D1.1

Analysis of use cases and system requirements

GES

Funded by the European Union

Work package	WP1
Task	T1.1
Due date	30-06-2023
Submission date	30-06-2023
Deliverable lead	GES
Version	Final
Authors	Luis M. Contreras (TID), Antonio de la Oliva (UC3M), Jorge Vázquez (GES), Marc Mollà Roselló (ERC), Luis Velasco (UPC), Fernando Agraz (UPC), Salvatore Spadaro (UPC), Marc Ruiz (UPC), José Luis Cárcel (ATOS), Péter Szilágyi (NOK), Sebastian Robitzsch (IDE), Renan Krishna (IDE), Chathura Sarathchandra (IDE), Fotis Faukalas (COG)
Reviewers	Stefano Vitturi (UNIPD), Marc Mollà Roselló (ERC), Péter Szilágyi (NOK), Antonio de la Oliva (UC3M)

Abstract

This document focuses on describing and analyzing the use cases that will demonstrate and validate the technologies to be tested in the PREDICT-6G project and establish the system requirements necessary to achieve the project's goals. Each use case will be described, outlining the targets and KPIs, and analyzing the technical components and systems, based on a common definition of the Key Performance Indicators (KPIs) that will be used to analyze and evaluate the technologies used in the project and a standard methodology to compare the uses case, which are described in this document. Taking this in account, a traffic characterization and the system requirements for the projects are also define in this document, as well as, an initial explanation of the architectural and security requirements.

Keywords

6G, Determinism, Time-Sensitive Networking, Smart Factory, Multi-domain communications, critical communications, localisation, sensing, KPIs

Document revision history

Version	Date	Description of change	Contributor(s)
v0.1	12-04-2023	D1.1 skeleton	Luis M. Contreras (TID) Jorge Vázquez (GES) Marc Mollà Roselló (ERC) Luis Velasco (UPC) Marc Ruiz (UPC) Davide Careglio (UPC) Salvatore Spadaro (UPC) Fernando Agraz (UPC) José Luis Cárcel (ATOS) Péter Szilágyi (NOK)
V0.2	03-06-2023	Additional use cases	Sebastian Robitzsch (IDE) Renan Krishna (IDE) Chathura Sarathchandra (IDE)
V1.0	15-05-2024	Editorial changes after first year review	Jorge Vázquez (GES)

Disclaimer

The information, documentation and figures available in this deliverable are provided by the PREDICT-6G project's consortium under EC grant agreement **101095890** and do not necessarily reflect the views of the European Commission. The European Commission is not liable for any use that may be made of the information contained herein.

Copyright notice

Document information

Nature of the deliverable		[R]
Dissemination level		
PU	Public, fully open. e.g., website	✓
CL	Classified information as referred to in Commission Decision 2001/844/EC	
SEN	Confidential to PREDICT-6G project and Commission Services	

* Deliverable types:

R: document, report (excluding periodic and final reports).

DEM: demonstrator, pilot, prototype, plan designs.

DEC: websites, patent filings, press and media actions, videos, etc.

OTHER: software, technical diagrams, etc.

Table of contents

Contents

Funded by
the European Union

List of figures

List of tables

Acronyms and definitions

AI	Artificial Intelligence
AICP	AI-driven Multi-stakeholder Inter-domain Control-Plane
CM	Configuration Management
DoA	Description of Action
DT	Digital Twin
E2E	End-to-End
FM	Failure Management
IETF	Internet Engineering Task Force
IP	Internet Protocol
KPI	Key Performance Indicator
MAC	Media Access Control
MDP	Multi-domain Data-Plane
ML	Machine Learning
MNO	Mobile Network Operator
OWD	One-Way Delay
PLC	Program Line Controller
PM	Performance Management
RAW	Reliable and Available Wireless

RTT	Round-Trip Time
SLA	Service Level Agreement
SotA	State of the Art
TCP	Transmission Control Protocol
TSN	Time-Sensitive Networking
VPN	Virtual Private Network
WP	Work Package

Table of partners

Short Name	Partner
UC3M	Universidad Carlos III de Madrid
NOK	Nokia Solutions and Networks KFT
ERC	Ericsson Espana SA
INT	Intel Deutschland GMBH
TID	Telefonica Investigacion y Desarrollo SA
ATOS	ATOS IT Solutions and Services Iberia SL
GES	Gestamp Servicios SA
NXW	Nextworks
COG	Cognitive Innovations Private Company
SIM	Software Imagination & Vision SRL
AUSTRALO	AUSTRALO Alpha Lab MTU
POLITO	Politecnico di Torino
UPC	Universitat Politecnica de Catalunya
CNR	Consiglio Nazionale delle Ricerche
UNIPD	Universita degli Studi di Padova
IDE	InterDigital Europe Ltd

1 Executive summary and key results

This initial deliverable focuses on describing and analyzing the use cases that will demonstrate and validate the technologies to be tested in the PREDICT-6G project. Its purpose is also to establish the system requirements necessary to achieve the project's goals.

The first part of the deliverable aims to describe and explain the Key Performance Indicators (KPIs) that will be used to analyze and evaluate the technologies used in the project. This will later serve as a reference in the description of the use cases.

The methodology used to analyze the use cases will be described, with an emphasis on the technical components that will be employed in the project. Each use case will be described, outlining the targets and KPIs, and analyzing the technical components and systems. A table will be used to summarize the methodology, facilitating the analysis of each use case individually and in comparison, with others.

Furthermore, a summary of other use cases described and analyzed in recent months will be provided, with a focus on identifying additional use cases that will enhance the solutions proposed by the project.

To analyze the system requirements, a traffic characterization model will be employed. The description and methodology for conducting this characterization will be defined in this deliverable.

Additionally, an initial explanation of the architectural and security requirements is also presented.

Considering all of this, this deliverable will define the requirements and specifications for the project, serving as the first step towards designing the solutions that will be implemented to achieve the targets of each use case.

In summary, three use cases were analyzed, covering a wide range of technologies and sectors. The first one focuses on the industrial sector, specifically smart manufacturing, exploring how a deterministic wireless network can bring new possibilities for flexibility and mobility in industrial processes.

The second use case pertains to mobility and critical communications, investigating how deterministic services can support the required service levels.

Lastly, the third use case is related to the telecommunications sector, where different technologies coexist within a multi-domain ecosystem, allowing the utilization of the best features of each solution.

Other use cases in the entertainment and research sectors were also identified and analyzed, contributing to a more detailed shaping of the other use cases and the overall project.

Based on the methodology and established KPIs, the use cases presented and will provide the environment necessary to test and analyze the level of determinism of the project.

Funded by the European Union

The key results of this deliverable can be summarized as:

- Definition of the KPIs to be used across the project, including the actual meaning and metric used for each of them.
- Definition of methodology to describe and analyse the use cases.
- Definition of the use cases to be covered by the project, indicating the different values for the different KPIs.
- Summarizing the use cases and requirements addressed in two key references for the multi-domain, multi-technology data plane, IETF RAW and DetNet.
- Definition and characterization of traffic data for each use case.
- Analyse of the system level requirements
- Initial description of the overall system architecture.
- Initial analysis of security threats.

2 Introduction

This deliverable aims to specify the use cases of PREDICT-6G, which will be later demonstrated and validated as showcase. It will analyse the advanced 6G use cases that were already described in the project proposal and are outlined in Section 5 of this document. Additionally, it will describe and analyse other potential use cases that can enrich the project by defining functional and non-functional requirements.

This analysis of use cases combined with the existing state-of-the-art knowledge (including ICT-52 projects, SDOs, and partners' expertise); will help identify the system requirements. It will also contribute to defining and characterizing the traffic model and addressing architectural and security considerations based on the specific use case requirements.

Consequently, we will evaluate the impact of these requirements on the design of PREDICT-6G's solution, including the need to ensure reliability and time sensitivity for flows across multiple domains and technologies.

Furthermore, the Key Performance Indicators (KPIs) will be defined and established for each use case. These KPIs will then form the basis for determining an optimal set of system requirements, encompassing end-to-end orchestration, low latency, high capacity, and optimal path selection while considering various constraints.

The outcome of this analysis will be the primary result of this deliverable (D1.1), and it will guide the overall system specification of the PREDICT-6G solution.

This document has a section 3 for the definition of KPIs. The aim of this section is to provide a common definition of Key Performance Indicators (KPIs) used in the PREDICT-6G project a method for the measurement, units, and measurement points. Section 4, a methodology has been defined so that the result of the analysis for each particular use case can be homogeneous in depth and comparable in details. An overview and analyse of each of the use cases covered in the project is describe in section 5. In section 6, additional use cases are analysed seeking for requirements that could enrich the project. In the next section (7), a traffic model methodology and characterization is defined for each use case. Sections 8, collects system level requirements of the PREDICT-6G system, considering the use cases, traffic characteristics and the overall scope of providing e2e deterministic services across multiple technology domains. In section 9, an initial insight and architecture is described, taking in account that for this project, the system provides deterministic services over multiple inter-connected domains and technologies. Finally, in section 10, a description of the possible threats for the system, with a cause and mitigation is define and split by the type of technology.

3 Definition of KPIs in the context of PREDICT6G

The aim of this section is to provide a common definition of the Key Performance Indicators (KPIs) used in the PREDICT-6G project, for avoiding (i) multiple definitions of the same KPI (e.g., Reliability), (ii) different understanding of a KPI (e.g., Latency) and (iii) different implementations of the same KPI. In addition, we want to bring the point of view of determinism to the different KPIs and metrics used in the project.

In this project, we understand **determinism** as "**the union of reliable, time sensitiveness** and **predictable** features" [1]. Time sensitive and predictability has well-known definitions but when we discuss about reliability, the different definitions and understanding appears and not only with this concept. For that reason, we present definitions of different KPIs that are required in a deterministic network,

3.1 KPI definition

For the definition of the KPIs, we followed the [2] best practice proposal. We define the KPI from end-to-end point of view, that is, from the view of the end-user of the communication networks. How those KPIs are implemented in a multi-technology and multi-domain network will be addressed in the technical Work Packages (WP2, WP3 and WP4).

Table 1 contains the template we follow in the KPIs definition:

KPI field	Description
Name	Name of the KPI
Description	High level description from end-to-end point of view
Method of measurement	Definition of what is going to be measured in this KPI, including the conditions and exceptions [3].
Units	Units of the KPI
Measurement points	Definition of the measurement point(s) from end-user perspective

Table 1. KPI definition fields

3.2 Reliability

This is probably the KPI with more different definitions in the scope of telecommunication service. We reviewed the definition proposed for [4] that focuses on the probability of transmitting a small data packet within a required latency in testing environments. In [5] Hexa-X project extends the previous definition by replacing the required latency with the "…QoS constraints…" which implies more aspects in addition to the latency. Finally, IETF RAW [6], introduces the concept of SLA (Service Level Agreement) that is going to be used in the definition. With all these considerations, the following definition of Reliability is proposed:

Name	**Reliability**
Description	Reliability is the success probability of performing a deterministic end-to-end communication service within a given time interval in the context of a defined SLA.
Method of measurement	The probability is measured for layer 2 or layer 3 packets with the application Packet Data Unit (PDU). The SLA is defined per use case and can involve any of the other KPIs defined in the project, so Reliability KPI shall aggregate other KPI measurements. The end-to-end reliability includes the global measurement of all network segments involved in the communication. Per-domain reliability is measured in each domain or segment. The probability calculation may include scenarios that stresses the resiliency of the network: e.g., it may be calculated for the scenario where one of the network segments involved in the communication is not available.
Units	Number expressed as percentage
Measuring point(s)	Border (TSN) bridges: • Bridges connected to end-stations. • Bridges connected to other TSN system (for per domain reliability)

Table 2. Reliability definition

3.3 Availability

In the case of availability, we adhere to the definition expressed in IETF-RAW [7] as described below:

Name	**Availability**
Description	Percentage of time in which deterministic networks successfully operate in the context of a defined SLA
Method of measurement	The availability is measured as the result of the *(uptime) / (uptime + downtime)*. *uptime* is the time during the network fulfils the SLAs for all the deterministic communications. *downtime* includes not only outage of service but also degradation. Per-domain Availability can be calculated using local metrics. Global Availability must consider multiple paths using different segments for aggregating the availability. An end-to-end measurement is recommended.
Units	Number expressed as percentage

Funded by the European Union

Measuring point(s)	Border (TSN) bridges: • Bridges connected to end-stations. • Bridges connected to other TSN system (for per domain reliability)

Table 3. Availability definition

3.4 Packet loss

For packet loss, we use the standard definition, as described in the following table:

Name	**Packet Loss**
Description	Percentage of the packets lost during a period of time
Method of measurement	The ratio between the numbers of lost packets regarding the total of packets (*packets lost / total packets)* during a period. In PREDICT-6 G, lost packets also include the packets that arrive late or out-of-order, so this KPI can refer to a latency requirement. Per-domain packet loss can be calculated using local metrics. Global packet loss must consider multiple paths using different segments for aggregating the availability. An end-to-end measurement is recommended.
Units	Number expressed as percentage
Measuring point(s)	Border (TSN) bridges: • Bridges connected to end-stations. • Bridges connected to other TSN system (for per domain reliability)

Table 4. Packet loss

3.5 Packet ordering

For measuring the order of the packets, we adhere to the definitions in [8], for in-sequence, out-of-order and duplicated packets. For the global KPI, we define:

Name	**Packet Ordering**
Description	Percentage of the packets in-sequence versus the total of packets in a deterministic network.
Method of measurement	For measuring the packet order, each packet has to include a sequence number (this typically happens when packets belong to a stream or are marked for whatever reason). Depending on the sequence number, packets can be in-sequence, out-of-order or duplicate [8]. An in-sequence packet is “A received packet with the expected Test Sequence number.” [8] An out-of-order packet is “A received packet with a sequence number less than the sequence number of any previously arriving packet.” [8]

	A duplicate packet is "A received packet with a Test Sequence number matching a previously received packet." [8]
Units	Number expressed as a percentage
Measuring point(s)	Border (TSN) bridges: • Bridges connected to end-stations. • Bridges connected to other TSN system (for per domain reliability)

Table 5. Packet ordering

3.6 Latency

Latency has a common definition that is used in almost all 5G and 6G projects [4] [5], but the interpretation varies depending on the use case, as sometimes it refers to a One-Way Delay (OWD) latency and sometimes is a combination (Round-Trip Time, two OWD in UE-to-UE communications). In all definitions, they assume small packets in ideal conditions. In this deliverable, it is proposed, to extend that to the real traffic of the application that uses deterministic networking.

Name	**Service Latency**
Description	Time required by a deterministic network to deliver an application packet when performing a specific end-to-end communication service.
Method of measurement	The Service Latency is measured at the border bridges, and it is obtained as the difference between the time a packet exits a multi-domain deterministic network and that it entered. It can be mapped as combination of: • Domain OWD: Time required for transmitting the packet through a deterministic network. • RTT: Time to receive a packet that contains the answer to a previous packet request. It is highly dependent on the use case and comprises not only network latency, but also application/protocol elaboration times
Units	Fraction of seconds (ms, us, ns)
Measuring point(s)	Border (TSN) bridges: • Bridges connected to end-stations. • Bridges connected to other TSN system (for per domain reliability)

Table 6. Service Latency

3.7 Jitter

For Jitter, we selected the definition in [9], using a strict upper value:

Name	Jitter
Description	Difference in milliseconds between the 0 quantile (minimum) and the 1-10^-3 quantile of the delay variation.
Method of measurement	(IP) delay variation is the difference between the OWD of two sequential packets in a flow. For end-to-end jitter, it is the OWD difference between the border bridges of a multi-domain deterministic network. Jitter is calculated by measuring the difference between the minimum delay variation and the 1-10^-3 quantile of the delay variation distribution.
Units	Fraction of seconds (ms, us, ns)
Measuring point(s)	Border (TSN) bridges: • Bridges connected to end-stations. • Bridges connected to other TSN system (for per domain reliability)

Table 7. Service Latency Jitter

3.8 Other KPIs

In this project, we use standard KPIs (Mobility, Spectral Efficiency, and Data Rate) that follows the definition in [3].

