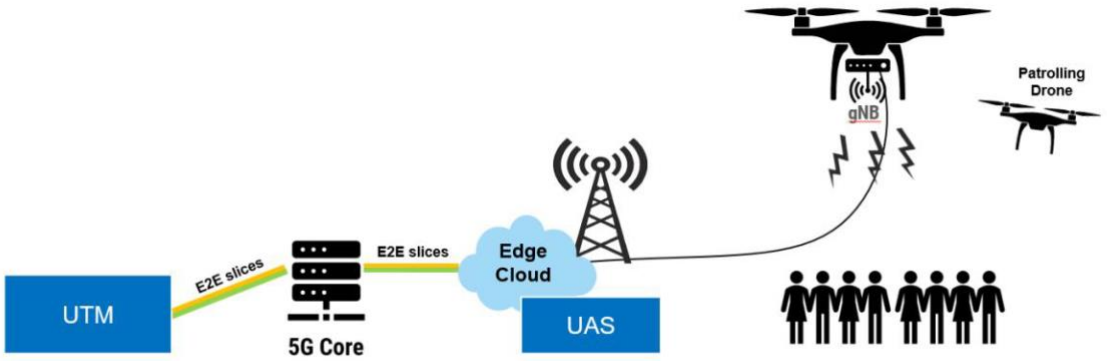


Figure 30: Use case architecture

Figure 31: High level architecture

2.12.1.8. 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 center 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 – possible consideration includes:

- 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	1 m

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 analyze 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:

3. An SMS / Email is sent to the involved stakeholders with the exact location of the event
4. 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 center, 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

Project - HUAWEI & NOVA-WIND PRESENT AN INNOVATIVE FIRE DETECTION PILOT SOLUTION USING 5G, ARTIFICIAL INTELLIGENCE AND DRONE TECHNOLOGY, see:

https://huawei.eu/press-release/huawei-nova-wind-present-innovative-fire-detection-pilot-solution-using-5g-artificial

2.12.2.3 Roles and Actors (more details are provided in Annex 1)

Actors & Roles

- **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.

Our main goals is 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

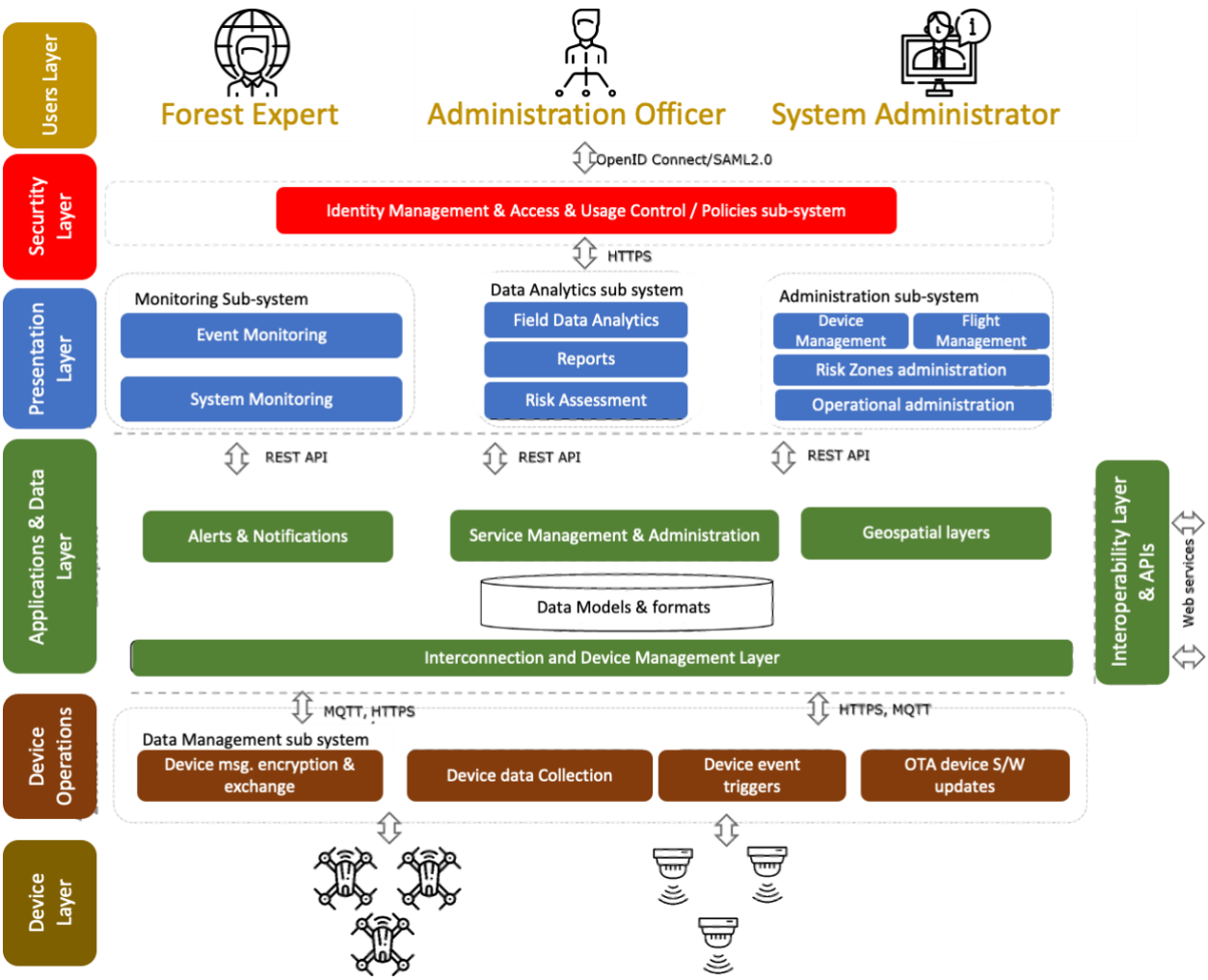
- No alternative flow

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

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

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+ kilometer 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 enrolls 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 sys- tem. 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 8 *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 8: 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 9** introduces the UAV payload communication requirements.

