Alliance for Internet of Things Innovation

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

Release 1.0

AIOTI WG Standardisation

7 September 2021

Executive Summary

This report highlights several IoT vertical domain use cases collected by the Alliance for Internet of Things 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.

Table of Contents

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.

[1] Networld2020 ETP has been renamed to NetwolrdEurope 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

2.1.1 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).

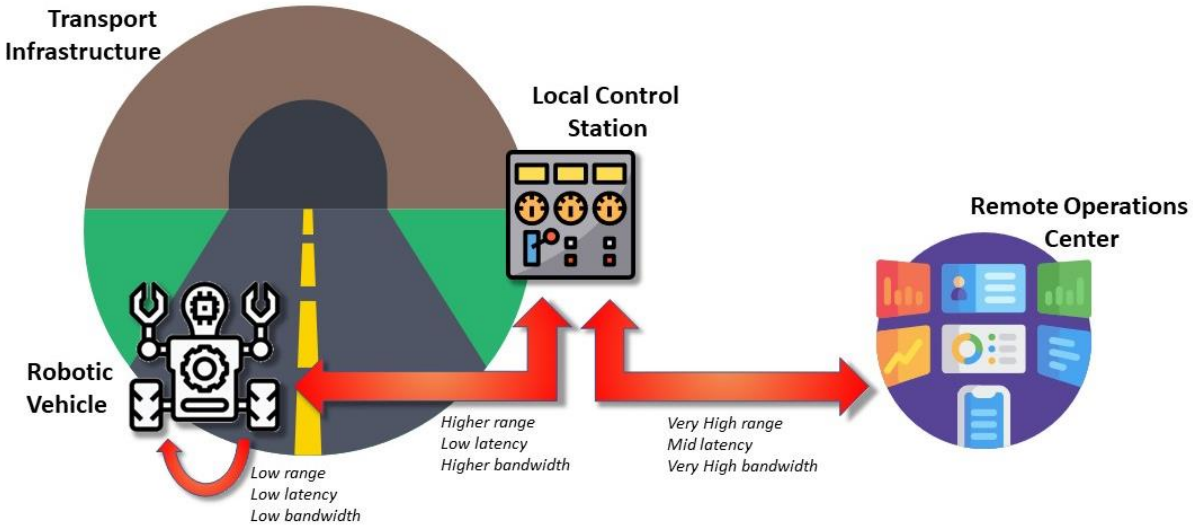
2.1.1.7 Alternative Flow

- 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 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?**
  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 center where data are processed. When P-waves are identified, an earthquake warning is emitted to warning broadcasting users.

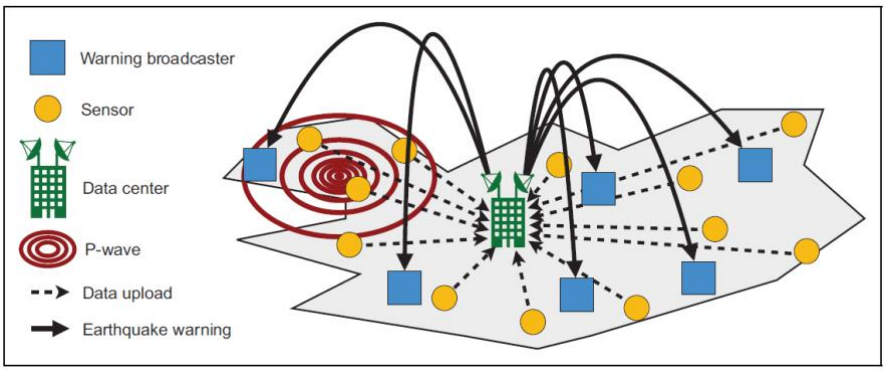


Figure 1: Use case in GeoSciFramework: Early Earthquake Warning (EEW) system.

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 neighboring 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)

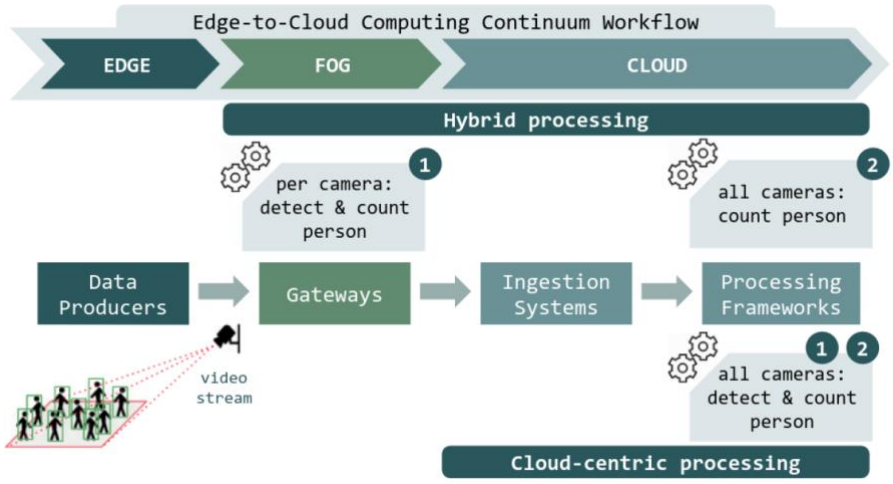


Figure 2: Use case in E2Clab: Smart Surveillance system.

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 lives (near) a critical infrastructure and needs to be protected or informed about potential risk that could affect their lives.
- **Governmental bodies**. Stakeholders required to organize the society and provide insights at higher level.
- **Civil Protection Organization**. Stakeholders dedicated to mobilizing and organize the citizens in emergency situations.

2.2.1.4 Triggers

GeoSciFramework project

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

Overflow project

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

Urbauramon project

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

2.2.1.5 Potential Requirements

Functional Requirements

GeoSciFramework project

- Real-time communication in case of emergency.
- Reliable communication between the stakeholders.
- Scalable communication to interconnect different critical infrastructures.
- Standard-based communication between critical infrastructures to align emergency information exchange.
- Requirements for data processing: Streaming of geodynamic data from sensors using specific tools, 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.

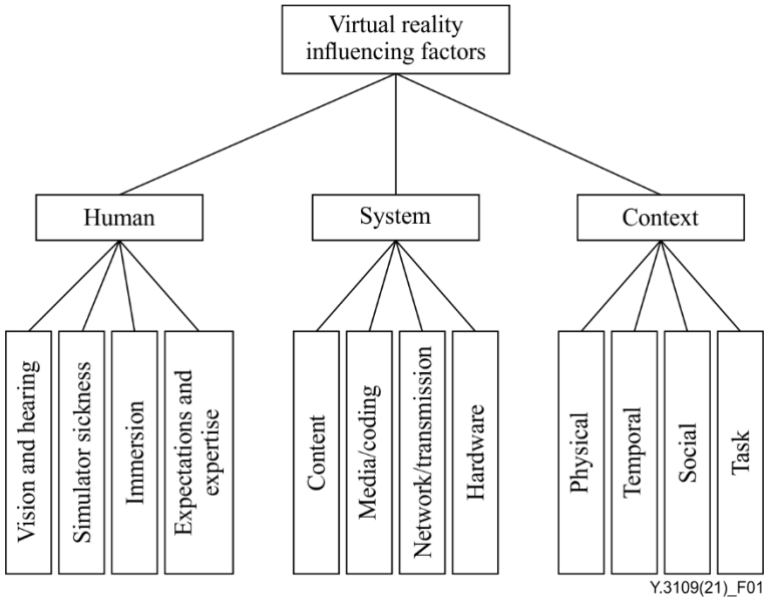


Figure 3: Virtual reality QoE-influencing factor categories, copied from **[ITU-T G.1035]**

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.

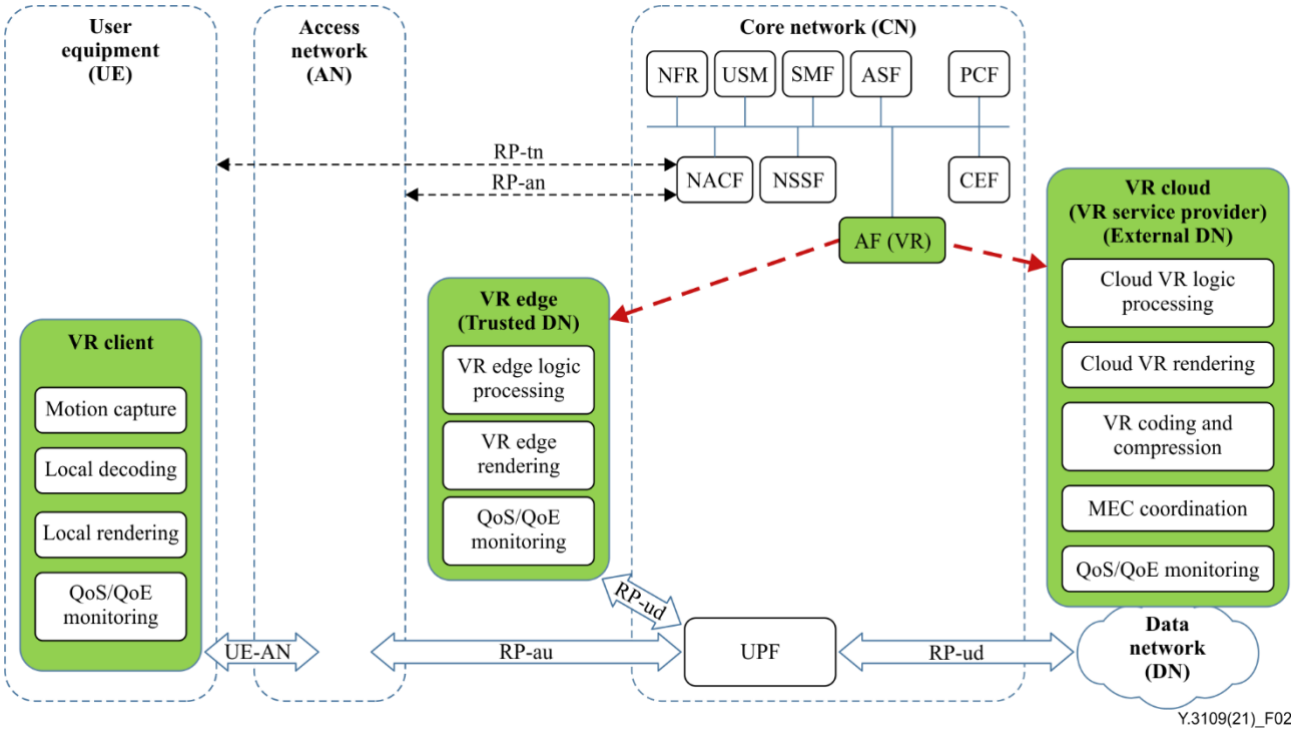


Figure 4: A conceptual architecture of the VR service framework, copied from [ITU-T SG13 Y.3109]

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].

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.