4 Use case analysis methodology.

To better understand the implications of the considered use cases, a common methodology has been defined so that the result of the analysis for each particular use case can be homogeneous in depth and comparable in details.

The methodology defined considers the following aspects:

- Technical components of each particular use case, so that the use case can be described in terms of characteristics such as traffic workload, infrastructure needs, etc.
- Other considerations relevant for the realization of the use case, like data sources that could be needed, or standard specifications supporting the use case.
- Definition of KPIs relevant to the validation of the use case, corresponding to the Service Level Objectives to be satisfied.
- Identification of requirements, both functional and non-functional, imposed by the use case, so that PREDICT-6G architecture needs to accomplish them.

The following subsections provide more details on these aspects.

4.1 Use case technical components.

A given use case is characterized through different dimensions. At the time of analysing a use case it is important to go through all that dimensions to avoid losing details that could be relevant for the final purpose of the use case, which is the validation of the PREDICT-6G solution as exercised with that use case.

Next, some relevant characteristics are described.

4.1.1 Workloads (including traffic characterization)

Any use case includes communication services with certain properties and behaviours. One of them is relevant to the characteristics of the workload, that is, how the use case is structured in terms of interchanged flows among the actors, and how those flows are described in terms of volume, frequency, nature (i.e., burst, plane, shaped, …), bit rate, etc. This is also applicable to the characteristics of the functions or applications participant of the communication service, in terms of data volume, etc., but also number of sessions, as well as other properties that could be relevant.

4.1.2 Data Governance

Such data can require special data governance policies that could imply specific treatment, for instance at the time of forwarding, storing or monitoring. Thus, it is important to consider any constraint applicable to the communication service, since this can impose requirements to some components in the final architecture.

4.1.3 Infrastructure (Communications, Cloud / Edge, Virtualization)

The realization of a use case has clear dependencies on the supporting network infrastructure in broad sense, that is, for both networking and computing. In the case of networking, aspects such as access and transport technologies support of specific data planes, queue management, protocol encapsulation or forwarding strategies (i.e., unicast, multicast, etc.). For computing, aspects such as number of CPUs, memory size or storage needs, as well as hardware accelerators or virtualization technologies are all relevant. Furthermore, other aspects such as the need of geolocation or proximity can also determine the way of realizing the use case.

The realization of a use case could imply some specific infrastructure options in the more restrictive case or allow multiple options in the more relaxed case. Moreover, restrictions could apply only partially.

4.1.4 Data & Analytics

The use case can also require the processing and analysis of data for its execution. For instance, determination of positioning, abnormal traffic patterns, or anomaly detection, can be situations needed for realizing a given use case.

Funded by the European Union

If these analytics are needed, then it can be necessary to deal with data collection, processing, storage, etc. The specific use case will determine the final needs in this respect.

4.1.5 Devices / Terminals

Finally, the type of devices or terminals that end-users require for the proposed communication service also characterizes every use case. The notion of end-user should be considered broadly, since not only humans but also objects or sensors could play that role.

The type of device or terminal determines the access technology in use (wireless, wireline) as well as other service conditions such as mobility, number of available interfaces, etc.

4.2 Further considerations

Additional considerations help to obtain a more complete understanding of the use case.

4.2.1 Data sources needed to develop the use case.

The realization or completion of a use case can depend on data sources to assess the system behaviour. For instance, this is the case of data sources that can generate a specific traffic profile, records of end-user positioning and attachment, or traces that could serve as training reference for a machine-learning component.

Understanding the kind of data sources needed assists to the execution of the use case, which finally serves to validate the architectural modules defined by PREDICT-6G.

4.2.2 Components or features not available today.

Since the final target of the project is to produce the definition of an architecture for 6G, the use cases present advanced capabilities beyond existing state-of-the-art. Despite the architecture will be defined on top of existing concepts and solutions, it is evident that new components or features can be required, either by means of novel approaches, integrating previously decoupled techniques, or by extending existing functionality improved in that way that the use case can be finally satisfied.

4.2.3 Stakeholders

In all the use cases, there are participant actors with distinct roles, played by different stakeholders. It is essential to understand how those stakeholders interact, what are the relationships among them, as well as the dependencies at the time of performing the use case, so that the different parties can be fully characterized. This description of stakeholders is a crucial input for the subsequent developing of all the techno-economic and business analyses necessary for understanding the economic and commercial viability of the path followed at the time of defining the PREDICT-6G solution.

4.2.4 Relevant standards related to the use case.

Since the industry is providing the first steps in the evolution to 6G, having a view of the use case needs in terms of standards (and open source) support is relevant for the identification of potential gaps. Thus, the definition of the use case can motivate the development of new functionalities suitable for contribution to standardization bodies, or to developments contributed to open-source communities. The exercise of the use case will help to validate the approach taken for covering identified gaps, in a manner that the contributions are contrasted against realistic situations in the path to 6G.

4.3 Use case KPIs.

The use case description will also help to understand the Key Performance Indicators associated to it. The KPIs are based on the expected Service Level Objectives (SLOs) necessary to satisfy the use case and set the thresholds that should be accomplished during service execution. This serves as benchmarking reference for contrasting the functionality developed in the PREDICT-6G architecture.

Section 3 has extensively described the KPIs of relevance for the project. Consequently, the use cases will be analysed with those KPIs in mind.

4.4 Use case requirements.

Another relevant outcome from the use case analysis will be to determine the set of requirements that these use cases impose to the PREDICT-6G architecture. The requirements are essential to fully defining the different components and modules of the architecture.

4.4.1 Functional

A functional requirement describes what a system is supposed to do. It defines a function or a feature of a whole system or one of its components, capable of solving a certain problem or replying to a certain need or request as identified in the use cases under analysis. This includes a functional capability, dynamic situation, a sequence, timing parameters, or an interaction.

The set of functional requirements present a complete description of how a specific system will operate, capturing every aspect of how it should work before it is built, including information handling, computation handling, storage handling and connectivity handling.

4.4.2 Non-functional

A non-functional requirement is a specification criterion that can be used to judge the operation of a system, rather than specific behaviours. This includes abnormal situations, error conditions and bounds of performance, as well as scalability, usability, etc.

In other words, it is a description of how well a system performs its functions, representing an attribute that a specific system must have. Other aspects of the system control the non-functional requirements.

5 Overview of demonstration use cases

Three use cases are analyzed in this section, covering a wide range of technologies and sectors. The first one focuses on the industrial sector, in this case for smart manufacturing. The second use case pertains to mobility and critical communications. Finally, the third one is related to the telecommunications sector, where different technologies coexist within a multi-domain ecosystem.

5.1 Smart manufacturing

Currently, many industrial companies have been committed to Digitization and Industry 4.0 for several years, with a clear vision: Create more efficient and flexible production factories with more consistent and reliable processes through the analysis of data, adding intelligence to processes under the umbrella of a new and disruptive Smart Factory model of the future.

This concept of Smart Factory can be defined as a connected, intelligent, virtualized, secure, and scalable factory that allows flexible, agile and efficient adaptation to the increasingly changing needs of the industry. In the Smart Factory, the materials are found unitarily in the industrial process and easily identifiable and locatable at any moment, seeking for cost effectiveness, maximum flexibility, and the individualization of the serial production [10].

To achieve the Smart Factory, it is necessary, to carry out the digitalization of the factory. This means, connect all processes of the company, and create a database, where other systems will also dump informational data, to have a unique point to store information, breaking down the information silos of the company. This data must be processed and accessible, to be consumed by the organization, with reporting, developments, or applications, that allow a faster root cause analyses and quick reaction for decision-making.

To enable concepts of flexibility, agility and mobility in the manufacturing process, it is necessary to evolve the current standard for automated manufacturing installation, to a new one in which the different new technologies converge and the dependency of the wiring is not anymore a constraint, for cost, determinism, latency and reliability.

Presently, in an automated manufacturing process, all components of the process are connected, by wire, to a PLC (Programmable Logic Controller), to receive and send signals that orchestrate and control all the automated actions, defined in the PLC program.

The PLC program is based on programming blocks, which work as sequences of commands and instructions to be followed to be able to carry out the automated actions as well as to ensure the safety (with safety in PLC) in the manufacturing process.

These programming blocks relay on inputs coming from different signals from different components. To be able to execute the program without any error, these inputs must be received at the right moment (in-time flows) to activate the subsequent sequences of the programs. This is the reason why determinism is critical to execute the program.

Therefore, all signals and commands must trigger the blocking program at the right moment, with no loss or delay bigger than the PLC cycle scan (10 ms), which is the time in between sending of the programming blocks. If this happens the manufacturing process will stop because the order of the programming blocks is not correct.

To be able to ensure this kind of determinism industrial machinery relays on one side on the industrial protocols, so signals and commands follow the correct order, and on the other side on the wire input, (i. e. a sensor) to be able to ensure that the signals are transmitted at the right time to the PLC.

To process all this data without interfering with the PLC processing, an industrial PC is installed to extract, transform, and load the information into the database, which is normally cloud based. This connection between PLC, Industrial PC and servers is implemented as a wired connection to increase reliability and reduce latency.

This architecture is represented in the following Figure 1:

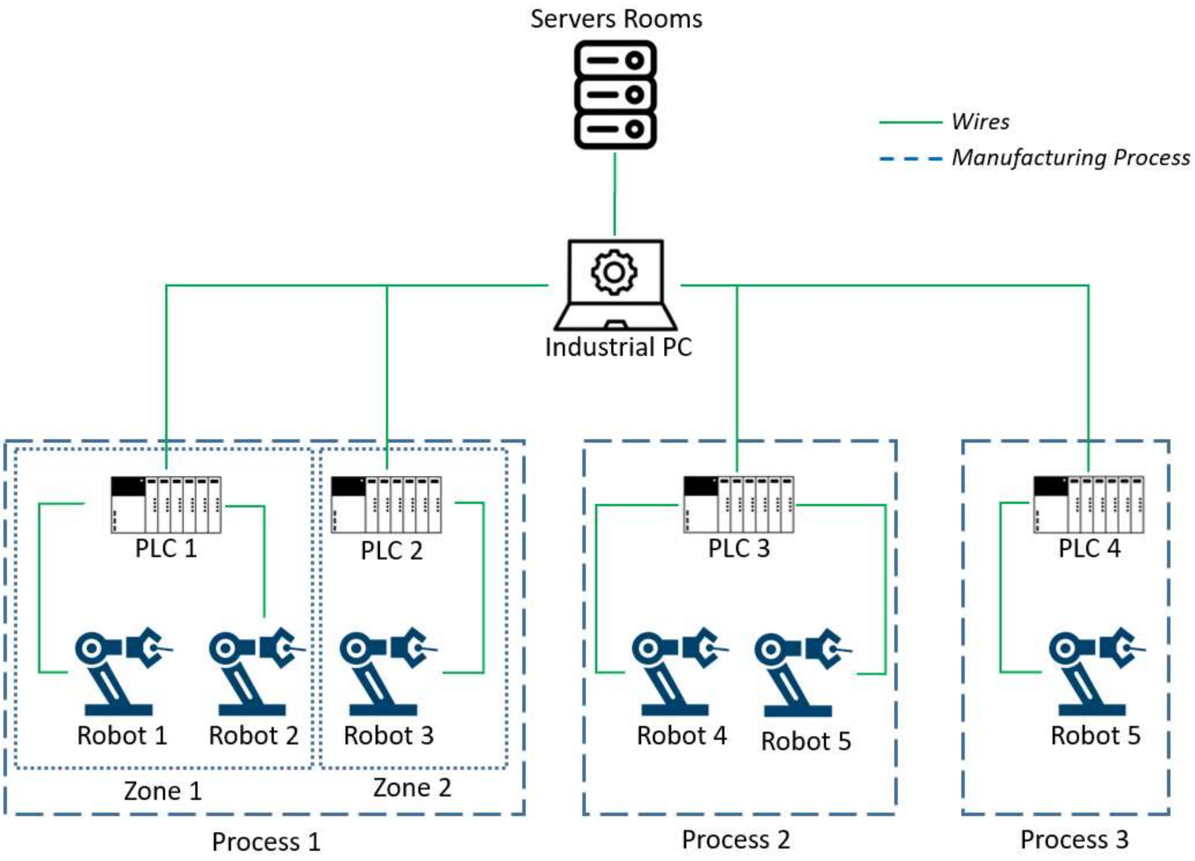

Figure 1. Current Architecture

All this wiring is a disadvantage to achieve the flexibility and mobility required in a Smart Factory (i.e., as movement of assets or combination of machinery).

With the current technologies, it is not possible to have a wireless connection with the same level of determinism, reliability, and latency as required via wires.

Additionally, industrial deterministic technologies are isolated from other networks to provide connectivity to the manufacturing process, which forces the industries to rely on in-house network deployments and computing architectures, not being able to benefit from the latest innovations brought for example by 5G.

Disaggregated architectures expected in 6G will allow wireless access with deterministic characteristics to robots controlled in the cloud.

Consequently, the current concept of automated manufacturing must evolve to an architecture as the one presented in the following Figure 2.

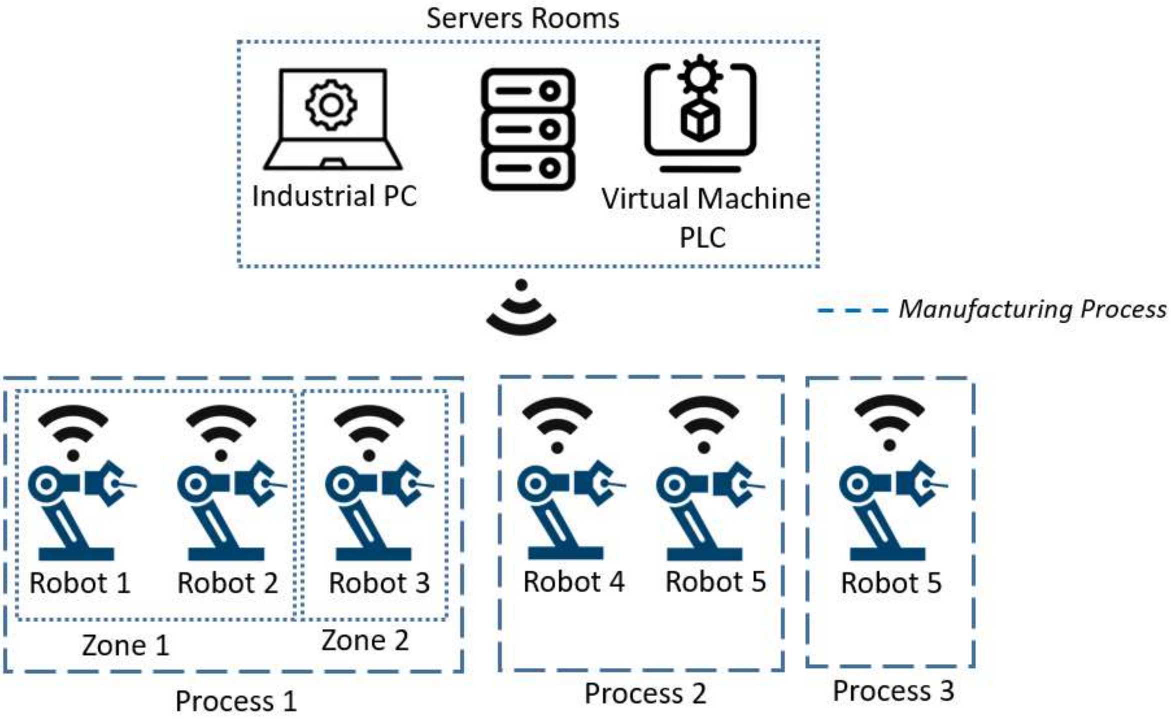

Figure 2. Future Architecture

Bearing in mind the possibility that new technologies contribute to wireless connection, the PLC can be virtualized, this means a PLC is implemented in a standard PC, with the possibility to operate in a virtual machine. This virtual machine will be hosted in the servers' room of the factory, with a real-time connection, using industrial protocols (i.e., Message Queueing Telemetry Transport).