Table 10 introduces the communication requirements from Drone based applications.

Table 9: 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 10: 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-Takeoff 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 center and from the pilots.

The pilots and the operations center, 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 center. 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

3. Emerging Topics

This section describes emerging topics that are related to IoT & 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 (DT)

It is important to define the meaning of Digital Twin (DT) 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 DT 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 DT 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 adopt 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 need to be considered is now the way the DT 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 emerges:

1. Data collection is carried out manually or automatically?
2. Data collection is executed only once at the creation of the Digital Twin 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 DT 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 DT. We introduce this terminology for Digital Twins, 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.

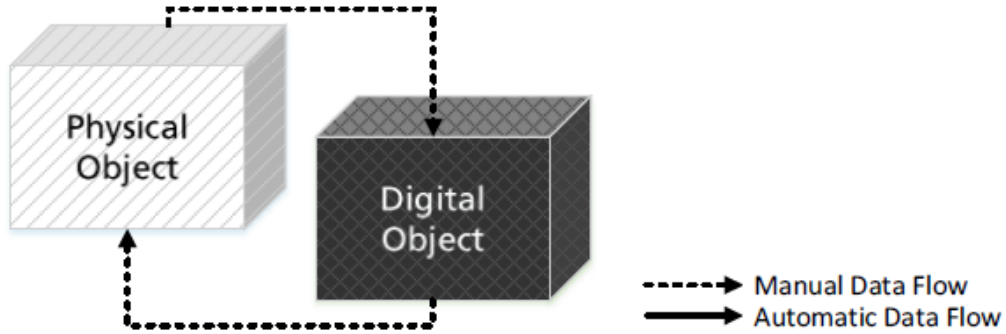


Figure 32: Data Flow in a Digital Model

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.

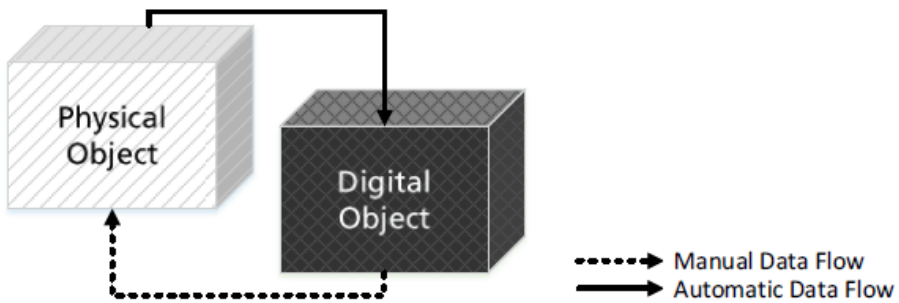


Figure 33: Data Flow in a Digital Shadow

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.

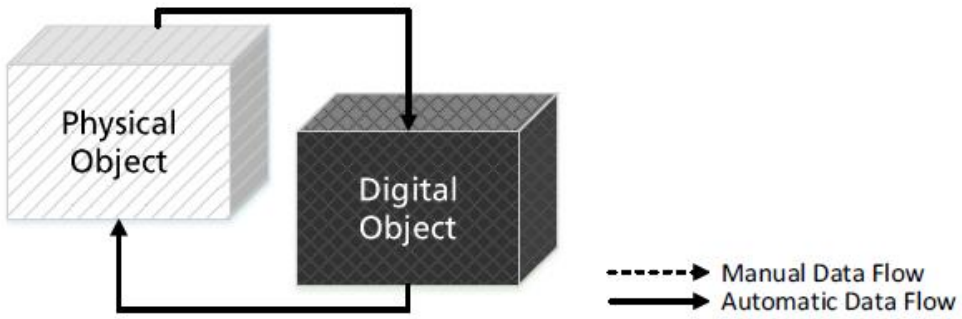


Figure 34: Flow in a Digital Twin

A more structured representation of DT 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 35, see [GaRo12].

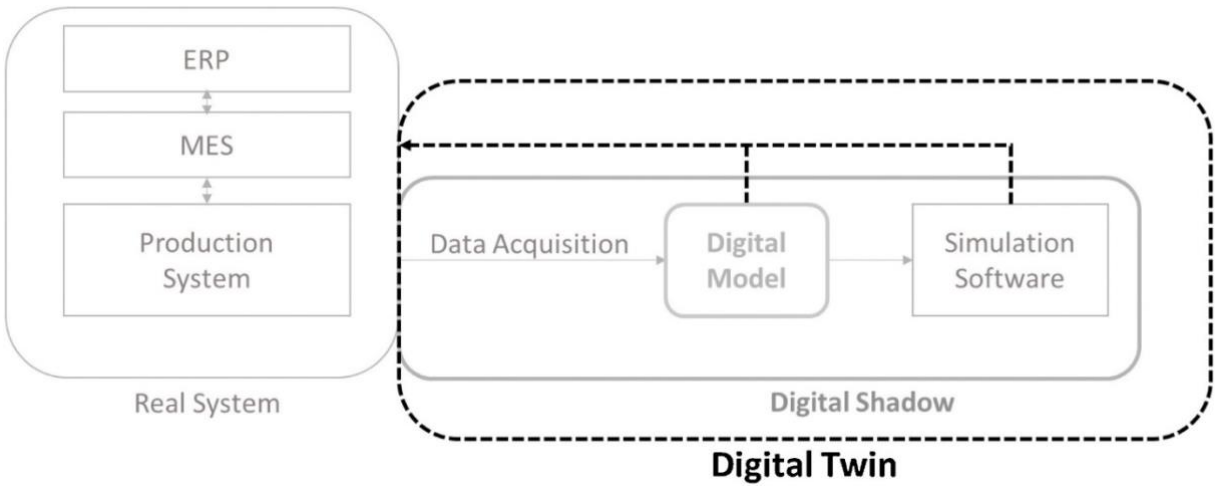


Figure 35: Digital Twin (DT) schema, copied from [GaRo12].