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

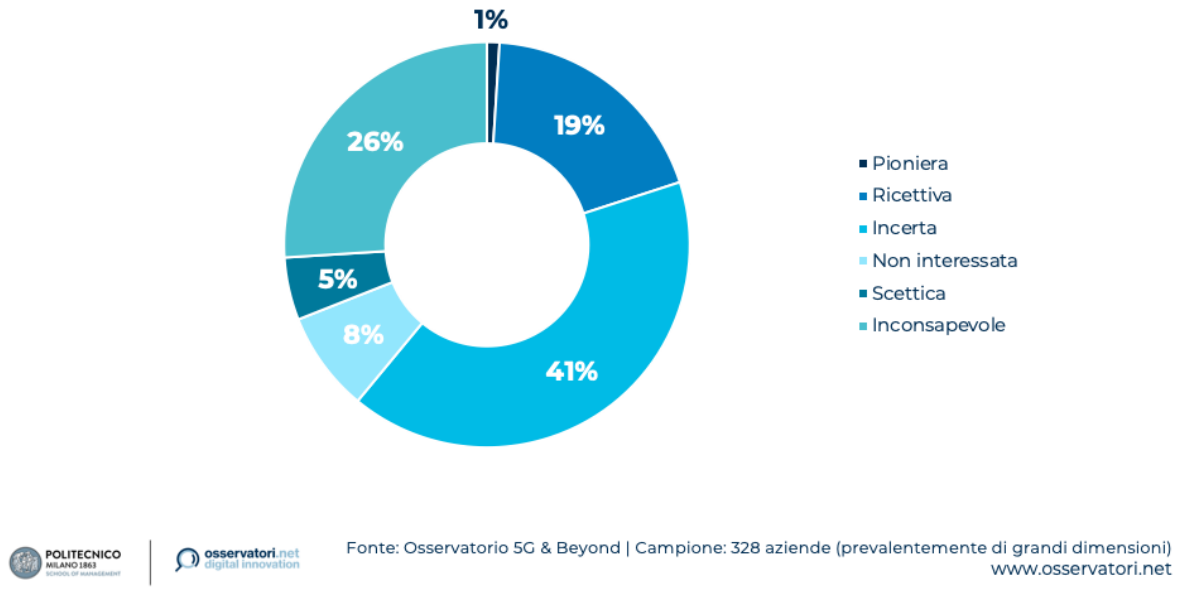


Figure 5: Potential Italian utilizer companies attitude towards 5G

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

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

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

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

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

Key advantages from the 5G technology are:

- Wireless connection of sensors at high speed, low latency of the data transmission. This can support hard real time application or massive data transmission.
- Availability of the Edge Computing platform (MEC) for fast processing close to the plant premises.

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

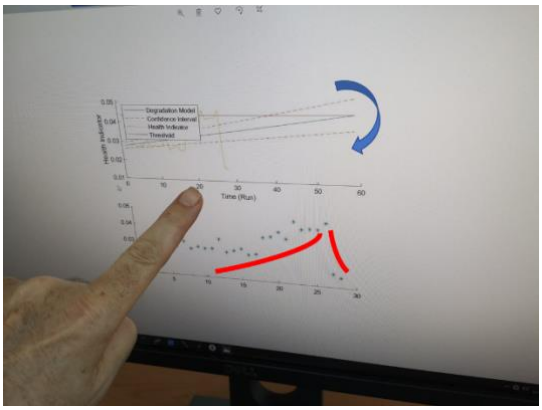
Use case is structured in two distinct flows, both of them leveraging 5G data transmission from sensors to backend and MEC functionalities.

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



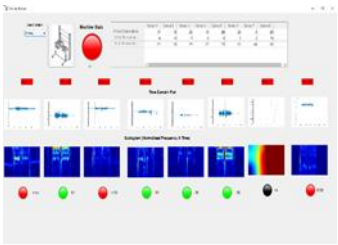
2. Self-Reconfigurable and Adaptive Production:

a. Data collected from the field and conveyed via 5G infrastructure are validated, features extracted and support creation/refinement of a CNN (Convulational 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