A secondary test will be to host the virtual machine in the cloud and test the performance of this architecture.

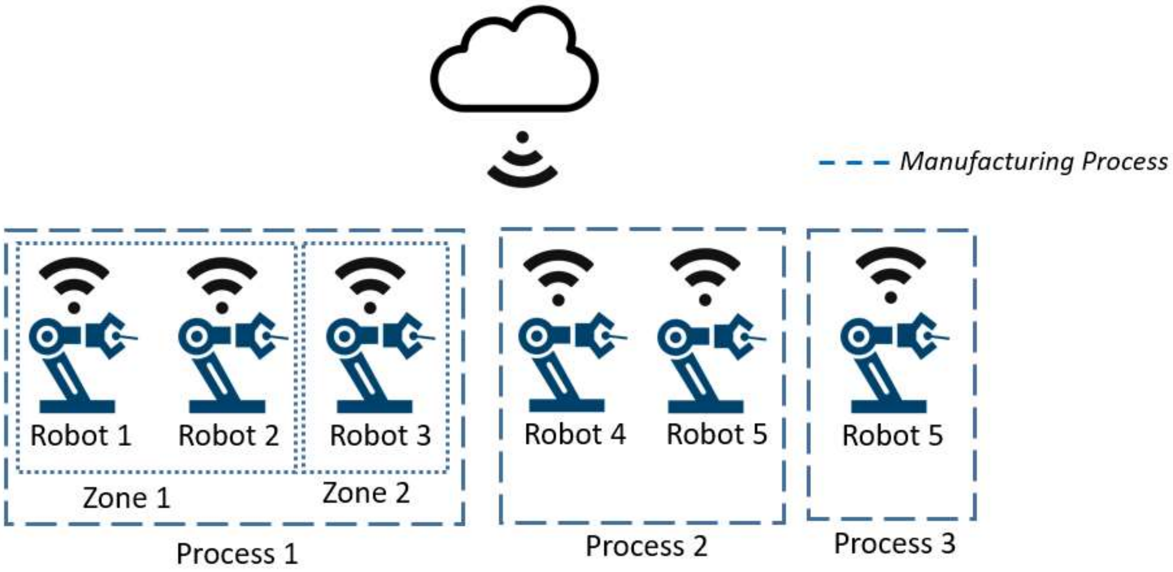

Figure 3. Cloud base architecture

This architecture opens the possibility to re-think the design of manufacturing processes, so wires can be reduced/removed when needed, and to move the automation and control of the manufacturing line out of the installation, via wireless connectivity, to the cloud.

PREDICT-6G, will open the possibility to re-think the design of the installation and be able to design an installation with a reduction of wire for connections and more important to move the automation and control of the process to the cloud with a wireless connection.

Table 8, presents a summary of the use case, following the methodology of section 4.

Topic	Description	SMART Manufacturing	
		Value	Comments
Use case technical components	Workloads	Send: 704 words by PLC cycle scan (10 ms) Received: 704 words by PLC cycle scan (10 ms)	1 Programing block of 1408 bytes is send every 10 ms. 1 Programing bloc of 1408 bytes is received every 10 ms. Word = 2 bytes. 704 words is a programming block
	Data Governance	N.A.	Security and privacy of the data

	Infrastructure	Cloud	Virtualized PLC Size of infrastructure
	Data & Analytics	N.A.	Block of programming (words). No Analytics (monitoring of robot movements)
	Devices/Terminals	Embedded UE with Release 16 for URLLC	To be defined for any application that the PLC is managing
Further Considerations	**Data sources needed to develop the use case**	Gateway MQTT to Radio	All data needed that is not managed by the PLC
	Components or features not available today	PLC Simulator in a Virtual Machine	Real-time connection with virtualized PLC.
	Stakeholders	N. A.	
	Standards	IEC 61499	Check compliant with IEC 61131 (TwinCat). Wireless Cybersecurity, VPN libraries, protocols real-time
KPIs Use Case	**Latency**	5 ms	One-Way Delay for sending or receiving a programming block, due to a PLC Cycle scan 10ms
	Reliability	99,9999%	Not lose any data. Send of program block.
	Jitter	2ms	
	Packet loss	Zero	
	Data acquisition	0,5 ms	
Use case requirements	**Functional**	Reliability	The important for this use case is the order and reliability of the program words.
	Non-Functional	TBD	

Table 8. Smart Factory Use Case Summary

5.2 Deterministic services for critical communications

A communication may be considered critical if the functional capability, operational capacity, and safety of the communication endpoints and their implemented solution depend on the communication service's availability, reliability, and performance. In such scenarios, the communication and thus the underlying network play an inseparable role in realizing an end-to-end solution. Example scenarios include cloud robotics; factory automation (e.g., implementing manufacturing or production workflows); AR/VR based interactions (potentially extended with cloud annotations); distributed sensor data collection, analytics, and command & control of physical devices; and many others. In such cases, the operation of the end devices, cloud application and the overall end-to-end solution imposes deterministic requirements on the network and communication service that interconnects them.

A typical traffic pattern is to generate periodic data at multiple locations (e.g., by HW sensors with specific resolution embedded in physical robots/actuators), generating multiple data streams that are expected to all arrive in sync at a local analytics cloud application (acting both as a rendezvous point and as workflow controller), which then provides time-bounded commands back to some of the robots/actuators, or provide alerts to a separate control escalation point where the entire workflow may be interrupted for safety concerns. In such cases, the group of deterministically communicating entities is defined by the workflow and is not expected to dynamically change within the execution of a workflow, as reconfigurations are executed offline.

Mobile devices such as AR/VR headsets or smartphone-based applications may also engage in collaborative tasks executed in the physical space requiring deterministic service. It requires that the network can provide deterministic communication within a dynamically evolving group, where devices are joining/leaving a group in an ad-hoc manner according to, e.g., the interest of their users, their interaction in the virtual space, their mobility or physical proximity. Cloud applications may be responsible for the monitoring and control of the devices and serving as rendezvous points to enable cloud-based group communication and data sharing across a large set of distributed devices that share a common task, physical or virtual environment or mission. In all these cases, it is important that the devices and the cloud applications participating in the same collaborative relation stay synchronized concerning their shared application state and thus need to exchange information, data, commands, and contextual information through deterministic and reliable communication services.

Example scenarios that may be implemented to demonstrate the PREDICT-6G capabilities are provided below. In an actual critical communication use case implementation, one or more of the scenarios could be selected (e.g., by creating applications with multiple traffic flows).

- Use Case: Sensor data collection and machine control.

  Multiple sensors attached to machines producing measurement data to be collected at a cloud compute host for real time analytics, with potential reverse command sent to the machines. In uplink, sensors may generate data towards the cloud in periodic batches (e.g., 200 KB/sec in 20 ms batches 4KB per batch), requiring time sensitive, deterministic service. In downlink, control commands may arrive as an aperiodic small data batch with urgency, requiring low latency, and ultra-reliable service.

- Use Case: Group communication.

  Multiple devices connected into the same virtual scene/session, synchronizing their status with each other in real time. Communication is enabled via a rendezvous point that receives data from multiple devices; identifies target devices per received data unit; performs data replication and transfer to target devices. In uplink, devices may generate state messages between 1-4 KB, sent periodically with 1-10 Hz frequency, requiring time sensitive, deterministic service. In downlink, multiple replicas of state messages (number of replicas is dynamically computed based on the current physical and virtual context/relation of the devices) are transferred to selected devices, requiring time sensitive, deterministic service. Additionally, the uplink and downlink time budget is coupled to provide a bounded round-trip time experienced by the end devices. Note that the uplink and downlink flows between the devices and the cloud are not symmetric and not mapped 1:1, which must be followed by the spread of the group communication service.

- Use Case: Camera sharing (special case of group communication)

  A device sharing its video stream with one or more other devices in real time. Communication is enabled via a rendezvous point that configures the sending device to start streaming its video; receives the video stream from the sending device; replicates the video stream towards receiving devices (if there are multiple ones); transfers the video stream to the target device(s). There may be multiple video streaming devices in a system simultaneously; video streaming starts/ends dynamically (based on explicit requests as well as current physical and virtual context/relation of the devices). In uplink, multiple devices send their video streams to the rendezvous point, where streams produce 0.5-5 Mbit/s traffic at specific frame rates depending on the video codec, requiring stable inter-frame delays and thus time sensitive, deterministic service. In downlink, selected uplink video streams are replicated towards devices where the inter-frame timing needs to be kept in sync with the uplink inter-frame times, again requiring time sensitive, deterministic service.

Topic	Description	Sensor data collection and machine control	
		Value	Comments
Use case technical components	Workloads	Uplink: 200 KB/sec in 20 ms batches 4KB per batch Downlink: control command as an aperiodic small data batch	Values are examples.
	Infrastructure	Cloud compute application	For receiving the uplink data
	Data & Analytics	At the cloud compute application	
	Devices/Terminals	Sensors, Machines	
KPIs Use Case	Latency	Uplink: 20 ms Downlink: 10 ms	
	Reliability	Uplink: 99,999%	

		Downlink: 99,9999%	
	Jitter	Uplink: 5 ms	
	Packet loss	Zero	Not to lose any data in uplink; even more importantly, not to lose and control command in downlink.

Table 9. Sensor data collection and machine control use case summary

Topic	Description	Group communication	
		Value	Comments
Use case technical components	**Workloads**	Uplink: 1-4 KB batches periodically with 1-10 Hz Downlink: multiple (dynamically changing) replicas (towards different devices) of the state replicas	Values are examples.
	Infrastructure	Cloud compute application as rendezvous point	For receiving the uplink data and relaying the data to interested devices in downlink
	Data & Analytics	At the cloud compute application	Dynamically managing the groups
	Devices/Terminals	Mixture of mobile and stationary devices	
KPIs Use Case	**Round-trip time**	50 ms	Between a source device sending a data in uplink and all interested devices receiving their own replica of the data through the rendezvous point in downlink
	Reliability	Uplink: 99,999% Downlink: 99,999%	
	Packet loss	Zero	Not to lose any data

Table 10. Group communication use case summary

Topic	Description	Camera sharing (special case of group communication)	
		Value	Comments
Use case technical components	**Workloads**	Uplink: 0.5-5 Mbit/s traffic at specific frame rates depending on the video codec Downlink: multiple (dynamically	Values are examples.

		changing) replicas (towards different devices) of the streams	
	Infrastructure	Cloud compute application as rendezvous point	For receiving the uplink stream and relaying the frames to interested devices in downlink
	Data & Analytics	At the cloud compute application	Dynamically managing the groups
	Devices/Terminals	Mixture of mobile and stationary devices	
KPIs Use Case	**Round-trip time**	50 ms	Between a source device sending a frame in uplink and all interested devices receiving their own replica of the frame through the rendezvous point in downlink
	Reliability	Uplink: 99,999% Downlink: 99,999%	
	Packet loss	Zero	Not to lose any frames

Table 11. Camera sharing use case summary

5.3 Multi-domain deterministic communication

A great majority of scenarios of applicability for deterministic communications apply to single domain cases, where the network and cloud environments are restricted to the full control and manageability of the involved resources by a reduced number of interworking and integrated stakeholders.

However, determinism can be required in situations where multiple providers and stakeholders, having a loose relation among them, intervene in the service provision and delivery as in the case of providing in-time or on-time services across, for instance:

- **Multiple, sparse sites of industrial enterprises:** Some enterprises may have different sites located sparsely. To avoid duplicating applications, agents from one site may use applications from another. In this way, robots will send measurements from their sensors and the application will respond with the control commands for the actuator.
- **Distributed critical communications:** As defined in section 5.2, critical communications are those, which cannot function or operate without some ensured capabilities from the communication system, for example, real-time group communication. Again, this kind of communications can happen in a distributed scenario, with different administrative domains.

These scenarios have been identified as extremely relevant for the coming years [11].

For that kind of services, it is relevant to guarantee latency and jitter boundaries within some given values of relevance for the specific application, not necessary of extreme low values but to be contained within some precise ranges. The following Figure 4 shows some of the flows mentioned above.

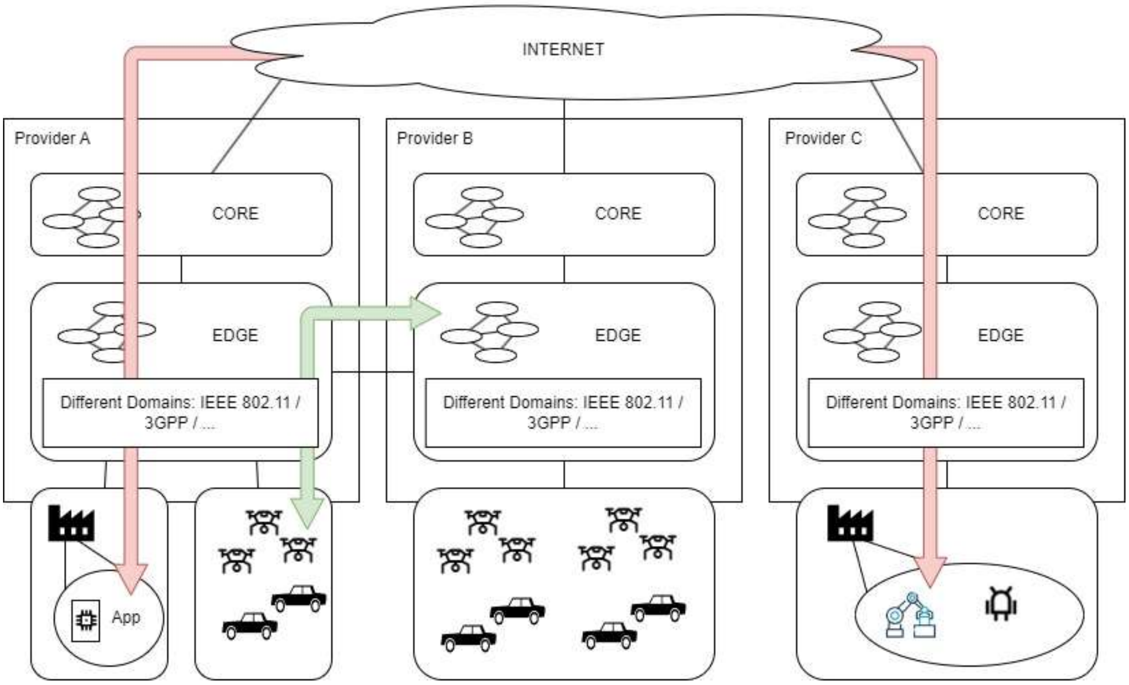
INTERNET
Provider A
Provider B
Provider C
CORE
CORE
CORE
EDGE
EDGE
EDGE
Different Domains: IEEE 802.11 / 3GPP / ...
Different Domains: IEEE 802.11 / 3GPP / ...
Different Domains: IEEE 802.11 / 3GPP / ...
App

Figure 4. Flows diagram for Multi-domain Deterministic Communications

This use case introduces large-scale multi-domain scenarios for the two already defined use cases (5.1 and 5.2) by exploring a combination of control and data-plane mechanisms to ensure in-time and on-time services described in each section. The integrated multi-domain multi-technology data plane is known as the MDP (Multi-technology Multi-domain Data Plane) in PREDICT-6G. The MDP will be implemented through the interworking of available technologies such as WiFi, 3GPP, TSN, Flexible Ethernet, DetNet and network programmability, enabling bounded E2E latency and reliability of the communication, as well as to extend the service awareness to the internal of the networks traversed.