State-of-the-art technologies such as the Internet of Things (IoT), Wireless and Mobile Communication, cloud computing (CC), big data analytics (BDA), and artificial intelligence (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, cyber–physical systems (CPS) and digital twins (DTs) 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.

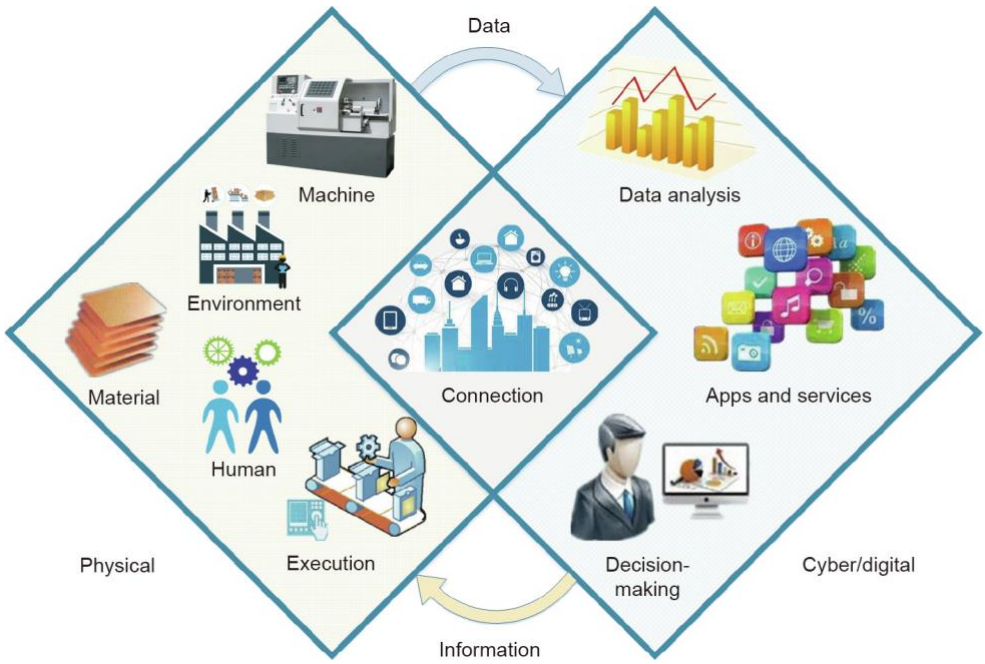


Figure 36: Mapping between physical and cyber/digital worlds, copied from [KrKa18]

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 12 12 the differences between the two terms are formalized.

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.

Table 12: Correlation and comparison of CPS and DTs. copied from [KrKa18]

Fast development and evolution of DT 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].

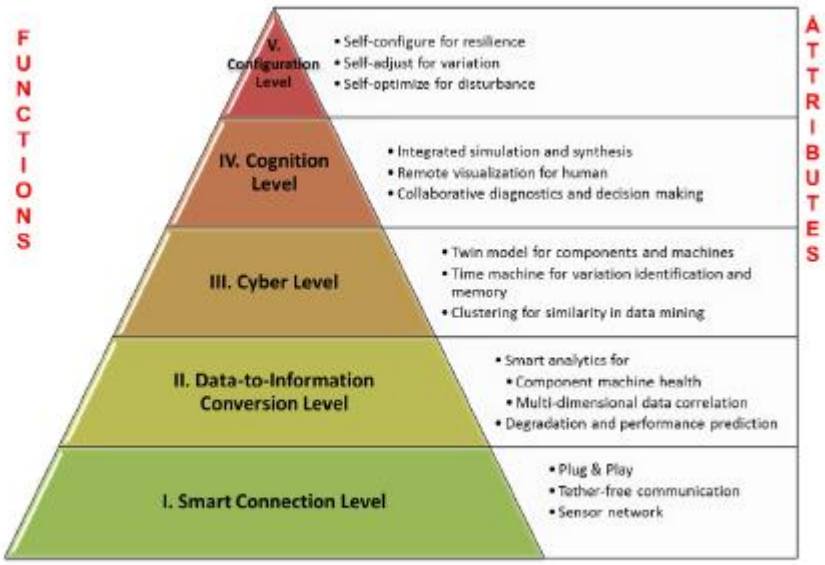


Fig. 1. 5C architecture for implementation of Cyber-Physical System.

Figure 37: 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].