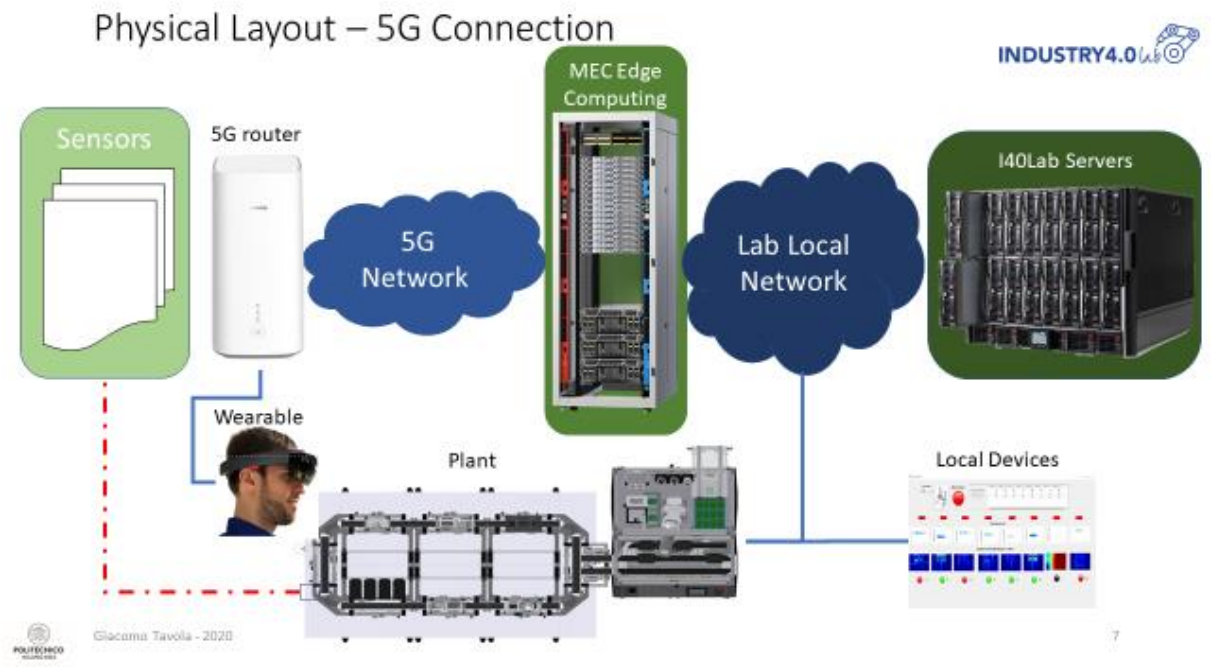


Figure 6: Physical Layout – 5G Connection

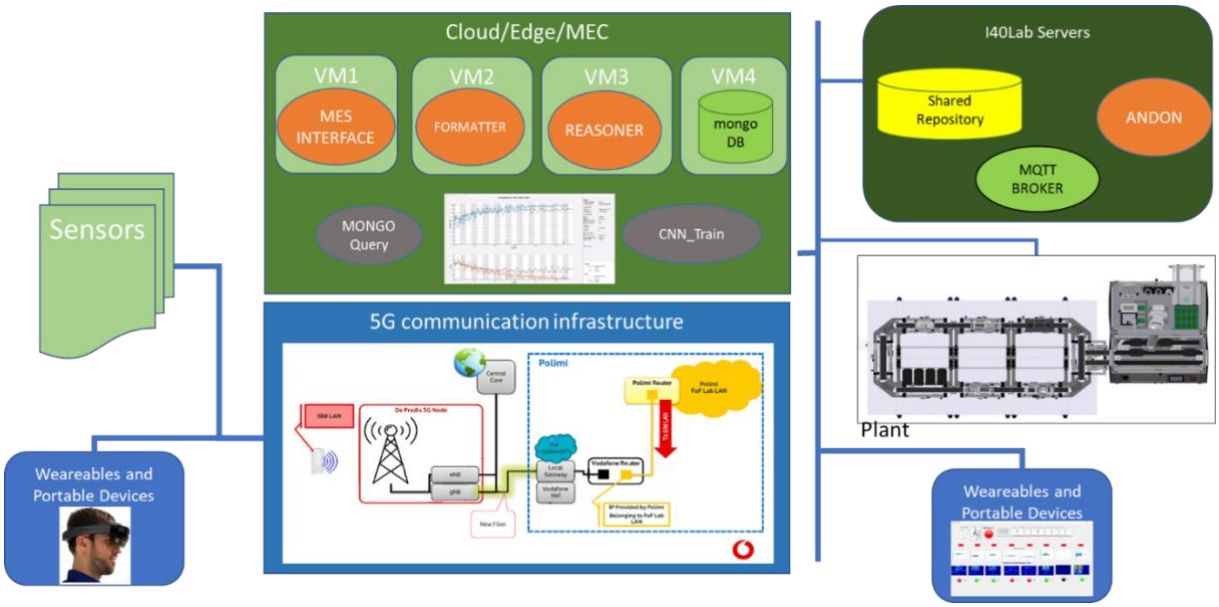


Figure 7: Network & Application Architecture

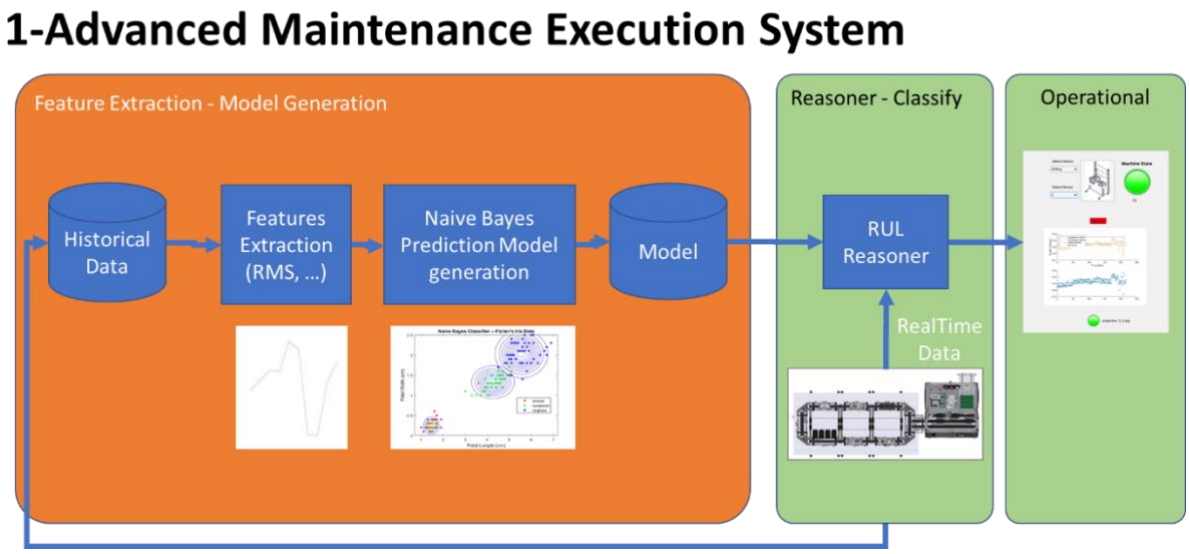


Figure 8: Advanced Maintenance Scenario

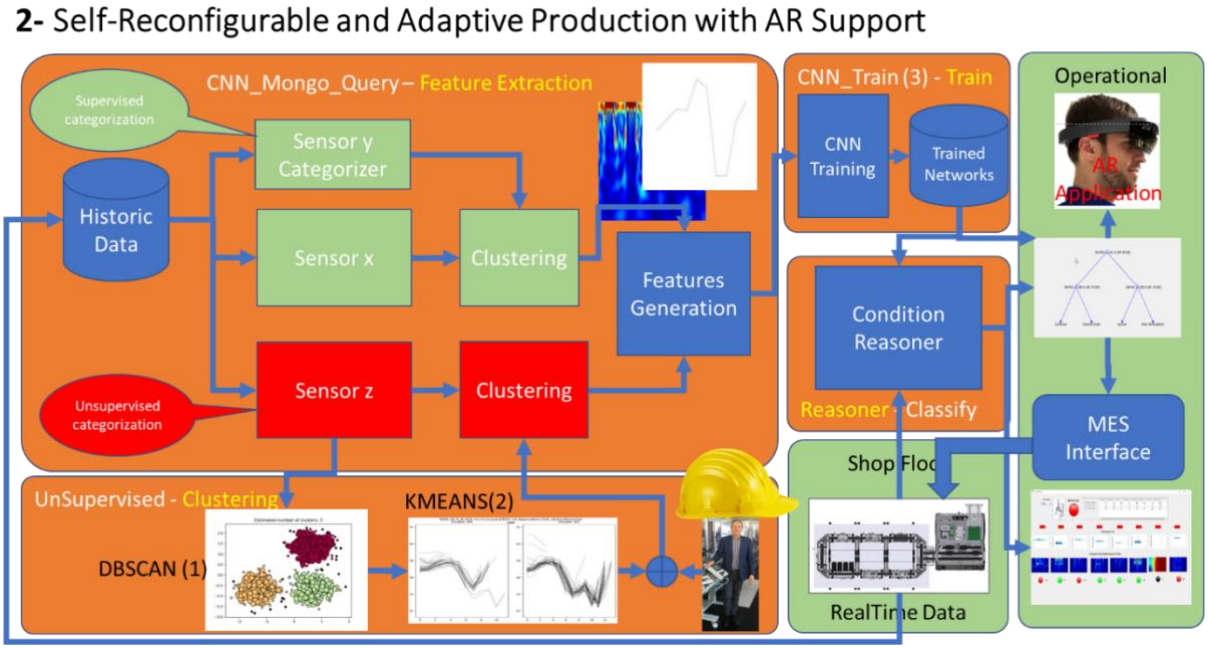


Figure 9: Condition Management and AR Support Scenario

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.

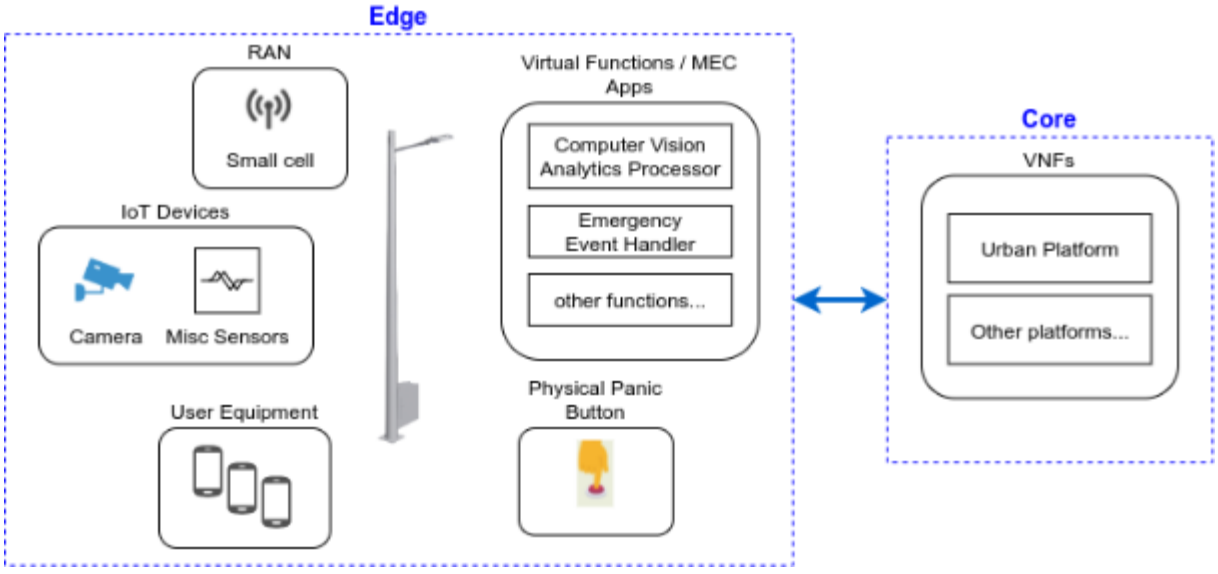
2.4.1.7 2.4.1.7 Alternative Flow

- None

2.4.1.8 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

2.5 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:

- 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?

2.6 Critical Infrastructure support applications

2.6.1 Smart Infrastructure Monitoring

2.6.1.1 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.

2.6.1.2 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/)

2.6.1.3 Roles and Actors

- Security management personnel of infrastructures
- Operations management
- CERT/CSIRT teams (emergency response)

2.6.1.4 Pre-conditions

- Monitoring of infrastructures requiring high connectivity of hundreds of IoT devices.
- Relatively low latency connectivity applications supporting infrastructure monitoring and sensing devices

2.6.1.5 Triggers

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

2.6.1.6 Normal Flow

- Data from hundreds of IoT devices reaching central control operations.
- Close to real-time connectivity and data assimilation of sensing devices

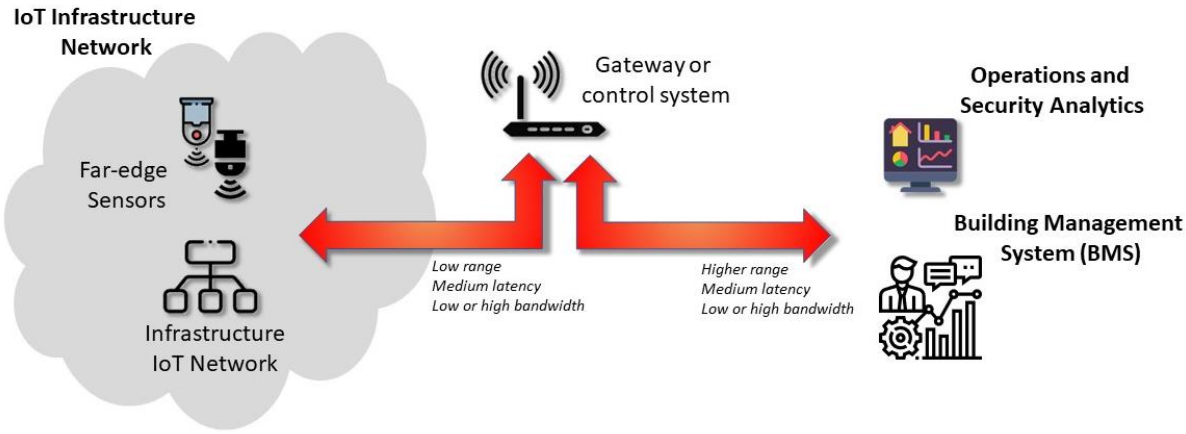
2.6.1.7 Alternative Flow

- None

2.6.1.8 Post-conditions

- Data analytics, almost real-time alerting, data communications
- Actuation decisions
- Security analysis and decision making

2.6.1.9 High Level Illustration



2.6.1.10 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.

2.6.1.11 Radio Specific requirements

2.6.1.11.1 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.

2.6.1.11.2 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

2.7 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 10 (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.

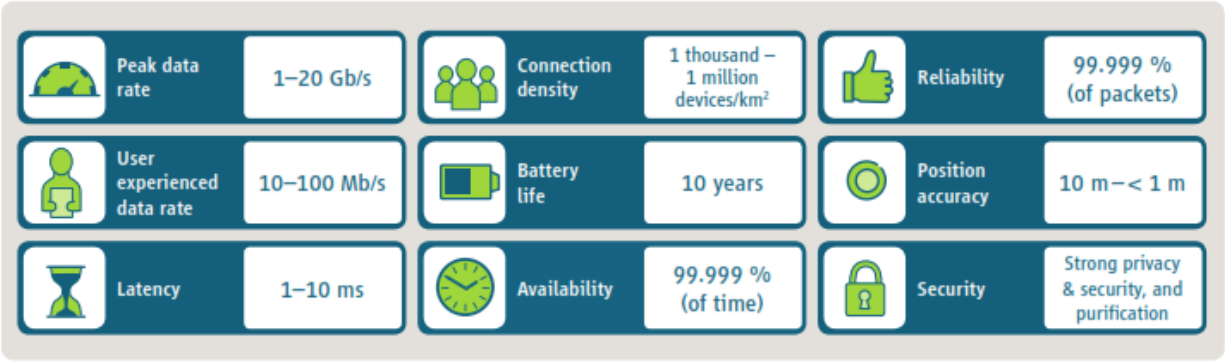


Figure 10: Selected target key performance indicators of 5G according to ITU-R (cf. [ITU-R M.2410-0])

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.

2.7.1 Factory of Future Use Cases

2.7.1.1 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 11 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.

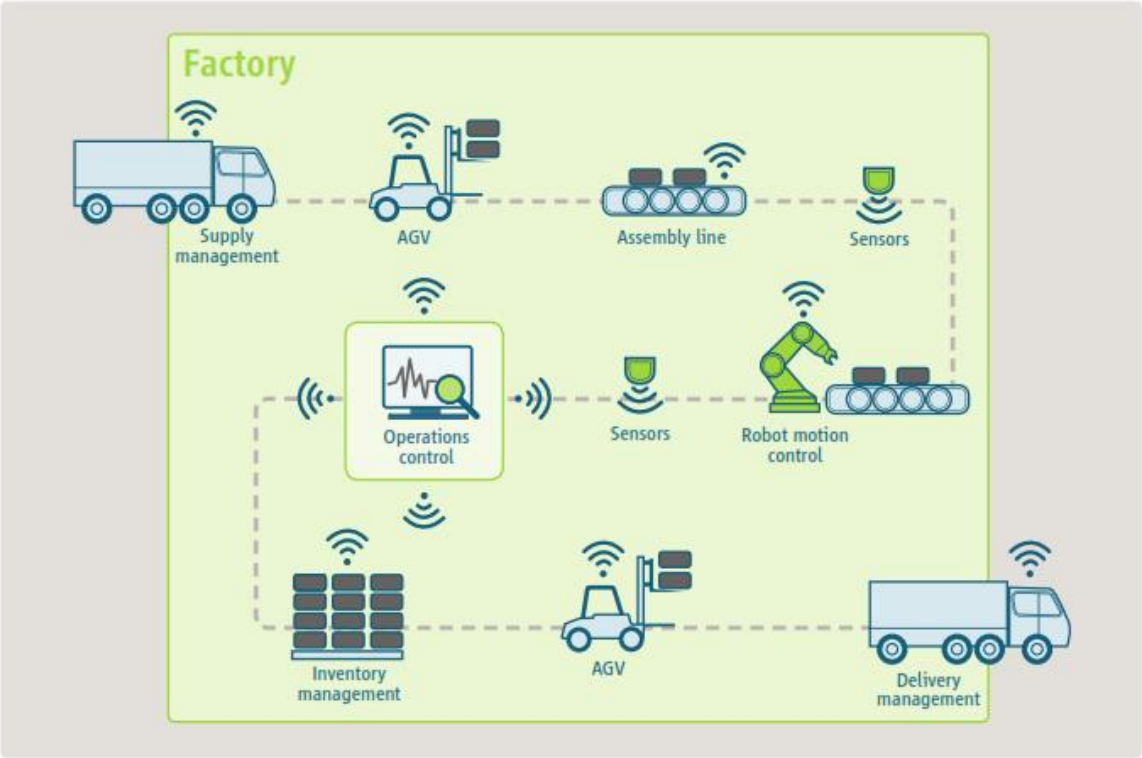


Figure 11: Exemplary application areas of 5G in the factory of the future

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 12, 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).