The control plane in charge of building, controlling, and managing the MDP is known as the AI-driven Multi-stakeholder Inter-domain Control-Plane (AICP) in PREDICT-6G. The AICP will be implemented, to ensure the commitment of service constraints.

For this purpose, a multi-domain scenario will be built with the objective of experimenting and developing techniques and guidelines assisting the extension of the deterministic approach at large scale of the scenarios described in 5.1 and 5.2. The goals related to the multi-domain deterministic communication use case are:

- Enablement of in-time and on-time services in a multi-provider scenario, interconnecting at least two sites.
- Development of control-plane mechanisms for enforcing in-time and on-time services, contributing them to standard development organizations.
- Integration of at least three data-plane technologies to ensure bounded latency and jitter, reporting guidelines for operation.

Topic	Description	Multi-domain deterministic communication	
		Value	**Comments**
Use Case Technical Components	**Workloads**	The use case shall support the workloads of previous use cases. We will focus for demonstration purposes on the Smart Manufacturing use case.	The idea of this use case is to demonstrate the other use cases in a multi-domain, multi-technology scenario. For demonstration purposes, we will focus on Smart manufacturing.
	Data Governance	N/A	This is an aspect to discuss in the project. Data governance needs to be defined per domain in the end-to-end communication.
	Infrastructure	Multiple islands of deterministic and non-deterministic technologies. Must include 3GPP, wired TSN and wireless networks.	Infrastructure of possible demonstrations still not defined.
	Data & Analytics	N/A	Now is not clear what kind of data would be needed to build end-to-end communication.
	Devices/Terminals	Robots/unmanned vehicles/UE devices	
Further Considerations	**Data sources needed to develop the use case**	N/A	Now is not clear what kind of data would be needed to build end-to-end communication.
	Components or features not available today	Multi-Link Operation, Restricted TWT: WIP IEEE 802.11be standard draft. DetNet data plane. 3GPP DS-TT and NW-TT.	
	Stakeholders		
	Standards	TSN: Time synchronization IEEE 802.1AS, Time-aware scheduling	

		IEEE 802.1Qbv, Configuration 802.1Qcc Frame replication and Elimination for Reliability 802.1CB. IEEE 802.11be/bn. 3GPP rel 16 onwards.	
KPIs Use Case	Latency	5 to 100 ms	Same as Smart Manufacturing use case, as example. Depends on the specific use case
	Reliability	99.9999%	Same as Smart Manufacturing use case, as example
	Jitter	1 to 10 ms	Same as Smart Manufacturing use case, as example. Depends on use case.
	Packet loss	Zero	Same as Smart Manufacturing use case, as example
	Data acquisition	0,5 ms	Same as Smart Manufacturing use case, as example
Use Case Requirements	Functional	Integration of multi-domain and multi-technology	
	Non-Functional	N/A	

Table 12. Multi-domain deterministic communication use case summary

6 Additional Use Cases

Additional sub-section per relevant use case identified and analysed for this task.

6.1 Localisation and Sensing

This use case is based on a currently on-going 3GPP feasibility study in SA1 on localisation and sensing [12]. This study entails the native support for sensing in mobile networks and provides a plethora of distinct user cases formulating the high-level requirements for a future work item to enable such vision. The next figure illustrates a holistic view on what 3GPP aims to achieve, i.e., UEs and Base Stations (BSs) perform sensing of the environment and generate a continuous stream of sensing data. This sensing data is considered to be raw data points on numerous sensing techniques providing a data on distance vs x-y-z coordinates, the sensing data is then processed in the 5G System (5GS) and offered as sensing results to third parties aka verticals. The third party then has the option to communicate actions in an Over-the-Top (OTT) fashion bash to the application running on a UE (does not have to be the one that provided the sensing data). It of significant importance to mention that the feasibility study clearly states that only the 5GS will process sensing data.

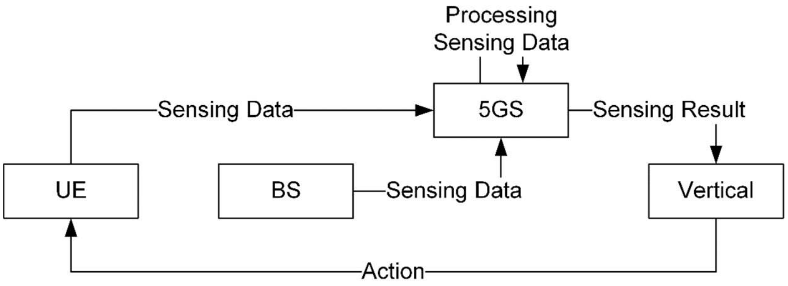

Figure 5: Holistic system view on sensing data and results exchange in future mobile networks

The processing of sensing data is foreseen to be conducted by ML-based solutions, it is important to deliver the sensing data in a deterministic fashion between UE/BS and the 5GS to guarantee the timely delivery of sensing results in scenarios such as collision avoidance or remote object control. In addition, this includes the sensing results to verticals, which are operating in a different technology domain and perhaps administrative domain.

Figure 6 depicts the narrative for use case designed to demonstrate the need for deterministic communications for localisation and sensing purposes. The use case is composed of two domains, which are logically in distinct locations, i.e., a robot to the left within a 3GPP domain and a human on the right within the Data Network domain. The human controls the robot (going forwards, backwards, left, right) via a glove and the robot provides a 4k camera feed pointing towards the direction of travel to the human. The video feed is presented either in a virtual reality headset or on a second screen. The mobile network illustrated in the figure serves all communication between the robot and the human. Furthermore, the mobile network offers a service to provide sensing results in form of collision avoidance notifications, which are configurable by the application the human being is using. Those notifications provide information about new objects within a specific configured range next to the sensor allowing the robot control application within the Data Network to intervene the robot control if an object is deemed too close to the robot and its direction of travel. To provide such sensing result, the robot is also equipped with a sensor that continuously senses the environment and provides the sensing results to the mobile network for further processing.

Funded by the European Union

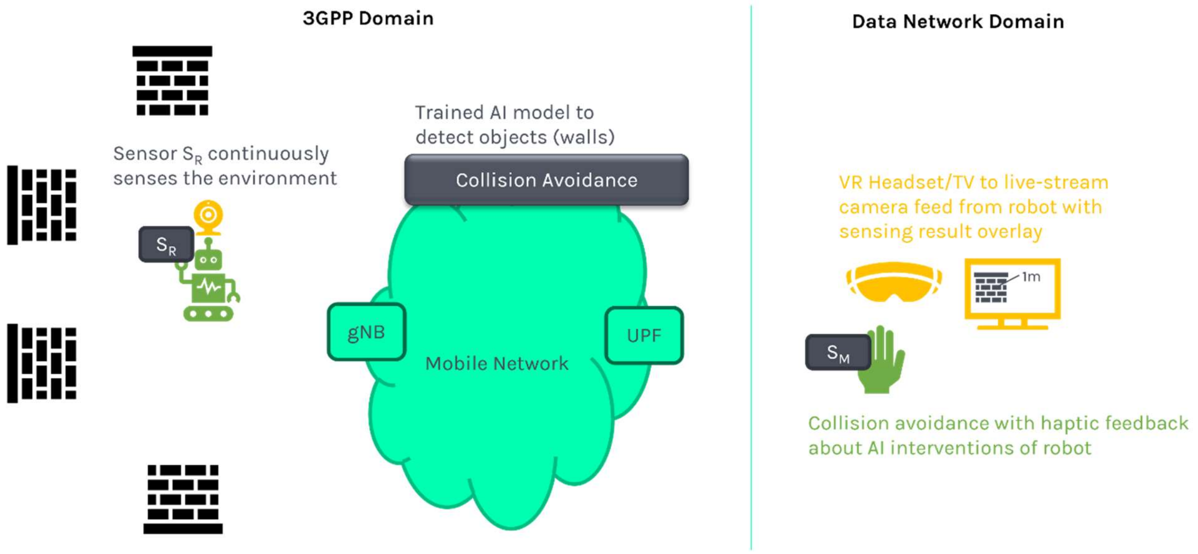
3GPP Domain
Data Network Domain
Sensor S_R continuously senses the environment
S_R
Trained AI model to detect objects (walls)
Collision Avoidance
gNB
Mobile Network
UPF
VR Headset/TV to live-stream camera feed from robot with sensing result overlay
1m
S_M
Collision avoidance with haptic feedback about AI interventions of robot

Figure 6: Localisation and sensing use case narrative

Topic	Description	Localisation and Sensing	
		Value	Comments
Use Case Technical Components	Workloads	~1kbps to 60Mbps Machine-consumed periodic data (for ML) requires deterministic delivery of data to work accurately in particular for time-sensitive tasks such as beamforming	Depending on the sensor, the data can range from three float numbers aggregated over a sampling interval as small a millisecond to video streams in extremely high definition for machine and human post-processing purposes at tens of hundreds of Megabits per second.
	Data Governance	Flexible governance based on user, operator and/or regulatory preferences	
	Infrastructure	Sensing hardware (Texas Instruments' mmW modules), COTS compute for deploying LAS Control and Data plane functions, haptic I/O devices (e.g. smart gloves), VR headsets (Meta Oculus) to display immersive content, GPU-enabled hosts for ML-based analytics Control Plane functions (Nvidia AEG), 4k camera and GPU-enable host for encoding purposes t	

	Data & Analytics	AI/ML to process sensory data and provide meaningful, but abstracted sensing results to NR layer in UE/BS or to third parties within the DN or on the UE	
	Devices/Terminals	Any device that comes with a wireless communication interface (mmW), radar capabilities, or camera	While transceiver (monostatic or bistatic) are considered 3GPP sensors, any sensing technology that is not used to communicate between a UE and BS is considered a non-3GPP sensor
Further Considerations	**Data sources needed to develop the use case**	n/a	All necessary data sources will be obtained from real mmW-based sensory equipment available in the LAS testbed.
	Components or features not available today	Utilising 5G NR for sensing is not available in current COTS solutions, as it is only being studied in Release 19 (SA1). Hence, dedicated sensory devices will be used to mitigate this.	
	Stakeholders	If there is software implementations of deterministic switching behaviour on a data plane out of WP2, this use case may utilise it in a 3GPP proposition. WP3 E2E Management Function developers are key stakeholders to integrate with a DetNet-only technology and administrative domain via the Domain MFs developed within this use case.	
	Standards	3GPP SA1/SA2	
KPIs Use Case	**Latency**	Human-centric data consumption: 20ms for haptic service flows, 100ms for video, 80ms for audio Machine-centric data consumption:	Taken from 3GPP's feasibility study on metaverse applications (22.856) and sensing (22.837)
	Reliability	Less than 2% packet loss at any point of time for a high MOS score Less than 1% packet loss for ML-based algorithms to generate sensing results	

	Jitter	Human-centric data consumption: Jitter for haptic <2ms, for audio & video <30ms. Furthermore, for inter-service type jitter, video must not arrive later than 20ms and audio 25ms after haptic data arrived. When video is first, haptic must arrive within 30ms and audio within 20ms. When Audio arrives first, haptic must not arrive later then 12ms and video 20ms. Machine-centric data consumption: Depending on the algorithm and how it was trained, jitter might have a significant impact on the accuracy of the ML-based results and shall not exceed the jitter inside the data set, which the ML algorithm was trained against.	Human-centric value taken from 3GPP's feasibility study on metaverse applications [12]
	Data acquisition	n/a	
Use Case Requirements	**Functional**	Sensing of the environment (~10m) and the delivery of sensing data to the network for being processed. Dedicated 6G control plane functions enable the coordination of the User Plane set-up for mobile networks. AI-driven URSP and PDRs for QoS enforcement of User Plane with domain MFs offering open programmability of the native sensing support in mobile networks within an E2E multi-domain and multi-technology set-up.	
	Non-Functional	The use case will be brought to exhibitions such as Mobile World Congress or EUCNC and must convey the innovations on MDP and AICP in a logical and convincing fashion.	

Table 13. Localisation and Sensing use case summary

6.2 XR use case.

This use case involves a distributed immersive gaming application service with XR systems' characteristics. Consider a scenario where multiple gaming sites are located at different geographical locations and cannot be commonly covered by a single Mobile Network Operator (MNO). Each local site is attached with a team of multiple players competing against all the other teams in remote locations. Through the XR technology, as the players at a particular location move around the site, they can watch and listen to what the other teams are acting in 3D scenes, and this can be overlaid by their XR headsets onto their real-world view space. The XR headsets may also display virtual objects to the scene, which are pre-built and cached in the game application system. All the local and remote players in the game session should be synchronized in receiving the live content with stringent time window so that everyone will have the immersive perception as if they were playing the game in a common physical space. In addition, given that the heavy XR content processing tasks (e.g., real-time rendering) is highly power consuming [13]; such tasks can be also completely or partially offloaded to the mobile edge depending on the current conditions of individual devices.

In the gaming application system, the XR application first processes the scene that the moving player is watching in real-time and identifies objects that will be targeted for overlay of ultra-high-resolution videos. It then generates high-resolution 3D images scenes related to the perspective of the player in real-time. These generated video images are then overlaid on the view of the real-world as seen by the player. The goal of delivering both streaming and interactive XR gaming data is to provide assured Quality of Experience (QoE) to all the users, including not only individual-based experiences but also the fairness requirements across participating teams in terms of both timeliness and quality of content delivered to user devices at different network locations.

Another important QoE requirement is to avoid motion sickness that results from a time lag between when the user moves his/her head and when the appropriate video scene is rendered. This time lag is often called "motion-to-photon" delay. Studies have shown that this delay can be tolerated at most 20ms and preferably between 7-15ms [14] [15] [16]. For providing auditory inputs to create an illusion of presence, latencies should be below 60ms (70% probability) for VR-based isolated auditory stimuli and below 38ms (70% probability) for AR-based reference tone stimuli [17]. It is worth mentioning that in the context of the PREDICT-6G project, all these requirements need to be fulfilled end-to-end across multiple autonomous, multiple technology network domains rather than covered by a single MNO.

Current cloud gaming providers such as Onlive, Gaikai, Google Stadia, GeForce Now, PS Now etc. run their game logic, GPU rendering, and video encoding modules in the public cloud (i.e., data centres towards the core of the Internet) without any SLA settlement with the local Internet connection provider on the user side. This introduces unpredictable latencies resulting in poor Quality of Experience (QoE) for the user in certain scenarios (e.g., high traffic times). This unassured QoE is a result of very strict delay threshold requirements of various game types. For example, delay thresholds for first person shooter games, role-playing games, and real-time strategy games are respectively 100ms, 500ms, and 1000ms. Indeed, 3GPP TR 26.928 document specifies that 45ms- 60ms are more accurate estimates of acceptable latency in games that are fast paced. Methods, procedures, and architectures are needed to reduce the network latencies within the best-effort service model of the current internet.