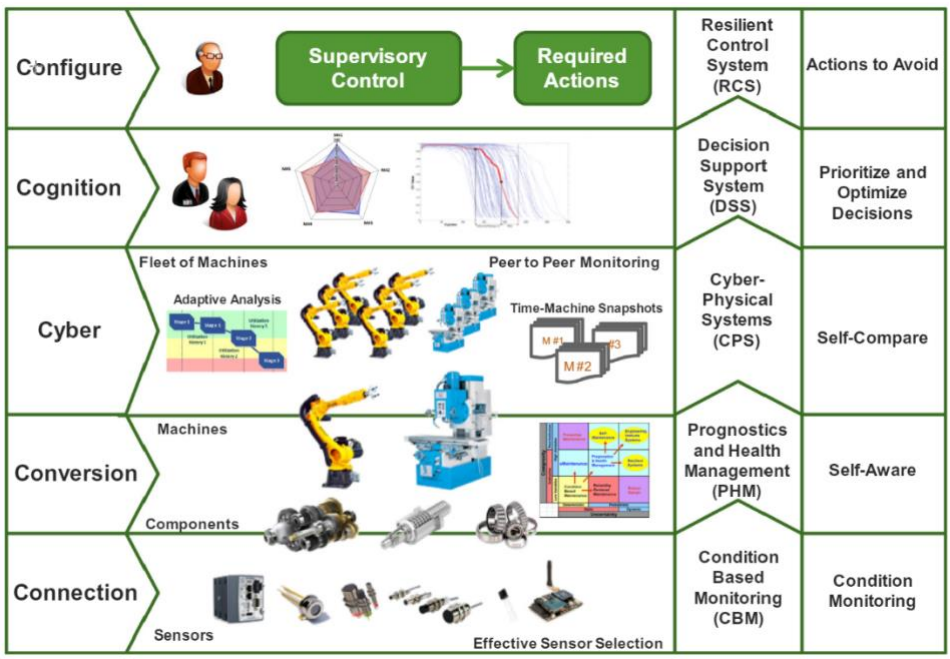


Figure 38: Applications and techniques associated with each level of the SC architecture, from [CiNe19]

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 Artificial Intelligence (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 / DT 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 autonomously and resiliently respond to failures in order to prevent catastrophic operational disruptions.

As for the DT, it is considered to be a new way of managing the industrial IoT. Integrating cloud technologies in DTs holds promise for ensuring the scalability of storage, computation, and communication. BDA, AI, and corresponding algorithms are also seen as important foundations for a DT. In the exploration of potential DT applications, new IT and not-IT technologies play a more and more important role, moving from a pure technology perspective towards an 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 DT/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.

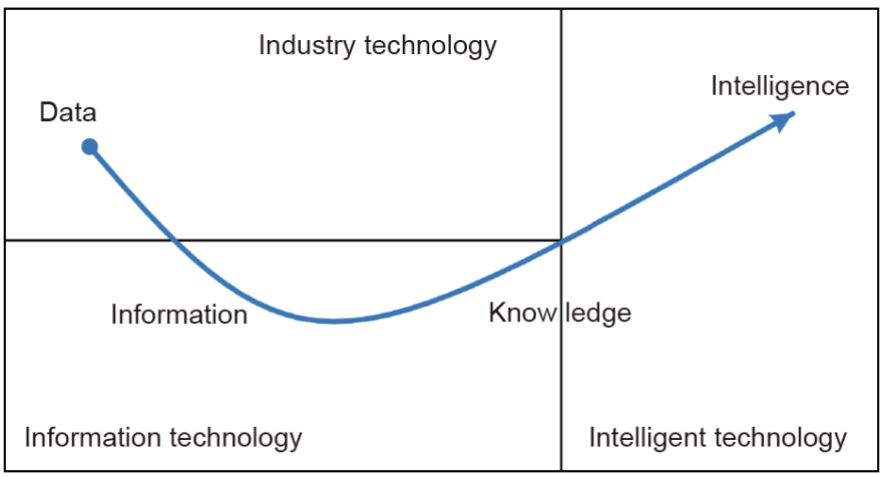


Figure 39: Integration of industrial technology, information technology, and intelligent, copied from [KrKa18]

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, Network Function Virtualization (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 are 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].

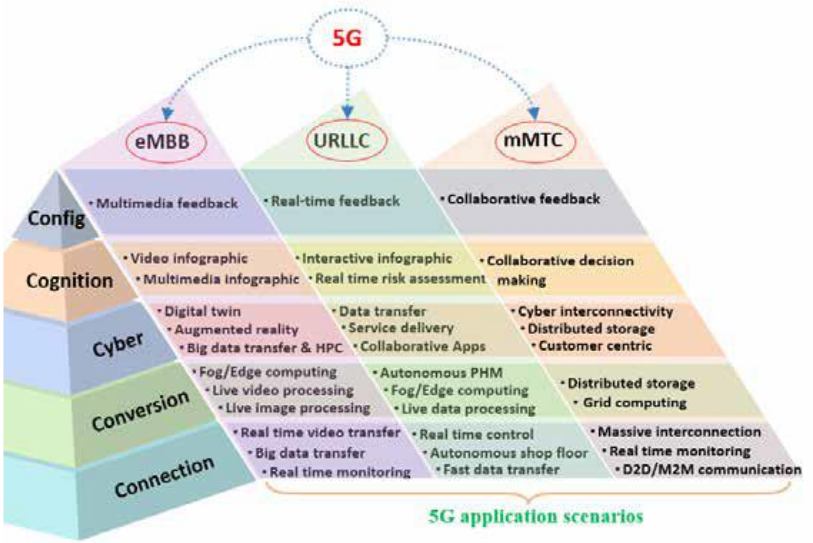


Figure 40: Application Scenarios, copied from [JML20]

3.2 Deep Edge, Terminal and IoT Device Integration in B5G communication infrastructure

This section is related to the Networld2020[12] 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.

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

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).

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[13]) the bandwidth is limited and not suitable to transfer large amount of data (e.g. multimedia data).

[33] See https://en.wikipedia.org/wiki/Narrowband_IoT

- **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.[14]

- **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[15].