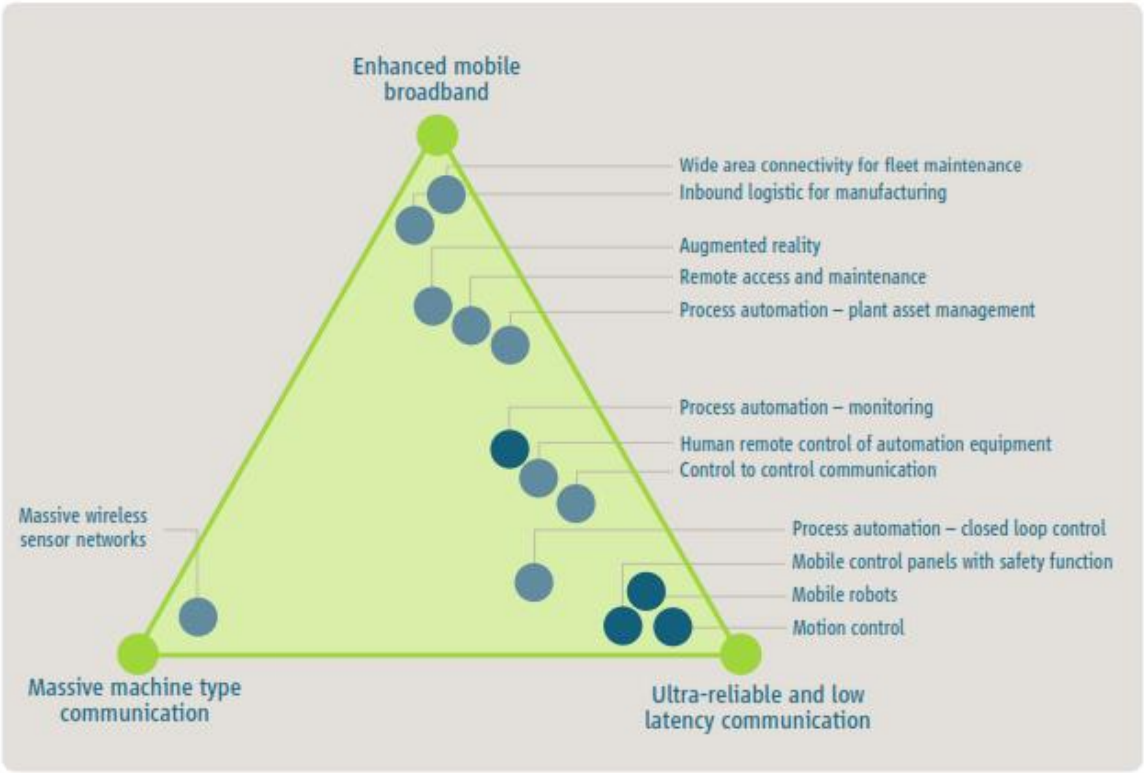


Figure 12: Overview of selected industrial use cases and arrangement according to their basic service requirements

2.7.1.2 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

2.7.1.3 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 13.

- 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.

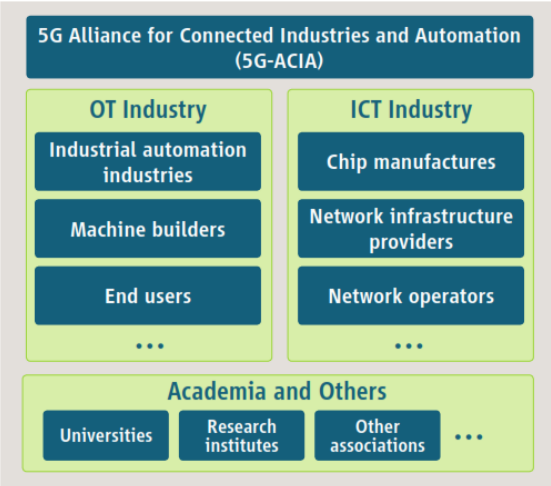


Figure 13: Overview of selected main stakeholder groups participating in 5G-ACIA

2.7.1.4 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.

2.7.1.5 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.

2.7.1.6 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 15. 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.

2.7.1.7 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.

2.7.1.8 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 14 shows the roadmap for the 3GPP standardization of Releases 16, 17 and 18 (Source: Puneet Jain, 3GPP Working Group Chair SA2)

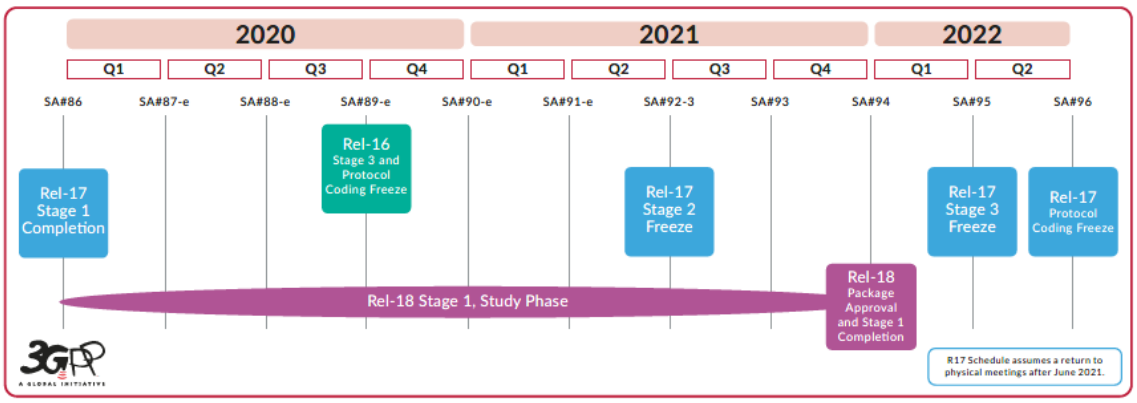


Figure 14: Overview of selected main stakeholder groups participating in 5G-ACIA

2.7.1.9 High Level Illustration

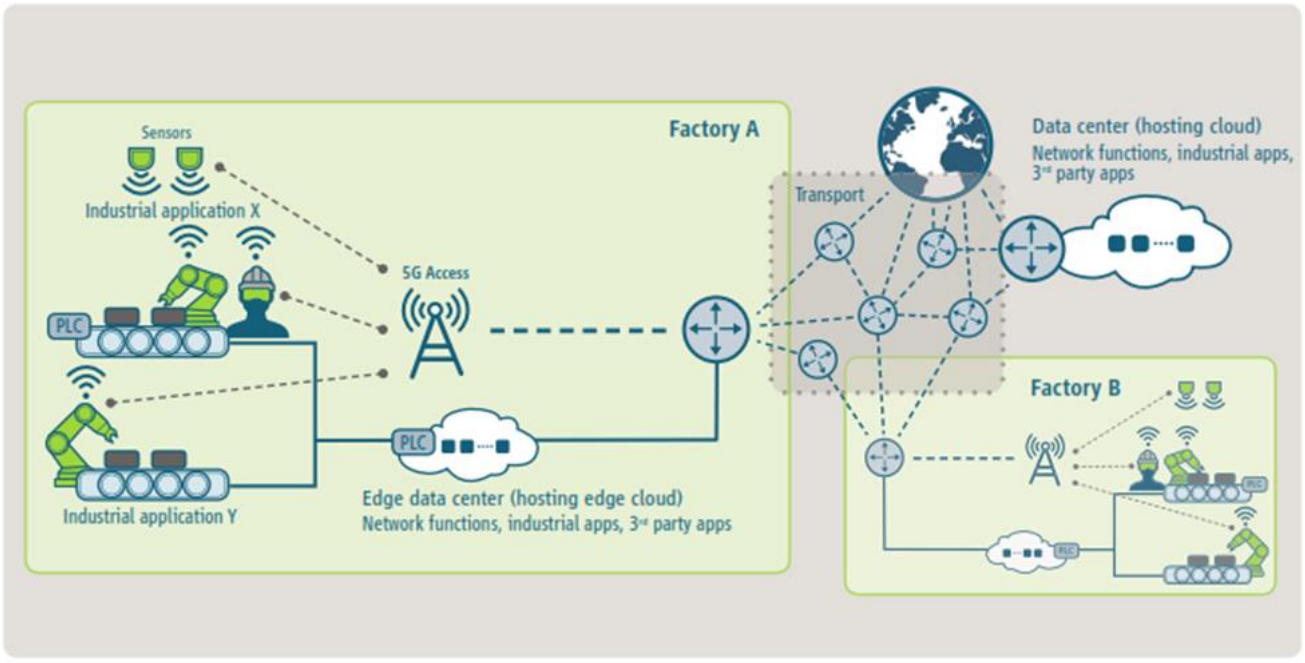


Figure 15: 5G-enabled smart factory scenario

2.7.1.10 Potential Requirements

Functional Requirements

Certain more detailed performance requirements of selected factory / process automation use cases (those indicated with a blue circle in Figure 12) are provided in Table 3 (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 3: 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 10 with those in Table 3 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 analyzes. 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 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.

2.7.1.11 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/;

2.7.2 5G Applied to industrial production systems

2.7.2.1 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.

2.7.2.2 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

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

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

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

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.

2.7.2.4 Pre-conditions

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

2.7.2.5 Triggers

Most of the use cases under exploration require constant dataflow, in order to detect patterns in sensor data behavior. 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.

2.7.2.6 Normal Flow

Commonly, the steps are the follows:

1. Critical infrastructure systems (IoT systems, MES, informational systems): machine data (production counters, condition monitoring sensors data) is permanently being collected.
2. 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.

3. 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.