Funded by the European Union

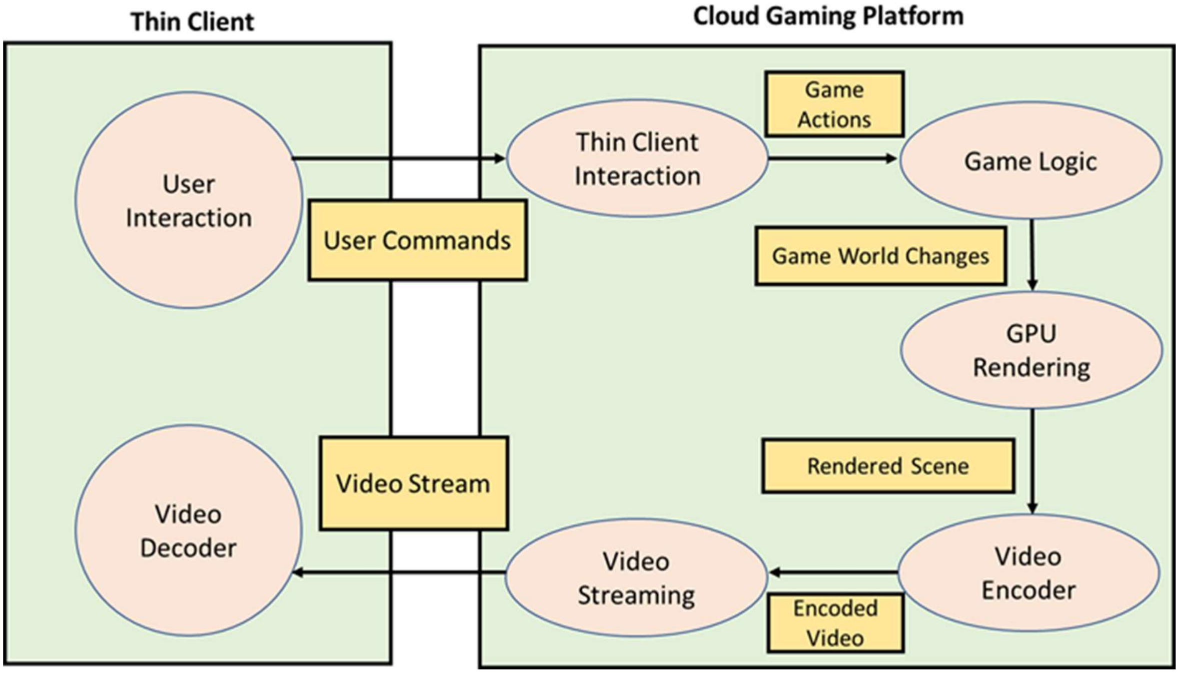

Figure 7. Typical game application architecture

The Figure 7 shows the typical game application architecture used by cloud gaming platforms. A thin client with the software components “User Interaction” and “Video Decoder” runs on the User Equipment (UE). The user’s actions in the game are captured by the “User Interaction” module and are sent as “User Commands” by the UE over a network to the cloud gaming platform running in a remote data centre. This data centre’s cloud gaming platform has a component called the “Thin Client Interaction” that receives the user commands from the client and converts them into “Game Actions”. Next, the “Game Actions” are interpreted as changes in the game world by the “Game Logic” module of the cloud gaming platform. These world changes are then converted into “Rendered Scene” by the “GPU Rendering” module. The “GPU Rendering” module then forwards the “Rendered Scene” to a “Video Encoder” which encodes (including compression) the video and sends that video to the “Video Streaming” module. Finally, the “Video Streaming” module sends the “Encoded Video” as a “Video Stream” over the network back to the thin client. This thin client’s “Video Decoder” component then decodes the video and displays it on the UE for the user.

In order to enable fully immersive experiences for end users in XR-based gaming applications regardless of where they are located, the PREDICT 6G solution will need to develop an architecture of edge-enabled application software components across multiple MNOs covering the geographical areas where players are located. This architecture will need to support technologies for scaling inter-computing systems, being able to provide native integration of AI for telecom and support an improvement in data plane performance across different network infrastructures. In addition, for the use case described above, multiple stakeholders are involved as data is being delivered between widely distributed end user locations. As previously elaborated, there are multiple dimensions of application requirements for achieving assured user QoE, including data rate, data transmission latency, motion-to-photon delay, and also real-time data synchronization among end users.

Topic	Description	XR	
		Value	Comments
Use Case Technical Components	Workloads	The parameters that capture the characteristics of XR application behaviour are heavy-tailed. Examples of such parameters include the distribution of arrival times between XR application invocation, the amount of data transferred, and the inter-arrival times of packets within a session.	Any traffic model based on such parameters are themselves heavy-tailed. Using these models to predict performance under alternative resource allocations by the network operator is challenging. For example, both uplink and downlink traffic to a UE device has parameters such as volume of XR data, burst time, and idle time that are heavy tailed
	Data Governance	Flexible governance based on user, operator and/or regulatory preferences	
	Infrastructure	Mix of specialised hardware for XR, to specialised software over COTS, to consumer electronics	
	Data & Analytics	AI/ML to process usage data and provide meaningful, but abstracted pattern to third parties within the DN or on the UE	
	Devices/Terminals	Head Mounted Devices (HMD) for AR/VR with wireless capabilities	These devices have limited battery power available to them and can get hot due to compute-intensive algorithms running on them
Further Considerations	Data sources needed to develop the use case	Head mounted Displays for AR/VR	
	Components or features not available today	Technologies to enable multi-domain multi-stakeholder reification of the use case	

	Stakeholders	Network Operators, Network equipment vendors, application and services providers	
	Standards	3GPP SA1/SA2, IETF MOPS, IETF MOQ, ETSI MEC	
KPIs Use Case	**Latency**	20ms	
	Reliability	High	
	Jitter	Quasi-periodic arrival jitter of at most 5ms	Packets arrive at the network with slightly irregular small offsets from the average interval of arrivals. This is caused by delay variations in application encoding and transport networks
	Packet Loss	Low- less than 2%	
	Data acquisition	N.A.	
Use Case Requirements	**Functional**	All the local and remote players in the game session should be synchronized in receiving the live content with stringent time window Tasks need to be completely offloaded to edge to save battery and prevent over-heating of HMDs Should be able to deliver both streaming and interactive data	
	Non-Functional	Fairness requirements across participating teams in terms of both timeliness and quality of content delivered to user devices at different network locations. To support technologies for scaling inter-computing systems, Being able to provide native integration of AI for telecom, Support an improvement in data plane performance across different network infrastructures.	

Table 14. XR use case summary

6.3 IETF RAW and DetNet use cases

The IETF DetNet group focuses on deterministic networking, which refers to the ability to provide guaranteed delivery of data with low latency and jitter. The group's main objectives are to document deployment environments and types of topologies within the scope of the DetNet architecture, and to identify DetNet Controller Plane approaches that reuse existing IETF solutions. The DetNet use cases include industrial applications, pro-audio and video, and latency-aware applications in different sectors. The group's work is independent from any path setup protocol or mechanism, and documents produced by the group are compatible with the work done in IEEE802.1 TSN and other IETF Working Groups. DetNet excludes modifications of transport protocols, OAM (Operations and Management), Layer 3 forwarding, and encapsulations, but it may discuss requirements for such modifications and coordinate with the Working Group responsible for the technology.

DetNet ensures deterministic data paths by providing guaranteed delivery of data with low latency and jitter. Here are some ways DetNet achieves this:

- DetNet operates over Layer 2 bridged and Layer 3 routed segments, where such paths can provide bounds on latency, packet loss, and packet delay variation (jitter), and high reliability [18] [19].
- DetNet uses a Software-Defined Networking layer to provide IntServ and DiffServ integration, and delivers service over lower Layer 2 bridged segments using technologies such as MPLS and IEEE 802.1 Time-Sensitive Networking [20] [21].
- DetNet aims to migrate time-critical, high-reliability industrial control and audio-video applications from special-purpose Fieldbus/Real Time Ethernet networks to packet networks and the IP in particular [20].
- DetNet provides a capability for the delivery of data flows with extremely low data loss rates, packet delay variation (jitter), and bounded latency, such as audio and video streaming, industrial automation, and vehicle control [20] [22].
- DetNet excludes modifications of transport protocols, OAM, Layer 3 forwarding, and encapsulations, but it may discuss requirements for such modifications and coordinate with the Working Group responsible for the technology.

DetNet mainly deals with wired environments. Its wireless counterpart is the IETF RAW group. The IETF RAW (Reliable and Available Wireless) group is focused on providing high reliability and availability for IP connectivity across any combination of wired and wireless network segments. The group's main objectives are to develop a set of use cases for RAW, to define the architecture and technologies needed to support RAW, and to provide OAM (Operations, Administration, and Maintenance) features for RAW. The RAW use cases include industrial automation, vehicular communication, and wireless backhaul. The RAW architecture aims to provide a framework for deterministic networking and to support a variety of wireless technologies, such as IEEE 802.11, 802.15.4, and 5G. The RAW group's work is related to IETF work done in other working groups, such as DetNet and 6TiSCH.

The RAW group is focused on providing high reliability and availability for IP connectivity across any combination of wired and wireless network segments. Here are some of the key technologies developed by the RAW group:

- RAW provides deterministic networking in networking environments where at least some segments of the network are wireless [6].
- RAW defines an architecture that provides for high reliability and availability for IP connectivity across any combination of wired and wireless network segments [7].
- RAW provides OAM features for high-reliability wireless networks [23].
- RAW aims to support a variety of wireless technologies, such as IEEE 802.11, 802.15.4, and 5G [2].

Currently the DetNet and RAW WGs are discussing the possibility of merging in a single group, due to all their synergies.

In the following table, we present a summary of the use cases defined in the different requirement documents.

No.	Use Cases	Specifics	KPIs	Requirements
1	Aeronautical Communications	-analogue voice is replaced by digital data communication. -supports the related trend towards increased autonomous data processing that the Future Communications Infrastructure (FCI) in civil aviation must provide.	-High bandwidth communication, -high reliability, - robustness, -latency	-**Overhead** needs to be kept at a minimum since aeronautical data links provide comparatively small data rates in the order of Kbit/s. -**Different safety levels** need to be supported, from extremely safety critical ones requiring low latency, such as a WAKE warning – - And **high resiliency**, to less safety critical ones requiring low-medium latency for services such as WXGRAPH - graphical weather data. -**Policy** needs to be supported when selecting data links--minimize the amount of routing information -**End-to-end mechanisms** can be applied to guarantee bounded latency where needed. -non latency critical

2	Amusement Parks	-Local area-sensors and actuators -Wearable mobile devices (exchange traffic locally (identification, personalization, multimedia) or globally (billing, child tracking)) -Computationally intensive applications. Edge (real-time apps) cloud (predictive maintenance, marketing)	-(Sensors and actuators) require bounded latencies < 10ms, -there are other applications as well that mostly demand reliability (e.g., safety related, or maintenance).	-The network infrastructure must support **heterogeneous traffic.** - The **transmissions must be scheduled** appropriately even in presence of mobile devices. **- IP enabled technology** is required to interconnect large areas, independent of the PHY and MAC layers. - need to **provide layer-3 mechanisms** able to exploit multiple co-interfering technologies. -Maintenance applications are non-latency critical
3	Wireless for Industrial Applications	-Control loops (factory automation) -Unmeasured data (monitoring & diagnostics)	-Reliable and scalable communication, -bounded latency, -jitter, packet loss, -manufacturer cost	-RAW mechanisms should be able to **setup a Track over** a wireless access segment and a wired or wireless backbone to report both sensor data and **critical monitoring** within a bounded latency. -**maintain the scalability and high reliability** of the flows over time. -It is also important to **ensure** that RAW solutions are **interoperable** with existing wireless solutions in place
4	Pro Audio and Video	-Uninterrupted stream playback (audio & video) -Synchronized stream playback (Virtual reality/ Augmented reality, CD, Blue-Ray disk mastering) - public address, media and emergency system at large venues (e.g., airports, train stations, stadium and theme parks)	-Packet loss, -delay, -bounded latency between audio and video streams -(synchronized streaming),	-Audio/video streaming applications require **low latency capability** -network infrastructure needs to support heterogeneous types of traffic (including **QoS**). -**Content delivery** with bounded (lowest possible) latency. -For synchronized streaming, **latency** must be bounded latency critical - The deployed network topology **should allow for multipath**. This will enable multiple streams to have different (and multiple) paths (tracks) through the network to **support redundancy.**

Funded by the European Union

				-However, the most critical requirement of this use-case is reliability
5	Wireless gaming	-Real-time mobile gaming (sensitive to network latency and stability, E2E latency) -Wireless console gaming (wired or Wi-Fi 5) -Cloud gaming (requires low latency capability, user devices might likely be connected wirelessly)	-Intra BSS Latency < 5ms -Jitter variance <2ms -Packet loss <0.1 %	-***Time sensitive networking extension:*** such as time aware shaping and redundancy (FRE) can be explored to address congestion and reliability problems present in wireless networks. - ***Priority tagging (stream identification):*** to provide better QoS for time-sensitive traffic is the capability to identify and differentiate time-sensitive packets from other (like best effort) traffic. - ***Time-aware shaping:*** eliminating congestion and ensuring that frames are delivered within the expected latency bounds. -***Dual/multiple link***: to improve latency stability -**Admission control** **-Reliability**
6	Unmanned Aerial Vehicles (UAVs) and Vehicle-to-Vehicle Platooning and Control	-aerial surveillance activities, traffic monitoring - emergency, transportation (e.g., medicine in rural areas) -*Cellular connectivity* (with control center, for remote manoeuvring as well as monitoring of the drone) - *IEEE 802.11* (for inter-drone communications (i.e., platooning))	-Latency, -bandwidth, -Jitter, -reliability	- **Requiring self-configuration** capabilities. - **Heterogeneous types of traffic** need to be supported, from extremely critical ones requiring **ultra-low latency and high resiliency,** to traffic requiring low-medium latency. - due to ultra-low latency communication offloading, the critical requirement is **reliability**, - And only for some platooning and inter-drone communications, latency is critical.
7	Edge Robotics control	-interconnected via an access network to the edge device or data center. - Multiple robots are simultaneously instructed to perform individual tasks -decomposition of a service on a small function -	-Ultra-low Latency -Bandwidth -Jitter	-Requiring **low latency** between robot and control intelligence reside - needs to support **heterogeneous types of traffic**, from robot control to video streaming. -combine **multiple communication flows** with some of them being latency critical

		distributed and chained among robots		- But some of communication flows (like some offloading tasks) that only demand **reliability and availability.**
8	Emergencies: Instrumented emergency vehicle	- Special purpose telemetering system for medical data (vital signs sensors) - radio-navigation sensor to relay position data to various destinations including dispatcher -Voice communication between driver and dispatcher or for ambulance attendant - Destinations might be either at the ambulance itself (local traffic), at a near edge cloud or at the general Internet/cloud.	-Reliability, -Latency, -availability	-Required **High availability** of the inter-network -Inter-network needs to operate in **damaged state** (e.g., during an earthquake aftermath, heavy weather, wildfire, etc.). -In addition to continuity of operations, **rapid restore** is a needed characteristic. **- E2E security**, both authenticity and confidentiality, is required of traffic. All data needs to be authenticated; some like medical needs to **be confidential**. -The radio-WAN has characteristics similar to cell phone -- the vehicle will travel from one radio footprint to another

Table 15. Summary of DetNet and RAM use cases

7 Traffic model methodology and characterization

This section focuses on providing an initial traffic characterization of the different flows related to the identified use cases. The intention is to understand on the one hand the number and characteristics of the flows that every application generates, and on the other, to understand the requirements for each of these flows.

In a second step, we plan to carry out real traffic captures and verify that the flows follow the characterization described in this document in the ideal scenario, I.e., where no networking devices connect the different actors of the flows. Armed with such captures, traffic flows will be modelled, so they can be used for different purposes, including traffic generation for simulation and machine learning training purposes.

7.1 Methodology

The traffic model methodology has been defined in several steps to be carried out for the three main use cases defined in Section 5:

1) Identification and definition of traffic flows. For each traffic flow, the following characteristics need to be defined:
   a. Involved actors, e.g., Controller, Robot1
   b. Direction, e.g., Controller -> Robot1
   c. Transported data, e.g., control commands from the controller to the robot
   d. Expected behaviour, e.g., 1 packet with XXX bytes every xms
   e. Flow class: e.g., TSN
   f. some other useful info
   g. MAC/IP/port of each actor
2) Traffic captures. Captures are carried out using Wireshark. The traffic should be captured in an intermediate network node between the source and destination of the flow. The length of the capture should be enough to include at least 10.000 packets/frames for each of the flows.
3) Capture and flow characteristics validation. A tool that extracts a number of random variables from the captures has been developed, so the characteristics defined for the flow can be checked. For each flow, the following variables are considered:
   a. Packet size (PS)
   b. Inter-packet time (IPT)
   c. Burst size (BS)
   d. Inter-burst time (IBT)
4) Traffic modelling. Random variables will be used to model the flows as statistical distributions.

7.2 Identification and definition of traffic flows

Use Case: Smart Manufacturing

Flow1: Send	**Involved actors**, Program Line Control (PLC), Robot Controller **Direction**, PLC -> Robot Controller **Transported data**, Programming blocks from the PLC to the robot controller **Expected behaviour**, 2x704 words (1 word = 2 bytes) by PLC cycle scan (10 ms) **Flow class**: TSN
	Filtering for the flow: Controller MAC/IP/port: TBD Robot1 MAC/IP/port: TBD
Flow2: Receive	**Involved actors**, Program Line Control (PLC), Robot Controller **Direction**, Robot Controller -> PLC **Transported data**, Programming blocks from the PLC to the robot controller **Expected behaviour**, 2x704 words (1 word = 2 bytes) by PLC cycle scan (10 ms)

	Flow class: TSN
	Filtering for the flow: Controller MAC/IP/port: TBD Robot1 MAC/IP/port: TBD

Table 16. Definition flow Smart Factory use case

Use Case: Deterministic services for critical communications

Use Case: **Sensor data collection and machine control**	
Multiple sensors attached to machines producing measurement data to be collected at a cloud compute host for real time analytics, with potential reverse command sent to the machines.	
Flow1: Measurement	**Involved actors**, sensors, cloud **Direction**, sensor -> cloud **Transported data**, measurements **Expected behaviour**, 200 KB/sec in 20 ms batches (4KB per batch) **Flow class**: time sensitive, deterministic
	Filtering for the flow: Controller MAC/IP/port: TBD Robot1 MAC/IP/port: TBD
Flow2: Control	**Involved actors**, cloud, machine **Direction**, cloud -> machine **Transported data**, control **Expected behaviour**, small data with urgency **Flow class**: low latency, ultra-reliable
	Filtering for the flow: Controller MAC/IP/port: TBD Robot1 MAC/IP/port: TBD

Table 17. Definition flow deterministic services for critical communications use case

Use Case: **Group communication**
Multiple devices connected into the same virtual scene/session, synchronizing their status with each other in real time. Communication is enabled via a rendezvous point that receives data from multiple devices; identifies target devices per received data unit; performs data replication and transfer to target devices.

Flow1: state transfer	**Involved actors**, multiple devices, rendezvous point **Direction**, device -> rendezvous point **Transported data**, device state **Expected behaviour**, state message between 1-4 KB sent periodically with 1-10 Hz **Flow class**: time sensitive, deterministic
	Filtering for the flow: Controller MAC/IP/port: TBD Robot1 MAC/IP/port: TBD
Flow2: state receipt	**Involved actors**, rendezvous point, multiple devices **Direction**, rendezvous point -> device **Transported data**, state message (multiple replicas of uplink data units – number of replicas is dynamically computed based on the current physical and virtual context/relation of the devices) **Expected behaviour**, replica of state messages **Flow class**: time sensitive, deterministic
	Filtering for the flow: Controller MAC/IP/port: TBD Robot1 MAC/IP/port: TBD

Table 18. Definition flow group communication use case

Use Case: Camera sharing	
A device sharing its video stream with one or more other devices in real time. Communication is enabled via a rendezvous point that configures the sending device to start streaming its video; receives the video stream from the sending device; replicates the video stream towards receiving devices (if there are multiple ones); transfers the video stream to the target device(s). There may be multiple video streaming devices in a system simultaneously; video streaming starts/ends dynamically (based on explicit requests as well as current physical and virtual context/relation of the devices).	
Flow1: video transfer	**Involved actors**, multiple devices, rendezvous point **Direction**, device -> rendezvous point **Transported data**, video stream **Expected behaviour**, depending on the video codec, 0.5-2 Mbit/s video stream **Flow class**: time sensitive, deterministic
	Filtering for the flow: Controller MAC/IP/port: dynamic Robot1 MAC/IP/port: dynamic

Flow2: video receipt	**Involved actors**, rendezvous point, multiple devices **Direction**, rendezvous point -> device **Transported data**, video stream (multiple replicas of uplink video stream – number of stream replica is dynamically computed based on the current physical and virtual context/relation of the devices) **Expected behaviour**, replica video stream **Flow class**: time sensitive, deterministic
	Filtering for the flow: Controller MAC/IP/port: TBD Robot1 MAC/IP/port: TBD

Table 19. Definition flow camera sharing use case

Use Case: Multi-domain deterministic communication

In this use case, currently we have two main actors with one-to-one mapping: 1) Robot as a physical object and 2) virtual object that contains all the algorithms for optimizing the performance of the physical object. The robot can have multiple actors in the form of sensors (e.g., LIDAR, camera, robot odometry) and the virtual object can have multiple actors in the form of algorithms that can consume the sensor information in order to update the virtual model of the robot, perform simulations to predict the behaviour. In this use case we have two main classifications of the traffic: • DL traffic (from the virtual object to the physical object (e.g., robot)) • UL traffic (from the physical object to the virtual object) For the DL traffic we usually have a single flow that is time sensitive (TSN class) with strict KPIs and this flow is used for the virtual object to control and navigate the physical object. For UL traffic we have a single flow is send form the robot to the virtual object to update the state of the virtual object in real time.	
Flow1: Update flow	**Involved actors: Robot, Virtual Object** **Direction: Robot -> Virtual Object** **Transported data**: Robot joint states that are send from the Robot to the virtual object. **Expected behaviour**: 1 TCP packet every 80ms (need to check the frequency and the size of the packet) **Flow class: Sensitive**
	Filtering for the flow: This is difficult to identify for this use case since it is implemented with ROS1 and ROS1 opens MAC ports randomly for every traffic flow. Controller MAC/IP/port: random Robot1 MAC/IP/port: random
Flow2: Control flow	**Involved actors: Robot, Virtual Object** **Direction: Virtual Object -> Robot** **Transported data**: Robot control commands that are send from the Virtual object to the robot. **Expected behaviour**: 1 TCP packet every 2ms (need to verify the frequency and the size of the packet) **Flow class: TSN**

	Filtering for the flow: This is difficult to identify for this use case since it is implemented with ROS1 and ROS1 opens MAC ports randomly for every traffic flow. Controller MAC/IP/port: random Robot1 MAC/IP/port: random

Table 20. Definition flow Digital Twin use case

8 System level requirements

This section collects system level requirements of the PREDICT-6G system, considering the use cases, traffic characteristics and the overall scope of providing e2e deterministic services across multiple technology domains.

Clock synchronization

The PREDICT-6G system should maintain clock synchronization across all technology domains and all User/Control/Management-planes. The synchronization should be robust against single point of failures and should provide built-in protection against the synchronization-driven security attacks.

Service ingestion and assurance

The PREDICT-6G system should be able to receive requests for end-to-end deterministic services with specific QoS parameters, where service endpoints may be in multiple technology domains.

The PREDICT-6G system should perform request validation (check conflict against system and domain capabilities) and admission control (check conflict against resources) for new service requests. Conflicts should be resolved, if possible, without rejecting the service request.

The PREDICT-6G system should autonomously create, fulfil and assure the service QoS parameters using a combination of end-to-end and domain-specific management and control actions.

User plane capabilities

The PREDICT-6G system should be able to separate flows in the U-plane with different QoS requirements to ensure specific treatments per flow or flow aggregate.

The PREDICT-6G system should be able to monitor and report its own state related to topology (service endpoints), deterministic capabilities, resources, capacities, load, real-time KPIs; both per domain and in end-to-end.

The PREDICT-6G system should provide cross-domain packet level mechanisms to ensure availability, reliability and packet loss targets.

The PREDICT-6G system should provide cross-domain service continuity on the border of multiple technology domains.

The PREDICT-6G system should provide means to identify flows of the same service across domains.

The PREDICT-6G system should preserve the order of packets in the e2e service flows.

The PREDICT-6G system should leverage existing technology specific domain capabilities to ensure deterministic services within each domain and in end-to-end.

The PREDICT-6G system should enable the integration of devices and domains with no built-in support for determinism.

Control and management capabilities

The deployment of the PREDICT-6G system should flexibly support different sets of technology domains, without pre-configured assumptions on the type of technologies, their topologies, resources and capabilities; the PREDICT-6G system should discover these in runtime.

The PREDICT-6G system should autonomously break down end-to-end service requests into domain specific service segments and provide the right parameterization for each service segment.

The PREDICT-6G system should have closed-loop mechanisms per domain and in the e2e context to autonomously fulfil domain specific service segments and e2e services.

The PREDICT-6G system should have predictive mechanisms to take proactive actions (e.g., re-configuration of domain level service segments, or re-balancing the e2e service requirements among the domains) that prevent e2e service degradation.

The PREDICT-6G system should profile and assess the deterministic capabilities of the different technology domains (including those with no built-in determinism support) and use it to validate/admit new services and drive closed-loop service assurance decisions.

9 Initial insights on architectural matters based on the use cases and the elicited requirements

The PREDICT-6G system provides deterministic services over multiple inter-connected domains and technologies, including 3GPP, IETF DetNet, IEEE TSN, Wi-Fi7 and potential others. End-to-end services in this context mean to interconnect devices that are attached to different networks; as an example, between a UE in a 3GPP network and a mobile station attached to a WiFi AP, where the two systems are connected through a third DetNet/IP network.

In PREDICT-6G, deterministic means reliability, time sensitivity and predictability. Reliability may be broken down to availability, low packet loss and failure resiliency; time sensitiveness is comprised of bounded latency and low jitter. Predictability refers to the system's ability to have insight to current and predicted states of its network/domain/e2e state, including its deterministic capabilities, topology, available resources, load, demand, etc.; and proactively initiate reconfiguration actions to assure each requested e2e deterministic service. Any e2e service may require only a subset of the total set of PREDICT-6G deterministic capabilities (e.g., require low jitter but not low latency); however, the PREDICT-6G system itself must be in principle able to sustain multiple e2e services with different deterministic requirements simultaneously (of course subject to resource availability and domain capability).

The PREDICT-6G system architecture is defined to support the above general concepts and requirements. The architecture leverages the separation of planes (such as user- and control-/management-planes) and a modular design that supports the extension to new technology domains without impact on already integrated ones. The overall PREDICT-6G system architecture is depicted in Figure 8. The architecture has two planes:

1. Multi-Domain Data Plane (MDP): providing integration, abstraction and programmable exposure of multiple U-plane mechanisms (with different levels of intrinsic deterministic capabilities);
2. AI-driven Multi-stakeholder Inter-domain Control-Plane (AICP): AI/DT based C/M-plane mechanisms with autonomous orchestration and assurance of e2e deterministic services.

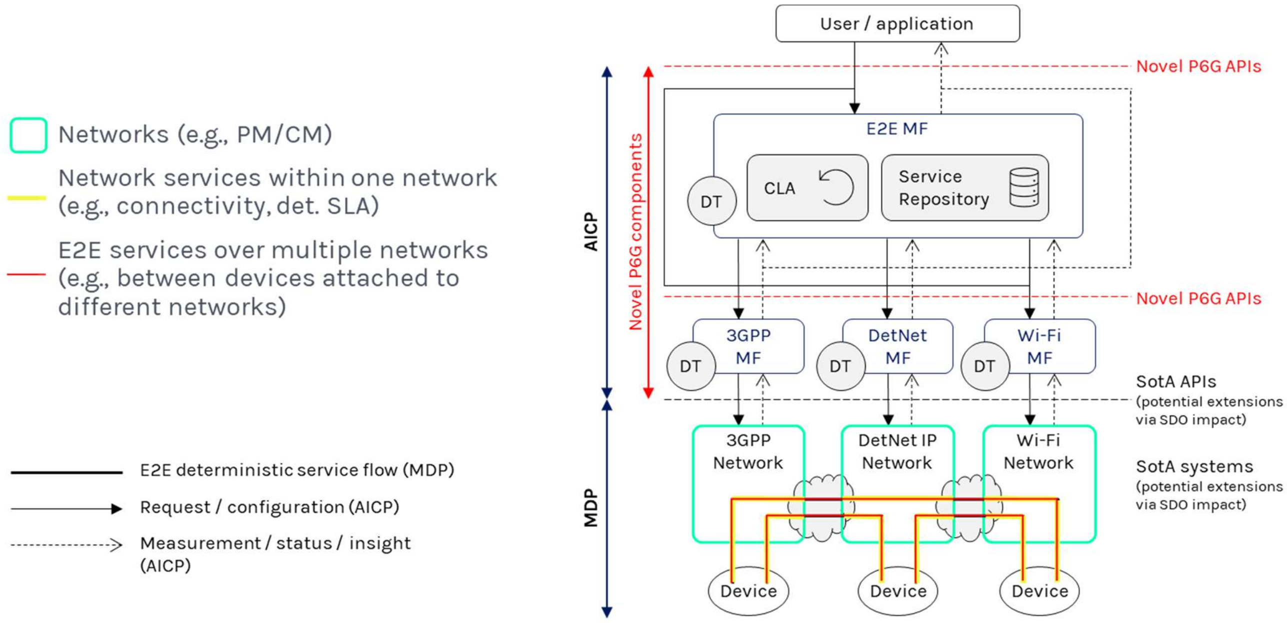
Networks (e.g., PM/CM)
Network services within one network (e.g., connectivity, det. SLA)
E2E services over multiple networks (e.g., between devices attached to different networks)
E2E deterministic service flow (MDP)
Request / configuration (AICP)
Measurement / status / insight (AICP)
User / application
Novel P6G APIs
AICP
Novel P6G components
E2E MF
DT
CLA
Service Repository
Novel P6G APIs
3GPP MF
DT
DetNet MF
DT
Wi-Fi MF
DT
SotA APIs (potential extensions via SDO impact)
MDP
3GPP Network
DetNet IP Network
Wi-Fi Network
SotA systems (potential extensions via SDO impact)
Device
Device
Device

Figure 8. Overview of the PREDICT-6G system architecture focusing on the AICP

PREDICT-6G integrates networks of different technologies at the service level to provide multi-domain e2e deterministic communication services. To achieve e2e service assurance, the PREDICT-6G AICP manages three types of entities:

- Networks (of different technologies): management on this level includes interaction with the network's configuration management (CM), performance management (PM), failure management (FM); the collection of network capabilities, topology, resource status, measurements, and insights from the network segments.
- Network services (within one network): creation, parameterization, modification, and termination of services within the boundaries of one domain (of a specific technology).
- E2e services (over multiple networks): composition of the PREDICT-6G e2e deterministic services by integrating multiple domain specific services.