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[16], LF Edge[17], Open Edge Computing[18] or OpenStack[19] (just to name a few).

[14] 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)

[15] See e.g. https://ieeexplore.ieee.org/document/9430853

[16] https://forge.etsi.org/rep/mec

[17] https://www.lfedge.org/

[18] https://www.openedgecomputing.org/

[19] https://www.openstack.org/use-cases/edge-computing/

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 centre.

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*[20] 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[21] 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).

"Edge computing represents the first step towards the decentralisation of Cloud computing, bringing the concept of Federated Cloud to its next evolutionary stage."[22]

[20] 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/

[21] https://www.gaia-x.eu/

[22] http://www.pledger-project.eu/FederatedCloud_RA_PP_022021.pdf

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[23], 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[24], but with this vision, the concept goes beyond the network functional splitting and can be applied to other fields.

In Noriega et al.[25] and Pastor et al.[26], 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.[27], 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] 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

[24] 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.

[25] 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.

[26] 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.

[27] 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.[28], 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[29] and El Khafhali et al.[30], the authors focus the efforts in the modelling and provision of the task distribution in the Cloud. In Lopez et al.[31], 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.).

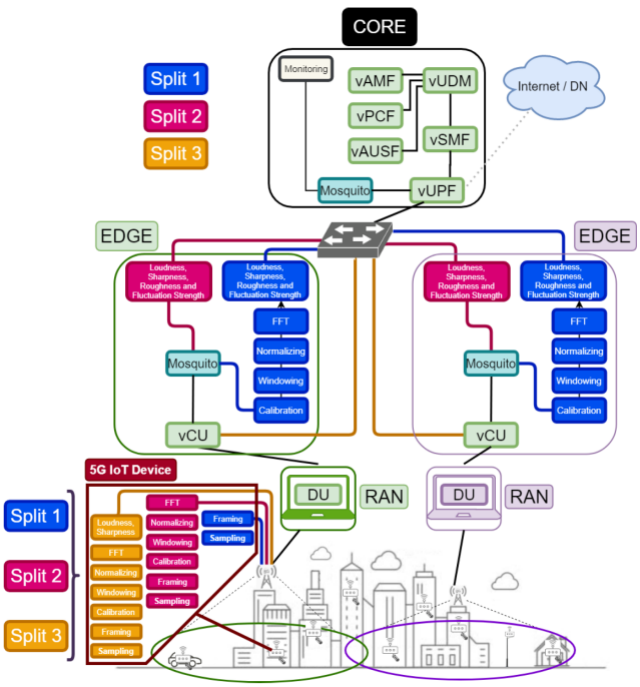


Figure 41: Conceptual diagram of the IoT architecture with different splitting options for the 5G complex metrics calculation system[5]

[28] 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

[29] 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.

[30] 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.

[31] 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 41 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[32], 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 42 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).

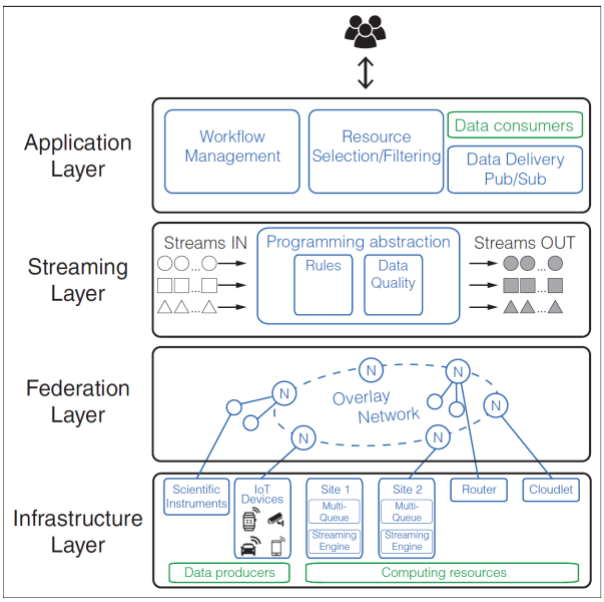


Figure 42: Overall layered architecture of the edge-based data-intensive IoT system.

[32] 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[33][34] 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*[35] 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)[36] 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[37] in home and small-business networks[38].

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

[33] 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.

[34] 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)

[35] https://ec.europa.eu/digital-single-market/en/news/building-ecosystem-where-iot-edge-and-cloud-converge-towards-computing-continuum

[36] E. Lear, D. Romascanu, and R. Droms, "Manufacturer Usage Description Specification (RFC 8520),", 2019

[37] T. Polk, M. Souppaya, and W. C. Barker, "Mitigating IoT-Based Automated Distributed Threats,", 2017

[38] NIST, "Securing Small-Business and Home Internet of Things Devices:NIST SP 1800-15," 2019

been considered in recent research activities[39]. 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[40]. 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[41]. 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[42].

[39] 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

[40] 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.

[41] 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.

[42] 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).

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[43], 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.

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 43.