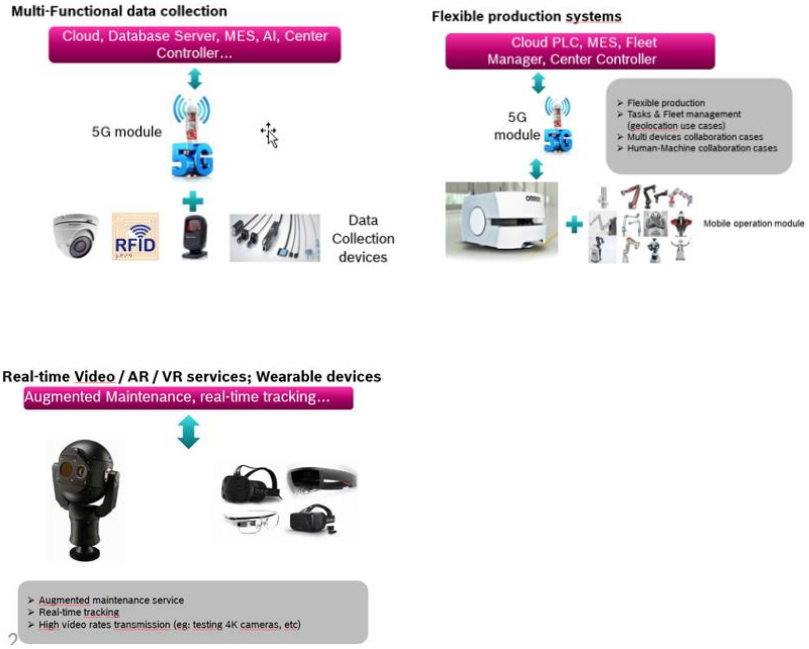
2.7.2.7 Alternative Flow

2.7.2.8 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.

2.7.2.9 High Level Illustration

There are three basic scenarios:



2.7.2.10 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).

2.7.2.11 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.

2.7.2.11.1 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.

2.7.2.11.2 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.

2.7.2.11.3 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

2.7.2.11.4 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.

2.7.2.11.5 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.

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.

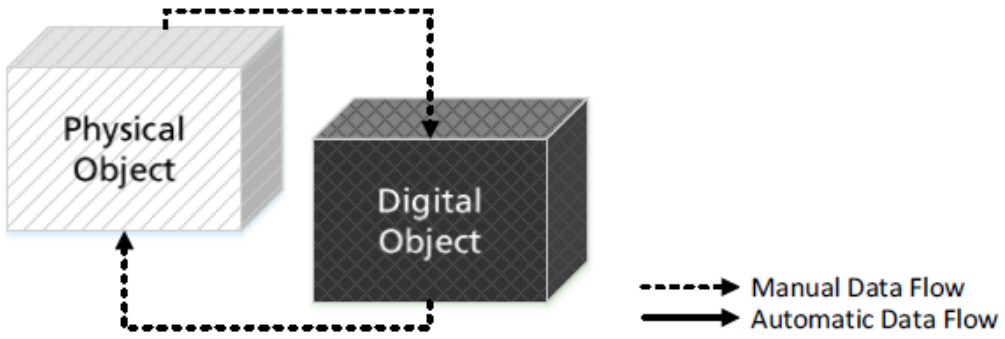


Figure 16: Data Flow in a Digital Model

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.

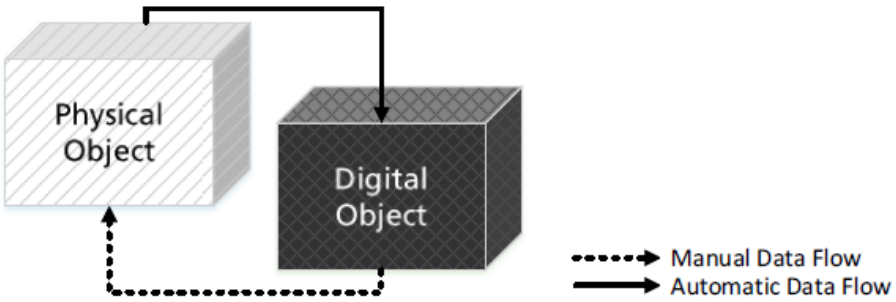


Figure 17: Data Flow in a Digital Shadow

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.

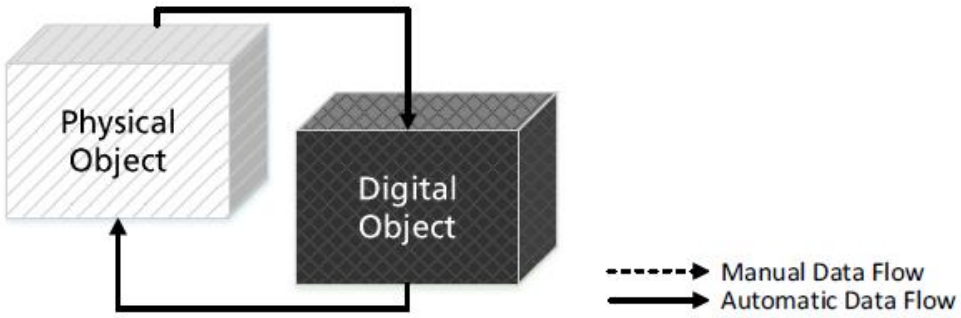


Figure 18: Flow in a Digital Twin

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 19, see [GaRo12].

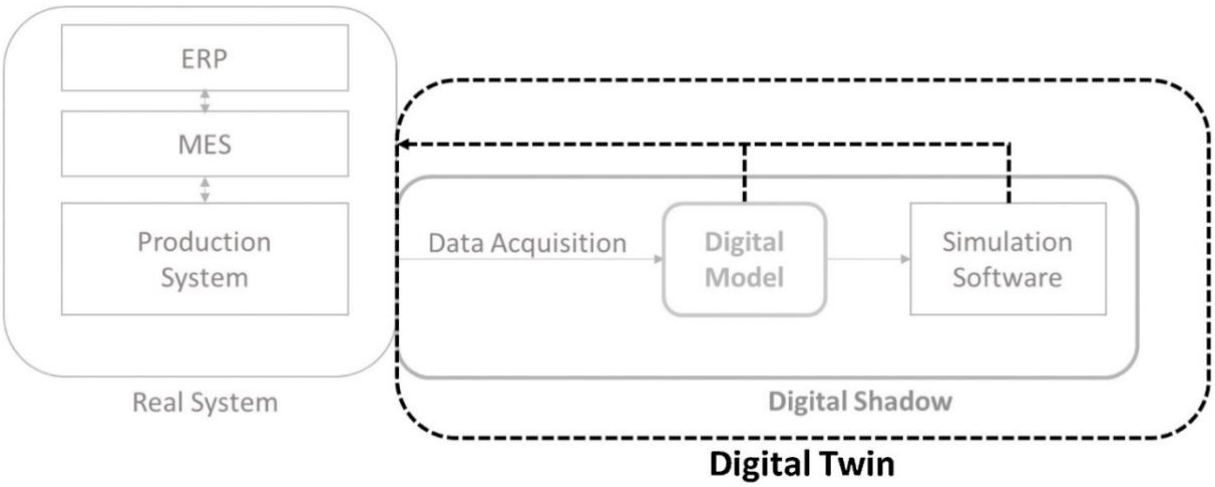


Figure 19: Digital Twin (DT) schema, copied from [GaRo12].

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.

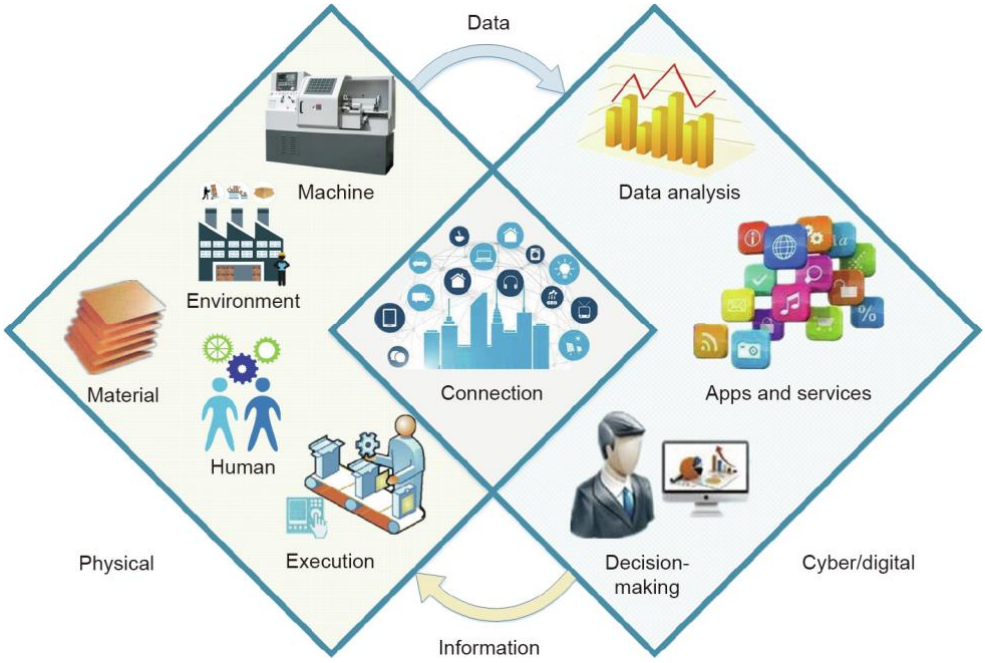


Figure 20: Mapping between physical and cyber/digital worlds, copied from [KrKa18]

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 4 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 4: 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].

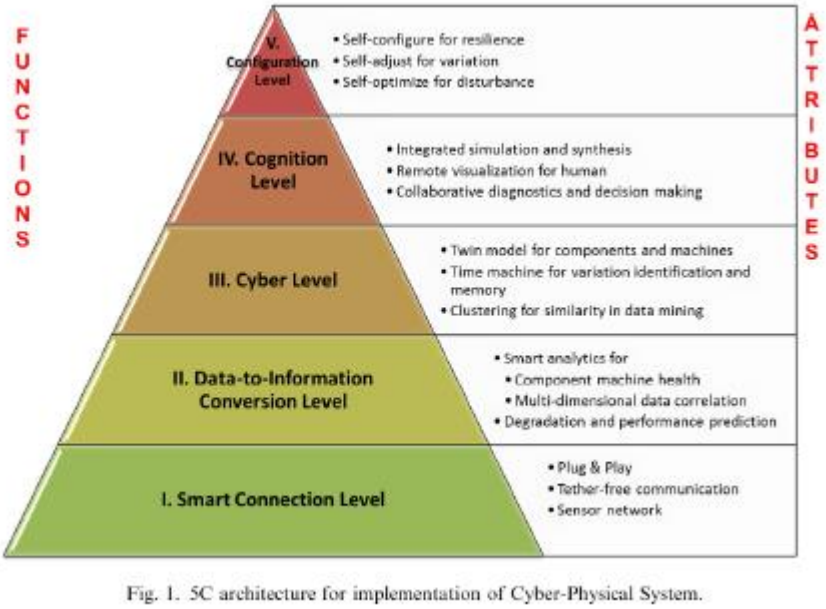


Fig. 1. 5C architecture for implementation of Cyber-Physical System.

Figure 21: 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].

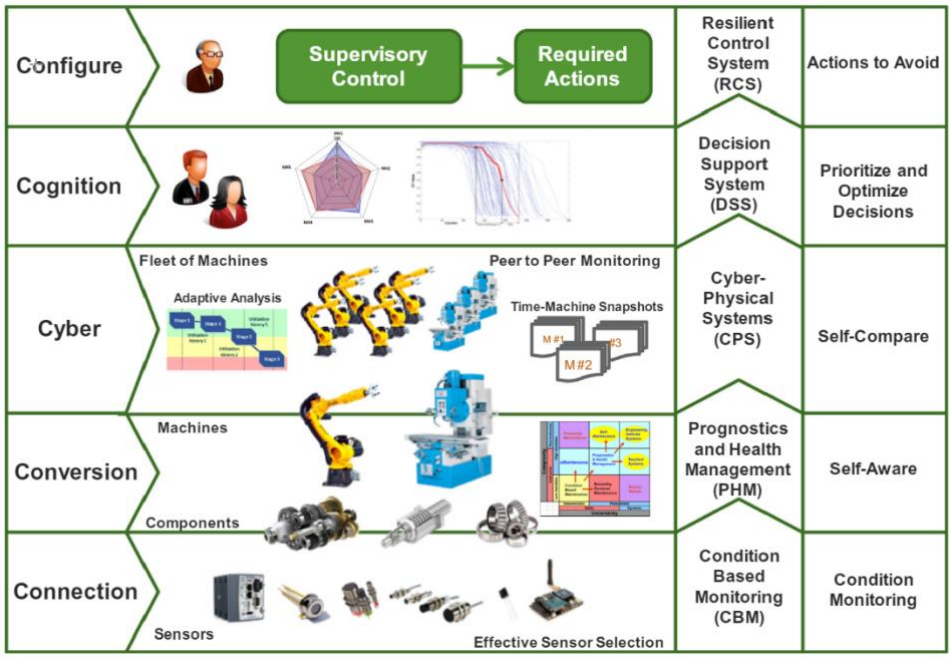


Figure 22: Applications and techniques associated with each level of the SC architecture, copied from [CiNe19]

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.

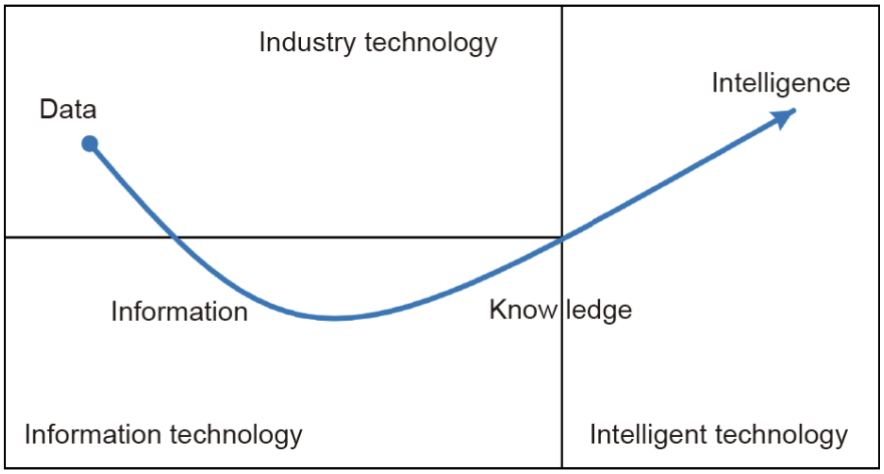


Figure 23: Integration of industrial technology, information technology, and intelligent, copied from [KrKa18]

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 Millimeter 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].

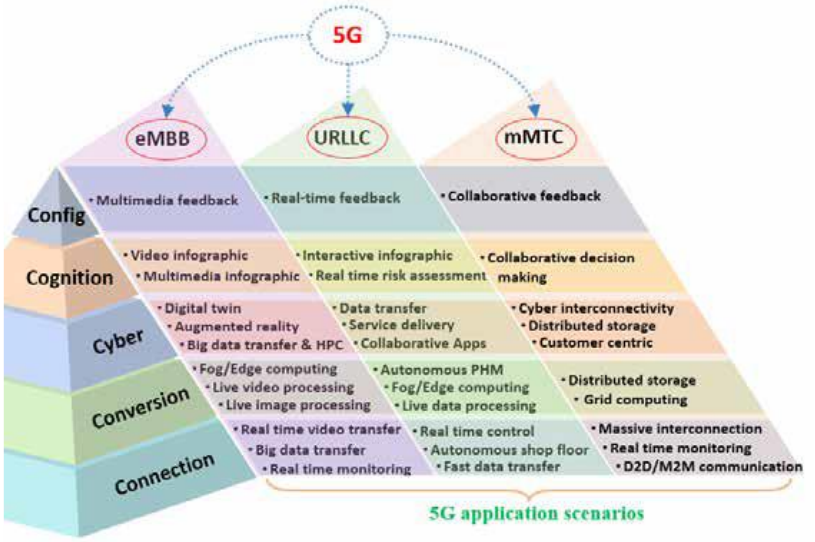


Figure 24: Application Scenarios, copied from [JML20]

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

This section is related to the Networld2020[9] SNS SRIA [Networld2020-SRIA] and focuses on challenges of the integration of deep edge, terminal and IoT devices in the SNS architecture.

Architecturally, the 'deep edge' with its IoT as well as end user or vertical industry devices is becoming part of the common resource pool, provided as a non-decomposable set of resources by some edge entity, such as an end user, industrial site owner, or a building owner. It is envisioned that tenant-specific resource usage to expand into the deep edge with the same control and data plane considerations and resource management considerations, applying to all those resources. In other words, in principle, we see aspects of controllability of those edge resources to equally apply together with the general programmability for the realization of compute tasks as well as for data and forwarding plane operations through those resources.

However, some edge resources might not directly fit into this vision. For instance, IoT will introduce particular, service-dedicated, possibly intelligent yet resource-constrained components (micro-electronics, battery driven components), which will need a particular consideration for the integration with the rest of the system. Indeed, such IoT components and devices might impose additional requirements on, e.g., volatility and longevity, punctual presence at any moment, persistence, generality, capacities, connectivity, interfaces and APIs from/towards the system. Hence, they might not support direct integration and require particular solutions instead (e.g., gateways or subsystems).

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,

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

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

- **Network Congestion**
  With a culminated capacity of the last mile exceeding the capacity of the core network by two orders of magnitude the core is becoming a bottleneck for huge amounts of data to be transferred to the cloud data centers while at the edge there is sufficient capacity available.[11]

- **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[12].

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[13], LF Edge[14], Open Edge Computing[15] or OpenStack[16] (just to name a few).

Developers will also have to deal with different levels of edge computing complexity. One dimension of complexity is the edge-awareness of the application. In the case of edge-unaware applications,

[10] See https://en.wikipedia.org/wiki/Narrowband_IoT
[11] 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)
[12] See e.g. https://ieeexplore.ieee.org/document/9430853
[13] https://forge.etsi.org/rep/mec
[14] https://www.lfedge.org/
[15] https://www.openedgecomputing.org/
[16] https://www.openstack.org/use-cases/edge-computing/

developers do not have to deal with the edge specifics and the network is responsible to handle client requests transparently in a manner that those are handled by the server instance with optimum network proximity (just like in today's CDNs). On the other hand, edge-aware applications will have to make use of the available edge-resources by exploiting the specific APIs that are exposed by the edge implementation.

A second dimension of complexity is mobility. When the device is mobile, this is uncritical as long as the edge application is running on the device itself ('device edge'). But if for example the processing is done at the base station ('far edge'), the application context needs to be moved from one base station to another as the user is moving through the mobile network. If roaming between different MNOs comes into play, things even get more complex.

As a side effect, to not send data to a central cloud can be seen as a gain in privacy. However, this presupposes that data security is guaranteed in the edge. This, in turn, is not a trivial task, because the attack surface increases enormously and the remote management of the high number of edge devices is a challenge and requires new methods and standards.

Availability can be another benefit of edge computing. Given the edge applications are programmed accordingly they can provide business continuity in situations of loss of network connectivity or downtimes (planned or unplanned) of the cloud data center.

While edge computing will certainly support the goals of the digital transition, we should not forget about the other side of the medal: sustainability and the green transition. On the positive side of the energy equation, edge computing reduces energy-hungry data transfers. On the downside, the intelligence and processing power required at the edge comes at a (energy) cost. Research should be undertaken on how the net carbon footprint of edge computing could be minimized. When the device is energy constrained (e.g. battery driven) other options like energy harvesting could be taken into consideration.

As the talks and discussions in the workshop *IoT and Edge Computing: Future directions for Europe*[17] have shown edge computing is expected to be the first evolutionary step towards a 'computing continuum' reaching from the cloud data center to the edge device. Cloud federation as investigated by the European Gaia-X project[18] 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."[19]

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.

[17] 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/
[18] https://www.gaia-x.eu/
[19] http://www.pledger-project.eu/FederatedCloud_RA_PP_022021.pdf

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[20], 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".

[20] 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

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[21], but with this vision, the concept goes beyond the network functional splitting and can be applied to other fields.
In Noriega et al.[22] and Pastor et al.[23], 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.[24], 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)). In Fayos et al.[25], 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[26] and El Khafhali et al.[27], the authors focus the efforts in the modelling and provision of the task distribution in the Cloud. In Lopez et al.[28], 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

[21] 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.
[22] 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.
[23] 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.
[24] 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.
[25] 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
[26] 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.
[27] 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.
[28] 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.

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.).

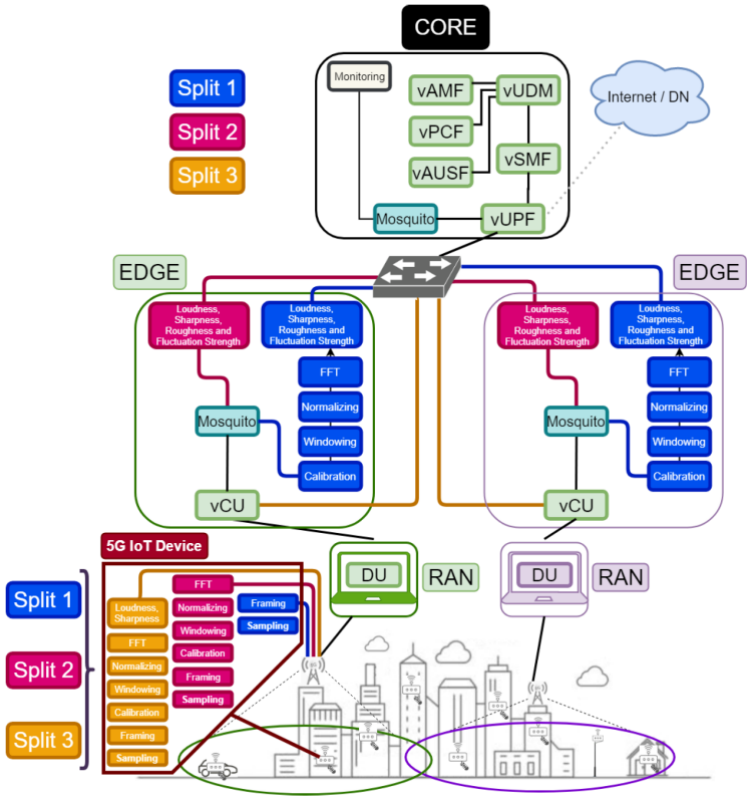


Figure 25: Conceptual diagram of the IoT architecture with different splitting options for the 5G complex metrics calculation system[5].

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 25 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[29], 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 26 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).

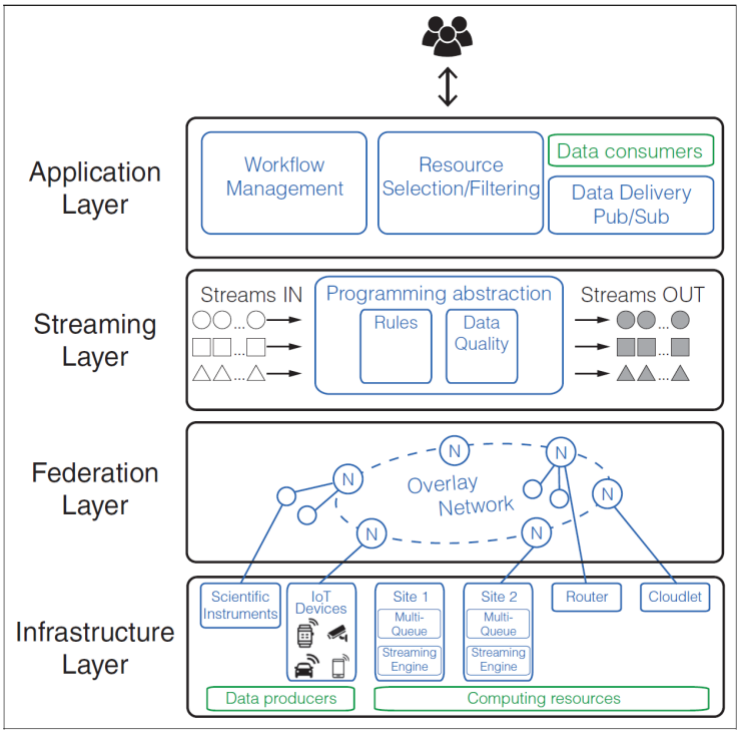


Figure 26: Overall layered architecture of the edge-based data-intensive IoT system.

[29] 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[30][31] 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 edge and IoT

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*[32] 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 behavior 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" behavior to train a certain model (e.g., a neural network). Therefore, the identification of potential actions that are not considered as normal behavior could be used to infer an attack or threat. In 2019, the Manufacturer Usage Description (MUD)[33] was standardized in the scope of the IETF for the definition of network behavior 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 behavior of their devices. Such behavioral 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 behavior. 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[34] in home and small-business networks[35].

[30] 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.
[31] 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)
[32] https://ec.europa.eu/digital-single-market/en/news/building-ecosystem-where-iot-edge-and-cloud-converge-towards-computing-continuum
[33] E. Lear, D. Romascanu, and R. Droms, "Manufacturer Usage Description Specification (RFC 8520),", 2019
[34] T. Polk, M. Souppaya, and W. C. Barker, "Mitigating IoT-Based Automated Distributed Threats,", 2017
[35] NIST, "Securing Small-Business and Home Internet of Things Devices:NIST SP 1800-15," 2019

One of the main potential applications derived from the MUD standard is the development of IDS (Intrusion Detection System) to be considered in IoT scenarios. Indeed, such approach has been considered in recent research activities[36]. 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 analyzed 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[37]. 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[38]. 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[39]. 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[40], which

[36] 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

[37] 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.

[38] 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.

[39] 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).

[40] 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.

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 27.

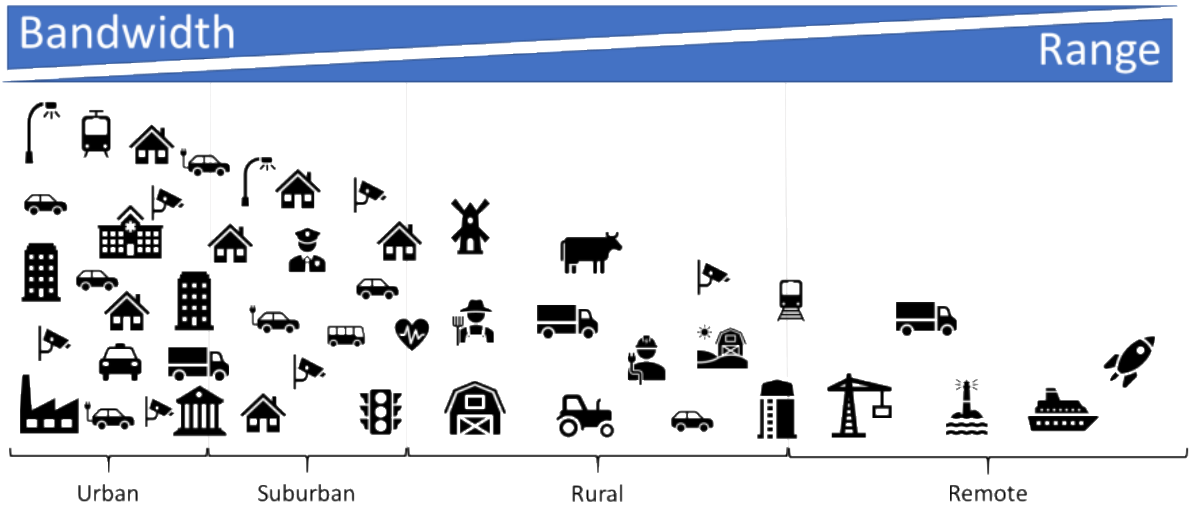


Figure 27: 5G/Satellite Coverage

Traditional Mobile Sat Systems (MSS) like Inmarsat, Thuraya, Iridium, Globalstar have been dominant in the M2M/IoT market, using their L-band spectrum with a focus on mobile and maritime applications. In the last 10 years they realised 3.5 - 4 million satellite IoT terminals in the field. With the availability of Ku-band and Ka-band satellite connections provides higher through-put to meet the demand on of the IoT sector such as fixed satellite systems like Eutelsat, Intelsat or Asiasat. Their higher bandwidths provide backhaul services connecting terrestrial local area IoT networks (e.g., NB-IoT, Lora, Wifi, BT) from high density sensor networks to the internet, see [Satell-market].

New satellite players take advantage of the new cubesat technology (using a range of UHF, VHF, S-band, and Ku-band services) to bring down their service costs, while the Low Earth Orbit allows the use of low power modems to connect the ground sensors, see [KoLa20].

Nanosatellites are defined as any satellite weighting less than 10 kilograms. They all are based on the standard CubeSat unit, namely a cube-shaped structure measuring 10x10x10 cm with a mass of somewhere between 1 kg and 1.33 kg. This unit is known as 1U. As the number Internet of Things (IoT) devices and Machine-to-Machine (M2M) communications increases at an exponential right rate. No communications system can provide end to end connectivity and satellite systems create the opportunity to provide extended coverage, see [NASA-cubesats].

Companies such as Astrocast, Myrioata, Lacuna, Kineis, Kepler Communications, Swarm technologies and Hiber provide service features, low cost, low power, low latency, makes them well suited for Direct-To-Satellite services.

For satellite systems to integrate with 5G networks the architecture will need to address a number of specific issues namely, see e.g., [ISTINCT]:

- Diversification of the spectrum usage across multiple technologies
- Edge networks to reduce the impact of the backhaul in the end-to-end system
- Adapted data path protocols to massive communication environments
- Application protocols adaptation through the virtualization environment
- Addressing the M2M communication needs in an efficient manner
- Participation within the main standardization organizations: 3GPP, ETSI NFV,ETSI MEC, IETF, ONF

3.5.1 Satellite connectivity for global IoT coverage.

Today, there are 1.7 billion cellular IoT devices active worldwide. By 2026, there will be 5.9 billion according to Ericsson [Ericsson20], an increase of nearly 350%. Given this tremendous growth, it is clear that the ability to connect diverse IoT device types, with different needs, at massive scale and with global coverage, is urgently needed.

Mobile network coverage is mostly focused on areas with mid to high population density. Areas with low density of population are underserved because of the small or null return on investment required to cover such regions. Currently only 30% of the Earth's landmass, or 10% of the Earth surface has mobile network coverage.

IoT applications such as vehicle monitoring, asset tracking, agricultural sensors and infrastructure monitoring cannot be deployed or used where there is no terrestrial network. Therefore, benefits provided by IoT applications cannot currently be achieved in large portions of the Earth surface.

The capability of satellites to provide global coverage makes them an excellent choice to address the lack of coverage in low populated, isolated and remote areas. The combination of satellite communications together with 3GPP standards offer the possibility to integrate terrestrial and non-terrestrial networks in an easy and simple way.

There are already satellites today that offer global connectivity services for IoT but the communication protocols used are not standard, which requires the development of dedicated terminals, and are typically dedicated to specific vertical solutions. Also current satellite solutions do not integrate with existing IoT terrestrial networks and, finally, its cost does not meet the price points required for massive IoT deployment.

The market today is demanding standard solutions based on roaming, such as 5G, which are interoperable with terrestrial networks, avoid vendor chipset and service provider lock-in, benefit from massive scale deployment and chipset manufacturers diversity. These requirements provide the lowest cost solution on chipset and service costs, reduce dependencies on manufacturers and service providers and protect investments on sensors. Combining terrestrial and satellite networks under 5G makes it possible to ensure seamless connectivity using the best available network at any time, see Figure 28.

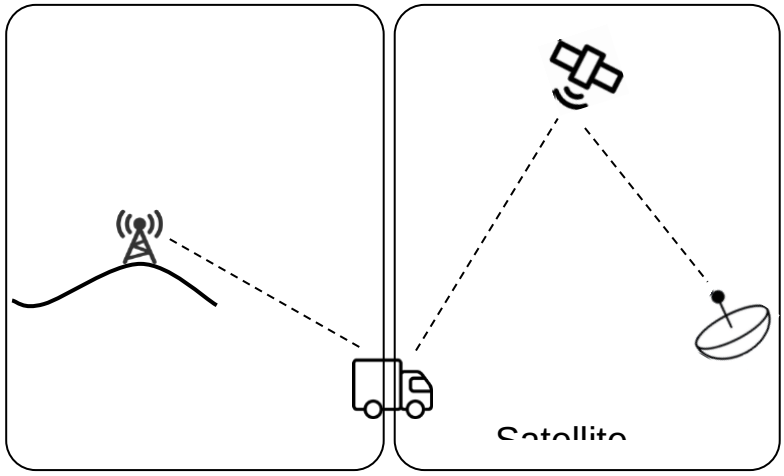


Figure 28: Integrated terrestrial and satellite IoT networks

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).

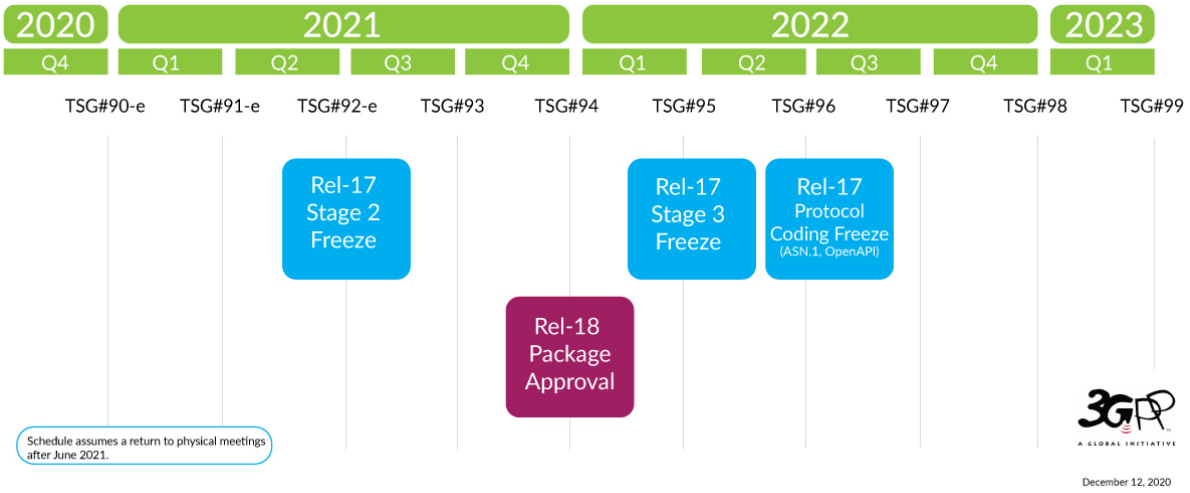


Figure 29: 3GPP Release 17 timeline, copied from 3GPP

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 29

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[41]. In this evolution, vehicles will be increasingly connected through different wireless standards like ITS

[41] 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.

G5 and LTE-V2X but they will also benefit by increasing level of automatism[42]. While, the possibility of having fully automated vehicles (level 5 of the J3016 standard)[43] 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[44]. There are considerable expectations for these new technologies and many studies and reports have identified a number of key benefits for the deployment of these technologies from the obvious and primary benefit to improve the safety conditions in the road to improvement in traffic management, improve compliance to regulation and so on.

The connectivity trend and the automated vehicle trend have evolved from different origins as the first (connectivity) trend is focused on providing connectivity to the vehicle for a variety of applications including safety while the second (automated vehicle) trend is focused on applying artificial intelligence to the processing and analysis of the data originating from the sensors to improve the awareness of the vehicle intelligence. 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[45].

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[46] 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)[47]. 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"[48]. The security (authentication and integrity) of V2X has been designed and described in ETSI and IEEE standards[49] 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).

---

[42] 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.
[43] SAE, S. (2014). J3016 standard: taxonomy and definitions for terms related to on-road motor vehicle automated driving systems.
[44] Yang, CY David, Kaan Ozbay, and Xuegang Ban. "Developments in connected and automated vehicles." (2017): 251-254.
[45] Tong, W., Hussain, A., Bo, W. X., & Maharjan, S. (2019). Artificial intelligence for vehicle-to-everything: A survey. IEEE Access, 7, 10823-10843.
[46] 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.
[47] 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.
[48] 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
[49] 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.

Beyond the technologies underlying these trends, we also investigate here the potential impacts (e.g., societal) and the potential applications of the combined connectivity and automated concepts, otherwise called CCAM (Cooperative, connected and automated mobility).

At the highest level of automation (level 5 in J3016), the concept of vehicles sharing have been proposed by various sources. In this concept, the vehicle is not owned and driven (for automation levels below 5) by a single proprietary but it can be shared among different users, thus leading to a new economy model where ownership is replaced by pay-by-use. The emergency of such sharing models can be applied not only to passenger's vehicles but also to commercial vehicles and to public transportation where the vehicles will be owned by the government. Such sharing models poses new challenges not only because they can be economically disruptive (businesses may disappear) but they can also generate great risks from a privacy and security point of view. From a privacy point of view, it is imperative that the data on the passengers is not disclosed or accessible to un-authorized party. From a security point of view, it is necessary that shared automated vehicles cannot be compromised and used for criminal activities[50]. The recent terrorist attacks where commercial vehicle were used to kill pedestrians[51] 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[52]. 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

[50] 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.
[51] https://www.history.com/this-day-in-history/2016-nice-terrorist-attacks
[52] 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.

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[53].

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.

[53] 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.

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 [54] and the US Executive Order on Improving the Nation's Cybersecurity[55]. ENISA has published several best practices documents on IoT security and securing the IoT supply chain[565758,] as well as other organizations such as NIST[5960] and GSMA[61] Specific to 5G networks the EU Cybersecurity Act will mandate certifications for specific components in 5G networks[62], 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

[54] NIS Directive, https://digital-strategy.ec.europa.eu/en/policies/nis-directive
[55] 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/
[56] ENISA Guidelines for Securing the Internet of Things, https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things
[57] ENISA Good Practices for Security of IoT, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1
[58] ENISA Baseline Security Recommendations for IoT, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
[59] NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline, https://csrc.nist.gov/publications/detail/nistir/8259a/final
[60] NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers, https://csrc.nist.gov/publications/detail/nistir/8259/final
[61] GSMA IoT Security Guidelines and Assessment, https://www.gsma.com/iot/iot-security/iot-security-guidelines/
[62] Securing EU's Vision on 5G: Cybersecurity Certification, https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

communication and networking solutions in Europe. These activities offer opportunities for start-ups to design communication modem chips and other components devised for many vertical applications.

Devices must be designed with a security first approach, considering the whole life cycle of devices. Especially for critical infrastructure this will be mandated early on but these requirements will also affect other devices as the threat landscape continues to evolve, expanding on the opportunity. For devices this means that manufacturers must adopt a holistic view on supply chain security including all components that go into the device. The device must contain enough security functionality to enable the user to adopt zero trust and zero touch architectures and paradigms including verifying the supply chain, secure deployment of devices and secure life cycle management of devices over the whole device lifecycle, including potential ability to upgrade to future post quantum cryptographic algorithms.

3.7.3 Requirements for IoT devices

Devices with IoT gateway capabilities in support of different IoT connectivity modes, both at local and public network level. In particular for each supported vertical industrial domain and as well cross vertical industry domains:

- requirements will be derived on which software and hardware capabilities and characteristics these multi-modal IoT devices and network elements should support, when integrated and used into the 5G and beyond 5G network infrastructures. Considering that these IoT devices support e.g., wireless technologies that are non-5G and beyond 5G radio technologies, such as Bluetooth, Wi-Fi, ZigBee, LoRa, Sigfox.
- integration and evaluation activities of these multi-modal IoT devices and network elements in the 5G and beyond 5G network infrastructures will be planned and executed.
- Hardware requirements for IoT Devices:
    - Requirements applied for each supported vertical industry domain and as well cross vertical industry domains when integrated and used into the 5G and beyond 5G network infrastructures.
    - At least three different frequency bands for sub-1 GHz, (700 MHz), 1 - 6 GHz (3.4 - 3.8 GHz), and millimetre-wave (above 24 GHz) and integrate multiple protocols in addition to cellular ones.
    - Functional and non-functional requirements, such as high data capacity, highest levels of reliability (connectivity), fast reaction times (low latency), sensing/actuating, processing and storage capabilities; low power consumption.
    - Strong security functionality with hardware cryptographic security modules, initial device identities and upgradable cryptographic algorithms.

3.8 EU legislative framework

Many of the gaps identified for the coverage of remote areas, or with very little population density are still not properly addressed today, where no public network coverage is available. This requires the need to create new technological solutions, where you can combine resources from different suppliers. One of the options could be linked to the use of equipment in the fields, which could be used as relays to reach an area covered by a tower. However, the implementation of such solutions should not modify the behaviour of the integrity of such equipment.

Many conformity assessments for safety and security are today supported by the Original Equipment Manufacturer (OEM) to validate the compliance of an equipment to get the CE marking and

homologations or certifications. These requirements are applied on equipment used in the fields and/or potentially used on a public network.

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. 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?**
    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.

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

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

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?

Critical Infrastructure support applications area (Section 2.6):

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?**
    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

Smart Manufacturing and Automation area (Section 2.7):

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 km²
	Video-operated remote control	>99.9999%	10 – 100 ms	15 – 150 kbytes	100	< 1 km²
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 km²	

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 10 with those in Table 3 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 Case: 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.

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 References

[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

[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

[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

[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.

[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.

[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

[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

[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.

[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.

[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.

[CiNe19] C. Cimino, E. Negri, L. Fumagalli, "Review of Digital Twin applications in manufacturing", Computers in Industry, 2019, 113, p.103130.

[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

[JML20] J. &. A. M. &. M. M. Lee, "5G and Smart Manufacturing," 2020.

[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.

[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.

[ErLi17] Ericsson and Arthur D. Little, "The 5G business potential", second edition, October 2017.

[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.

[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.

[Satell-market] http://satellitemarkets.com/satellite-iot-game-changer-industry

[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.

[NASA-cubesats] https://www.nasa.gov/mission_pages/cubesats/overview

[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

[Ericsson20] Ericsson Mobility Report: https://www.ericsson.com/4adc87/assets/local/mobility-report/documents/2020/november-2020-ericsson-mobility-report.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

[ISO 2413] ISO 24113:2019 Space Systems-Space Debris Mitigation Requirements: https://www.iso.org/standard/72383.html

[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

Annex II Template used for Use Case descriptions

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 0 and 0.

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[63] (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: $>1\text{-}10^{-5}$	$>1\text{-}10^{-6}$	$>1\text{-}10^{-7}$	$>1\text{-}10^{-8}$
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)

Selected KPIs Forecast for Satellite Radio Communications during the short, medium, and long -term evolution of 5G NR.

KPI	Short tTerm 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%

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

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]	1Gb/s	~10Gb/s	>25Gb/s	>50Gb/s

	(business)				
	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 enviroments	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 ~2025	Medium term ~2028	Long term ~2030
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 ~2025	Medium term ~2028	Long term ~2030
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 ~2025	Medium term ~2028	Long term ~2030
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.

Short-term Evo. ~2025	Medium-term Evo ~2028	Long-term Evo. ~2030
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 Evo. ~2025	Medium-term Evo ~2028	Long-term Evo. ~2030
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 Evo. ~2025	Medium-term Evo ~2028	Long-term Evo. ~2030
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 Evo. ~2025	Medium-term Evo ~2028	Long-term Evo. ~2030
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 5 shows a consolidated view of the 5G requirements, while **Table 6** provides more details on the 5G requirements coming from verticals.

Table 5: 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/km^2 Number of devices: 1 mio/km^2	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 km^2	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 6: 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

Annex V Editor and Contributors to this Deliverable

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)
- 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)
- Holger Kellerbauer (Caterpillar / CECE Digital Task Force)
- Thomas Klein (IBM)
- Zbigniew Kopertowski (Orange)
- Antonio Kung (Trialog)
- Konstantinos Loupos (INLECOM)
- Sean McGrath (University of Limerick)
- Daniel Morros (Sateliot IoT Services)
- Toon Norp (TNO)
- Joao Peixoto (Ubiwhere)
- Ranga Rao Venkatesha Prasad (Technical University Delft)
- Uwe Rüddenklau (Infineon)
- Natalie Samovich (Enercoutim)
- Jaume Segura (Universitat de València)
- Erwin Schoitsch (Austrian Institute of Technology - AIT)
- Antonio Skarmeta (University of Murcia)
- Flemming Sveen (Hafenstrom)
- Giacomo Tavola (Politecnico di Milano)
- Ricardo Vitorino (Ubiwhere)

Acknowledgements

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT Innovation in Europe, bringing together small and large companies, start-ups and scale-ups, 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 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 Innovation in society.

AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies. We also put them in practice in vertical application domains with societal and economic relevance.