The PREDICT-6G AICP has an architecture where domain specific management functions (MF) are responsible for network and service management in their specific domain, and an E2E MF is responsible for the composition and assurance of e2e services from domain specific services. The consumers of the PREDICT-6G system (users, applications, end devices) may request e2e deterministic services from the E2E MF; the E2E MF uses the capabilities and services of domain specific MFs to compose and assure e2e services from the individual services of the respective domains; the domain specific MFs use the capabilities of their managed domain's technology to deliver service segments within the boundaries of their domain. Domain specific MFs provide a uniform presentation of their domain's capabilities and services towards the E2E MF (i.e., APIs between the domain specific MFs and the E2E MF are technology-agnostic); while they are using state-of-the-art technology specific APIs (such as the N-bound APIs of network/domain controllers) to exercise control over the network and services within their own technology domain. New domains may be added by defining a domain specific MF that leverages the technology of the new domain to create and manage services within that domain and report a more uniform presentation of the domain towards the E2E MF.

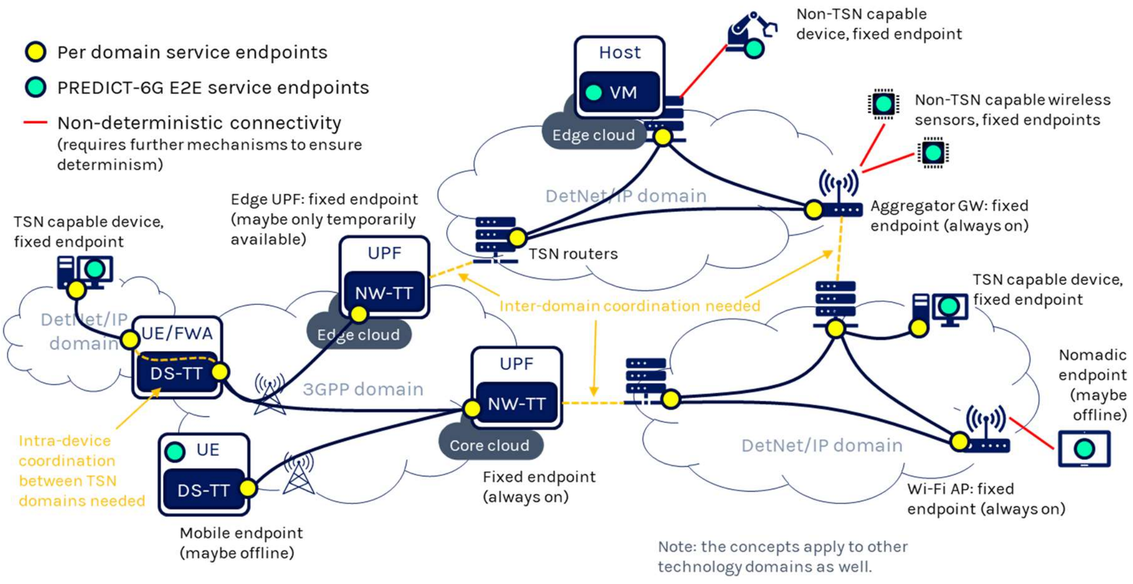
Per domain service endpoints
PREDICT-6G E2E service endpoints
Non-deterministic connectivity
(requires further mechanisms to ensure determinism)
Host
VM
Edge cloud
Non-TSN capable device, fixed endpoint
Non-TSN capable wireless sensors, fixed endpoints
DetNet/IP domain
Aggregator GW: fixed endpoint (always on)
TSN routers
Edge UPF: fixed endpoint (maybe only temporarily available)
UPF
NW-TT
Edge cloud
TSN capable device, fixed endpoint
DetNet/IP domain
UE/FWA
DS-TT
Inter-domain coordination needed
3GPP domain
UPF
NW-TT
Core cloud
TSN capable device, fixed endpoint
Nomadic endpoint (maybe offline)
DetNet/IP domain
Intra-device coordination between TSN domains needed
UE
DS-TT
Mobile endpoint (maybe offline)
Fixed endpoint (always on)
Wi-Fi AP: fixed endpoint (always on)
Note: the concepts apply to other technology domains as well.

Figure 9. PREDICT-6G MDP architecture components

The architecture of e2e services on the PREDICT-6G MDP is composed of two levels as depicted in Figure 9:

1. The services within a domain's boundary are spanning between per domain service endpoints that are within the same domain.
2. The PREDICT-6G e2e services are defined between e2e service endpoints that may be in different domains.

The e2e service is composed by chaining domain specific services, with inter-domain coordination between domains and at domain boundaries. Coordination is exercised through multiple mechanisms:

1. Cross-domain flow harmonization: the granularity of QoS control in general and Time Sensitive Communication (TSC) varies across technologies. Providing e2e deterministic services for a set of e2e flows (e.g., IP flows) across multiple technology domains requires that each domain be configured to recognize and treat the same set of packets with specific deterministic requirements.
2. Service configuration harmonization: the parameterization of each domain's service is done so that the U-plane mechanisms (e.g., delay sensitive scheduling) are set up at different domains in a synchronized and complementary manner. For example, if there is an e2e delay or jitter target, the delay sensitive schedulers (or equivalent QoS mechanisms) in each domain should be configured in a way that the domain level targets and the realized delay/jitter values together support the e2e targets.
3. Distributed TSC mechanisms: packet replication, elimination, and ordering functionality (PREOF), hold-and-forward, etc., which are originally defined per domain, should be distributed, and synchronized across multiple domains. For example, E2E PREOF requires that replication and elimination functionality be put in different domains of different technologies, therefore domain specific technologies needed to be capable of activating only part of their PREOF functionality and apply them to the same set of packets (see cross-domain flow harmonization). De-jittering or enforcing on-time packet delivery through hold and forward mechanisms also requires coordination between domains.

Besides cross-domain coordination, the MDP also needs to handle links or entire network segments with no intrinsic deterministic capability. Link level lack of determinism is anticipated whenever PREDICT-6G e2e service endpoint is a legacy device (such as sensors, robots, industrial devices, embedded computers) with no determinism support in its network stack (or, in some cases, no support for any open programmable/controllable network stack whatsoever). Still, the PREDICT-6G consumer's intention is to define deterministic service between such devices and, e.g., a data collection and analytics service running at an edge cloud, therefore the MDP should be extended to handle such devices and links as well. Network segments with no integrated determinism support (e.g., a pure IP or Ethernet network) may also be present (and unavoidable) between e2e service endpoints without APIs to explicitly control them (or even without the ability to explicitly define any services over them). The aim of PREDICT-6G is to still be able to leverage the intrinsic capabilities of such network segment to the extent that is permitted by their capacity, resources, and intrinsic U-plane mechanisms; those however should be inferred based on measurements, analytics, admission control and ingress/egress traffic management delegated to the adjacent domain's boundaries.

10 Initial insights on security matters

This section provides a thorough analysis regarding the threats that could exist and be triggered in a type of PREDICT-6G mobile network, I.e. multi-domain, technology and deterministic time sensitive network. To this end, the tables below are grouped into two parts: one to list the threats in case of multi-domain and technology and the second in case of deterministic and time sensitive networks. Both tables provide the threat, the cause, and the mitigation descriptions. Notably, the mitigation is subject of further investigation within the WP1 and T1.3 in particular, where corresponding solutions is expected to be specified.

Multi-domain and technology threat analysis

Threat analysis	Cause	Mitigation
Detected incidents reports are shared across domains to enable common defence actions e.g., against distributed-denial-of-service attacks.	Distributed denial-of-service attacks.	To investigate different anomaly detection strategies with focus on resource allocation and mobility-oriented attacks as well as low-rate DDoS.
Application data flowing through the network can be analysed in detail when packet traces (header and payload data from different protocol layers) are available.	Encryption prevents such inspections anywhere other than in the originating and destination domains.	IPSec version for 6G.
Programmability of network services.	The administrator may introduce complex rules and programs for the control layer, which are then consistently executed in the data plane.	To improve the detection accuracy, the parameters to detect the attack, e.g., threshold can be defined by a server or SDN controller based on a global view of the traffic, while the traffic analysis can be performed in the network elements.
Security adaptation and control mechanisms.	Security adaptation mechanisms change the behaviour of 5G networks and security control mechanisms based on inferred knowledge on risks and trust levels	AI technologies claimed to detect security risks in advanced computing in details.
Micro-segmentation enabler facilitates creation and control of slices. It organizes and isolates network traffic flows.	The enabler is a software component that uses a virtualization platform, access control functions, and an SDN controller to create slices, manage, and adapt traffic flows.	Each slice can be architected to separate the enterprise's control and user traffic while providing the opportunity for tailored security to match the use case. Slice-specific

		mutual authentication ensures that only authorized devices have access to the slice.
The Trust Level Agreement (TLA) mechanism and Trust Metric Enabler facilitate knowledge exchange across administrative domains.	The TLA enables the orchestration of end-to-end trustworthy slices.	Trust Level Agreement messaging-The framework aggregates, filters, and brokers of security information between domains.
The system allows devices to authenticate directly with the home network using.	A standard authentication and key agreement (AKA) protocol.	Taking this in view, we propose a cost-effective scheme that provides all the security features including perfect forward secrecy.
Service-based Security Architecture in 5G is upgraded into End-to-End service-based and Policy-based security architecture in 6G.	6G will take this feature to a new level, End-to-End Service-based Architecture or even Policy-based architecture domain security, to satisfy the personalization and micro-deployment flexibility.	TLS must be deployed and used. The TLS certificates should indicate the actual SBA node type.
In Identity-based cryptography (IBC), a trusted party named Key Generation Center (KGC) is responsible for creating the private key based on the identity of an entity. This mechanism is widely used in a closed domain, where an administrator has full control of the devices in the domain.	IBC cannot be directly used for cross-domain device authentication, as one-domain lacks of control of devices in another domain due to the peering relationship among domains.	Consortium blockchain can be exploited to construct trust among different domains, where each domain has a representative node responsible for maintaining the global ledger.

Table 21. Multi-domain and technology threat analysis

Time sensitive and deterministic threat analysis

Threat	Cause	Mitigation
An attack can compromise the service of applications that are sensitive to high delays or to high delay variation.	An attacker can maliciously cause delay (Delay Attack) to DetNet data flow traffic.	Using a performance monitoring system to validate that timing guarantees are being met and to detect timing violations or other anomalies and forward simultaneously DetNet flow over multiple paths, using Path redundancy.
DetNet Flow Modification or Spoofing can cause DetNet flow resource allocation unable to guarantee the performance that is presumed when the flow identification works properly.	An attacker can modify header fields of end route packets in a way that causes the DetNet flow identification mechanisms to misclassify the flow or can inject traffic that is tailored to appear as if it belongs to a legitimate DetNet flow.	Implementing Integrity Protection to detect modified packet headers, with Message Authentication Code (MAC) combined with a secret key, DetNet Node authentication and Path redundancy can verify the identity of nodes and enable the mitigation of DetNet Flow Modification or Spoofing attacks.
Increased resource consumption, data disruption, non-deterministic delay, increased impacts of other attacks and enabling other attacks by increased Attack Surface.	An attacker can manipulate the Path Choice (Path Choice attack) by modifying or injecting Control or Signalling Packets in order to disrupt or manipulate the DetNet path/resource allocation while augmenting impacts of other attacks and enabling other attacks by increasing the Attack Surface.	Protect the signalling and control messages with the use of encryption, authentication, and integrity-protection mechanisms.

Danger of leaked information about end route DetNet flows that can be used to invoke other attacks on some or all of the flows.	An eavesdropper by identifying DetNet flows and then gathering important information about end route DetNet flows, e.g., the number of DetNet flows, their bandwidths, which nodes are communicating with which other nodes, including when, how often, and with how much data, or other temporal or statistical properties, and correlating the timing of packets with external events such as action of an external device their schedules (Reconnaissance attacks).	Masking observable, by attackers, transmission patterns in the flows and regularize the timing of packet transmission by using Synthetic Traffic Insertion. Preventing the attacker from accessing the packet header or contents using encryption.
Exhausted network resources, increased resource consumption and data disruption by injected traffic that shares resources with DetNet packets to cause them to be dropped or delayed.	Due to implementation constraints, some resources may potentially be partially shared, and an attacker may try to exploit this property by injecting traffic that may be part of DetNet flows or non-DetNet traffic (Resource Segmentation, Inter-segment Attack) or overloading the exception path queue on a router.	Using Path Redundancy and a monitoring system, that incorporates Dynamic Performance Analytics, and it detects unexpected behaviours, and then cause the proper actions to be initiated to address the situation in an appropriate and timely manner, either at the data plane or controller plane or both in concert.
Danger of Packet Replication and Elimination when an attacker can cause excess consumption of resources, add extra delay to the system and increase the Attack Surface because packets headers are maliciously manipulated.	An attacker manipulates the replication-related header fields, by changing the SN (Sequence Numbers) of the packets and forwarding both replicas of a packet (similar to a replay attack), eliminating both replicas and compromising some of the advantage of Path Redundancy, hijacking the DetNet flow and causing packets to be dropped and being replaced with malicious packets, injecting packets in a flow that is to be replicated and having the attack amplified because of the replication process.	DetNet node authentication and Integrity protection. (encryption)
Non-deterministic delay, increased resource consumption, data disruption.	An attacker may try to specifically attack the Time Synchronization mechanisms of the synchronization protocol, thus affecting the DetNet service.	Implementing Path redundancy, Control message protection and a monitoring system that incorporates Dynamic Performance Analytics can enforce mitigation against attacks to Time Synchronization mechanisms.
Network and system exploitation and tampering by abusing Type Length Value(TLV) frames, used for management purposes in a Time Sensitive Network that uses Precision Time Protocol, in Industrial network scenarios.	An attacker can exploit TLVs to reconfigure, manipulate, or shut down time synchronization, by de-synchronizing the clocks, through a Reconnaissance attack.	Preventing attacks by making the exchange of TLVs more secure by implementing TLV encryption, using symmetric encryption with shared keys or asymmetric encryption enabled by a public key infrastructure and thus, also eliminating vulnerabilities to dictionary or brute-force attacks. Also, detecting attacks by continuous monitoring of all the TSN assets that contribute toward time synchronization a baseline can be established and

		any outliers like time drifts of greater than a few microseconds, sudden time jumps in the leader clock, or sudden clock frequency changes, falling outside the monitored baseline could then be detected using conventional statistical methods or the latest modelling techniques by using AI/ ML.
In an automotive scenario, an attacker may acquire the ability to know about the network schedule and the content of the streams on the network, can control (block, delay, replay) frames which are routed through the switch the attacker controls, can attempt to masquerade as another End System the attacker does not control by faking the source address of streams the attacker sends, has access to the key material in the End System they control, can flood the network with many frames.	In automotive scenario an attacker is capable of gaining access to some End Systems or switches in a system that uses TSN, e.g. through an external gateway or physical access to our nodes.	The combination of TESLA (Timed Efficient Stream Loss-Tolerant Authentication), Constraint Programming and TSN protocol features (e.g., authentication, scheduling and filtering) can prevent such attacks.
AI model output is used as-is for further analysis, insight creation, orientation, decision making or action, without sanity checking or validation.	AI models susceptible to adversarial attacks or trained on a compromised data set.	The AI models should be embedded in a SW module that provide validation and sanity checking on the output (and on the input) of the models. AI training best practices (including selection and organization of training and validation data) adopted and applied within a documented and traceable workflow.

Table 22. Time sensitive and deterministic threat analysis

11 Summary of KPIs

Smart Manufacturing		
KPIs	Latency	5 ms
	Reliability	99,9999%
	Jitter	2 ms
	Data acquisition	0,5 ms
	Packet loss	Zero

Table 23. Smart Manufacturing KPIs Summary

Sensor data collection and machine control		
KPIs	Latency	Uplink: 20 ms

		Downlink: 10 ms
	Reliability	Uplink: 99,999% Downlink: 99,9999%
	Jitter	Uplink: 5 ms
	Packet loss	Zero

Table 24. Sensor data collection and machine control KPIs summary

Group communication		
KPIs	**Round-trip time**	50 ms
	Reliability	Uplink: 99,999% Downlink: 99,999%
	Packet loss	Zero

Table 25. Group communication KPIs summary

Camera sharing (special case of group communication)		
KPIs	**Round-trip time**	50 ms
	Reliability	Uplink: 99,999% Downlink: 99,999%
	Packet loss	Zero

Table 26. Camera sharing KPIs summary

Multi-domain deterministic communication		
KPIs	**Latency**	5 ms
	Reliability	99,9999%
	Jitter	2 ms
	Data acquisition	0,5 ms
	Packet loss	Zero

Table 27. Multi-domain deterministic communication KPIs summary

12 Conclusions

A definition of the KPIs has been used across the project, including the actual meaning and metric used for each of them has been described in the document. A methodology for KPIs definition has been described in section 3.1. All KPIs are defined with the same structure, with a description of the KPI, a method of measurement, units, and measure points. Seven KPIs are defined for the project, reliability (section 3.2), availability (section 3.3), packet loss (section 3.4), packet ordering (section 3.5), latency (section 3.6) and jitter (section 3.7) Also other KPIs are mention in (section 3.8). In the Appendixes (section 14.1) control KPIs have been identified to further investigation

In addition, a definition of methodology to describe and analyse the use cases has been stablished. In section 4 of the document, describes a methodology to analyze, compare and categorize the uses cases. This methodology is a standard to define requirements and contributions for each use case. Components, stakeholders, standards, or data sources have been defined in this methodology to compare the different use cases.

With this standard, a definition of the use cases to be covered by the project, indicating the different values for the different KPIs has been analyzed. Three use cases are described in section 5. These use cases cover different areas such as industrial or entertainment sectors, as well as different requirements for time-sensitiveness and determinism. Each use case has been defined and evaluated in detail, following the methodology described in section 4, indication KPIs targets and summarized in such a way to be compared with each other. Smart factory use case (section 5.1), will focus in how to remove wiring in the manufacturing process, using a deterministic network, to add flexibility and mobility to the process. Deterministic services for critical communications (section 5.2) use case, three use cases are presented, sensor data collection and machine control, group communication, camera sharing, where the operation of the end devices, cloud application and the overall end-to-end solution imposes deterministic requirements on the network and communication service that interconnects them. Finally, multi-domain deterministic communication (section 5.3), two scenarios are identified, multiple, sparse sites of industrial enterprises and distributed critical communications, where it is relevant to guarantee latency and jitter boundaries within some given values of relevance for the specific application, not necessary of extreme low values but to be contained within some precise ranges.

Additional use cases and requirements have been addressed in two key references for the multi-domain, multi-technology data plane, IETF RAW and DetNet. These use cases have been defined following the methodology described in the document, and are localisation and sensing (section 6.1), XR (section 6.2) and IETF RAW and DetNet (section 6.3), seeking for requirements that could enrich the project.

As well, a definition and characterization of traffic data for each use case have been described. In section 7.1, a methodology to characterize the traffic model has been defined. In section 7.2, traffic models for each use case are described as well as the main actors involve in these flows, following the methodology defined in previous section.

Section 8 collects system level requirements of the PREDICT-6G system, considering the use cases, traffic characteristics and the overall scope of providing e2e deterministic services across multiple technology domains. Requirements as, clock synchronization, service ingestion and assurance, user plane capabilities and control and management capabilities, that the system should profile and assess for the different technology domains (including those with no built-in determinism support) and use it to validate/admit new services and drive closed-loop service assurance decisions.

An initial description of the overall system architecture has been defined in section 9, aims to support the concepts and requirements defined in previous sections. These requirements define an architecture with two planes, user- and control-/management-planes and a modular design that supports the extension to new technology domains without impact on already integrated ones. Taking this in account can be concluded, that the system architecture must be able to leverage the intrinsic capabilities of such network segment to the extent that is permitted by their capacity, resources, and intrinsic U-plane mechanisms; those however should be inferred based on measurements, analytics, admission control and ingress/egress traffic management delegated to the adjacent domain's boundaries.

On top of that, an initial analysis of security threats for the use case has been defined in section 10. In this analysis have been characterized the threats by multi-domain and technology or by time-sensitiveness and determinism with a description of the threat, the possible cause, and the mitigation. This analysis will support the security requirements of the system.

To summarize, in this document has been described and analyze different use cases as well as a definition of the initial requirements for system, architecture and security, foundation for the rest of the WPs of the project.

13 References

[1] A. d. l. O. Delgado, “PREDICT-6G: The importance of determinism in 6G networks,” in *EuCNC 2023 - WS10 Future deterministic programmable networks for 6G*, Gotemburgo, 2023.

[2] Ashwood-Smith, “IMT 2020,” International Telecommunication Union ITU, 2016. [Online]. Available: https://www.itu.int/es/ITU-T/focusgroups/imt-2020/Pages/default.aspx.

[3] M. Tyler, "Guidelines for evaluation of radio interface technologies for IMT-2020. ITU-R M.2412-0," October 2017. [Online]. Available: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2412-2017-PDF-E.pdf.

[4] M. Tyler, “Minimum requirements related to technical performance for IMT-2020 radio interface(s),” November 2017. [Online]. Available: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf.

[5] L. Nielsen, A. Gavras, M. Dieudonne, I. Mesogiti, P. Roosipuu, D. Houatra and E. Kosmatos, “Whitepaper Beyond 5G/6G KPIs and Target Values,” 02 June 2022. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2022/06/white_paper_b5g-6g-kpis-camera-ready.pdf.

[6] Thubert P, Cavalcanti D, Vilajosana X, Schmitt C and Farkas J, "Reliable and Available Wireless Technologies," Internet Engineering Task Force. Datatracker, 12 June 2023. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-raw-technologies.

[7] P. Thubert, "Reliable and Available Wireless Architecture," Internet Engineering Task Force. Datatracker, 10 June 2023. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-raw-architecture/.

[8] Poretsky S, Perser J, Erramilli S and Khurana S, “Terminology for Benchmarking Network-layer Traffic Control Mechanisms. RFC4689,” Internet Enginneering Task Force. Datatracker, October 2006. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4689.

[9] M. Tyler, “Network performance objectives for IP-based services. ITU-T Y.1541,” International Telecomunications Union, 2011.

[10] K. Douaioui, M. Fri, C. Mabroukki and S. E. A., “The interaction between industry 4.0 and smart logistics: concepts and perspectives,” *International Colloquium on Logistics and Supply Chain Management (LOGISTIQUA),* vol. 00212667984883, pp. 128-132, 2018.

[11] M. Tyler, "New Services and Capabilities for Network 2030: Description, Technical Gap and Performance Target Analysis. FG NET-2030," International Telecommunication Union, 2019.

[12] A. Sultan and M. Pope, “22.837: Study on Integrated Sensing and Communication. Release 19,” 3GPP, 2023.

[13] S. Seneviratne, Y. Hu, T. Nguyen, G. Lan, S. Khalifa, K. Thilakarathna, M. Hassan and S. A., “A survey of wearable devices and challenges,” *In IEEE Communication Surveys and Tutorials,* vol. 4, no. 19, pp. 2573-2620, 2017.

[14] K. Mania, B. D. Adelstein, S. R. Ellis and M. I. Hill, "Perceptual sensitivity to head tracking latency in virtual environments with varying degrees of scene complexity," *In Proceedings of the 1st Symposium on Applied perception in graphics and visualization,* pp. 39-47, 2004.

[15] P. Usai and M. Pope, "26.928: Extended Reality (XR) in 5G. Release 16," 3GPP, March 2020. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3534.

[16] B. Lang, “Oculus Shares 5 Key Ingredients for Presence in Virtual Reality.,” Road to VR, 24 September 2014. [Online]. Available: https://www.roadtovr.com/oculus-shares-5-key-ingredients-for-presence-in-virtual-reality/.

[17] P. Usai, J. M. Meredith and M. Pope, "26.918: Virtual Reality (VR) media services over 3GPP. Release 14," 3GPP, September 2017. [Online]. Available: https://www.3gpp.org/ftp//Specs/archive/26_series/26.918/26918-f20.zip.

[18] J. Farkas and L. Berger, "Deterministic Networking (detnet)," Internet Engineering Task Force. Datatracker, December 2023. [Online]. Available: https://datatracker.ietf.org/wg/detnet/about/.

[19] L. Berger and J. Farkas, "IETF DetNet Working Group Overview," 11 November 2018. [Online]. Available: https://www.ieee802.org/1/files/public/docs2018/detnet-tsn-berger-detnet-overview-1118-v03.pdf.

Funded by the European Union

[20] E. Bednar, "Deterministic Networking," Wikipedia, 20 March 2023. [Online]. Available: https://en.wikipedia.org/wiki/Deterministic_Networking.

[21] E. Grossman, "Deterministic Networking (DetNet) Data Plane: MPLS. RFC 8964," Internet Enginnering Task Force. Datatracker, 22 January 2021. [Online]. Available: https://datatracker.ietf.org/doc/rfc8964/.

[22] Finn N, Thubert P, Varga B and Farkas J, "Deterministic Networking Architecture. RFC 8655," Internet Engineering Task Force (IETF), October 2019. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8655.pdf.

[23] E. Figueroa, A. Asterjadhi, T. X. Han, J. Lansford, R. Burbidge, G. R. Hiertz, D. Sabella, E. M. Schooler, R. Taylor, T. Rodrigues, J. C. Zhang, K. Figueredo and M. Vanetti, "STANDARDS NEWS," IEEE Communications Standards Magazine, December 2020. [Online]. Available: https://ieeexplore.ieee.org/iel7/7886829/9316431/09316644.pdf.

[24] S. Gourav, P. Dhruvin, J. Sachs, M. Andrade, J. Farkas, J. Harmatos, B. Varga, H.-P. Bernhard, R. Muzaffar, M. Atiq, F. Duerr, D. Bruckner, E. Montesdeoca, D. Houatra, H. Zhang and F. Gross, "Towards Deterministic Communications in 6G Networks: State of the Art, Open Challenges and the Way Forward," ResearchGate , 2023.

14 Appendixes

14.1 Appendix A – Control KPIs

In section 3 a list of KPIs that will be used to assess the PREDICT-6G system performance has been defined. Such list puts the focus on numerically evaluating the performance of the different data plane technologies in support of the established deterministic services. Nonetheless, to have a complete view of the PREDICT-6G system performance, there are other dimensions that need to be evaluated. In this regard, an insight about the control plane performance evaluation is provided in this appendix. Given that control plane processes are tightly bounded not only to the system requirements but also to the specific use cases or applications to be served, here a general view of how the control plane performance could be assessed is provided. The control plane operation can affect the three dimensions targeted by the project to implement deterministic networks, namely reliability, predictability, and time sensitiveness. While time sensitiveness is more bounded to the data plane technology, the control plane has a paramount role on the implementation of reliability and predictability. The main drivers of such implementation are the so-called control loops, which, in brief, are composed of detection, decision taking and actuation phases. However, as said, these control loops are very dependent on the particular use case and feature that need to be implemented. For example, for predictability, an AI-based control loop to predict a service degradation may not have a specific requirement in terms of time performance (e.g., seconds or milliseconds), but just needs to be 'on-time'. On the other hand, a more reactive control loop may have stringent time requirements in terms of detection, decision taking and actuation. For this reason, instead of providing a closed list of KPIs, we provide here an elaboration of a set of control plane requirements that can be further specified into quantitative indicators when associated to a concrete use case, application, or feature.

Prediction Accuracy

Name	Prediction Accuracy
Description	Refers to the prediction phase of a control loop and would be defined as the accuracy of the predictions regarding network performance. This definition has been created with support of references coming from other related research initiatives [24]
Method of measurement	We propose to use the Mean Absolute Percentage Error defined as: Difference between actual value and prediction. Performance values can be per packet or periodically, depending on how the underlying KPI related to the network performance is measured.
Units	Number expressed in a percentage.
Measuring point(s)	This KPI is an end-to-end KPI so it must aggregate per-domain KPIS and/or metrics.

Table 28. Prediction accuracy

Detection time

Name	Detection time
Description	Refers to the detection phase of a control loop. The goal is to detect some failure and/or degradation in the system that require for an action from the control plane.
Method of measurement	In the case of a failure, it can be computed as the difference between the time an event occurs in the system (e.g., network failure) and the time the control plane understands some action is needed.

Units	Seconds. Nonetheless, different time units may be defined according to the specific use case.
Measuring point(s)	PREDICT-6G Control Plane

Table 29. Detection time

Decision taking time

Name	**Decision taking time**
Description	This refers to the decision stage of a control loop and would be defined as the time required by the control plane to decide the action to be undertaken to fix a detected, predicted, etc., degradation of a service.
Method of measurement	It can be computed as the difference between the times the control plane has realized an action is necessary and the time that action is undertaken. .
Units	Seconds. Nonetheless, different time units may be defined according to the specific use case.
Measuring point(s)	PREDICT-6G Orchestration system

Table 30. Decision taking time

Actuation Time

Name	**Actuation Time**
Description	Refers to the time necessary to carry out a corrective action upon an anomaly detection.
Method of measurement	Difference between the time from the initial request to enforce a proper configuration to correct the deviation and the time when the configuration has been done.
Units	Seconds. Nonetheless, different time unis may be defined according to the specific use case.
Measuring point(s)	PREDICT-6G Orchestration system

Table 31. Actuation time

Related to the time sensitiveness aspect of the deterministic networking, the control plane may play a role in the cross-domain time synchronization. In this regard, the accuracy of the cross-domain synchronization can be defined as a KPI.

Maximum Time Synchronization error

Name	**Maximum Time Synchronization error**
Description	The maximum error in Time Synchronization during a period of time

Method of measurement	Maximum difference in absolute value between the domain time and the TS signal received from GM clock.
Units	Seconds
Measuring point(s)	Per-domain synchronization points

Table 32. Maximum time synchronization error

From a computation perspective, it is worth noting here that samples for the control plane KPIs are expected to be measured less frequently compared to the user plane KPIs, therefore obtaining statistically relevant number of measurements for evaluating the AI-based control plane (AICP) of the PREDICT-6G system would require extended amount of runtime. Thus, reports on these KPIs are expected to be delivered as a summary of historical measurements rather than displaying them on a real time dashboard.