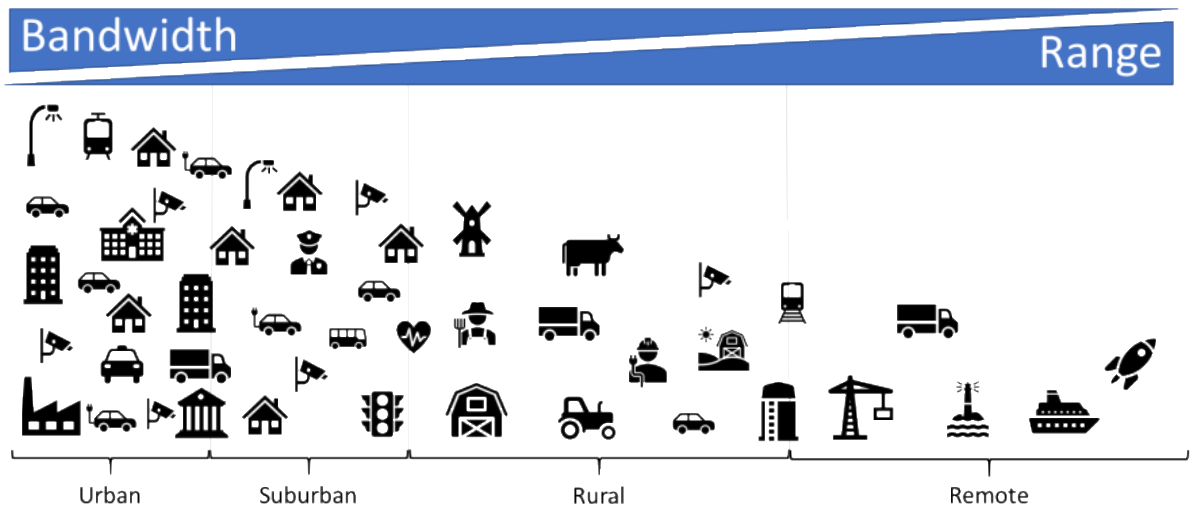


Figure 43: 5G/Satellite Coverage

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].

[43] 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.

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 44.

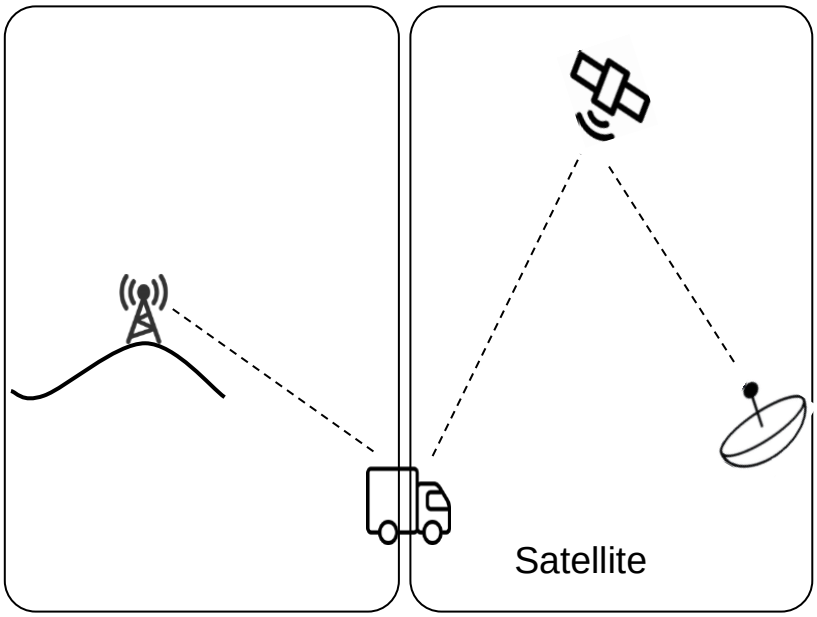


Figure 44: Integrated terrestrial and satellite IoT networks

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).

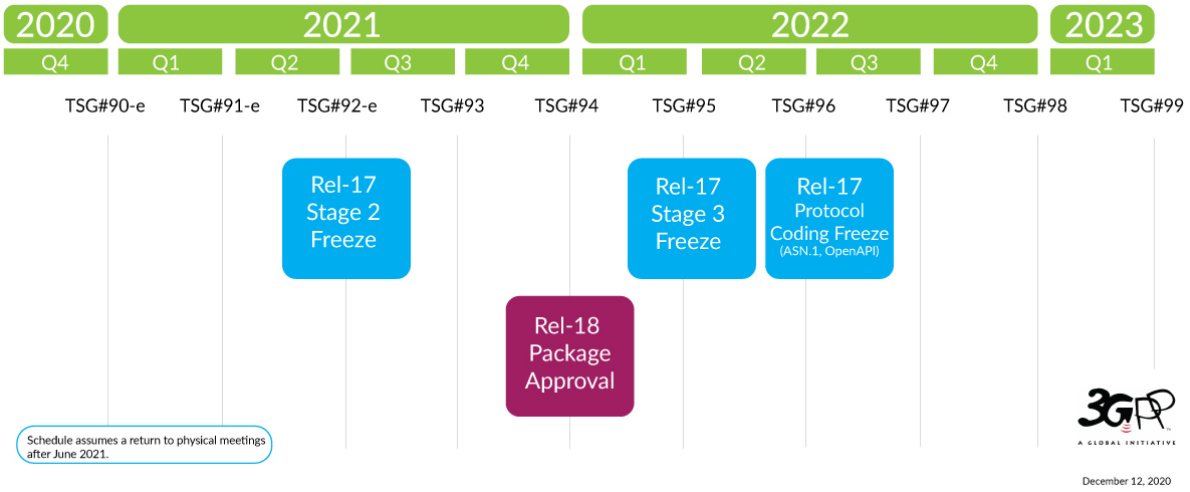


Figure 45: 3GPP Release 17 timeline, copied from 3GPP

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 45.

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[44]. 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[45]. While, the possibility of having fully automated vehicles (level 5 of the J3016 standard)[46] 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[47]. 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

[44] 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.

[45] 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.

[46] SAE, S. (2014). J3016 standard: taxonomy and definitions for terms related to on-road motor vehicle automated driving systems.

[47] Yang, CY David, Kaan Ozbay, and Xuegang Ban. "Developments in connected and automated vehicles." (2017): 251-254.

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. 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[48].

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[49] 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)[50]. 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"[51]. The security (authentication and integrity) of V2X has been designed and described in ETSI and IEEE standards[52] 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.

[48] Tong, W., Hussain, A., Bo, W. X., & Maharjan, S. (2019). Artificial intelligence for vehicle-to-everything: A survey. IEEE Access, 7, 10823-10843.

[49] 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.

[50] 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.

[51] 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

[52] 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.

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[53]. The recent terrorist attacks where commercial vehicle were used to kill pedestrians[54] 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[55]. 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[56].

[53] 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.

[54] https://www.history.com/this-day-in-history/2016-nice-terrorist-attacks

[55] 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.

[56] 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.

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. 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. The new Horizon Europe SNS and KDT Partnerships 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 KDT Partnership 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[57] and the US Executive Order on Improving the Nation's Cybersecurity[58].

[57] NIS Directive, https://digital-strategy.ec.europa.eu/en/policies/nis-directive

[58] 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/

ENISA has published several best practices documents on IoT security and securing the IoT supply chain[59][60][61], as well as other organizations such as NIST[62][63] and GSMA[64] Specific to 5G networks the EU Cybersecurity Act will mandate certifications for specific components in 5G networks[65], 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.

The proposed Smart Networks and Services Partnership will not directly be involved in component research, development and design. However, the research and development in Smart Networks and Services 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 ECSEL JU and/or the proposed Key Digital Technologies Partnership by promoting the development of European added value embedded solutions for innovative and secure applications. Smart Networks and Services 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 ECSEL JU and/or the proposed Key Digital Technologies Partnership can be leveraged. From the Smart Networks and Services 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. The Smart Networks and Services will 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 ECSEL JU and/or the proposed Key Digital Technologies Partnership 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.

[59] ENISA Guidelines for Securing the Internet of Things, https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[60] ENISA Good Practices for Security of IoT, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

[61] ENISA Baseline Security Recommendations for IoT, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[62] NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline, https://csrc.nist.gov/publications/detail/nistir/8259a/final

[63] NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers, https://csrc.nist.gov/publications/detail/nistir/8259/final

[64] GSMA IoT Security Guidelines and Assessment, https://www.gsma.com/iot/iot-security/iot-security-guidelines/

[65] Securing EU's Vision on 5G: Cybersecurity Certification, https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

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.

We need to use European and international standards 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.

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 (Alliance for IoT Innovation) 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 SDOs (Standards Developing Organizations), such as 3GPP (3rd Generation Partnership Project), 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.

In particular, this report lists first relevant IoT and edge computing use cases and their possible requirements on an underlying 5G and Beyond 5G communication infrastructure. The Release 2.0 version of this report includes several 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.

4.1 Requirements

By analysing the requirements that are derived from the presented use cases, see Section 2, it can be concluded that for these use cases the requirements listed in [Networld2020-SRIA] report, see as well Annex III are covering the needs that each of these use cases impose on the underlying 5G and Beyond 5G infrastructure.

In particular, the following requirements are identified by these use cases:

Robotic Automation area (Section 2.1):

Use case: Transport Infrastructure Inspection and Maintenance

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).

Radio Specific requirements

Radio Coverage

- **Radio cell range**
  - **Does the radio link crosses public spaces? Or is it constrained to indoor or customer premises?**
    1. Radio link crosses public spaces and includes indoor and outdoor premises.
- **Is Multicell required?**

  Multicell may be required for remote connectivity at regional level
- **Is handover required? Seamless? Tolerable impact in delay and jitter?**
  2. 100 Milliseconds delay can be tolerated.
- **Mobility: maximum relative speed of UE/FP peers**
  3. Robotic vehicle moving around 5-50km/h.

Bandwidth requirements

- **Peak data rate:** 1000Mbps
- **Average data rate:** 100Mbps

Edge Computing and Processing area (Section 2.2):

Use Case: Functional Splitting for Edge Computing

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, see Section 2.2.1.
- 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: This 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 specific nodes with microphones for audio gathering and soundscape description. Also, the Edges for signal processing according to the necessities of the system.

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

Potential Requirements

Functional Requirements

RTT, Bandwidth and Packet Loss: The below tables are copied from [ITU-T SG13 Y.3109]

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

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

Digital Twin (DT) area (Section 2.3):

Use cases: Digital Twin (DT) in Industry 4.0

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.

Radio Specific requirements

Radio Coverage

- Radio cell range : Mainly indoor
- Is Multicell required? No

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

Bandwidth requirements

- Peak data rate 100 Mb/s
- Average data rate 10 Mb/s
- Is traffic packet mode or circuit mode? TBD

URLLC requirements

- Required Latency 10 ms one way
- Required Reliability 99.9 %
- Maximum tolerable jitter TBD

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

Extreme pervasiveness of the smart mobile devices in Cities area (Section 2.4)

Use case: Smart City Edge and Lamppost IoT deployment (Section 2.4)

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

Radio Specific requirements

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

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

Use Case: Multi-tenant real time AI video/audio analytics (Section 2.4)

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

Radio Specific requirements

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

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

URLLC requirements

Required Latency: below 2ms

(specify if it is one way or roundtrip)

Required Reliability 99,9999%

Maximum tolerable jitter: 0.5ms

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.

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

Autonomous Urban Transportation (Section 2.5)

Use Case" - Intelligent Assistive Parking in Urban Area

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:

- regulative 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 can not be redefined as suitable for parking without some kind of planning and reallocation.
- insurance: insurance companies are very vary 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 communicate 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. are 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?

Maritime Transportation (Section 2.6):

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

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 17**;
- 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.

Phase 2:

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

Radio Coverage

N/A

Bandwidth and URLLC requirements

Specific requirements linked to the Use Case for each NetApp of the service are presented in **Table 4** - **Table 7** as KPIs for latency, throughput, availability, dependability, and connectivity.

Table 11: 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 12: 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 13: 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/m² or Km²)	Mbps/m²			10	
9	Device Density	Dev/Km2		100	1000	

Table 14: 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/m² or Km²)	Mbps/m²			10	
9	Device Density	Dev/Km2		100	1000	

Critical Infrastructure support applications area (Section 2.7):

Use Case: Smart Infrastructure Monitoring

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.

Radio Specific requirements

Radio Coverage

- **Radio cell range**
    - **Does the radio link crosses public spaces? Or is it constrained to indoor or customer premises?**
        4. 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.

Bandwidth and Latency requirements

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

Use Case: AURORAL HEALTH PILOT for Strengthening Preparedness In Health-Critical Remote Operations

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 prioriterisation		
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		

Smart Manufacturing and Automation area (Section 2.8):

Use cases: Factory of Future

Potential Requirements

Functional Requirements

Certain more detailed performance requirements of selected factory / process automation use cases. 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.

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 22: 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**:
  - 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:**
  - 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 centers 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 center to reduce latency.

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: https://www.5g-acia.org/publications/;

Use Cases: 5G Applied to industrial production systems

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).

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.

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.

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.

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

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.

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.

5G cloud-RAN (Section 2.10)

Use cases: Virtualized base station for 5G cloud-RAN

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.

Radio Specific requirements

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?**

1 Radio link is constrained to indoor (lab) premise.

- **Is Multicell required?**

(If YES, specify the required scope of the multicell arrangement. I.e. "building", "city", "global")

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.

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?**

URLLC requirements

- **Required Latency**

(specify if it is one way or roundtrip)

50 ms one way for Control Plane.

50 ms one way for User Plane.

- **Required Reliability**

(I.e 99,99999%)

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

- **Maximum tolerable jitter**

100ms

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)

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

Other requirements

- **UE power consumption**
    - **Rechargeable or primary battery?**

2 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.

Preliminary 6G use cases (Section 2.11)

Use cases: Hexa-X 6G based Use Cases

Potential Requirements

Figure 29: 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.

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 fulfillment 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.

Drones (Section 2.12)

Use case: Connectivity during crowded events use case, when drones are used (Section 2.12)

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 center 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 – possible consideration includes:

- Safe distance from spectators
- Approved Flight Plans
- Certified Drone operators
- Connectivity shall be provided in a secure manner
- Approved Flight Plans of tethered Drones

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.

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	1 m

Use case: An innovative fire detection pilot solution using 5G, Artificial Intelligence and drone technology (Section 2.12)

Potential Requirements

- *Functional requirements*
- *Non-functional requirements – possible consideration includes*:
  - Flexibility
  - Scalability
  - Interoperability
  - Reliability
  - Safety
  - Security and privacy
  - Trust

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).

Radio Specific requirements

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+ kilometer 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 enrolls 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 sys- tem. 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:

4. *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.*
5. *Air Traffic Control (ATC) Relay Communication:-Communication between the air traffic control system and UAV operator via ATC relay.*
6. *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 8 *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 15: 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

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 9** introduces the UAV payload communication requirements.

Table 10 introduces the communication requirements from Drone based applications.

Table 16: 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 17: 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

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-Takeoff 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 center and from the pilots. The pilots and the operations center, 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 center. 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

4.2 Emerging topics

The following emerging topics that are related to IoT & edge computing and 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.

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[66] (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)

[66] 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 21 provides 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:

Rui Aguiar (University of Aveiro)
Arne J. Berre (Sintef)
Gianmarco Baldini (EC JRC)
David Boswarthick (ETSI)
Marco Carugi (Huawei)
Agnia Codreanu (BEIA)
Nikos Giannakakos (UniSystems)
Damir Filipovic (AIOTI Secretary General)
Christophe Gossard (John Deere)
Tomas Gustavsson (Primekey)
Asbjørn Hovstø (Hafenstrom)
Jose Luis Hernandez (EC JRC)
Georgios Karagiannis (Huawei)
Vasileios Karagiannis (Austrian Institute of Technology - AIT)
Thomas Klein (IBM)
Christian Kloch (Force Technology)
Zbigniew Kopertowski (Orange)
Antonio Kung (Trialog)
Konstantinos Loupos (INLECOM)
Sean McGrath (University of Limerick)
Maria Niculae (BEIA)
Toon Norp (TNO)
Joao Peixoto (Ubiwhere)
Ranga Rao Venkatesha Prasad (Technical University Delft)
Mari-Anais Sachian (BEIA)
Natalie Samovich (Enercoutim)
Jaume Segura (Universitat de València)
Erwin Schoitsch (Austrian Institute of Technology - AIT)
Antonio Skarmeta (University of Murcia)
Flemming Sveen (Hafenstrom)
George Suciu (BEIA)
Giacomo Tavola (Politecnico di Milano)
Ricardo Vitorino (Ubiwhere)

Acknowledgements

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT and Edge Computing Innovation in Europe, bringing together small and large companies, academia, policy makers and end-users and representatives of society in an end-to-end approach. We work with partners in a global context. We strive to leverage, share and promote best practices in the IoT and Edge Computing ecosystems, be a one-stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT and Edge Computing Innovation in society. AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT and Edge Computing ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies.