NEXT GENERATION INTERNET

Grant Agreement No.: 957216
Call: H2020-ICT-2018-2020

Topic: ICT-56-2020
Type of action: RIA

D2.1 USE CASES, KPIS AND REQUIREMENTS

Revision: v.1.0

Work package	WP2
Task	T2.1
Due date	31/03/2021
Submission date	31/03/2021
Deliverable lead	ASTI
Version	1.0
Editors	Nuria Molner (UPV), José Luis Cárcel (FV), Laura Gonzalez (ASTI)
Authors	Julián Campo (ASTI), Laura Gonzalez (ASTI), Christos Politis (SES), Juan Jose Garrido Serrato (SES), Ahmad Nimr (TUD), Jaime Ruiz (NOK), Ignacio García (NOK), Miguel Cantero (5COMM), Manuel Fuentes (5COMM), David Martín Sacristán (5COMM), Héctor Donat (5COMM), Jose Costa-Requena (CMC), Saimanoj Katta (CMC), Bereket Woldemicael (CMC), Efstathios Katranaras (SEQ), Guillaume Vivier (SEQ), Clemens Saur (NCG), Carlos Alcaide (TID), José Luis Cárcel (FV), Joan Meseguer (FV), Carsten Weinhold (BI), Giacomo Bernini (NXW), Erin Seder (NXW), Pietro Piscione (NXW), Gino Ciccone (TEI), Giuseppina Carpentieri (TEI), Cosimo Zotti (TEI), Anton Luca Robustelli (TEI), Alexandr Tardo (CNIT), David Gómez Barquero (UPV), Javier Renart (UPV), Jussi Poikonen (AWA), Joe Cahill (IDR), Eddy Higgins (IDR), Shane Bunyan (IDR), Jahveen Davis (IDR).
Reviewers	José Luis Cárcel (FV), Nuria Molner (UPV), Carsten Weinhold (BI), Julián Campo (ASTI), Laura Gonzalez (ASTI), Ahmad Nimr (TUD), Ignacio García (NOK), Clemens Saur (NCG), Christos Politis (SES), Alexandr Tardo (CNIT), Manuel Fuentes (5COMM), Joan Meseguer (FV).

Abstract	This deliverable defines and compile the different scenarios gathered in six use cases that are relevant for the project as part of the supply chain ecosystem. For each use case, partners have defined explicit requirements and KPIs (both network and service related) that will be targeted on the development phase.
Keywords	Use case, requirements, KPIs

Document Revision History

Version	Date	Description of change	List of contributor(s)
V1.0	30/03/2021	Final version	Laura Gonzalez (ASTI), José Luis Cárcel (FV), Nuria Molner (UPV)

Disclaimer

Copyright notice

Project co-funded by the European Commission in the H2020 Programme		
Nature of the deliverable:	**R**	
Dissemination Level		
PU	Public, fully open, e.g., web	✓
CL	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to iNGENIOUS project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc.

Executive Summary

This document describes the project use cases and specifies the respective requirements and Key Performance Indicators (KPIs) identified in task T2.1. Use cases, requirements and KPIs will be targeted in the development of technological solutions in technical Work Packages (WPs), i.e. WP3, WP4 and WP5.

iNGENIOUS use cases represent from a high-level perspective different scenarios and processes of the supply chain ecosystem. In particular, the project focuses on different segments like factories, transportation or maritime ports for exploring and exploiting disruptive technologies and defining six novel use cases:

- Automated robots with heterogeneous networks
- Transportation platforms health monitoring
- Situational understanding and predictive models in smart logistics scenarios
- Improved driver's safety with Mixed Reality (MR) and haptic solutions
- Inter-modal asset tracking via IoT and satellite
- Supply chain ecosystem integration

The document starts by outlining the methodology developed within the Work Package for the definition of the different use cases. In particular, use cases will be identified and defined by performing a set of goal-oriented interactions between stakeholders and technological solution providers. The definition will include the description of relevant aspects such as the expected innovation, actors involved, services and data flows, verification means, etc.

For each use case, partners will define explicit requirements and KPIs that will be targeted to benchmark the state-of-the art technologies and to develop new technological solutions within iNGENIOUS. Requirements will be defined considering both user and system needs. KPIs will address instrumental, service-validation and operational aspects. All KPIs will be evaluated accordingly in the context of several IoT-related SDOs like ITU, NGMN, 5G-PPP, AIOTI, or 3GPP.

Finally, after defining use cases, requirements and KPIs, the document provides an analysis of the main implications of requirements and KPIs in technical WPs for each specific use case.

Co-funded by the Horizon 2020
Framework Programme of the European Union

Table of Contents

Co-funded by the Horizon 2020
Framework Programme of the European Union

List of Figures

Co-funded by the Horizon 2020
Framework Programme of the European Union

List of Tables

Co-funded by the Horizon 2020
Framework Programme of the European Union

Abbreviations

5GAA	5G Automotive Association
5GC	Fifth Generation Core
AGV	Automatic Guided Vehicle
AI	Artificial Intelligence
AIS	Automatic Identification System
API	Application Programming Interface
AR	Augmented Reality
ATD	Actual Time of Departure
BSM	Business Service Management
CCTV	Closed-Circuit Television
CT	Container Terminal
DBMS	Date Base Management System
DLT	Distributed Ledger Technology
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DVL	Data Virtualisation Layer
ETA	Estimated Time of Arrival
ETD	Estimated Time of Departure
FDMA	Frequency Division Multiple Access
FPGA	Field Programmable Gate Array
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GUI	Graphical User Interface
GW	Gateway
HMI	Human Machine Interface
HW	Hardware
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IOTA	Internet of Things Association
IP	Internet Protocol
ISO	International Organizations for Standardization
IT	Information Technology
KPI	Key Performance Indication
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Medium Access Control
MANO	Management and Network Orchestration
MEC	Multi-access Edge Computing
ML	Machine Learning

Co-funded by the Horizon 2020
Framework Programme of the European Union

MPLS	Multi-Protocol Label Switching
MQTT	MQ Telemetry Transport
MR	Mixed Reality
M2M	Machine to Machine
NEF	Network Exposure Function
NFV	Network Function Virtualization
NG-IoT	Next-Generation Internet of Things
NR	New Radio
NSA	Non-Stand-Alone
NTN	Non-Terrestrial Networks
NWDAF	Network Data Analytics Function
OCR	Optical Character Recognition
OS	Operating System
PCS	Port Community System
PHY	Physical Layer
PMIS	Port Management Information System
PoC	Proof of Concept
QoS	Quality of Service
RAN	Radio Access Network
REST	Representational State Transfer
RF	Radio Frequency
RIC	Radio Intelligent Controller
RTA	Real Time of Arrival
SA	Stand Alone
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SDR	Software-Defined Radio
SIM	Subscriber Identity Module
SW	Software
TCU	Trusted Communication Unit
TLS	Transport Layer Security
TOS	Terminal Operating System
TSN	Time-Sensitive Networking
TTT	Truck Turnaround Times
UC	Use Case
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communication
VBS	Vehicle Booking System
VHF	Very High Frequency
VR	Virtual Reality
WP	Work Package

Co-funded by the Horizon 2020
Framework Programme of the European Union

1 Introduction

In the coming years, IoT is called to evolve into more trusted and energy-efficient smart networks and infrastructures through the exploitation of disruptive technologies such as 5G, Distributed Ledger Technologies (DLT), decentralised edge architectures, or future cost-effective communication systems based on Artificial Intelligence (AI) and Machine Learning (ML).

At the same time, during the last decades, supply chains have become huge networks of individuals, organizations and resources involved in the creation, storage, delivery and sale of products to end users. In such complex environments where manufacturers, suppliers, transporters, logistics hubs, and customers interact, the complexity, variability and volatility of processes are becoming critical risks to address when performing the different supply chain activities. In this context, the appearance of new technological advances is catalysing the digitalization of supply chain management, changing how products and services are made and delivered, and enabling the creation and sharing of information in new ways by a more diverse set of actors.

Under this paradigm, INGENIOUS project aims at developing and exploiting some of the most innovative and emerging technologies for contributing to develop the Next-Generation IoT (NG-IoT) and creating the technical and business enablers required to enhance supply chain management solutions.

In particular, iNGENIOUS aims to digitalize and monitor the whole supply chain ecosystem, starting by automatizing tasks right in the factories, continuing by tracking the transportation of assets and ending with automation of maritime port operative. To do so, as shown in Figure 1, the project has identified six different use cases where NG-IoT is expected to enhance the existing supply chain operative:

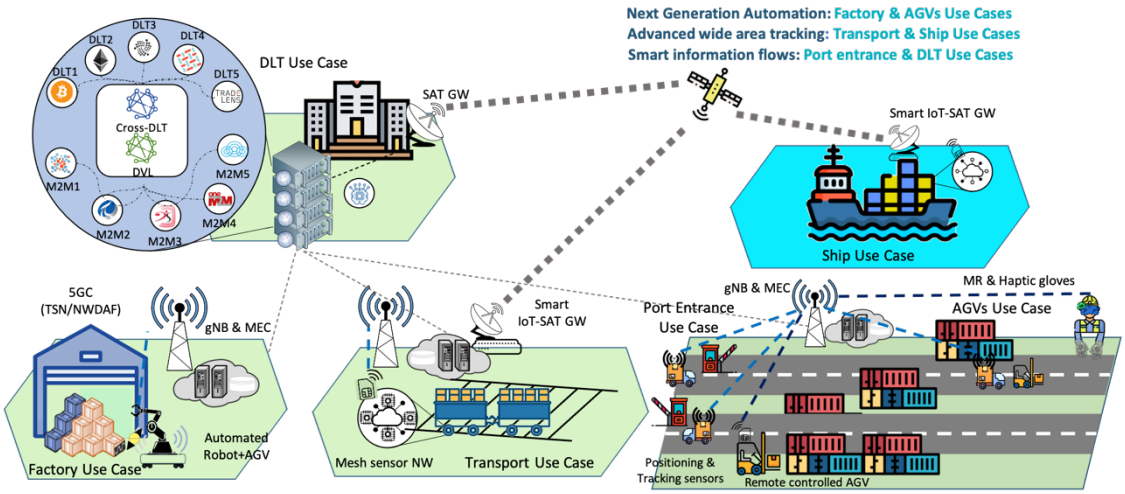


Figure 1: iNGENIOUS use cases and interrelation

- *Automated robots with heterogeneous networks:* The project foresees the use of 5G-enabled automated robots in future smart factories targeting the so-called tactile internet where sensors and machinery synchronously work with latencies of few milliseconds. This use case also explores the interoperability with wired Time Sensitive Networking (TSN) environments.
- *Transportation platforms health monitoring:* iNGENIOUS aims to demonstrate that asset health tracking can lead to low operational costs and high asset availability with new data-based services provided by low-power edge distributed network and intelligent sensor modules installed in the transportation platforms.

Co-funded by the Horizon 2020
Framework Programme of the European Union

- *Situational understanding and predictive models in smart logistics scenarios:* The project targets the development of AI/ML-based predictive models to estimate and optimise truck turnaround times for optimising the access and reduce the wait for vehicles at the port accesses, leading to corresponding savings on direct costs for carriers.
- *Improved driver's safety with Mixed Reality (MR) and haptic solutions:* This safety-centric use case aims to explore the remote transportation of goods with Automated Guided Vehicles (AGVs) thanks to tactile internet, edge computing and immersive enablers (MR and haptic gloves) so that employees will be safe while working away from hazardous environments such as fuel port terminals.
- *Inter-modal asset tracking via IoT and satellite:* iNGENIOUS aims to provide End-to-End (E2E) intermodal asset tracking with IoT and satellite connectivity for enabling enhanced real-time monitoring of shipping containers when they are transported in both terrestrial and maritime segments.
- *Supply chain ecosystem integration:* In this use case the project aims to overcome the absence of a virtual interoperability between existing M2M and DLT solutions through the development of interoperable IoT and DLT layers that will be capable of securely and semantically exchange the information flows between the different actors that can take part along the supply chain ecosystem.

1.1 Objective of the Document

This document aims at describing the different use cases that iNGENIOUS solution will address for the definition of the supply chains of the future, as part of Task 2.1 work.

The proposed methodology for defining the different use cases is herein described, highlighting the specific elements that play a relevant role in each scenario. Complementing the use case definitions, the document also identifies and describes requirements and KPIs for each use case, covering user and system needs together with instrumental, service, and operational aspects.

Finally, the document provides an analysis of the impact of use cases in supply chain scenarios, while also considering the most affected technological modules as well as their relationship with some of the other Work Packages in the project.

Through this document, iNGENIOUS will not only explore the development of the aforementioned use cases but also their convergence and interconnection. Nevertheless, it is not the intention to prescribe particular technical solutions to address the use cases. The detailed technical solutions and verification means will be covered in WP3, WP4, WP5 and WP6.

1.2 Structure of the Document

The document is structured as follows:

- Chapter 2 explains the methodology followed for defining the project use cases, requirements and KPIs.
- Chapters 3 to 8 provide a detailed description of the six different use cases (one chapter per use case), describing requirements and KPIs.
- Chapter 9 analyses the common points and differences between the use cases, focusing on their impact and convergence on supply chain scenarios while highlighting the necessity of specific technological components to cover requirements and KPIs.

Co-funded by the Horizon 2020
Framework Programme of the European Union

2 Methodology

Figure 2 shows the procedure carried out in iNGENIOUS to define use cases and identify requirements and KPIs during T2.1 lifetime. The first step is the use case definition, which has been carried out by performing a set of goal-oriented interactions between the different partners involved in each scenario. Then functional, non-functional and design aspects have been captured by defining user and system requirements. After that, these requirements have been measured by identifying qualitative and quantitative KPIs.

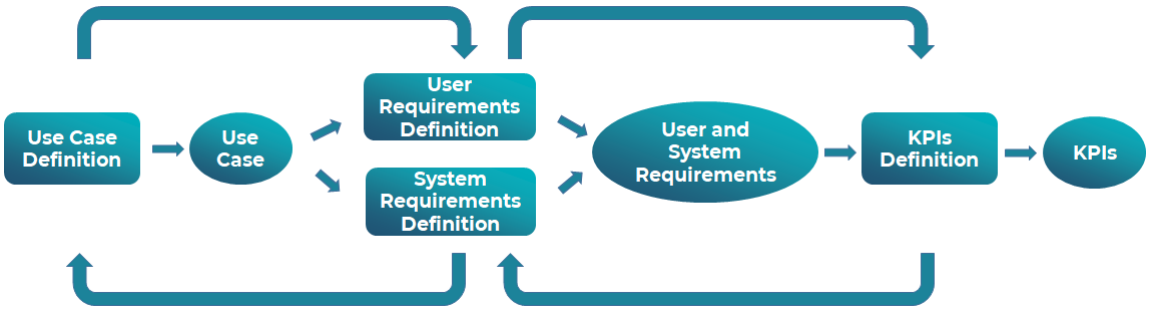


Figure 2: Methodology to compile the scenario and use cases

This main flow is complemented by a continuous feedback. During the identification of the KPIs, the requirements could be updated if needed. In the same way, use cases could be updated if new requirements were identified.

To carry out this methodology, both offline and online activities have been performed. Figure 3 shows the two different blocks of activities and the related tasks associated to each procedure:

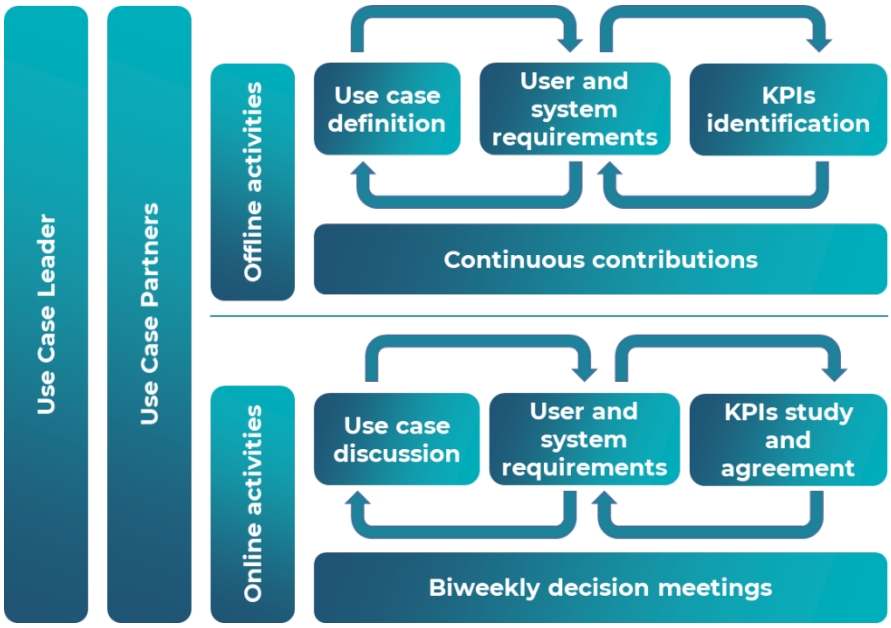


Figure 3: Breakdown of the methodology into activities and iterations

To execute this methodology and in order to follow the same structure in all use cases, a set of templates have been designed to define use cases and describe requirements and KPIs. The different templates together with the details of each iteration are described in next subsections.

Co-funded by the Horizon 2020 Framework Programme of the European Union

2.1 Use Case Definition

Use cases are considered as specific situations in which a product or service could potentially be used. In iNGENIOUS, use cases are the basis for the technical work that will be performed during the project lifetime. As a consequence, a clear definition of each use case is necessary.

For this purpose, a use case template has been designed for collecting all the information required to define each use case. As shown in Table 1, the template has been divided into different fields where specific aspects have to be identified by the different partners involved in the use case:

Use Case Definition	
Description	'What was the status of the use case before the project started?' 'What is the use case about?'
Workflow	'What is the workflow of actions in the use case?'
Expected innovation	'What is the motivation of the use case? Which innovation is expected?'
End user and environment	'Who is the end user? Where does the use case occur?'
Actors	**'**What is the role of partners involved?'
Data and Service(s)	'Which data, services and applications are delivered within the use case?'
Asset(s)	'Which assets (devices, systems, platforms, infrastructure) are involved in the use case?'
State-of-the-art assessment	'Which are the state-of-the-art technologies for this use case? What would be the outcome if the state-of-the-art technologies were applied?'
Requirements and KPIs	'Which functional and non-functional conditions need to be fulfilled? What improvements are targeted?'
Operational, business, societal and environmental outcomes	'What business, societal and environmental implications and/or benefits are expected after the project execution?'
Verification means	'How will the requirements and KPIs be validated and evaluated?'

Table 1: Use case definition template

2.2 Requirements and KPIs

Requirements are conceived as a detailed set of conditions that need to be fulfilled for enabling a particular use case. Depending on the nature of these conditions, requirements can be related to user or to system conditions:

- *User requirements* identify functionalities that must be fulfilled by the application to satisfy the user's expectations.
- *System requirements* identify functionalities that are needed by a system in order to satisfy the user's expectations.

In iNGENIOUS, user and system requirements are defined on the base of the use case descriptions. In order to collect all requirements, a mixed online and offline approach has been carried out. First, all partners filled Table 2 and Table 3 for listing all user and system requirements per use case:

User Requirements
UR_n: *Short description - Name of the partner that suggested the UR*

Table 2: User requirements template list

Co-funded by the Horizon 2020 Framework Programme of the European Union

System Requirements
SR_n: *Short description - Name of the partner that suggested the UR*

Table 3: System requirements template list

Once this list has been completed and agreed by all the use case participants, a new table has been used to have a detailed description per each requirement. The partner that suggested each requirement (user or system), completed the information of Table 4 [1], [2] offline:

Requirements		
Requirement's Name: *Name of the identified requirement*		**Identifier:** *#1*
Category: Functional, Non-functional, or Design constraints	**Priority:** Must have, Should have, Could have or Won't have	
Type: *Security, Privacy, Performance, Semantics, Data Model, Architecture, Interoperability, Legality, Communication, Commercial, Operational, Usability*	**Affected Module:** *Sensor Network, Infrastructure, IoT, Platform, Information Reporting, Smart IoT Gateway, DVL, Smart Sensors, HW Security, Network Security, MANO, Slicing Service Platform, M2M Wrappers, Cross-DLT, Applications, AI-Based Analytics, TSN Framework, 5G layer*	**Use Case:** *Involved use case*
Rationale: *Reason of involvement*		
Requirement Description: *Brief description of the requirement*		
Acceptance criteria: *Conditions that requirement must satisfy to be accepted*		
Source: *EU project, Stakeholder, Standard (e.g., ITU-T, ISO), Regulation, Partner's expertise*	**Identified by:** *Partner who has identified this requirement*	**Registration Date:** *Date of registration* *Date of update*

Table 4: Requirement definition template

After that, in order to meet the set of requirements, use case aspects have been translated into specific KPIs, which evaluate the success of a system or application when performing a specific activity. Only those requirements and KPIs that are relevant for WP3, WP4, WP5 and WP6 to carry out work within the scope of the project have been considered. For this work the same procedure as for requirements has been followed. Firstly, an initial table has been defined to list the KPIs:

KPI	Target Value	Verification Means
KPI_n description	*Expected value with units*	*Inspection, analytical, simulations or demonstrations*

Table 5: KPIs template list

Once the list has been completed and agreed among all the participants, a new template has been set to describe each KPI. The partner that suggested each KPI completed the different aspects shown in Table 6:

Co-funded by the Horizon 2020 Framework Programme of the European Union

KPI		
KPI Name: *Name of the identified KPI*		**Identifier:** *#1*
Category: *Functional, Non-functional, or Design constraints*	**Priority:** *Must have, Should have, Could have or Won't have*	
Type: *Security, Privacy, Performance, Semantics, Data Model, Architecture, Interoperability, Legality, Communication, Commercial, Operational, Usability*	**Affected Module:** *Sensor Network, Infrastructure, IoT, Platform, Information Reporting, Smart IoT Gateway, DVL, Smart Sensors, HW Security, Network Security, MANO, Slicing Service Platform, M2M Wrappers, Cross-DLT, Applications, AI-Based Analytics, TSN Framework, 5G layer*	**Use Case:** *Involved use case*
Rationale: *Reason of involvement*		
KPI Description: *Brief description of the requirement*		
Acceptance criteria: *Conditions that KPI must satisfy to be accepted*		
Source: *EU project, Stakeholder, Standard (e.g., ITU-T, ISO), Regulation, Partner's expertise*	**Identified by:** *Partner who has identified this KPI*	**Registration Date:** *Date of registration* *Date of update*

Table 6: KPIs definition template

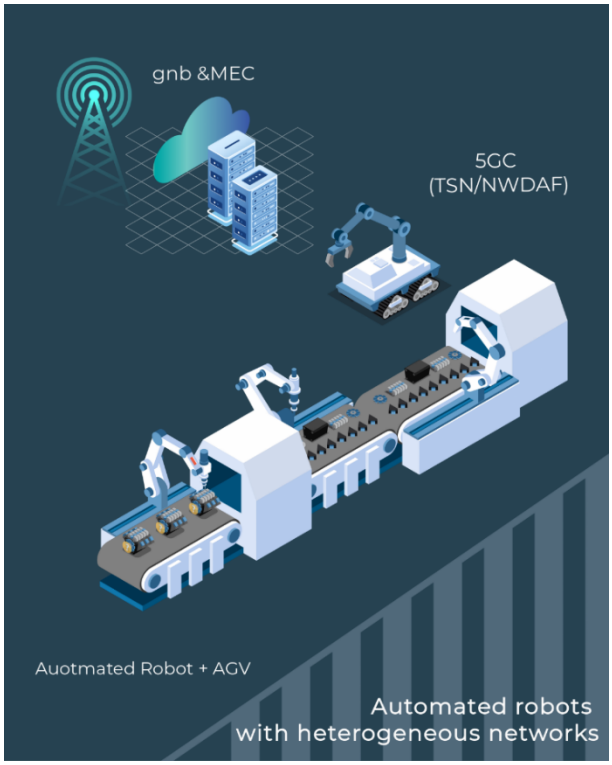
Following this approach, the project compiled all the inputs required to start working on the execution of use cases.

Co-funded by the Horizon 2020 Framework Programme of the European Union

3 Automated Robots with Heterogeneous Networks

Robots have been widely used in industrial automation. The majority of industrial robots are fixed and consist of jointed arms to perform specific tasks. Industrial networks are used to control multiple robot arms in factory production line. Most of the used communication technologies are wired-based and employ well-known control systems such as the supervisory control and data acquisition (SCADA) architecture as shown in Figure 4. This compromises verities of sensors, actuators, controller human machine interfaces (HMI), and supervisory computers for programming, network management and data collection.

In addition to fixed control plants, automated guided vehicles (AGVs) are a form of mobile robot that has been typically used to transport heavy loads following programmed paths.



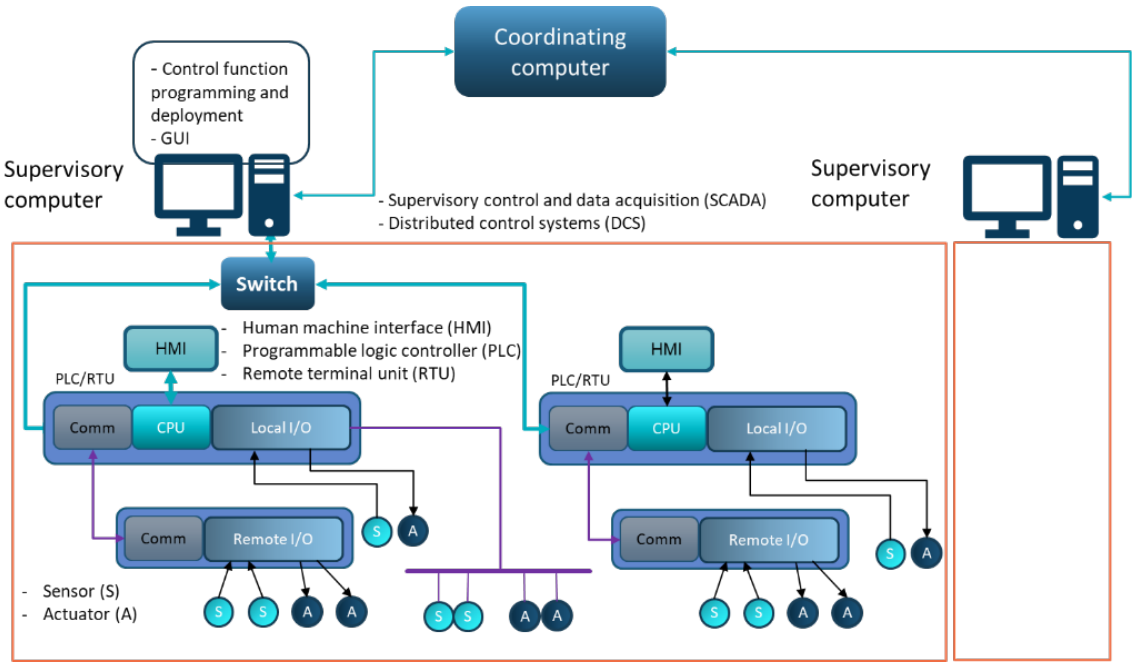


Figure 4: SCADA architecture

Industrial IoT (IIoT) is an evolution of industrial automation and IoT. It relies on wireless connectivity and edge and cloud computing to add mobile assets, increase flexibility, reduces cost, and improve quality. The communication requirements of industrial automation are studied in 3GPP TR 22.804 under the factory of future use case. In addition, several projects focus on 5G industrial communication, e.g., the German projects TACNET4.0 [3].

Co-funded by the Horizon 2020
Framework Programme of the European Union

This use case focuses on automated robot control in a wide sense by considering different types of sensors, actuators, and parallel control loops to create a smart distributed application. In addition, interaction with humans is attained by means of graphical user interface (GUI) for monitoring and remote operation.

The network consists of different type of devices connected by means of different access technologies. The devices range from simple IoT sensors to mobile robots (AGV + robot arm). The radio access network (RAN) is constructed of several access points and gateways connected to the core network, as illustrated in Figure 5. The network also deploys processing units such as multi-access edge computing (MEC). The wireless network is interconnected with the fixed network at the IP layer to integrate fixed devices in the overall system as shown in Figure 6.

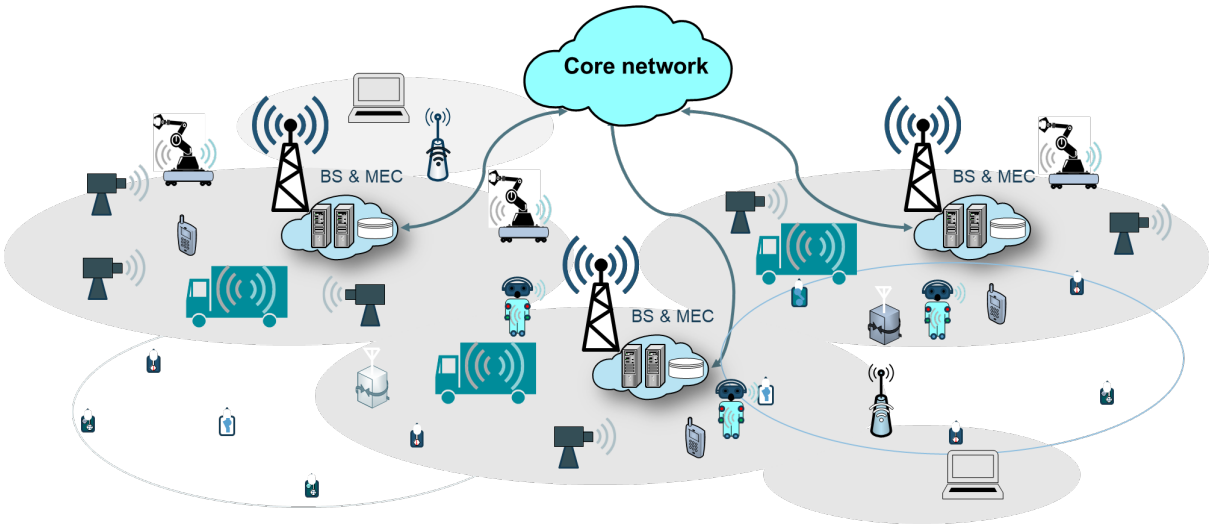


Figure 5: Heterogeneous RAN network

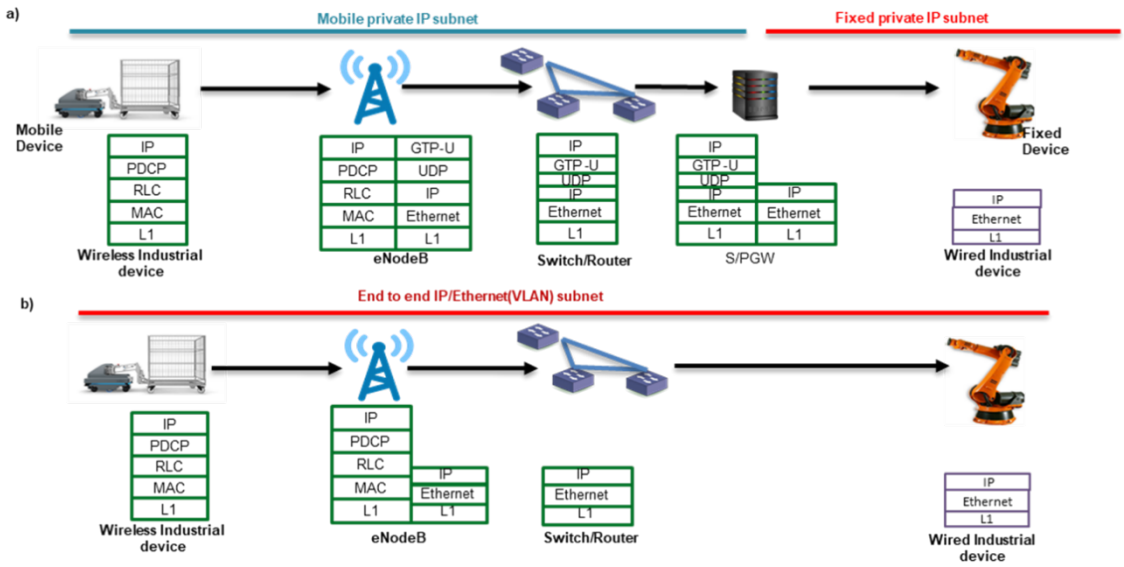


Figure 6: Wireless and fixed network interconnection

3.1 Workflow

The workflow consists of the following steps:

1. First, the industrial IoT service must be instantiated as an end-to-end network slice, Figure 7. The cross-layer MANO components take care of provisioning the network slice composed

by the combination of virtualized network functions, control applications and network connectivity services. This is achieved by coordinating the deployment and placement of network and computation resources. In practice, this translates into the automated deployment (and configuration) of either dedicated or shared 5G Core network functions combined with the provisioning (and configuration) of network resources at RAN and transport segments to fulfil the end-to-end industrial IoT service requirements and to setup the communication data path. This also includes the deployment of the industrial IoT control routines as virtualized network functions at appropriate location (e.g., at proper edge location to fulfil specific latency requirements). Such control routines handle the I/O interaction with the devices in addition to performing the control algorithm.

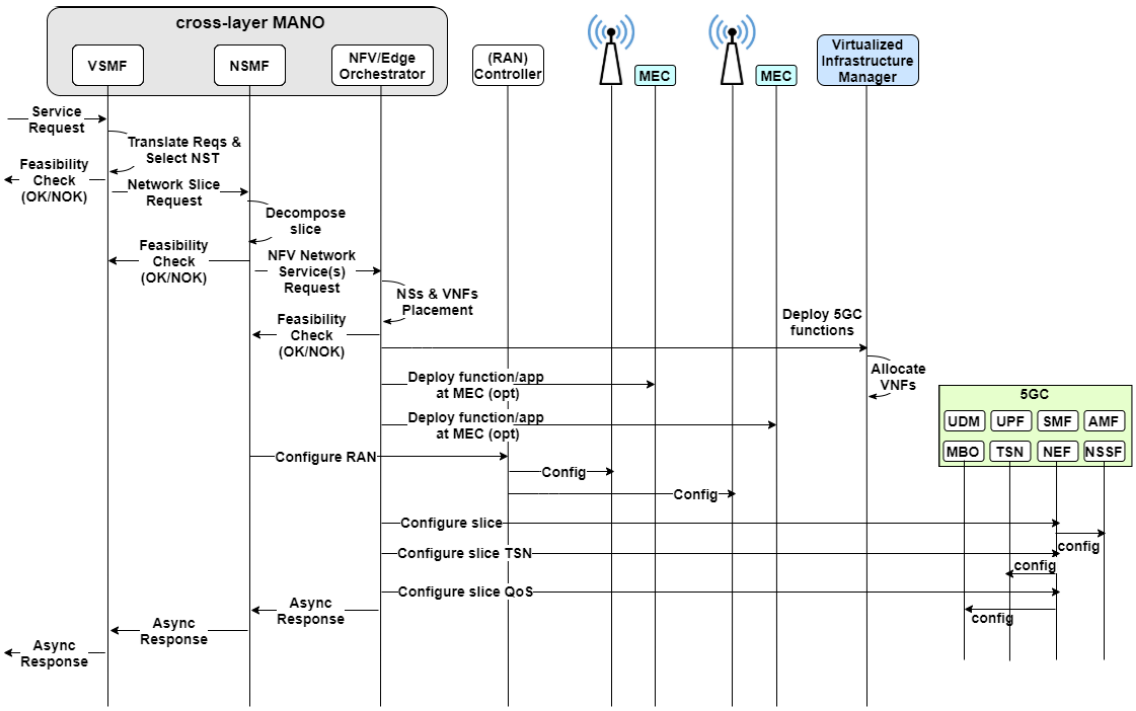


Figure 7: Cross-layer MANO service instantiation

2. IoT devices are connected to the network and their status information, such as location and status are known. This information is updated periodically via control channel. The 5G Core network during the registration process of the devices will assign different UPF-MEC functions closer to the device to minimize the latency, Figure 8. In the core network, the Network Exposure Function (NEF) can provide an interface to external applications i.e., controller to request the location of the devices.

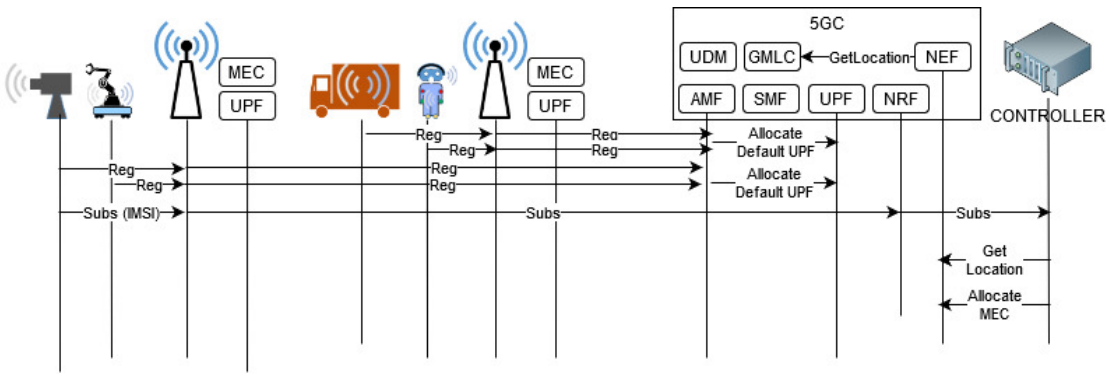


Figure 8: Device registration

Co-funded by the Horizon 2020 Framework Programme of the European Union

3. The network infrastructure can be modelled by a distributed computer architecture with multicore processors, where IoT devices are the I/O as presented in Figure 9.

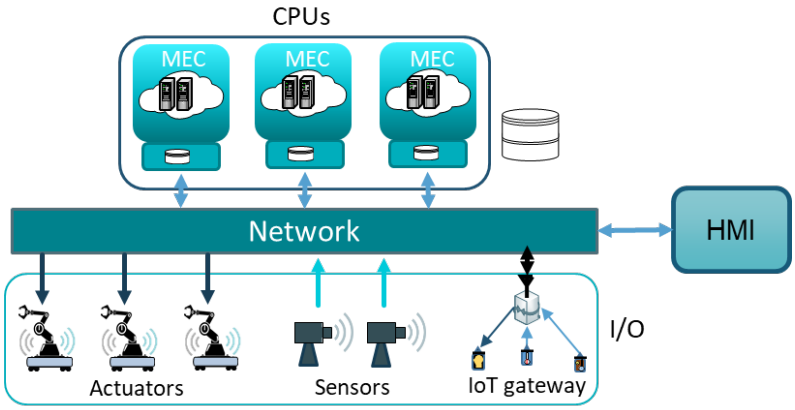


Figure 9: Network architecture as distributed computer

4. Device drivers or communication interfaces are available to interact with devices for sending commands and acquiring data.
5. The application is composed of closed-loop control threads that involve sensors and actuators. The control parameters can be adjusted by an operator using an HMI, which can be a software GUI, or other HMI devices connected to the network.
6. The execution of the application is performed in two phases:
   - *Running:* sensors start sending data to the control function, which calculates the control commands to the actuators. Status information is sent to the user interface. The operator can also modify the control loop parameters and send remote control commands. Moreover, logging data concerning the network performance can be collected and reported. The Time-Sensitive Network (TSN) protocol ensures the synchronization among different nodes and supports deterministic communications between devices that are registered as part of the TSN network. Moreover, during runtime phase, the end-to-end network slice is monitored by the MANO components to collect statistics and information about the actual usage and status of the network and the computation resources to enable slice optimizations.
   - *Termination:* when the application is terminated as the job is done, terminated by the operator, or due to emergency stop, all computational and network resources part of the end-to-end network slice supporting the industrial IoT service should be released by the MANO components and made available to other concurrent applications.

3.2 Expected Innovation

State-of-the-art industrial networks are primarily based on wired fieldbus systems and industrial Ethernet technologies. Some wireless technologies have also been recently investigated based on WIFI and Bluetooth. However, these approaches are not sufficient to meet the strength requirements of critical missions and closed-loop control. Tactile Internet (TI) provides a promising opportunity through high-performance wireless connectivity. The wireless connectivity is required to decrease the cost of cabling in wired network, allow flexible deployment, and enable new applications that require movement.

While 5G-NR focuses on wireless networks that enable TI, the IEEE Time-Sensitive Networking (TSN) working group aims to enhance the reliability, security, and real-time capabilities of the standard Ethernet. The developed standard includes time synchronization, scheduling, traffic

Co-funded by the Horizon 2020
Framework Programme of the European Union

shaping, fault tolerance, path selection, and path reservation. 3GPP Release 16 defines network functions to integrate IEEE TSN networks into 5G system and the Network MANagement and Orchestration (MANO) frameworks provide fundamental coordination functionalities for the unified provisioning and operation of services at various levels that include network connectivity and can integrate with service and application capabilities. These features are of extreme relevance in complex scenarios like the iNGENIOUS use cases where heterogeneous IoT network technologies and devices have to interwork with the 5G network to provide smart and innovative supply chain services. In particular, two main aspects can be covered by MANO frameworks: network slicing and network service management and orchestration.

This use case will contribute to the realization and testing of industrial IoT with URLLC requirements and integration with massive IoT networks. The focus is mainly on the network architecture and application programming interface. We consider a local area heterogeneous network on the scale of an industrial factory. This network interconnects heterogeneous IoT and tactile devices and provide the communication requirements for different applications and services. It can be integrated with standard remote area networks by means of a gateway to provide remote services for remote deployment, monitoring, and operation of industrial applications. The following innovation areas are targeted:

- Software defined communications: the project will exploit software-networking in the different layers of the communication system protocol stacks. The software-defined physical layer (SD-PHY), software-defined medium access control (SD-MAC), software-defined networking (SDN) and network function virtualization (NFV) will be exploited in the realization of the network. The network will run on standard hardware with CPUs and reconfigurable FPGAs. This approach will facilitate the integration of multiple standards, and keep the door open for the testing of new advancement without extra hardware costs.
- Adaptive networking at all layers: the network will provide different type of services with different requirements. Based on the running network application, the network will adapt the communication protocols not only at the network layer but also at the radio access level to fulfil the needs, while maintaining high energy and spectral efficiency. Moreover, the network will benefit from the deployed IoT sensors and relying on machine learning and artificial intelligence (AI) to predict and model the wireless channel, in order to optimize the resource usage.
- Time synchronization in heterogeneous networks: Time synchronization in mobile networks is defined in 3GPP and latest Release 16 is proposing synchronization mechanisms for the distribution of the clock and timestamping, according to IEEE 802.1AS. 3GPP proposes the usage of generalized Precision Time Protocol (gPTP).
- Automated management and orchestration: a fully automated approach in the deployment and operation of supply chain and industrial IoT services with time sensitive requirements is required, leveraging on 3GPP-based network slice management principles and their integration with control and operation of NG-IoT technologies.
- Application programming interface: the software and hardware including sensor/actuators and other computation and storage devices in the network will be considered as resources, which can be programmed to achieve certain tasks. iNGENIOUS will extend the concepts of software engineering and operating systems to include the network resources as extended I/O peripherals and computational cores. The computational and storage units represent processors cores and memories, and the sensors/actuators are the I/O. The wireless communication is the internal bus of the system. A tactile application uses a set of input sensors, a set of output actuators and control functions that define the relationships and behaviour. The network will provide an API for the developers to implement and debug the applications before deploying them on the network.

Co-funded by the Horizon 2020
Framework Programme of the European Union

3.3 End User and Environment

This use case can be used to deploy industrial networks in manufacturing, power generation and distribution, oil and gas, mining and chemical processing. An industrial network is essentially an interconnected system of specialized components and applications, which is used to monitor and control physical equipment in industrial environments. Industrial networks demand high level of reliability, responsiveness, and determinism.

The industrial communication comprises monitoring and control applications. The monitoring applications gather various sorts of sensory information for diagnostic purposes, and thus, they do not have real-time requirements, but reliable data delivery is essential. There are two types of control applications with different requirements.

- *Closed-loop control*: bidirectional exchange between the controller and the device. This requires a strong real-time connectivity with high reliability and low jitter. Closed-loop control may also involve communication between different industrial controllers.
- *Open-loop control*: typically, event-triggered, and may demand strong real-time connectivity with high reliability and bounded latency when safety is the concern.

All of these translate into strict network performance and QoS requirements for the targeted industrial communications, that can be accommodated by creating dedicated logical end-to-end networks that span from the IoT devices, up to the RAN, edge/MEC locations and core network. This can be achieved leveraging on the 5G network slicing paradigm, augmented with industrial IoT and time sensitive requirements. A dedicated network Management and Orchestration (MANO) framework is required to coordinate the provisioning of isolated logical networks built of IoT, RAN, edge and core network functions in virtualized environments. In addition, an AI/ML engine integrated with the MANO can help in supporting automated network and industrial service optimization.

3.4 Actors

Radio access network specialists will develop software-defined PHY/MAC approaches and develop a real-time waveforms framework to support smart air interface and flexible resource allocation.

Radio access technology providers provide standard equipment such as real-time and non-real-time O-RAN radio intelligent controller (RIC), Amarisoft 5G/NB-IoT gNB/eNB, and potential NR-RedCap/Light SDR UE, 5G modem.

Testbed providers provide commodity computing platforms, software development libraries and frameworks, in addition to development and measurement tools.

5G core network providers will bring core network implementation including NFV and TSN.

Network Management and orchestration experts will focus on network resources and slices provisioning (in IoT, RAN, MEC and core domains), integration of AI-assisted MANO with TSN control functions for time sensitive network slice provisioning (e.g., dynamic functions placement at MEC, slice scale in/out, etc.). They will provide AI-assisted MANO, and AI/ML based network slice and network resource optimization.

Automation industries provide devices such as AGV and robotic arms, sensors and provide hardware and software interfaces for connectivity and application development.

Co-funded by the Horizon 2020
Framework Programme of the European Union

3.5 Data and Service(s)

The heterogeneous network integrates different IoT technologies enabling different types of communications including massive IoT, URLLC and enhanced Mobile BroadBand (eMBB). It also integrates wired and wireless industrial networks. Different types of data will be exchanged depending on the application:

- *Videos* will be captured mainly to perform object detection at the MEC.
- *Sensor data* will be collected and sent to the control function.
- *Commands* for steering the AGV and controlling the robot arm.
- *Status information* will be delivered to the remote operators (AGV location, environment status such as temperature, pressure or humidity, surveillance data to update virtual/real scene).
- *Network statistics* such as packet loss and SNR.

The services provided by the use case concern both connectivity and applications:

- *Database* listing the connected devices and computation platforms and their capabilities.
- *Device status tracking* (e.g., occupancy, localization).

Network services and functions to support different requirements:

- *API for the implementation of customized applications* using the available IoT devices, MEC, and network resources. The API provides GUI tools for remote control and monitoring, control loops function such as PIDs, and device drivers for data acquisition and control.

3.6 Asset(s)

The main assets involved in the development of this use case are:

- *Different types of IoT devices* such as positioning and environmental sensors, cameras, and robot arm and AGVs.
- *Functions* corresponding to control algorithms and data acquisition.
- *Radio access technologies* including, IoT Gateway, 5G-gNodeB, 4G eNodeB, 5G/4G modem, O-RAN and Flexible PHY/MAC implemented on FPGA and SDR.
- *Core Network assets* such as 5GC, TSN and MEC.
- *AI/ML-enabled MANO* for the coordination of resource provisioning in the various network segments (RAN, edge/MEC and core) to create network slices in support of seamless end-to-end communications for supply chain and industrial IoT services, with integration of AI/ML engine to support the decision-making procedure for either allocating, liberating or tuning network slices resources at runtime.

3.7 Requirements

User Requirements	Description
#1: The robot operator should be able to install in the robot a radio modem that connects to local sensors, camera and robot control system.	The operators should be able to easily install new communication devices where existing sensors can be connected without additional changes. The 5G communication device should include standard ports where existing devices in the robot can be connected without any changes.

Co-funded by the Horizon 2020 Framework Programme of the European Union

#2: The system operator should be able to visualize in a O&M console the location of the robots and status of the connection to each robot.	The operators should have access to a management console where they can see the status of the network and the devices connected to the network.
#3: The system operator should be able to assign different devices in the robot to different network slices based on latency/bandwidth requirements.	The operators should be able to register new devices and during the registration process assign the devices to different network slices depending on the requirements from the device.
#4: The system operator should be able to restrict the access of different robots to different parts of the fixed network infrastructure.	The fixed network will be separated into areas where the access can be restricted to different devices. The system manager should have a management console where the devices will be assigned the access restrictions to selected parts of the fixed network.
#5: The system operator should be able to create applications using the available devices. The application consists of used devices and control loop functions.	The operators should be transparently able to create and execute high level applications exploiting devices and computational resources. This includes resource query and reservation, defining the interaction between input and output devices, and design and interaction with end-user human interface.

System Requirements	Description
#1: The radio modem in the robot would provide standard Ethernet connectivity (e.g., RJ45) to all the peripherals (e.g., sensors, camera, robot control) in the robot.	The devices in the robot do not need to be updated and can utilize standard Ethernet RJ45 ports to connect to 5G communication module and connect to 5G network.
#2: The network should provide monitoring information to visualize the status of the system.	The 5G system incudes management console where the operator can register new devices and visualize when they are connected and what their status is.
#3: MANO platform for the management, orchestration and monitoring of network resources using TSN control functions for the KPI satisfaction.	The MANO shall be able to deploy and orchestrate the 5G network functions including the resources for running TSN translator in the 5G network that allow the communication between mobile devices and TSN devices connected to the fixed infrastructure.
#4: Orchestration and deployment of MEC applications for robot control through MANO platform.	The AI/ML assisted MANO shall be able to deploy and orchestrate the robot control application as part of the industrial IoT slice provisioning and select a proper edge/MEC location to fulfil the latency requirements.
#5: MANO platform collects network and application data for proactive network slice management using an ML algorithm.	The AI/ML assisted MANO shall collect network related data from the network functions, controllers and devices deployed and used for industrial IoT network slice at different locations and network segments (including RAN, transport, core), with the purpose of improving the knowledge of network slices and resources status and behaviour.
#6: MANO platform should be able to onboard supply chain network slice.	The AI/ML assisted MANO shall provide dedicated interfaces/APIs to onboard industrial IoT network slice templates and descriptors.
#7: MANO platform should be able to manage the lifecycle of the supply chain network slices.	The AI/ML assisted MANO shall take care of the industrial IoT network slice lifecycle management. This means it shall provide mechanisms and procedures for the automated creation, operation and termination of network slices, taking care of interacting with the network and computing

Co-funded by the Horizon 2020
Framework Programme of the European Union

	infrastructure (i.e., controllers, devices, etc.) to respectively provision, operate and release all the required network and computational resources according to industrial IoT requirements.
#8: MANO platform should be able to interact with all the network infrastructure components for the supply chain network slices provisioning.	The AI/ML assisted MANO shall be able to interface with controllers, network functions and devices in the network and computing infrastructures (such as RAN controllers, 5G Core functions, virtualized infrastructure managers) with the aim of provisioning and configuring resources for industrial IoT network slices according to the service requirements.
#9: The RAN should be able to connect devices from different technologies (e.g., Bluetooth, WIFI, LoRA, etc.) using gateways.	To connect devices, form different 3GPP and non-3GPP standards (e.g., Bluetooth, WIFI, LoRA, etc.) to the IoT core network, the RAN should be equipped with gateways that provide multiple radio interfaces. The gateway can be managed by the 5G core control plane or directly connected to the data plane.
#10: The network should provide APIs for application development. The APIs list the available devices, functions to interact with the devices, GUI tools for devices visualization, monitoring and control.	Applications development should be simplified by means of APIs that abstract the underlying network resources and operations. These APIs provide developers with tools to reserve resources and specify the application requirements. It also includes functions and libraries for accessing the devices I/O and implement the control loops on MEC. Furthermore, it enables interacting with end-user interface for acquiring status information and sending remote commands.
#11: AI/ML assisted network slice optimisation.	The AI/ML assisted MANO shall provide ML-based automated mechanisms and procedures for proactively adjusting and adapting the provisioned industrial IoT network slices at runtime to optimize their performance profile, network and control functions size and location, network resources usage and configuration.

3.8 Key Performance Indicators (KPIs)

KPI	Target Value	Verification Means
Coverage	0.01 km^2	System-level simulation and proof-of-concept trials
Mobility	10 km/h	Link-level and system level simulations, in addition to proof-of-concept trials
Positioning accuracy	20 cm	Simulation and Proof-of-concept trial of the used position techniques
Security	High	Theoretical analysis and proof-of-concept test
Availability for sensors	99.9 %	Theoretical analysis and field trials with sufficiently long period of time.
Availability for devices in control loops	99.9999 %	Theoretical analysis and field trials with sufficiently long period of time
Battery life for sensors	12 years	Device test for a sufficient period of time under different conditions
Data rate for IoT sensors	0.1 Mbps	Link-level and system-level simulation, proof-of-concept trials and measurement
Data rate per camera	6-24 Mbps	Link-level and system-level simulation, proof-of-concept trials and measurement

Co-funded by the Horizon 2020 Framework Programme of the European Union

Data rate per robot	10 Mbps	Link-level and system-level simulation, proof-of-concept trials and measurement
Connection density for sensors	1.4 M/ km^2	System-level simulation, and proof of concept with a small-scale deployment
Connection density for robots	10 K/ km^2	System-level simulation, and proof of concept with a small-scale deployment
E2E latency for environmental sensors (sensor to application)	1 s	Link-level and system-level simulation, proof-of-concept trials and measurement
E2E latency for remote control (Command from application to remote device)	10-50 ms	Link-level and system-level simulation, proof-of-concept trials and measurement
E2E latency for human-in -loop control (from sending the command to receiving the feedback)	1 - 5 ms	Link-level and system-level simulation, proof-of-concept trials and measurement
E2E control-in-loop control (from sending the feedback from sensors, control process, applying command on actuator)	1- 5 ms	Link-level and system-level simulation, proof-of-concept trials and measurement
Reliability for IoT sensors	99.99%	Link-level and system-level simulation, proof-of-concept trials and measurement
Reliability for remote control	99.999%	Link-level and system-level simulation, proof-of-concept trials and measurement
Reliability for human-in-loop control	99.99999%	Link-level and system-level simulation, proof-of-concept trials and measurement
Reliability for control-in-loop	99.9999%	Link-level and system-level simulation, proof-of-concept trials and measurement
Remote control timing (cyclic time, time to apply control, jitter time)	(50 ms, 5 ms, 500 us)	Timing measurement with proof of concept.
Human-in-loop control timing (cyclic time, time to apply control, jitter time)	(0.5 ms, 0.25 ms, 1 us)	Timing measurement with proof of concept.
Control-in loop timing (cyclic time, time to apply control, jitter time)	(2 ms, 1 ms, 5 us)	Timing measurement with proof of concept.

Co-funded by the Horizon 2020 Framework Programme of the European Union

3.9 Operational, Business, Societal and Environmental Outcomes

Automation provides economic benefits for customers and service providers. It allows to improve the response time by increasing the operational productivity. Automation facilitates the optimization of resource allocation and material utilizations, enabling lower production costs and creating opportunities for new services. Moreover, the consistency and reliability of services or products can be enhanced relaying on automatic measurements and testing.

These benefits lead to improving the QoS and customers experience, which in turn increase brand and service loyalty. Furthermore, automation can be exploited to replace human workers in dangerous tasks or to perform risky experimentations. On the other hand, job loss is a critical social side effect of relying on automation. Nevertheless, the automation opens the doors of new jobs for high skilled people, which motivates more investing in the education and training fields. The decision to apply automation in different stages of supply chain depends mainly on the relative cost compared to human labour work. The cost should not consider only the average hourly rate and the equipment prices but also the indirect costs resulting from faults and possible hazard caused by failures or unauthorized access. An important factor to consider is the safety of people and security of the data.

3.10 Verification Means and Actors Involved

The connectivity requirements will be determined based on the control loop model shown in Figure 10, which considers the processing at the sensor, actuator, and the control function processing time. The connectivity requirements will be evaluated based on link-level simulations and proof of concept using hardware in-loop and real-time prototyping.

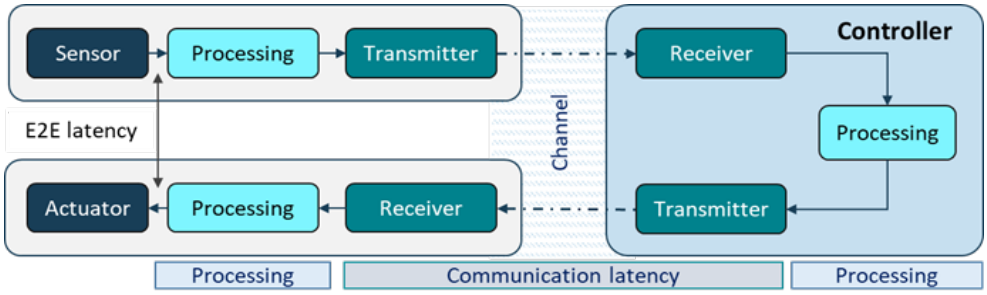


Figure 10: Control loop model

Link and system level simulations: Link-level simulations will be considered as a first step to validate the targeted link KPIs. In addition to computer simulation, hardware-in-loop will be considered to evaluate realistic wireless channels. System-level simulation will be considered to validate the scalability and the overall performance of the network considering models and realistic measurements.

Proof of concept demonstration of flexible RAN using SDRs: A basic heterogeneous RAN will be set on a testbed using various SDR and commodity computation platforms including FPGA, personal computers and servers depicted in Figure 11. Different types of physical or emulated devices will be connected to SDRs to obtain IoT devices with diverse capabilities encountered in a realistic scenario. The access points are realized with more powerful SDRs and additional computation to serve multiple users with different RATs.

Co-funded by the Horizon 2020
Framework Programme of the European Union

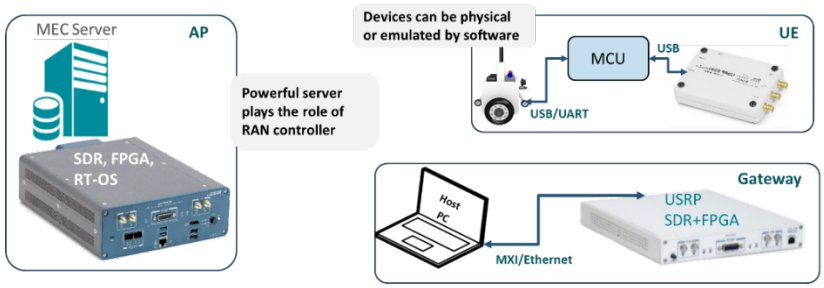


Figure 11: Hardware devices

Figure 12 illustrates a deployment scenario for the network including IoT devices belonging to the three main categories, AGVs and robot arms with URLLC requirements, a camera which belongs to MBB, in addition to several sensors for the mMTC scenario. This deployment will allow demonstrating PoCs in relation to flexible PHY/MAC to support multiple air interfaces, dynamic reconfiguration of PHY/MAC in the context of smart RAN.

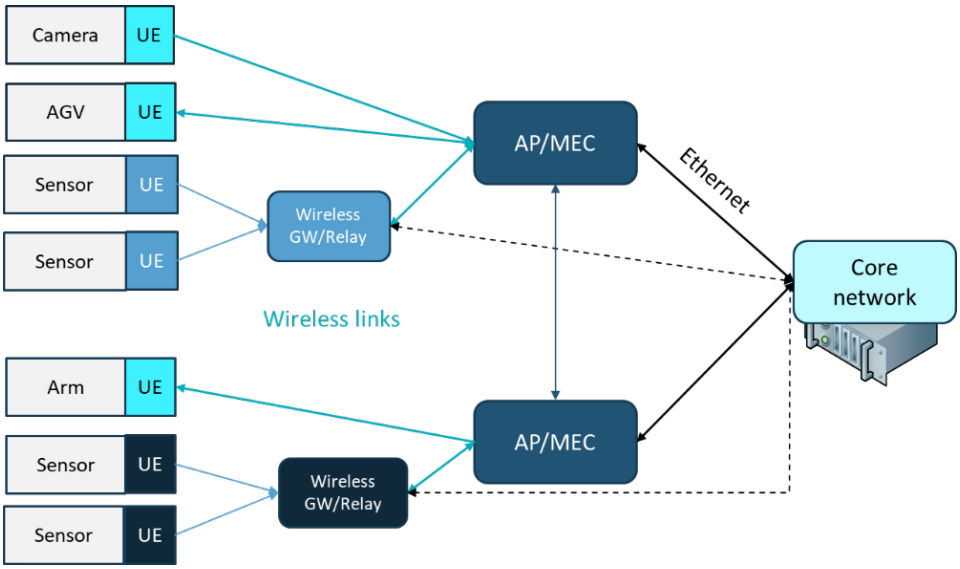


Figure 12: Network infrastructure

Proof of concept core network: The core network will include all the required functions for registering devices and assigning them the UPF-MEC required for reducing the round-trip delay. The signalling component of the UE and gNB could be added and communicate via fixed IP connection to demonstrate the usage of different sensors that do not include 5G connectivity yet.

Proof of concept MANO: The cross-layer MANO software prototype will be integrated in the TUD testbed and will provide all the vertical service and slice orchestration functionalities required to manage the lifecycle of the end-to-end industrial IoT network slices (including provisioning, monitoring, runtime optimization, termination) according to the vertical service requirements, and integrating with the available network and cloud infrastructure.

Proof of concept application: Virtual devices will be used to demonstrate the concept of API, where each IoT device will be emulated by software.

Real-life scenario using IoT devices and standard network infrastructure: A demonstration will be implemented in ASTI factory using an AGV and a robot arm with different sensors and cameras.

Co-funded by the Horizon 2020 Framework Programme of the European Union

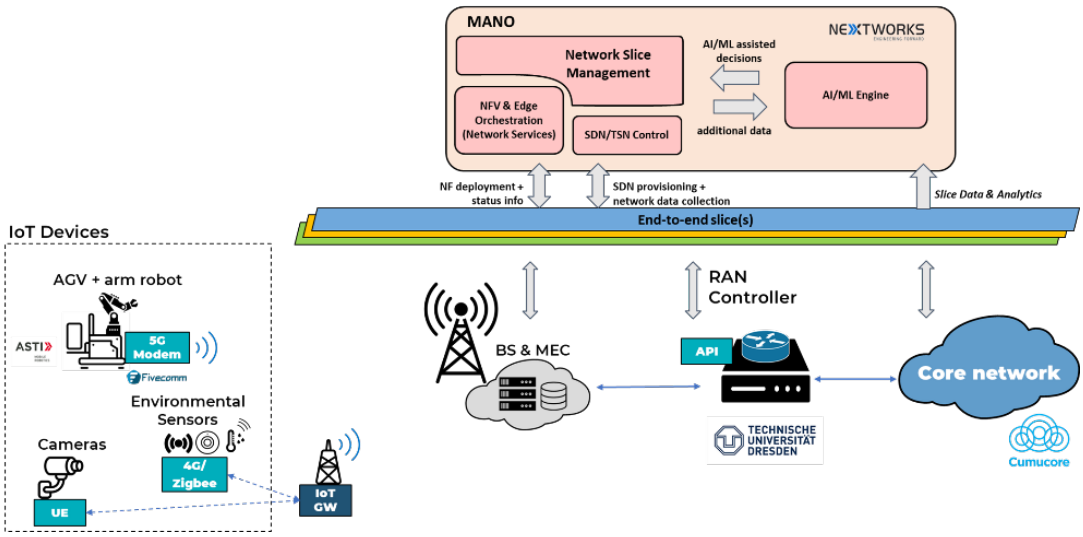


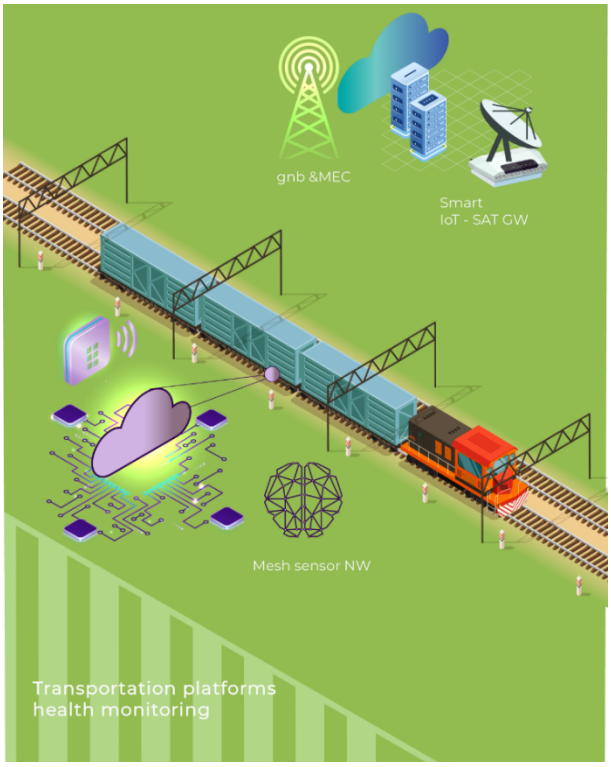
Figure 13: MANO communication diagram

In order to realise these verification tasks, several actors are involved:

- TUD will focus on software defined PHY/MAC approaches and develop a real-time waveforms framework to support smart air interface and flexible resource allocation based on FDMA and TDMA. The framework will be tested and evaluated by means of link-level simulation, hardware in loop, and FPGA prototyping. In addition, TUD will design and test an API for application developments. TUD will provide testbed with verities of SDRs, FPGA, and network infrastructure.
- UPV will support in link level simulation and measurement campaigns for trials. They will provide real-time and non-real-time O-RAN radio intelligent controller (RIC), Amarisoft 5G/NB-IoT gNB/eNB, and potential NR-RedCap/Light SDR UE
- Fivecomm will support in system-level simulations and provide help with link-level simulations if needed. They will provide 5G UE connectivity for AGVs with a simple and compact 5G-Modem. Also, Fivecomm will contribute carrying out measurement campaigns for trials and with a 3D planning tools to model the scenario.
- Cumucore is 5G core network provider and they will focus on core network including NFV and TSN.
- Nextworks will work on orchestration of network resources and slices (in IoT, RAN, MEC and core domains), integration of AI-assisted MANO with TSN control functions for time sensitive network slice provisioning, and AI/ML based network slice and network resource optimization (e.g., dynamic functions placement at MEC, slice scale in/out, etc.). They will provide AI-assisted MANO, TSN control functions and AI/ML based network slice and network resource optimization.
- ASTI MOBILE ROBOTICS will contribute to the software and hardware developments for connectivity and remote control and provide AGV and robotic arm with sensors.

Co-funded by the Horizon 2020 Framework Programme of the European Union

4 Transportation Platform Health Monitoring



Rail-Health, the early detection of safety critical detects of wheels and bearing, has found its way to high-speed commuter trains, where safety regulations are extremely stringent and associated safety costs are readily accepted, but this is not the case for widespread commercial logistic platforms. Without corresponding safety regulation, safety benefits, however important, need to proof commercial benefit. Fortunately, there is a business case for more safety, but the targets are challenging and meeting these targets requires new innovative IoT approaches.

The guiding principles of logistics are faster, cheaper, and more accountable. Planning transparency, uptime availability, and cost effectiveness are just a few essential operational parameters. Transport health in any form, whether it is the distribution centre, a vessel, a delivery truck, a trailer, a railcar, or other, is an important variable in keeping the logistic gears smoothly going.

This Use Case targets rail health for logistic chain improvements. Bringing low cost, low power, lifelong health monitoring with near continuous connectivity to the edge is a great target for next generation IoT innovation.

The Business Case for Rail Health Monitoring is simple, it needs to extend standard maintenance cycles from 6 years to 12 years – a cost saving of 250€ per axle – by extending position connectivity with rail platform health information. In other words, the project proposes a concept of IoT-sizing rail axles with Edge Health Sensors which aims to operate autonomously for 12 years and identify significant Flat Spots and emerging Bearing Defects at least 2 months prior to critical events, without exceeding the cost of current regular six-year service intervals.

The challenge consists of two parts:

- The edge health sensor: Sensor/UE (Edge sensors for transportation should be low power).
- Near seamless connectivity: RAN/Backhaul connectivity (limited connectivity in rural areas).

Today's solutions are too expensive (70-250€), require power connectivity or huge energy harvesters, and are mostly targeted on passenger carriages which communicate to the trains diagnostic information system. Freight cars by comparison do not have direct connectivity to the freight engine, do not have power connectivity, transport hazardous materials, and have variable loads. While flat spots on passenger carriages require repaired upon detection for acoustic passenger comfort, freight cars accept non safety critical flat spots below 60mm in width and require consequently smarter edge performance to classify defect criticality under various load conditions. As a consequence, no practical solutions for freight car health monitoring are available on the market today.

Co-funded by the Horizon 2020
Framework Programme of the European Union

4.1 Workflow

The use case will conventionalize and partially demonstrate a practical system solution for Rail Transport Platform Health Monitoring focusing on the above challenges.

The envisioned architecture and the technical contributions of the partners to this use case are shown in Figure 14.

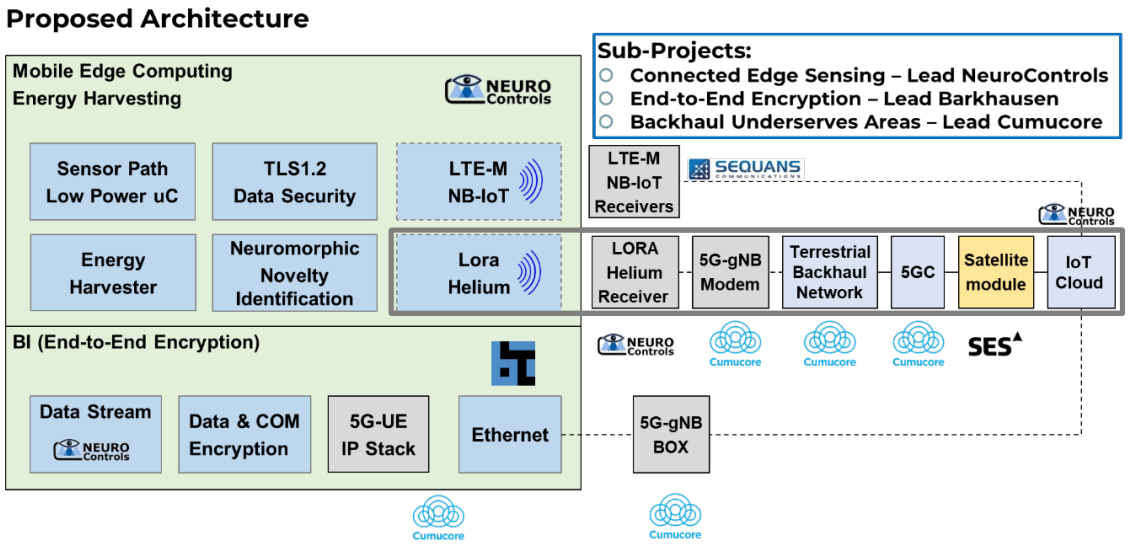


Figure 14: Transportation platform health overview

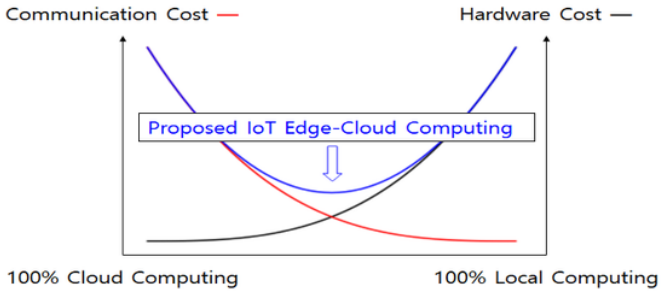
A cloud-hosted middleware and monitoring application will provide stakeholders information about the status of the transportation platform:

- Where is the transportation platform (Forwarders)?
- What or in what condition is the transport content - Loading, Content, Security (Operators)?
- What is the health condition of the transport platform (Asset Owner/Leasing)?

4.2 Expected Innovation

Next Generation Mobile Edge IoT is about connecting mobile and physical objects to the Internet of Things. The motivation for the Transportation/Mobile Edge Use Case is to conceptualize and demonstrate how next generation Transportation/Mobile Edge connectivity could look like.

The basic challenge of Mobile Edge Connectivity is the balance between cloud and edge computing, driven by the availability of connectivity, connectivity cost, and information latency allowance. The optimal solution depends on the use-case. Therefore, there is not one solution but rather a suitcase of solutions which must be statically or dynamically adjusted to specific requirements.



If time as a variable can be eliminated, the equation to be optimized is:

$$Sensing\ Cost: \frac{Cloud}{Computing} + \frac{Data}{Transmission} + \frac{Edge\ Data}{Storage} + \frac{Edge}{Computing} + \frac{Edge}{Power}$$

In this case, typically the cheapest data transmission model can be applied. Connectivity gaps would not be seen as very relevant.

Typically, raw data or compressed data streams are needed for data science. While collecting raw data streams can be attractive to argue complete coverage, it is both impractical and definitely not next generation state-of-the-art. Data diversity is a key factor for good data science, which makes this Use Case wanting to enable swarm intelligent learning solutions, meaning that edge sensors, or at least a fraction thereof must be capable of detecting novelty events.

Time as a variable defines the level of connectivity coverage needed. If connectivity coverage cannot be guaranteed, but local alert within a defined latency window is essential, then alert computing must be done locally (edge). If global alerts must be warranted, then solutions to achieve the proper level of communication coverage and robustness must be targeted:

$$Connectivtiy\ Coverage: \frac{Primary}{Connectivity} + \frac{Blind\ Spot}{Connecticity} + \frac{Connectivity}{Redundancy}$$

With these two KPIs defined we can reflect on typical use case frameworks. There is different type of sensing events that can range from tiny to gigantic:

- Sensor Status, Value, or Threshold
- Known Sensor Signal (Meta Data)
- Unknown Sensor Signal (Raw Data Burst)
- Raw or Compressed Data Stream

Typically, we consider the following ranking in data volume requirements:

$$DATA\ Volume: \frac{OK}{NOK} \gg \frac{GPS}{DATA} \gg \frac{Error}{Message} \gg \frac{Point\ of}{Interest} \gg \frac{Raw\ Data}{Burst} \gg \frac{Raw\ Data}{Stream}$$

Raw Data Burst and Raw Data Streams data volumes can be huge. Modern Automotive Imaging Systems work at 8MP resolution and 30fps. High bandwidth acoustic sensors operating at 1 GHz at 24bit resolution are not easy to manage. Neither are point cloud sensors.

Neuromorphic data stream computing is a very effective method for real-time data analysis. As shown in Figure 15 known Data Streams are labelled as Meta-Data. Unknown Data Streams are recorded or transmitted for subsequent machine learning applications.

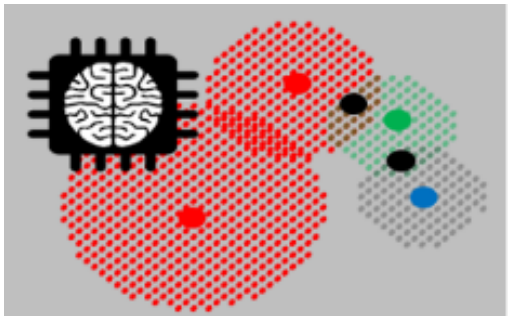
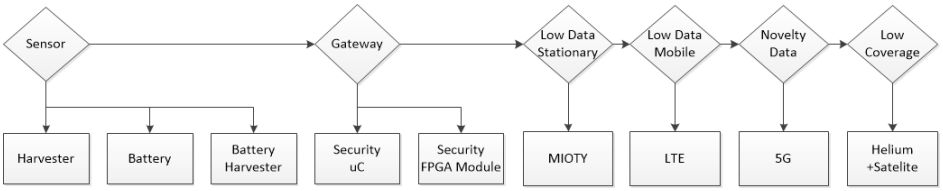


Figure 15: Neuromorphic clustering (known clusters & unoccupied feature space)

Putting these considerations together, this iNGENIOUS Use Case focuses on Mobile Edge Devices and pursues the following IoT landscape:

Co-funded by the Horizon 2020
Framework Programme of the European Union



The expected innovations from this use case are both application specific and generic.

The *application specific innovations* are:

- Freight Car Health Monitoring as an economically viable business case for more safety
- Edge-Network Power/Cost optimized, resulting in a technical solution meeting economic requirement
- Situational energy optimized edge computing for Rail Health Determination
- Economically feasible Rail Heath Monitoring for Rail Freight Logistics

The generic innovations are:

- New Concept for efficient data collection for machine learning applications. The concept uses context-based data clustering at the Edge using neuromorphic networks.
- Demonstration of Secure Communication concepts for End-to-End Communication with Encrypted Loads: A hardware/software co-design for a tile-based computer architecture is used to improve IoT device security based on an isolation-by-default design. A microkernel-based operating system called M^3 has been co-designed to run on this low-power tiled hardware architecture. A “tile” in this hardware platform (designed for system on chip, but currently realized as FPGA) can be a general-purpose processing core, an accelerator, or any other I/O device and all types of tiles are treated in the same way. All tiles are isolated by default and a custom “Trusted Communication Unit” (TCU) located between the tile and the Network on Chip (NoC) enables select communication on a need-to-cooperate basis. The TCU enables point-to-point communication between tiles (if configured by M^3 OS kernel based on a security policy) but disallows all other access the NoC and hence all other (unwanted) communication. In contrast to commonly used OS/hardware architectures in IoT devices, the TCUs help enforce the principle of least privilege by following a secure-by-default approach based on hardware-enforced isolation; security is not an afterthought, but the key design principle of the M^3 hardware/software co-design. The tiled hardware architecture together with the TCUs enables system designers enforce information flow in hardware; in this use case, it is used to implement an encryption component (to be placed between the sensor module and the network device) that guarantees that all communication between the sensor with its neuromorphic clustering module and the centralized data middleware in the operations / health monitoring centre are encrypted and integrity protected. Additionally, both endpoints are cryptographically identified based on Remote Attestation, which is a cryptographic protocol to enable trust in the end-to-end security of this IoT system.
- Multi-model Communication Concept for near seamless and bandwidth optimized communication between Edge Sensors and Cloud Applications: Ubiquitous connectivity with seamless switch between appropriate terrestrial and satellite communications links will be used.

Co-funded by the Horizon 2020
Framework Programme of the European Union

4.3 End User and Environment

End users for connected mobility and transport logistics platforms are Asset Owners, Asset Operators and Asset Users/Forwarders. Thus, since this use case focuses on Rail Health, it will be demonstrated with the support of Rail Health related Stakeholders, such as Nexxiot, a service provider for Rail IoT Data. Nexxiot with the help of their customers (e.g., VTG) will provide access to a rail logistic platform to allow data collection, machine learning development, and use case demonstration.

4.4 Actors

Transportation Platform Asset Owners and Leasing Companies: want to know the health of their assets. In case of problems, they want to be able to contact the asset operators to schedule maintenance.

Asset Operators: want to get early notification of maintenance events, so that they can schedule assets for maintenance in the most efficient way. Asset operators also want to minimize asset down time, so that operations do not get interrupted.

Logistic Forwarders: want to know where their assets are, so that they can manage the next logistic leg, and inform their customers of the logistics status. Forwarders are only an indirect participant of asset health information. The asset health information can be used to notify them of unscheduled downtimes.

4.5 Data and Service(s)

Data handling and services in this use case can be summarized as follows:

- *Rail Freight Car Wheel & Bearing Health Monitoring:* Edge Sensors for Data Collection, Data Collection, Data Engineering, Data Science with Multi-Level Algorithm for Defect Detection and Sensor Optimization.
- *Diverse Data Collection for Algorithm Verification:* Neuromorphic Edge Sensor for Context based Cluster Data Collection, Data Diversity Analysis and Blank Spot Estimation.

4.6 Asset(s)

The main assets involved in the development of this use case are:

- *Edge Sensors* will be used for condition monitoring of rail freight carriages and for continuous data stream signal novelty analysis. Sensors will integrate diverse IoT connectivity modules.
- *A secure communication module based on an FPGA* will implement the tile-based architecture described in Section 4.2. Ideally, for cost and power consumption reasons, a tight integration with the sensor/clustering module and the network device should be realized. However, in order to demonstrate this technology within the project duration the module will be provided as a separate FPGA device that connects to a sensor module. As a common denominator, the project aims at connecting a network gateway to their M3-based FPGA module via IP over Ethernet in order to get connectivity to the cloud / operations / health monitoring centre.
- *LTE-M/NB-IoT module or modem*. An option is to provide a small size embedded modem including a module from the Sequans Monarch family of solutions. Monarch is a single-chip

Co-funded by the Horizon 2020
Framework Programme of the European Union

LTE Cat-M1/Cat-NB1 solution where BB, RF transceiver, power management, and Random Access Memory (RAM) memory are integrated into a tiny 6.5 x 8.5 mm package, running carrier-proven LTE protocol stack, an OMA lightweight M2M (LWM2M) client for over-the-air device management, and a rich set of AT commands. The embedded modem features 1 U.FL port, connectivity via Serial Universal Asynchronous Receiver-Transmitter (UART) or USB, and is pin-compatible - with a 20-pin interface - for integration with the sensor solution. The embedded modem features throughputs of 375Kbps download and 375Kbps upload, supports cellular frequencies from 700MHz to 2.2GHz and also includes a removable Micro-SIM card slot.

- *Core 5G NSA and SA with CIoT support*, which might be deployed either on-site in the train and on the cloud. Also, with a compact 5G Core including CIoT compliant with 3GPP Release 13 to provide standalone private 5G network to be deployed locally on train and utilize satellite link for connecting to public Internet (i.e., cloud with IoT platform). And with a 5G core including CIoT to provide 5G network do be deployed on the cloud and utilize satellite link for connecting to radio base stations deployed on train or ship. The 5G core on the cloud might include local breakout (i.e. UPF) connected to the base stations on the train or ship.
- *Satellite ground system equipment* to include satellite hub will be installed already as SES teleport in Betzdorf, updated to support iNGENIOUS use case and other use cases within the project. And with a satellite modem installed in the ST Engineering iDirect engineering lab, including: ST Engineering iDirect satellite modem, 1.2m fixed antenna with associated BUC and LNB and associated cabling and routing equipment.
- *SES equipment* offered to the project is composed of: GEO satellite, Ku-band, Teleport uplink facilities in Betzdorf, Luxembourg, and IP/MPLS global teleport access network.

4.7 Requirements

User Requirements	Description
#1: Rail-Health Primary Targets.	User/Control-centre should be able to track location and monitor rail-wheel health (e.g., Flat-Spots, Flat-Spot Width, Bearing Defects) of transportation Platform in real-time.
#2: Edge Sensor Health	User/Control-centre should be able to monitor the Edge Sensor Health (e.g., sensor defects, battery level, etc).
#3: Railcar-Gateway-Sensor Mating	User/Control-centre should be able mate an edge sensor to a railcar dedicated gateway. (e.g., Railcar Type, Bogie Type, Suspension Type, Bearing Type, Axle Position, Rail-wheel Diameter, Installation Date, Sensor ID, Gateway ID, Cross-Sensor ID.
#4: Performance Evolution	User/Control-centre should be able to log diversity data via custom data logger for development of cloud-based health database (e.g., Neuromorphic Diversity Data Logger which is installed on Rail-Axles with defects which are called in for maintenance).
#5: Trend & Incident Alerts	User/Control-centre should be able alarmed on trending & critical events.
#6: Graphical user interface to manage/monitor the IoT backhaul options	User/Control-centre should be able to manage and monitor the IoT backhaul options.

System Requirements	Description
#1: Lifetime Operation.	The sensor should be able to monitor defect-free axles for 12yrs without maintenance (i.e., no battery replacement).

Co-funded by the Horizon 2020 Framework Programme of the European Union

#2: Connectivity Frequency.	The gateway should be able to operate up to 30 edge sensors and maintain cloud connectivity every 30 minutes for 12 years without maintenance (i.e., energy optimized Sensor-Gateway Protocol and COM Strategy, energy optimized Gateway-Cloud connectivity.
#3: Connectivity Coverage.	The gateway connectivity should be omni-presence to guarantee a Fault Communication Time within 30-minute intervals. This shall be achieved, if necessary, with alternative or redundant connectivity methods between Gateway and IP connectivity. (e.g., NB-IOT, LTE-M, Wi-Fi, TE-M, 5G, Satellite, etc.).
#4: Edge Storage.	In case of lost connectivity, sensors and gateways shall store relevant data until communication connectivity is restored.
#5: Multimodal Connectivity.	The Gateway shall scan for alternative connectivity modes in case the primary connectivity mode is lost or is not stable. See SR3.
#6: Monitoring Resolution.	The sensor shall monitor relevant motion event at least once every 120 minutes.
#7: Monitoring Capability.	The sensor shall differentiate between Flat-Spots, Flat-Spot Width, and Bearing Defects.
#8: Defect Validation via Cloud.	The sensor shall record highly probable defect data for cloud confirmation.
#9: Defect Validation via Gateway.	The gateway/sensor system shall enable defect confirmation via crosstalk evaluation.
#10: Security Attack (Phishing).	The gateway/sensor system shall be robust against security attacks.
#11: Security Attack (Listening).	The gateway/sensor/cloud communication shall have end-to-end security encryption.
#12: Security Attack (Programming).	The gateway/sensor firmware updates shall be robust against security attacks.
#13: Security Attack (Commanding).	In addition to protecting confidentiality and integrity of the communication channel between Platform and Control-centre, the identity of both endpoints should be validated using Remote Attestation. To ensure confidentiality, integrity, and availability of sensor data, it must be ensured that only correctly functioning (i.e., no fake or compromised) sensors are connected to the right and securely operated, cloud-hosted control centre / middle ware and vice versa. Remote Attestation solves this problem, as it provides a cryptographic link between a device identity anchored in a Root of Trust (in hardware).
#14: Local Data Encryption.	For asynchronous communications, the payload (e.g., metadata, raw data) shall be encrypted and cryptographically authenticated (e.g., signed) such that it can be stored securely when not in transmission (either locally on the Platform, or in Control-centre).
#15: Functional Safety.	Bearing fault detection shall be Safety Integrity Level 2 compliant.
#16: Fire/Explosion Safety.	The gateway/sensor electronic shall be ATEX certifiable.
#17: The radio access should be able to run local application processing when user selects low latency for selected applications.	The operator has visibility of the devices that will connect to the network and which of those devices require low latency if they have to be controlled remotely. The operator through some platform console should be able to select the devices that will be connected to applications that have to be running closer to the radio access. The operator will select those devices and the required computing resources.
#18: There should be an IP connection between the different radio access	The platform should be able to include multiple radio technologies that can be manged from common packet core. All those technologies should be connected to the core through IP

Co-funded by the Horizon 2020 Framework Programme of the European Union

technologies and mobile core for the signalling and user data.	connection; thus, the core will include the required protocols for each radio access technology.
#19: The platform shall be able to use the most appropriate radio technology depending on network access and communication demands.	The platform will integrate different radio technologies depending on the end device and the distance to the application or service that will process the data from the device. Thus, the depending on the device the platform should be able to utilize different radio technologies.
#20: Over-the-Air (OTA) upgradeability.	The platform shall support secure software updates and deployment (i.e., only updates from an authorized party are installed to ensure security and availability). To close previously unknown security vulnerabilities in the deployed device software, a valid new version must be able to be installed, but no fake/compromised update. Also, function updates are desirable to add new features or to adapt to new regulations/requirements.
#21: Satellite shall support multiprotocol data.	The satellite link that connects the 4G base-station, 5G base-station, LoRa gateway, or mobile edge gateway to the Internet must be capable of backhauling the data.
#22: The mobile edge gateway, and/or IoT Backhaul infrastructure, should be able to detect, monitor, and report on availability of backhaul connectivity.	The mobile edge gateway, and/or IoT Backhaul infrastructure, should detect the status of the backhaul connection. This will allow the operator to use the information for decision-making, and to troubleshoot the backhaul connections as part of a troubleshooting process. This requirement is different from #SR5 because #SR22 requests connectivity information for proactive connection decision-making in contrast to reactive connectivity.
#23: The mobile edge gateway, and/or IoT Backhaul infrastructure, must be configurable to allow the operator to configure the connectivity decision process, e.g. choice type of connectivity.	The mobile edge gateway, and/or IoT Backhaul infrastructure, runs a backhaul selection algorithm when required. The criteria used in the selection algorithm can be simple or complex.

4.8 Key Performance Indicators (KPIs)

KPI	Target Value	Verification Means
Autonomous Operability	12-year operability without maintenance. Up to five measurements per day.	Energy Simulation Endurance Testing
Critical Event Monitoring	Wake up on energy spikes	Energy Simulation Endurance Testing
Cost Effectiveness	Less than €25 per Sensor	Bill of Materials Concept below €12.50
Functional Safety	SIL Level 2 PFH/PFD Metrics	Fault Diagnostic Coverage, Sensor Fault Classification, Sensor Gateway Fault Classification, Sensor-Cloud Fault Classification
Fire & Explosion Safety	ATEX Compliance	Thermal Event Safety
Security Attack Robustness	Gateway-Cloud Security Senor-Gateway Security	End-to-End Security Payload Encryption Firmware Attack
Connectivity Coverage	Gap < 120 Minutes (Service)	Estimation

Co-funded by the Horizon 2020 Framework Programme of the European Union

	Gap < 30s (Catastrophic Events)	Simulation Measurement
Low End to End Delay	10ms (5G) 50ms (CIoT) 200ms	Via iperf tool
Low Latency MEC	5-20ms (5G, CIoT, Sat)	Via iperf tool

4.9 Operational, Business, Societal and Environmental Outcomes

The challenges of mobile edge IoT are the cost targets, given enough budget and resources anything is possible. However, the business case behind mobile edge IoT is based on cost reductions and productivity improvements.

Typically, maintenance on rail carriages is conducted every six years at a cost of 250€ per axle. There are virtually no failures. If maintenance could be extended to 12 years, then on average a cost saving of 230€ per axle is expected. Rail carriage wheel damage causes secondary damage to rail tracks. Carriages with health sensors are likely to cause less damage to infrastructure. This can result in marginally reduced rail network usage fees. Catastrophic failures typically are not singular events, but prolonged material degradations initiates by lesser events. Early detection of degradation can reduce catastrophic events which would not be identified in-time by regular maintenance intervals. Asset tracking transparency can enable better asset utilization. As well as asset status transparency can enable better asset management.

The resulting total cost advantage of Mobile Edge IoT can be summarized as follows:

- Just in Time Maintenance: 880€ per Rail Carriage per lifetime (Increase Maintenance interval from 6 years to 12 years where possible)
- Elimination of catastrophic events. €50 Million / 10 Years / 400k Carriages x 12 Years Maintenance Interval = 150€ per lifetime
- Better utilization or resources / productivity increase by 0.5% = 3750€ per lifetime

This translates into a cost-benefit of €4.780 per carriage per lifetime which must cover costs for:

$$Cost\ Benefit \geq Sensor\ HW + COM\ Cost + IT\ Cost + Other\ Cost + Overhead\ Cost$$

The cost of Data can be estimated as follows:

- GPS Data: Every 20min @ 10 Bytes
- Loading Data: Every 20min @ 10 Bytes
- Health Meta Data: Every 20min @ 10 Bytes
- Health Raw Data: Every 20min @ 150 Kbytes/wheel x 8 / Carriage

This total communication cost sums as follows:

$$Lifetime\ COM\ Cost = \frac{Data}{Day} * 36m \frac{Days}{Year} * 12\ Years * \frac{COMCOST}{GB}$$

In 2017, the average cost per Gigabyte of LTE connectivity was 13.4 EUR/GB, numbers in which are based the previous computations.

Freight rail health unlike passenger carriage health is a blue ocean. In this moment, there is not an economically scalable solution in the market. The potential market for digitalization of rail-heath assets in the next four years is estimated at 10mllion carriages. The potential maintenance savings alone would amount to 2,3billion EURO, half of which would have to be invested in new sensors and operational monitoring.

Co-funded by the Horizon 2020
Framework Programme of the European Union

4.10 Verification Means and Actors Involved

This use case will be validated by field and lab demonstrations and proof of concepts (PoC). The KPIs will be validated partially by physical demonstrators, and partially by simulations and estimations. All KPIs have been assigned to this use case partners and achievement will be assessed in joined review sessions. Those results will be presented to stakeholders and sponsors for further review. The two physical demonstrators will be:

- NeuroControls Freight Rail Health Sensor & Neuromorphic Cluster Logger, integrating the highlighted components in Figure 16.

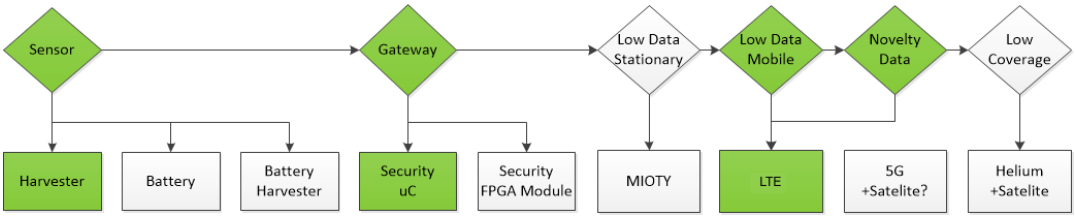


Figure 16: Sensor components to be evaluated in this use case.

- Barkhausen Institut state-of-art PoC for IoT computer hardware architecture, encryption technologies, end-point attestation. A block diagram of the architecture (without Root-o-Trust for remote attestation) is shown in Figure 17. An Ethernet device instead of a wireless modem could be used, if integrating the latter is not practical for the PoC.

Use case validation will be focused on:

- NeuroControls will demonstrate Edge Sensing Applications for dedicated and exploratory data driven edge tasks, edge sensors for condition and novelty monitoring, condition monitoring of railcars carriages (wheel flat spots and bearing defects) for 12-year autonomous power operation, continuous data stream signal novelty analysis and edge sensor demonstration with diverse IoT connectivity.

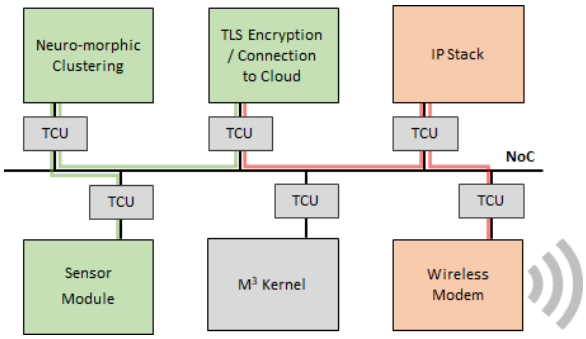


Figure 17: Secure-by-default embedded computer architecture for this use case

- Barkhausen Institute will demonstrate data encryption and integrity protection for secure communication based on state-of-the-art Transport Layer Security (TLS). The TLS implementation will be integrated with Remote Attestation service based on a Root-of-Trust (RoT) in the tile-based computer architecture running the M3 OS. Barkhausen Institut's hardware/software co-designed platform will be used to secure the communication channel between the sensor/clustering module and the centralized operations / health monitoring centre in a cloud server. Ways for secure and reliable software updates for the component based M3 architecture will potentially be investigated within this use case.
- Sequans will demonstrate low power LTE Connectivity on Smart Edge Devices, to be integrated with NeuroControl's sensor platform as indicated in Figure 16. This low-rate, low-power communication Cat-M/Cat-NB module/modem can be attached to cellular network (thus, using LTE-M/NB-IoT cellular technology) in order to provide real-time data from sensors' transportation platform health monitoring (orthogonal to end-to-security using the Barkhausen Institut platform).
- Cumucore, ST Engineering iDirect and SES will demonstrate Hotspot GSM/Satellite Connectivity for remote underdeveloped regions.

Co-funded by the Horizon 2020 Framework Programme of the European Union

5 Situational Understanding and Predictive Models in Smart Logistics

Nowadays, the rise of international trading and the continuous increase of the container vessel sizes are having a direct impact on the congestion of road operations at the entrance/exit of maritime ports and terminals. These factors, together with a bad scheduling for the flows of trucks entering and exiting port accesses, are leading to significant levels of congestions in peak traffic times at port facilities.

For monitoring and understanding the main cause of these issues, maritime ports and terminals collect events and data streams (e.g.: number of trucks, number of containers, scheduled time of arrival and departure for vessels) by means of sensors and digital systems and platforms. Nevertheless, data and information flows are treated separately by the different port entities, that is, there is not a holistic view of the available information. As a consequence, the disaggregation of the different data sources makes the prediction and optimization of the port performance an impossible task.

This use case focuses on enhancing the situational understanding of events in maritime ports and terminals by means of collecting and aggregating data processing. A subsequent optimization and prediction performed on this data will reduce the time that trucks spend inside the port and terminal facilities, i.e., truck turnaround times (TTT). The outcomes of the monitoring and optimization processes are expected to be visualized in a dashboard and map interface.

Depending on the service performed by trucks in maritime ports, the use case considers three possible operational actions:

- *Cargo Loading:* An unloaded truck enters the port and terminal facilities where it is loaded with a specific cargo; the truck leaves the terminal with an associated cargo afterwards.
- *Cargo Unloading:* A loaded truck enters the port and the terminal facilities, where the cargo is unloaded. After that, the unloaded truck leaves the terminal.
- *Cargo Unloading and Loading:* A loaded truck enters the port and the terminal facilities, where the cargo is unloaded. Once the cargo is unloaded, the truck is loaded with a new cargo and leaves the terminal and the port facilities with an associated cargo.

For the three considered operations, trucks perform a similar procedure for accessing and exiting the port and terminal facilities. As part of this procedure, data is collected when different events take place:

- Trucks access the maritime port in order to perform a loading/unloading operation. When a truck arrives to the port entrance, the plate and container number is read and the level of radioactivity of the truck is measured. If the vehicle is authorised to enter the port facilities,

Co-funded by the Horizon 2020
Framework Programme of the European Union

the data and time of access is registered, and the barrier is lifted. All data related to the port access is registered at the Port Community System (PCS) and/or at the port's M2M platform.

- After accessing the port facilities, the truck drives towards the terminal gate, where the truck identity is checked again. The date and time of access to the terminal together with the truck plate number is registered at the Terminal Operating System (TOS) and/or at the port's M2M platform.
- If the vehicle is authorised to enter the terminal, the truck accesses the terminal facilities where a loading or unloading operation is performed. The date and time when the loading/unloading operation is performed is also registered at the TOS and/or at the port M2M platform.
- After performing the loading/unloading operations, the truck leaves the terminal and the port facilities. For allowing the truck exit, the plate and container number is registered and validated to check if the truck is authorised to leave the terminal and the port with that associated cargo. The date and time of exit at the terminal and the port is registered at the TOS and PCS, respectively, and/or at the port M2M platform.

Along the aforementioned steps, different factors may affect the port and terminal operations, leading to congestion at the terrestrial segment:

- Delay when performing the driver and vehicle identification.
- Barrier delay at the port access.
- Traffic congestion at the port or the terminal access and at some locations inside the port facilities due to potential accidents, number of vessels port calling at the same time, etc.
- The truck has to wait for the cargo due to a delay at the vessel stops.
- Type and dimensions of the transported cargo.
- Harsh environmental conditions (wind, precipitations, visibility) making the operations slower.
- Size (#containers) of vessels port calling at the maritime port.
- Error in LPR/OCR phases which cause mismatch between entry and exit read plates.

5.1 Workflow

The objective of this use case resides on the development of analytical and predictive models to estimate and optimize trucks turnaround times in ports thanks to the aggregated ingestion of the different port and terminal data sources. Analysis and predictions of TTT will be performed by exploiting ML techniques that will allow to identify the TT times across the different phases (terminal TT, gate TT, idling times) of the port operative. Analytical and predictive services will be deployed at iNGENIOUS platform by exploiting REST API architecture. The outcome of the analysis and predictions will be visualized in a graphical interface composed of dashboards and maps.

Additionally, for enhancing the accuracy of situational understanding and predictive models, the use case will install real-time IoT tracking sensors on trucks as a new data source able to help estimating TTT. Tracking sensors will be integrated into the system architecture by considering wireless IoT technologies like LoRa [4], LTE-M or 5G. Network resources required for tracking trucks will be ensured by integrating a MANO component.

Considering the envisaged features, the workflow of events in the use case is detailed as follows (see Figure 18):

Co-funded by the Horizon 2020
Framework Programme of the European Union

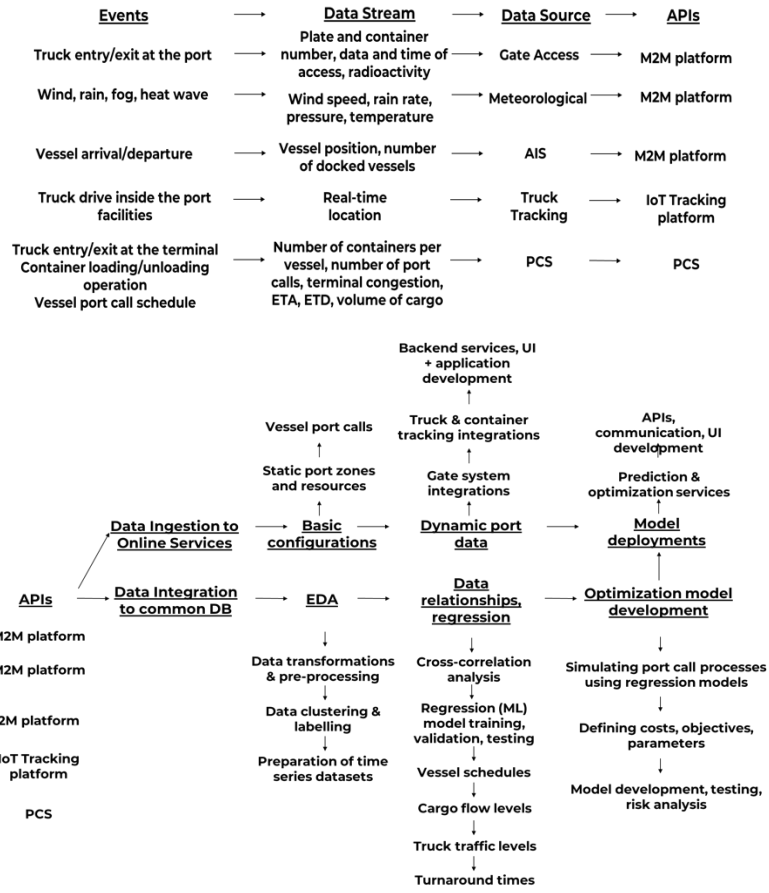


Figure 18: Use case flow chart

1. *Events:* Different events will occur due to the arrival and departure of trucks and vessels to the port and terminals. Events related to terminal operations and meteorological aspects will also be considered.
2. *Data Streams:* Events will generate multiple streams of data that will be relevant for the TTT prediction and optimization. On the one hand, truck access and driving events will be associated to truck plate numbers, container numbers, data and time of access and location of trucks. On the other hand, the scheduling and arrival of vessels will bring information related to the vessel identity, position, ETA and ETD, number of containers, number of port calls in a day, terminal congestion, etc. Additionally, meteorological information such as the wind speed, or rain rate will also be of interest for the TTT optimisation.
3. *Data Source and IoT Platforms:* Data streams will be produced and registered by sensors, systems and M2M platforms. Truck access and meteorological information will be collected by using gate access and meteorological sensors, and later gathered in a M2M platform. Vessel position, identity and number of docked vessels will be collected by the AIS. Real-time information will be collected by IoT tracking sensors installed on trucks. Finally, all data related to the port call scheduling, the arrival and departure of vessels will be collected at the PCS.

The next step can be divided into two main tracks: i) Data Analysis and Model Development, related to the analytics work performed using historical data sets, and ii) Service and Application Software Development, related to the software development work using integrated data sources. These tracks can be advanced in parallel, with the restriction that the final part of SW development is related to deployment of models developed in step i).

- *Data Analysis and Model Development* is performed offline and it is composed of different subtasks:

Co-funded by the Horizon 2020 Framework Programme of the European Union

- Data integration and Exploratory Data Analysis (EDA): All information included in data and services section will be integrated in a common database and analysed for performing the subsequent modelling. This analysis will include data transformations and pre-processing, data clustering and labelling and the preparation of time series data sets. For this last step new features like vessel traffic levels, congestion metrics, port call durations, cargo flow and truck traffic levels, and truck turnaround times will be defined.
- Definition of relationships and training of models: Exploration of relationships between the considered data sets and time series features, using for example: i) cross-correlation analysis, transfer functions ii) ML based regression model development and feature importance analysis, including the prediction models for port call features and events, e.g., berth/terminal occupancy prediction based on ETA and port call duration models.
- Optimization model and development: This phase is focused on the simulation of port call processes using prediction models outlined above. It will also include the definition of costs and objective functions (e.g., minimizing turnaround times), the definition of adjustable parameters and ranges (e.g., requested times of arrival for vessels and trucks), and model development, testing, and risks analysis.

- *Service and Application Software Development:* The development of real-time services and user interface-level demonstrations is divided into three phases requiring different data sources. On a high level, these phases are basic visualization of vessel port calls and static port resources and addition of dynamic resources such as trucks and containers:
  - Visualization of vessel port calls and static port resources: Basic port visualization requires of information on port infrastructure and static resources such as berth areas, names, and codes, terminal areas and types, gate locations, etc. Additionally, it also requires the integration of current port call information from some APIs such as national single window or port community systems.
  - Addition of dynamic resources: Dynamic visualization of port operations requires the integration of gate systems, container handling and truck tracking systems. After that, vessel traffic prediction model customization, training, and testing will be performed considering primarily destination, trajectory, and time of arrival prediction models.
- *Deployment of prediction and optimization models:* The last phase will be focused on the development and packaging of models following the micro services approach. This stage will require testing, verification and performance evaluation of models, as well as the access management configuration for external uses, and the implementation of messaging solutions and a visualization tool for exploring the outcomes of the deployed models.

5.2 Expected Innovation

The main innovation of this use case is focused on the development of new analytical and predictive models to estimate and optimize trucks turnaround times in ports. In addition to new ways of interaction and combination of the current techniques and data sources to create a richer data set and more accurate models.

The proposed innovations (dark blue blocks in the architecture picture shown in Figure 19) will be integrated together with the existing sensors, M2M platforms and other systems across the proposed architecture composed of four different layers or stacks.

For TTT real-time estimation and analysis the integration of all data sources at one place is also very important. For this particular case, the gathered data from the sources will be delivered to a novel cloud-based digital platform for maritime ports: Awake AI platform [5]. This platform will be used to provide the mentioned AI analytics.

Co-funded by the Horizon 2020
Framework Programme of the European Union

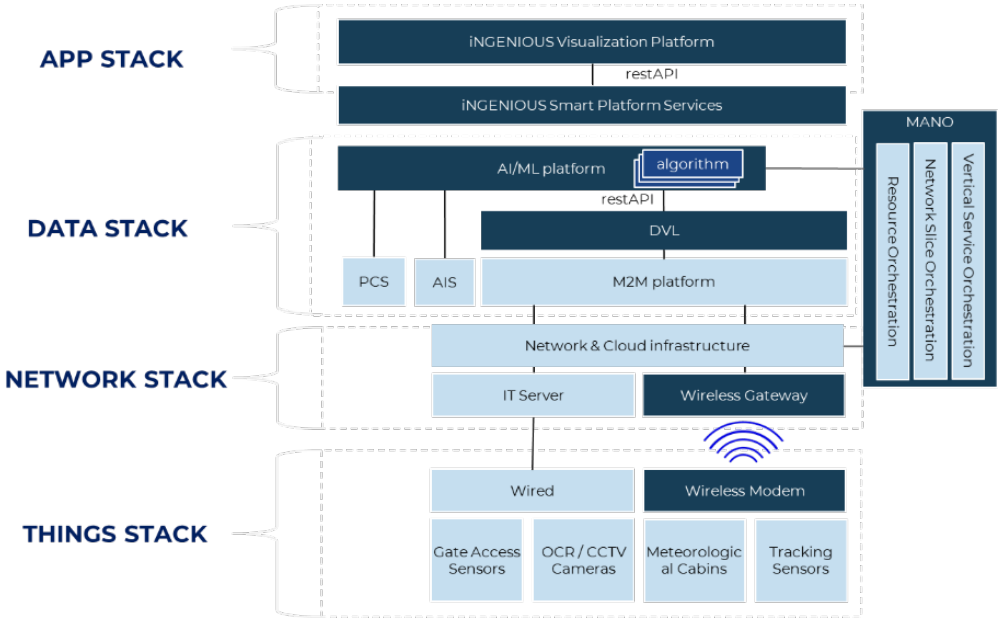


Figure 19: Use case stack diagram

Regarding prediction and estimation algorithms, there is a wide variety of techniques that could be explored for the port's TTT optimization. In this use case the usage of combinations of several techniques will be explored. Some of them to consider are Rule-based classifiers; regression models like Artificial Neural Networks [6] (a.k.a ANN), Random Forest Regressors or K-Nearest Neighbours regression; and even heuristic based algorithms. For the development of the model's various ML libraries will be used: TensorFlow [7] and PyTorch [8] for complex ANN model development and training, Sklearn [9] for ML modelling and data preparation, and Jupyter Notebook [10] as a development environment in data science, etc.

5.3 End User and Environment

This use case takes place in maritime ports and terminals involving different end users such as port authorities, port terminals, hauliers, freight forwarders, shipping agencies, etc.

5.4 Actors

Port Authorities will give access to the port infrastructure and the Port digital systems that could be used as data sources for enriching the turnaround estimation and prediction.

Port Terminals will give access to the port terminal infrastructure where trucks will enter and exit for the loading or unloading of cargo. Port and terminals facilities will be the scenario where the use case will be developed.

Hauliers will transport the cargo for performing loading or unloading operations inside the port and terminal facilities.

Sensor and IoT Providers will deploy sensors and IoT devices for collecting information on access, cargo tracking, meteorological conditions, arrival of vessels, etc.

Communication and Network Management entities will improve the wireless and IoT connectivity inside the port facilities for enabling the real-time tracking and the transmission of the data collected by the IoT sensors.

Big Data Analytics Providers will analyse and exploit the data collected by the different sensors and IoT devices in order to model and develop situational understanding and predictive models.

Co-funded by the Horizon 2020 Framework Programme of the European Union

This data will be made available on cloud-based platforms where data will be stored and made accessible through the use of APIs.

5.5 Data and Service(s)

The data streams to be exploited within this use case are split into five different categories depending on the source:

- *Gate access:* vehicle plate number, container plate number, data and time of access, truck driver data, truck radioactivity levels, cargo info (size, type).
- *Meteorological data:* wind speed, wind direction, precipitation, pressure, rain rate, average temperature.
- *Port Community System:* estimated time of arrival (ETA), real time of arrival (RTA), port call berth, estimated time of departure (ETD), actual time of departure (ATD), type/volume of cargo, number of full containers loaded per vessel, number of full containers unloaded per vessel, number of empty containers unloaded per vessel, number of port calling vessels, terminal, number of transport orders (import/export), shipping line, number of containers under inspection.
- *Automatic Identification System:* vessel position, number of docked vessels at the port terminal.
- *Additional next-generation IoT sources:* truck real-time position (IoT sensors), container position (IoT sensors), truck driver and operator fatigue levels (IoT sensors).

5.6 Asset(s)

The main assets involved in the development of this use case are:

IoT Sensors:

- *OCR and CCTV traffic cameras:* used to identify truck and container plate numbers.
- *Gate access sensors and PLCs:* used to detect the flow of trucks and the exact time at which trucks access. Also used to measure speed and heights.
- *On-board units/Road-side units (OBU/RSU) devices:* used to allow vehicular communications.
- *Meteorological cabins*: used to measure wind, rain gauge, visibility, humidity, etc.

Digital Systems:

- *Automatic Identification System (AIS):* provides real-time information about the positioning and identity of port calling vessels.
- *Port Community System (PCS):* provides information about port calls, estimated arrival times, and also gathers information related to terrestrial accesses.
- *Vehicle Booking System (VBS):* provides information about the appointments set between terminals and hauliers.
- *Port Management Information System (PMIS):* provides information about other management aspects related to the port operative.
- *Port Call Scheduling Systems:* provides information about the port call events and communicates the different entities involved in port call operative.

Digital Platforms and Network Infrastructure:

- *M2M Platforms:* Industrial IoT Platform for data capture, transformation and streaming (Data pool included).

Co-funded by the Horizon 2020 Framework Programme of the European Union

- *Computational platforms:* Pool of high computational and storage resources (private cloud and servers cluster).
- *Fixed access networks:* optic fibre backbone.
- *Wireless networks:* LTE/LTE-M/NB-IoT connectivity and experimental 5G networks.

5.7 Requirements

User Requirements	Description
#1: Users must get a real-time estimation of TTT in different scenarios	Different maritime port users like port authorities, terminal operators, hauliers and freight-forwarders must be able to obtain a real-time estimation and prediction of Truck Turnaround Times (TTT) depending on different operational factors such as the type of cargo, the terminal operator, the date and time of operation, etc.
#2: Users must have access to historical TTT through a web-service based application.	Different maritime port users like port authorities, terminal operators, hauliers and freight-forwarders must be able to access historical Truck Turnaround Times (TTT) related to the access, loading and discharge of cargo, and departure of trucks to port and terminal facilities through a web-service based application.
#3: Users should visualize real-time and historical TTT estimations.	Different maritime port users like port authorities, terminal operators, hauliers and freight-forwarders should be able to visualize the real-time and historical estimation of Truck Turnaround Times performed for each of the different processes carried out in the maritime port operation.
#4: Users must be able to keep their identity private and anonymous.	Maritime port users like hauliers should be able to keep private and anonymous their identity when involved in Truck Turnaround Times estimation and prediction processes. Additionally, data streams related to the identification of operational assets, e.g., truck plates, container numbers, real-time location of trucks, etc, should be considered as sensitive data, and therefore should be kept private and anonymous during the TTT estimation and prediction process.
#5: Users should visualize the predictions' performance metrics of the models.	Different port maritime users like port authorities, terminal operators, hauliers and freight-forwarders should be able to see the current predictions' performance metrics of the models in order to follow the estimations in more or less degree. These errors should be fully understandable by the end user, so the unit of measurement should be in % or in the unit of the parameter being predicted. For each prediction, there should be an API that will answer the corresponding estimated error (e.g., Mean Square Error (MSE), Mean Absolut Error (MAE)) to that forecast so that the user can take the decision to follow the prediction or not. The predictions should be stored in a database and the AI application should compute the performance metrics with the real values measured. The AI application visualization tool should display these metrics in real time.

System Requirements	Description
#1: Truck Turnaround Time prediction should be performed by exploiting online and offline data ingestion services.	Truck Turnaround Time estimation and prediction should be performed by exploiting both online and offline data ingestion services. Offline data ingestion services will be used for obtaining data coming from different sources like M2M platforms, PCS and AIS systems in order to develop and train AI-based prediction models. Online data ingestion will enable the retrieval of real-time data for performing and estimation and prediction of TTT.

Co-funded by the Horizon 2020 Framework Programme of the European Union

#2: Truck Turnaround Time estimation mean error should be reduced.	The system should provide predictions that are as reliable and adjusted as possible according to the available input data while aiming to minimize the performance metrics defined for the model as much as possible (MSE, Root Mean Square Error (RMSE), MAE, etc.)
#3: Truck Turnaround Time prediction should lead to increase the port and terminal performance.	Truck Turnaround Time prediction should optimise the existing port and terminal performance. In particular, the TTT prediction should be accurate enough in order to translate predicted times into operational gains.
#4: Data source sufficiency should be ensured to estimate and predict TTT.	Data source sufficiency must be ensured for obtaining different data streams that are required for modelling and predicting TTT. In particular, existing and new data sources in port and terminals like Gate Access and Meteorological sensors, Port Community Systems, Automatic Identification Systems, or IoT tracking devices, must be considered as valuable sources of information for modelling maritime and terrestrial logistics scenarios.
#5: Sensitive historical and real-time data must be pseudo anonymized.	Historical and real-time data obtained from existing and new data sources (Gate Access, Meteorological, PCS, AIS and IoT tracking) should be pseudo anonymized to preserve the users and asset's identity, as well as other data that could be identified as sensitive due to its relevance to the maritime port operative.
#6: Common database to ensure optimum data accessibility.	Historical and real-time data sets obtained from existing and new data sources such as Gate Access Systems, meteorological sensors, PCS, AIS and IoT tracking should be integrated into a common database to ensure an optimum data accessibility.
#7: Real-time tracking of trucks inside port and terminal facilities.	Real-time tracking of trucks inside port and terminal facilities should be enabled by installing IoT tracking devices on trucks. By tracking trucks, real-time positioning of vehicles could be used to identify potential bottlenecks inside the port facilities as well as to identify the specific path driven by trucks when collecting or dropping cargo.
#8: Web-service based application for visualizing Truck Turnaround Time estimation and prediction outcomes.	A web-service based application should be developed for visualizing TTT estimation and prediction outcomes. The visualization module must include a dashboard and an interactive maps interface in order to allow the graphic visualization of the TTT estimation for a specific day and the daily forecast in the short and medium term. The dashboard should be functional and intuitive for the end user.
#9: Capability to generate alerts of near future TTT peaks.	Sometimes, the user may be attending to other matters and not be aware of a future worsening of the port's performance metrics. Therefore, the system must be able to alert the user of this possible future situation. The tool must include the ability to generate alarms and notify the end users about future ports' performance metrics going below some predefined thresholds. Such metrics could be congestion levels, TTT values, long truck waiting times, etc. The threshold values can be entered manually end users or modified upon request to the cloud-based application via an API.
#10: Continuous (automatic) training capability of the situational understanding and predictive models.	To keep the quality of the cloud-based AI application predictions, the models should be able to be periodically validated with new test data that will be obtained through the storage of new ingested data coming from data sources. This will enable the update of the models in case the prediction performance falls below a predefined threshold. To do so, there should be an offline cycle-based job that continuously keep training the prediction models with new data gathered from data sources. This job can be triggered periodically or by a reduction

Co-funded by the Horizon 2020 Framework Programme of the European Union

	in their prediction's error metrics. The system should continuously monitor the performance of predictions.
#11: End-to-end integration of IoT tracking devices and visualization framework.	Tracking devices will be attached to trucks for monitoring their driving path inside the Port of Valencia. These devices should send the data to a cloud platform which will also be connected to the visualisation platform. With the E2E integration, the visualization of real time data as well as data storage in the cloud for historical data will be guaranteed.
#12: AI/ML module assisting MANO stores the data retrieved from DVL.	The ML-based module assisting the MANO shall be able to store IoT related application data collected from DVL in order to train the ML algorithms and find possible network slice optimization.
#13: Supply chain network slice onboarding.	The AI/ML assisted MANO shall provide dedicated interfaces/APIs to on-board supply chain network slice templates and descriptors.
#14: Lifecycle management of supply chain network slice	The AI/ML assisted MANO shall take care of the supply chain network slice lifecycle management. This means it shall provide mechanisms and procedures for the automated creation, operation and termination of network slices, taking care of interacting with the network and computing infrastructure (i.e., controllers, devices, etc.) to respectively provision, operate and release all the required network and computational resources according to supply chain requirements.
#15: AI/ML assisted MANO interaction with network and computing infrastructures.	The AI/ML assisted MANO shall be able to interface with controllers, network functions and devices in the network and computing infrastructures (such as RAN controllers, 5G Core functions, virtualized infrastructure managers) with the aim of provisioning and configuring resources for supply chain network slices according to the service requirements.
#16: AI/ML assisted network slice optimization.	The AI/ML assisted MANO shall provide ML-based automated mechanisms and procedures for proactively adjusting and adapting the provisioned supply chain network slices at runtime to optimize their performance profile, network and control functions size and location, network resources usage and configuration.
#17: Time event information on vessel, container, and truck movements.	To measure and model traffic flows in the port, it is necessary to have data at least on when resources such as vessels, containers, and trucks enter and leave the port. Such data can be aggregated to analyse the overall traffic levels and to estimate connections e.g., between vessel, container, and truck traffic volumes over time.
#18: Unique IDs for connecting vessel, container, and truck events.	Without unique identifiers for resources such as vessels, containers, and trucks, it is not possible to fully track and analyse the events and traffic patterns caused e.g., by the arrival and discharge of a container vessel. Therefore, time events as described in SR17 should be complemented by identifiers which enable e.g., tracking the movement of containers between vessels and trucks.
#19: Identification and measurement of idle waiting times for current truck turnarounds.	It can be assumed that a significant part of the truck turnaround time in a port is associated with operations such as handling documents, moving in the port, or loading and unloading cargo, which cannot be optimized using the means considered in the project. In contrast, congestion due e.g., to high container traffic volumes may result in increased idle waiting time, which could be reduced by predicting and mitigating congestion by improved scheduling and communication. To set realistic optimization targets, the statistics of optimizable waiting time should be known.
#20: Vessel arrival schedule prediction to estimate future traffic levels at port.	Vessel arrival times should be predicted as early as possible with low average error to enable estimating future traffic levels at port.

Co-funded by the Horizon 2020 Framework Programme of the European Union

#21: Data retrieval from M2M platforms by means of DVL.	In order to perform TTT prediction and optimization, it is necessary to store information coming from different events (and data sources) which take place as a consequence of the arrival and departure of trucks and vessels to/from maritime ports.
#22: Integration between DVL and Port Community Systems.	In order to perform TTT prediction and optimization, it is necessary to store information coming from different events (and data sources) which take place as a consequence of the arrival and departure of trucks and vessels to/from maritime ports.
#23: Integration between AI-based platform and DVL.	DVL must allow AI-based platform to consume aggregated data for the prediction algorithm training by means of an interface. Data will come from M2M platforms and External Systems.
#24: User's log-in operation.	The outcomes of the monitoring and optimization processes are expected to be visualized in a dashboard provided by the visualization platform. The access to this platform will be based on log-in operation from the users' side (ID and password).
#25: Data Virtualization Layer shall act as Pseudonymization Entity.	Personal Data should be anonymized as soon as possible avoiding being exposed in clear text. As DVL is the closest point to M2M (data generator from an Interoperable Layer point of view) it will have to act as Pseudonymization Entity.
#26: According to GDPR, any Personal Data shall be stored in pseudonymized form (pseudonym). Note: Personal Data should not be transferred across borders.	Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. According to GDPR, Personal Data can be pseudonymized to protect individual identity.
#27: Additional Information, used to reverse pseudonym, shall be stored in a separated encrypted repository.	Pseudonymization is a reversible process. To do it "additional information" (e.g., encryption keys, conversion Tables...) are necessary. This information has to be protected.
#28: Supply Chain Users shall only access the Personal Data for which they have been properly authorized.	Personal Data has to be accessible in clear format only by authorized entity.
#29: Storage of personal data shall follow specific retention times which are aligned with the purposes of processing. In addition, 'right to be forgotten' requests from Data Owner shall be considered.	Personal Data are not "for ever", they have to be deleted according to data owner's agreements. Furthermore, the data owner has the right to request the deletion of his personal data.
#30: Collection, processing, and transfer of personal data shall be limited to what is necessary for the purposes.	Personal data are retained only if strictly requested.
#31: Product shall implement appropriate Access Control and Access Rights Management.	Only personnel who has a valid reason to access personal data should be able to do so. Access shall be granted on a need-to-know basis, only for specific personnel that must perform a certain task with the personal data and only to specific set of personal data that needs to be known.
#32: Product shall support logging of privacy related events so that: Logs shall include information related to personal data processing	Logging privacy event is of crucial importance to create evidence to be used as audit trail, for example in case of a privacy breach to identify responsibilities and the root causes of the breach itself. This requirement is particularly important, because its implementation will put INGENIOUS in the position to provide the evidence of

Co-funded by the Horizon 2020 Framework Programme of the European Union

and Access to the logged privacy related event information shall be limited.	misusing the personal data, hence being on a much safer side in terms of legal liability.

5.8 Key Performance Indicators (KPIs)

KPIs	Target Value	Verification Means
Truck Turnaround Times Idling Times	10% reduction	Truck Turnaround Times and Idling Times will be calculated through data analytics simulations and analysed and validated with data obtained in real life demonstrations by means of real-time tracking data.
Time Prediction Accuracy	90%	Time prediction accuracy will be calculated by applying models' evaluation metrics commonly used in regression problems (MSPE, MSAE, R Square, etc.). Models' performance will be cross checked and validated with new available data different than the historical data used for models' training.
Positioning Accuracy	≤ 5 m	Positioning accuracy will be tested in real-life demonstrations by installing IoT positioning sensors on trucks. Positioning data received from the sensor will be stored and compared with actual path followed by the trucks.
Data Availability	≥ 99% uptime	The services querying the target data sources should store logs of the query results. The uptime can then be estimated as the ratio of successful vs. total number of queries over time.
Data Source Sufficiency	≥ 5 sources (PCS, AIS, Meteorological Data, Gate Access Sensors, IoT tracking sensors)	Data Source Sufficiency will be verified by inspecting the number of data sources available for calculating TTT in the considered maritime port scenarios. Additionally, other aspects such as the quality of data provided by a given source should be assessed, e.g., data does not provide an added value to the estimation.
Data Quality	Sufficient by ISO/IEC 25012 metrics	Data quality is expected to be ensured following the metrics defined by ISO/IEC 25012. The verification of these metrics will be ensured and adjusted before carrying out WP6 demonstrations.
Data Protection Impact Assessment (DPIA)	DPIA report approved	DPIA available and shared with UC owners and approved by DPO (Data Protection Officer)
Privacy User Guide Availability	Privacy User Guide approved	Privacy User Guide is available and shared with UC owners and approved by DPO (Data Protection Officer)
Confidentiality and integrity protection of personal data	100%	Controlling any sensitive data at rest, in transit and in use, it is never in clear text format
Logs of privacy events	100%	Analysis of whatever privacy event logs shall not contain cleartext personal data

Co-funded by the Horizon 2020 Framework Programme of the European Union

5.9 Operational, Business, Societal and Environmental Outcomes

Operational Outcomes: The analysis of turnaround time KPIs of ports and its terminals will generate accurate reports about port and terminals' performance KPIs. The development of predictive models using vessel traffic could also contribute to develop a potential single window. The creation of a web-service based application will help to deliver TTT predictions and analytics.

Environmental Outcomes: The usage of optimization algorithms to develop a truck transaction booking system will lead to minimize waiting times and ensuring a more efficient operation and reducing emissions caused by truck congestions. Reducing congestions could lead to improve the city operative in cases where the port is located inside the city.

Business Outcomes: The development of the use case will contribute to transfer pilot's knowledge via consulting services to other logistics operators and ports.

5.10 Verification Means and Actors Involved

This use case will be verified by performing real demonstrations for optimising truck turnaround times and other operations (waiting time, number of moves per vehicle, queue length, etc.) at the Port of Valencia and the Port of Livorno.

The Port of Valencia is the sixth largest port in Europe in terms of traffic volume, being the top port in the Mediterranean in import, export and transhipment operations.

The access procedure performed by trucks to enter and exit the Port of Valencia is the following: usually, freight forwarders notify the expected time for collecting or dropping the container to the truck driver with 24h in advance for both import and export operations. Nevertheless, in some particular cases, the forwarder could let the container stored in CT area for some time by paying a fee.

Figure 20: Port of Valencia

Considering that the trucker goes to the port to drop or collect the container, the procedure is:

1. Trucks drive through the South Access of the Port of Valencia for performing a loading/unloading operation. When the truck arrives to the port entrance, the plate and

Co-funded by the Horizon 2020 Framework Programme of the European Union

container number is read and the level of radioactivity of the truck is measured. Then the vehicle is authorised to enter the port facilities, the data and time of access is registered, and the barrier is lifted. All data related to the port access is registered at the port M2M platform.

2. After accessing the port facilities, the truck drives towards the terminal gate. Before reaching the terminal gate, some truckers are able to check the pre-gate status via a mobile app depending on the assigned terminal (only available at COSCO Terminal). Once the truck reaches the terminal gate, the truck plate number and the container number are read, and this data is checked and compared with the information on at the transport order. This query is performed by the terminal thanks to the connection between the PCS and the TOS.
3. If the vehicle is authorised to enter the terminal, the barrier is lifted, the date and time of access is registered at the TOS and the PCS, and the terminal operator gives some additional information to the trucker for picking or dropping the container, e.g., location of the container, crane number, etc. This information is also sent to the crane operator for identifying the desired container in case of imports.
4. The truck arrives to the terminal location and the container is loaded/unloaded. After performing this event, the crane sends a CODECO message for notifying the operation.
5. In the loading case, the container leaves the terminal gate where the truck plate number, the container number and the Customs status of the cargo is checked through the TOS, the PCS and Customs status. If the Customs status is not authorised, the trucker is not allowed to leave the terminal.
6. After leaving the terminal, the truck drives towards the South Access where a new truck plate, container number, radioactivity and PCS query for checking the Customs status is performed. In case any radioactivity or Customs status issues are faced, all barriers are blocked, the truck is inspected, and it may be even forced to drive back to the terminal through the return lane. Additionally, at the exit random periodic inspections can performed for empty containers.

Regarding LTE-M/NB-IoT connectivity, it is not confirmed yet if there is full coverage for these technological solutions at whole port area. In case full LTE-M coverage cannot be guaranteed, commercial LTE connectivity will be used.

The data sources of interest available at the Port of Valencia are:

- *Gate Access Systems:* Vehicle Plate Number, Container Plate Number, Data and Time of Access, Radioactivity Levels
- *Meteorological:* Wind Speed, Wind Direction, Precipitation, Average Temperature, Humidity
- *ValenciaPCS:* Estimated Time of Arrival (ETA), Real Time of Arrival (RTA), Port Call Berth, Estimated Time of Departure (ETD), Actual Time of Departure (ATD), Type/volume of Cargo, Number of full containers loaded per vessel, Number of full containers unloaded per vessel, Number of empty containers unloaded per vessel, Number of port calling vessels, Terminal, Number of transport orders (import/export), shipping line, Number of containers under inspection, etc.
- *Automatic Identification System:* AIS Receiver Data

Port of Livorno is one of the largest ports in the Mediterranean Sea, becoming an essential enabler for Tuscany's commercial and leisure industries.

Regarding port accesses, the port of Livorno does not have a single access gate due to its geographical position. There are several distributed gates in order to access the container terminal operative areas; these unique gates guarantee at the same time the access to the Port of Livorno.

Co-funded by the Horizon 2020
Framework Programme of the European Union

In terms of connectivity, the Port of Livorno confirmed there is NB-IoT/LTE-M coverage at that area. Connectivity can be reached by purchasing SIM cards.

Regarding access procedure at the Port of Livorno, usually freight forwarders need to get the container as fast as possible and this is why they try to notify the expected time of arrival to the truck driver as soon as possible (24h/48h in advance).

In export operations, containers accept time windows are available within the container terminal website. Based on this, the forwarder provides the information to the truck driver so that he can deliver the container within the expected time window. In imports, the forwarder checks the container status through TPCS (Tuscan Port Community System). In case the container has been already unloaded form the vessel, the forwarder asks the truck driver to take charge of it. In case the container is still under customs control, the forwarder should wait until all controls are finished. In some particular cases, the forwarder could choose to let the container stored in CT area for some time by paying the relative exemption.

Considering that the trucker goes to the port to drop or collect the container, the procedure is:

1. The truck driver scans his own badge to get permission to access Container Terminal gate and perform container loading/unloading operations (if not available, a releasing procedure will be activated first). The plate number is recorded. The CT gate operator checks some relevant documentation (e.g., identity card, truck plate number, etc.) and provides (in case of success) a document named Interchange so that the truck's driver can reach the proper destination within the CT area (depends on IMPORT/EXPORT operations). Interchange document includes information like container number, vessel code, stacking and storage position.
2. The truck's driver reaches the destination reported within Interchange. From now, CT's operators will load/unload the requested container checking truck's driver authorization by means of Tablets. When the loading/unloading operations are finalized, the CT operator updates the container status (container loaded or unloaded event) via their Terminal Operating System (TOS). This information is shared with TPCS by means of File Transfer Protocol (FTP) protocol (COARRI and CODECO EDIFACT files). When TPCS receives these files, gate-in or gate-out (CODECO) events as well as loading/unloading from vessel operations (COARRI) can be considered fulfilled. The truck exits the gate terminal and the plate number is recorded again.

The data sources of interest available at the Port of Livorno are:

- *Port Community System (TPCS):* Provides IMPORT and EXPORT data (MMA and MMP – incoming/outcoming cargo manifests).
- *Gate Transit Security (GTS3):* Detects trucks' transit at gates (plate number, transit time, truck driver info, etc.).
- *Port Monitoring System (MonI.C.A.):* Port of Livorno Digital Twin for monitoring purposes (vessels forecast, IoT data, dangerous goods).
- *AIS Dispatcher:* AIS data from IHS Markit and Nation AIS network.
- *Meteorological Station:* provides real-time weather data within Port of Livorno area (pressure, temperature, dew point, rain rate, daily rain).
- *M2M Standard Platform:* collects data from IoT networks.
- *Vehicle Booking System (VBS):* alpha version for trucks arrival management (ETA, plate number, truck driver data, destination, departure, cargo info, etc.

Co-funded by the Horizon 2020
Framework Programme of the European Union

Figure 21: Port of Livorno

Co-funded by the Horizon 2020
Framework Programme of the European Union

6 Improve Driver's Safety with MR and Haptic Solutions

Although Automated Guided Vehicles (AGVs) for the transportation of goods can be found, there is no evidence about driving them remotely using Mixed Reality (MR) and haptic solutions concerning the driver´s safety. This makes the use case a very novel solution that motivates this project to envision a submission for a potential UC contribution to the 5GAA standardization [11]. Although there will be action points that can be optimistically satisfied, the biggest challenge is to satisfy an end-to-end (E2E) wireless communication with reasonably good throughput at its lowest latency. Additionally, there is an existing non-5G public Base Station (BS) infrastructure that needs to be adapted for the purpose. There is no evidence that any remote-controlled cockpit has been ever implemented at the site, requiring the new Internet of Things (IoT) devices to connect a futuristic devised cockpit to the backhaul.

This safety-centric UC aims at providing improved driver's safety with MR and haptic solutions to remotely control the transportation of goods along a maritime port using AGVs for the aid (when necessary) of the fully automated transport system. This is performed via an immersive remote indoor cockpit wirelessly connected to an IoT 5G Radio Access Network (RAN) with corresponding data control services at a compatible far-edge Multi-access Edge Computing (MEC) and related Core Network infrastructure. This is achieved by a tactile internet, edge computing and immersive enablers (MR engines, haptic gloves) allowing operators to remote control the AGVs in a safe mode by standing away from outdoors where hazardous working environments and adverse weather conditions can be encountered.

Telepresence is supported by two 180º low-latency video cameras and some proximity sensors installed in AGVs. These cameras and sensors are used for the Mixed Reality (MR) 3D visualisation delivered to the cockpit´s controller. Additionally, a 5G network is used to provide uplink and downlink connectivity to all cameras and sensors installed on the vehicles and the hosting of MEC applications. The UC diagram of connectivity is shown in Figure 22.

Co-funded by the Horizon 2020
Framework Programme of the European Union

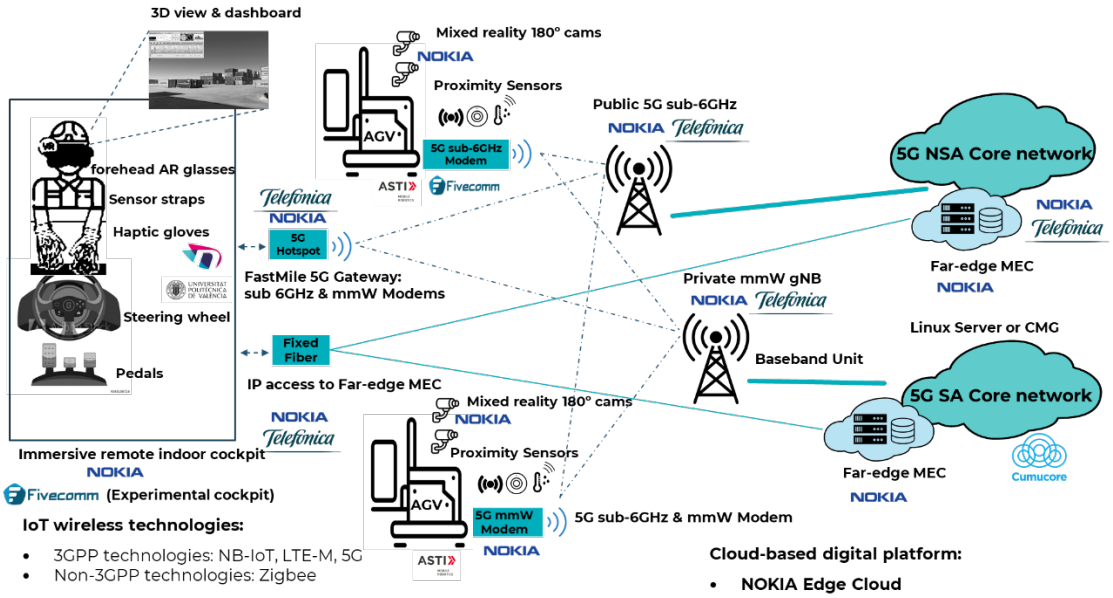


Figure 22: Overall architecture showing the immersive devices in the driver's safety use case.

6.1 Workflow

In order to fulfill the challenges and tasks of the use case, the following workflow actions have been defined:

- Automated routes for the transport of goods in the maritime port terminal will be defined. AGVs will follow this close loop programmed route with stopovers for the loading/unloading of assigned bays.
- Each AGV will be equipped with two 180º cameras and proximity sensors to monitor its route and automatically detect unexpected behaviours from an immersive remote indoor cockpit wirelessly.
- Each AGV is further equipped with either a 5G sub-6GHz Modem or a 5G millimetre wave (mmW) Modem for uplink and downlink communication to a Public 5G sub-6GHz for the former and/or to a Private mmW gNB for the later.
- These Public 5G sub-6GHz and/or Private mmW gNB deliver the data communication to the far-edge MEC (cloud-based digital platform) up to either a Standalone / Non-standalone (SA/NSA) 5G Core network for data processing and is bounced back to the AGV and/or to devised cockpit for the remote driving.
- On mission, the self-driving AGV load/unload goods from origin to destination and the immersive remote indoor cockpit allows the operator to take full control of the AGV remotely and perform alternative missions in non-automated zones.
- During the round-trip mission, the AGV sends real-time positioning and status updates to the network infrastructure that is acknowledged by the immersive remote indoor cockpit.
- The immersive remote indoor cockpit enables telepresence and controls the AGV wirelessly by an operator fully equipped with forehead Augmented Reality (AR) glasses (for the 3D view & dashboard of the real scene) + a sensor trackband and haptic gloves + steering wheel and pedals.
- Through these haptic gloves and sensor strap, tactile sensations are felt by the operator and in the event of immediate risks. The immersive remote indoor cockpit is additionally in charge for the translation of these sensations to a far-edge MEC via fixed fibre (IP access) and/or 5G Hotspot (FastMile 5G Gateway: sub-6GHz & mmW Modems) wirelessly. Haptic

Co-funded by the Horizon 2020
Framework Programme of the European Union

gloves and sensor trackbands together with a steering wheel and pedals will also capture hand-arm displacement during the remote driving and register biometric signals that provide information about driver's psychological and physical status.

The corresponding use case stack diagram is shown in Figure 23.

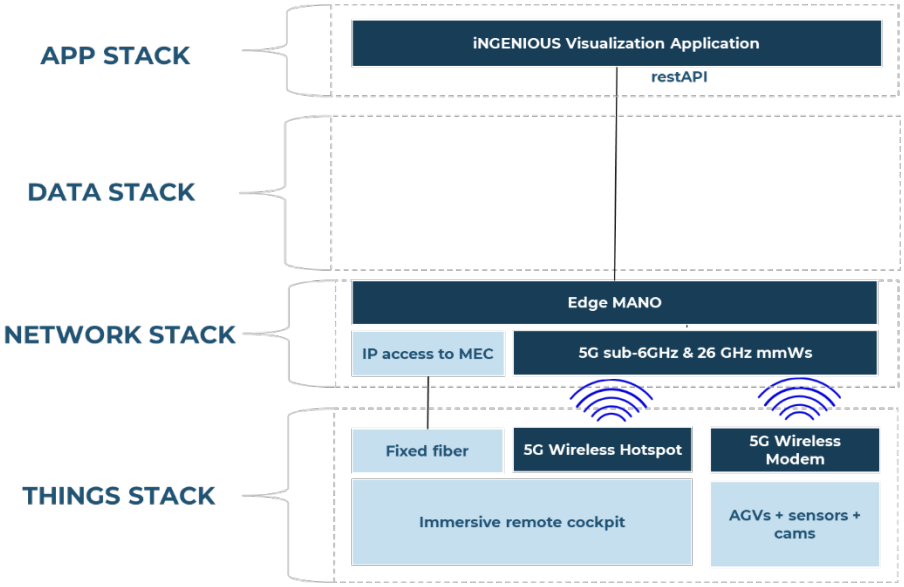


Figure 23: Use Case Stack diagram

6.2 Expected Innovation

The main innovation comes from the fact that is a novel UC to the community and there is no evidence about driving AGVs remotely using Mixed Reality (MR) supported by haptic solutions for the sake of the driver´s safety from a futuristic immersive remote indoor cockpit.

The realisation of the futuristic immersive remote indoor cockpit supports the improved driver's safety using an end-to-end (E2E) wireless communication with throughput guarantees at its lowest latency. Additionally, another innovation is the deployment of a novel Time-Sensitive Networking Application Function (TSN-AF) that maps 5G network slicing with fixed TSN Central Network Controller (CNC) polices.

Finally, these innovations are supported by a potential submission of this UC contribution to the 5GAA standardization [11].

6.3 End User and Environment

The end users of this use case are the port authorities, the port terminals, the hauliers and the freight forwarders. Additionally, the concerning environment around this use case is the maritime port.

6.4 Actors

Port Authorities will give access to the Port of Valencia´s terminal, infrastructure and its digital content.

Hauliers will intelligently and immersivity transport the cargo in the terminal.

Sensors and IoT providers will provide cameras, proximity sensors and IoT for collecting information on access, cargo tracking, meteorological conditions, driver´s condition, etc.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Automation industries will provide AGVs with corresponding hardware and software interfaces for connectivity and application development.

Radio communications and network providers will provide wireless 5G/IoT connectivity in the port for enabling real-time tracking and E2E data communications and a core network to support for Narrow Band IoT (NB-IoT) and Time Sensitive Networking (TSN) features.

6.5 Data and Service(s)

The data used in this use case involves:

- Videos automatically recorded in AGV´s tracks.
- 3D models of the maritime port infrastructures.
- Biometric information from immersive gloves and trackbands.
- Casual driving of the AGV.
- Network function and network slice statistics.
- Monitoring data of 5G connectivity to AGVs.

Parallelly the services involved in this use case are:

- Automated routes of AGVs for the transport of goods in the maritime port terminal with dedicated support (i.e.: when stuck in unexpected circumstances) by human decision/control.
- Remote supervision of the self-driving AGV through the immersive remote indoor cockpit with immediate decision making to manual mode control.
- Human safety since the AGV is controlled (when needed) remotely from indoors.
- E2E wireless communication with good reasonable throughput at its lowest latency.

6.6 Asset(s)

The assets to be used for the realization of UC are the following:

- Port of Valencia: Zone 0 - offices, Zone 1 - car park, Zone 2 - handling terminal.
- An AGV with two 180º cameras and proximity sensors for the handling and supervision, supported by 5G communication and teleoperation, visual navigation, advanced traffic, and perceptive abilities. A control software is implemented for communication to the edge computing.
- A 5G sub-6GHz and/or a 5G mmW modem.
- An immersive remote indoor cockpit composed of: forehead AR glasses, a sensor strap and haptic gloves and a steering wheel and pedals.
- Fixed fibre (IP access) and/or 5G Hotspot (FastMile 5G Gateway: sub-6GHz & mmW modems).
- A Public 5G sub-6GHz and/or a Private mmW gNB.
- A far-edge 5G MEC with some virtual network functions (VNFs) and remote-control application to support the immersive remote indoor cockpit features; a new visual experience and interactivity using AR Engine, rendering, video encoding and streamed augmentation.
- An SA and/or an NSA 5G Core network.
- An SA 5GC with network functions for device monitoring and management.

Co-funded by the Horizon 2020 Framework Programme of the European Union

6.7 Requirements

User Requirements	Description
#1: The devices should include a 5G module that will provide the device 5G connectivity. The device should have secure mechanism for authenticating and authorizing the device. The user should be able to place the 5G modem on the AGV with the nano-SIM and automatically will authenticate and connect to the 5G mobile network.	The devices should include a 5G module that will provide the device 5G connectivity. The device should have secure mechanism for authenticating and authorizing the device.
#2: The end-user, via the management console should be able to allocate selected devices identified by SIM information to different network slices differentiated by the levels of delay, reliability and bandwidth.	The network manager should have a console that allows to easily select the devices based on the SIM credentials and assign them to different network slice based on the traffic requirement.
#3: The end-user, via the management console should be able to select the devices that should be able to access different parts of the fixed network according to the definition of industrial security zones (IEC 62443).	A management console is required for the network manager to operate the system and map 5G network slices into industrial security zones. The console should allow the network operator to select the devices based on security identity and assign the network slice and the security zone the device can access.
#4: The end-user should be able to drive and control the AGV remotely and in real-time by using the immersive remote cockpit, using Mixed Reality (MR) and haptic solutions for the sake of the driver´s safety. The control is performed upon the end-user´s wish as it can swap from automatic to manual mode easily, but the other way around can but is more tedious.	The futuristic cockpit is intended to respond accurately and in real-time so that the controller (end user) can operate the AGVs remotely (automatic to manual mode and vice versa) from a safer location.
#5: The immersive remote indoor cockpit should connect wirelessly to an IoT 5G Radio Access Network (RAN) with corresponding data control services at a compatible far-edge Multi-access Edge Computing (MEC) and related Core Network infrastructure.	The futuristic cockpit is intended to connect to the network infrastructure for the provision of corresponding data control services.

System Requirements	Description
#1: The RAN should support network slicing, to be managed from the 5GC management console to allocate devices to different slices and define the parts of the fixed LAN that each device can access.	The RAN and network should support network slicing to be able to assign different slices with different resources to different applications and connect those slices to different parts of fixed networks.
#2: All data transmitted and received for the remote control of AGVs should be secured avoiding security threats (e.g., hijacking).	Cargo ports like the Port of Valencia are critical infrastructures where critical and risky operations take place. Some examples of these operations are the management of containers in container yards, vessel docking, management of dangerous goods, etc. In this use case, the remote control of heavy machinery is an operation that needs to be very carefully carried out in order to avoid fatal accidents or huge damages to property.

Co-funded by the Horizon 2020
Framework Programme of the European Union

	For this reason, the supporting 5G network infrastructure should provide secured and isolated communications, to avoid data link interferences, spoofing and hijacking. In some critical port operations requiring high accuracy in the manoeuvres, like loading/unloading of containers or remote docking of huge vessels, the supporting communications infrastructure should definitely ensure very high reliability and ultra-secured links. The 5G network used must include the ability of creating highly isolated network resources for this kind of operations.
#3: The 5G network shall provide sufficiently low latency to ensure the immersive experience when controlling the AGVs.	To feel a real immersive experience with the gloves, a low latency specification is needed. Otherwise, the delay would be appreciable by the user and the experience would not be immersive.
#4: The 5G network should ensure enough system capacity in terms of throughput to send the data in real-time from AGVs to the VR devices. This also includes control data.	VR video requires a high data rate to have a proper user experience. For this purpose, enough throughput is needed. The data transmitted will include VR video data and control data.
#5: Telepresence should be supported by 2 x 180o low-latency video cameras and other proximity sensors installed in AGVs.	The futuristic cockpit is provisioned with the IoTs (cams and sensors) that are mounted in the AGVs.
#6: A 5G sub-6GHz Modem or a 5G millimetre wave (mmW) Modem should be installed in the AGV for enabling up- and down-link communication to a Public 5G sub-6GHz and/or Private mmW gNB.	AGVs are provisioned with a modem to communicate wirelessly to the network infrastructure and the cockpit.
#7: The cockpit should be fully equipped with forehead Augmented Reality (AR) glasses (for the 3D view & dashboard of the real scene) + a sensor trackband and haptic gloves + steering wheel and pedals.	The futuristic cockpit is provisioned with all the necessary equipment to offer a cockpit with full immersive features.
#8: The cockpit should wirelessly deliver communication to far-edge MEC via fixed fibre (IP access) and/or 5G Hotspot (FastMile 5G Gateway: sub-6GHz & mmW Modems).	The futuristic cockpit is provisioned with a fixed fibre and a 5G hotspot to communicate wirelessly to the network infrastructure.
#9: AGVs should incorporate the necessary security to avoid collisions and accidents in case of no 5G connectivity or human errors. This may be implemented using sensors or restricted locations.	Security is as high impact consideration when talking about remote controlling. A security system should be implemented to contemplate the risks of a network or human error. This can be implemented with sensors or restricted areas to avoid the AGV entering in a dangerous zone or getting too close to other objects or humans. The installation should be carefully planned in advance in order to identify the necessary works to be done on the field where the use case pilot will take place. The works should follow all the security and time schedule protocols of the Port Authority of Valencia.
#10: Adapt current port's infrastructure to the 5G equipment	The installation of 5G network equipment in a heavy industrial environment like in a port is not an easy task. The installation of

Co-funded by the Horizon 2020 Framework Programme of the European Union

installation maximizing the reuse of existing resources.	antennas, edge nodes or optical fibre cables, usually requires civil works at the port facilities. As the port is a critical infrastructure, these processes must follow strict security and time protocols. Such works should not interfere with the port's normal activities. For the above reasons, the installation of new equipment for the realization of the use case demonstration should be adapted to the current public infrastructure. The installation of the necessary equipment on the field (i.e., the port) should make use, where possible, of available infrastructure such as lampposts, refrigerated site huts, optical fibre ring, etc. The installation should be carefully planned in advance in order to identify the necessary works to be done on the field where the use case pilot will take place. The works should follow all the security and time schedule protocols of the Port Authority of Valencia.
#11: Satisfy an end-to-end (E2E) wireless communication with good reasonable throughput at its lowest latency.	The Improve Drivers' Safety with MR and Haptic Solutions is provisioned with end-to-end (E2E) latency as determined in the actual project proposal.
#12: An Internet of Things (IoT) devices to be used to connect a devised cockpit to the backhaul.	The futuristic cockpit is provisioned with the IoTs functionalities to the backhaul.

6.8 Key Performance Indicators (KPIs)

KPI	Target Value	Verification Means
Time to capture one video frame	8.33ms	Product sheet, loopback encoding tests
Time to encode one video frame	33.33ms	Product sheet, loopback encoding tests
E2E Latency round trip	65.00ms	Network tests ping, messages timestamps
Transmission delay	5.56ms	Network field tests, configuration parameters
Time to decode one video frame	10.00ms	Product sheet, loopback decoding tests
Time to render one video frame	5.00ms	Product sheet, loopback displaying tests
Human factor video	20.00ms	External studies
Car command exec delay	10.00ms	Network field tests
Cockpit sensing delay	40.00ms	Product sheet, loopback encoding tests
Encoded video bitframe	20.00ms	Encoder configuration
Transmission bitrate	60.00ms	Network field tests
Encoded Video Frames per second	60.00ms	Encoder configuration
Latency for Uplink channel	40.00ms	Network field tests

Co-funded by the Horizon 2020 Framework Programme of the European Union

Latency for Downlink channel	25.00ms	Network field test
Human factor Glove Actuator	rising 9.00ms falling 15.00ms	Actuators' manufacturer datasheet specs
End-to-End latency	<100ms	Network field tests
Throughput for VR support	>25 Mbps (depending on video quality)	Network field tests
Availability	>99.999 %	Network field tests
Reliability	>99.999 %	Network field tests
Mobility	<30 km/h	Network field tests
Network slicing	8 slices/UE	Network manager can assign a top of 8 slices to each UE
Security	Slice-Security zone	Traffic allocated to different slice will be confined to the security zone associated to each slice
Network slicing	QFI per slice	Traffic assigned to different slice will be assigned different QoS flow ID (QFI) and RAN and priority at network transport

6.9 Operational, Business, Societal and Environmental Outcomes

This use case revolutionizes the supply chain from an automated handling of goods using tailored AGVs at the port terminal. The use case also improves labour health & safety thanks to the human controller at the immersive remote indoor cockpit by circumventing outdoors hazardous scenarios and exposure to adverse weather conditions. Additionally, is offers scalability, since the solution can be escalated to other sites and/or to multiple AGVs, improving the distribution and delivery time of goods, while allowing the multiple sites to be remotely controlled by a single controller (human).

This benefits the operational, business, societal and environment since the current supply chain is revolutionised with an optimised track & trace delivery of goods that leads to a better operational setting with implicated better business and revenue as a result that brings the attention to current and potential stakeholders for investment. The outdoor unmanned supply chain that brings the immersive remote indoor cockpit has a double benefit effect, the improved operational setting, and an improved societal and environmental contribution since humans (the controllers) remain indoors. The controller guarantees the secure transport of goods and because staff remain indoors it is easy to spot burglars in the surroundings since no human should be at the handling terminal (outdoors). This brings additional cost-savings to the operational business, and the data that is in the cloud could be used for a constant health & safety monitoring of the employee (the controller) contributing to the general wellbeing position of the company and implicated cost.

6.10 Verification Means and Actors Involved

Verification is made by demonstration, validated by implementing the proposed UC improved driver´s safety with MR and haptic solution experimentally and evaluated in a real scenario, the Port of Valencia. Through this demonstration, the requirements and KPIs are validated and evaluated. Certain simulations might complement this evaluation prior experimental results. The following technical outcomes ensure the verification means:

- Broadband 5G-IoT up- and down-link communications for the control of the AGV remotely.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- Data from the AGV and its environment collected in the 5G cloud (far-edge MEC).
- An immersive remote indoor cockpit with end-to-end (E2E) wireless communications with good reasonable throughput at its lowest latency.

The partners involved in this use case are: Nokia (NOK), ASTI, NeuroDigital (NED), Fundación Valencia Port (FV), Universitat Politècnica de València (UPV) and Fivecomm (5CMM). The role of each partner within the use case is the following:

- FV in collaboration with the port authority, grant access to the Port of Valencia´s terminal, infrastructure and its digital content for prediction measurements, facilitates Nokia on deploying the 5G RAN infrastructure at the site, and creates the plan and involves in the demonstrations.
- ASTI will contribute with devices supplied with the required software (SW) and hardware (HW) alterations for the remote control of its own AGV, facilitates NOK with the integration of the cameras, proximity sensors, with either a NOK or 5CMM modem for the wireless communication, and deploys the AGV in the Port of Valencia´s site for the demonstration.
- 5CMM provides the 5G modem for the connection of the AGVs to the 5G network in the sub-6GHz band, performs system-level simulations and compare them with other State-of-the-Art (SoA) technologies, as defined by the 3GPP. Additionally, 5CMM develops a planning tool with 3D scenarios to complement these results. Finally, 5CMM collaborates with UPV, NOK and NED in the integration of the NED in-house haptic gloves in the cockpit, carrying out measurement campaigns in the trials when needed.
- Hauliers transport the cargo using a devised immersive remote indoor cockpit by NOK, where forehead AR glasses, sensor straps, steering wheel and pedals are provided by NOK, and the haptic gloves by NED.
- NED develops immersive gloves including 10 vibrotactile Linear Resonant Actuators (LRAs), Inertial Measurement Unit (IMU) based movement tracking and gesture recognition capabilities. Additionally, they will implement biometric sensors that permit to assess the immersive remote indoor cockpit controller´s (the user) physical and emotional suitability for task performance (the AGV control). Some of these sensors measure: posture, breathing, heart rate variability and blood volume pulse as well as information about fatigue, drowsiness and stress.
- Communication providers, NOK granted by Telefonica, provide wireless 5G/IoT connectivity inside the port facilities for enabling real-time tracking and data transmission collected by IoT sensors; this is deployed using mmW radio coverage and distributed MEC applications with the immersive remote indoor cockpit features.
- UPV validates the UC key performance indicators (KPIs) by performing link- and system-level simulations to demonstrate these performance requirements are guaranteed and assist with the measurement campaigns in the trials when needed using commercially available simulator Amarisoft 5G/NB-IoT gNB/eNB.
- Although Cumucore (CMC) was not included in the UC initially, they intend to assist with the provision of a 5G Core (5GC) connected to NOK RAN and MEC to deliver private network with support for Narrow Band IoT (NB-IoT) and (TSN) features; there is no obligation by the UC partners for its final implementation. If needed the CMC 5GC can include additional network functions (Network Data Analytics Function (NWDAF), TSN AF and Network Exposure Function (NEF)) to monitor and manage the devices in the AGV that requires low latency and high availability.

Co-funded by the Horizon 2020
Framework Programme of the European Union

7 Inter-Model Asset Tracking Via IoT and Satellite

Currently, no real-time data can be collected and exchanged along the whole supply chain. Ships are equipped with legacy communication networks allowing to exchange information with port terminals when ship is docking, but not when it is sailing. No sensors are installed in containers to monitor and collect real-time data on cargo location and conditions and container safety.

Thus, this use case aims at providing E2E asset tracking via satellite backhaul from the IoT RAN to the corresponding data/control centre, enabling real-time periodic monitoring of predetermined parameters (temperature, humidity, movement, bumps, etc.) of shipping containers when they are sailing on the sea, while terrestrial IoT connectivity is provided when the ship approaches the port. To enable the ubiquitous coverage, IoT tracking devices will be installed on the shipping containers transported by ships and trucks on both segments. The end-to-end intermodal asset tracking would allow shipment information to be ubiquitously available across all connected platforms and interested parties in real-time. Data analytics on this rich and timely data would further allow supply chain players to achieve operational excellence, major reductions in operational uncertainties, and increased revenues.

7.1 Workflow

The workflow considered within this use case is the following:

1. A 20 feet shipping container will be equipped with a certain number of heterogeneous IoT devices able to monitor the internal environment of the container (accelerometer, temperature, humidity) as well as to detect critical events (physical shocks, door opening).
2. The shipping container will be loaded on a truck and will be transported from the inland to the port of origin.
3. During the trip, the heterogeneous IoT devices will send regular status updates, the Smart IoT gateway on the truck will gather and process the data and the connectivity with the IoT cloud/Data centre will be obtained through terrestrial access network.
4. The shipping container will be discharged from the truck and it will be loaded on a ship.
5. The shipping container will be transported from the port of origin to the port of destination and vice versa. During the trip, depending on the service level required by the container owner and the supply chain associated, heterogeneous IoT devices will send regular updates (frequency could go from one message per hour to one message per day).
6. The messages from the heterogeneous IoT devices will be aggregated by a Smart IoT Gateway installed on the bridge or IT room of the ship.
7. When the ship is travelling on the sea the data will be sent to the IoT cloud/data centre through satellite backhaul (a satellite terminal will be installed on the ship). The baseline

Co-funded by the Horizon 2020
Framework Programme of the European Union

space segment to be used corresponds to the SES's GEO satellite fleet, which will provide seamless connectivity between the ship satellite terminal and the innovative 3GPP compliant hub platform located at the SES teleport in Betzdorf, Luxembourg.

8. When the ship arrives at the first port, the data will be sent to the IoT cloud/Data centre through satellite backhaul or terrestrial access network.
9. Then, the shipping container will be discharged from the ship and loaded on a truck.
10. The truck will leave from the first port and it will transport the shipping container. During the trip, the heterogeneous IoT devices send regular status update, the Smart IoT GW on the truck gathers and processes the data and the connectivity with the IoT cloud/Data centre is obtained through terrestrial access network.

In Figure 24, the ideal scenario of this use case is described. In this ideal case the satellite terminal and the smart IoT GW are both installed on the ship enabling tracking and monitoring of the assets when the shipping container is sailing on the sea.

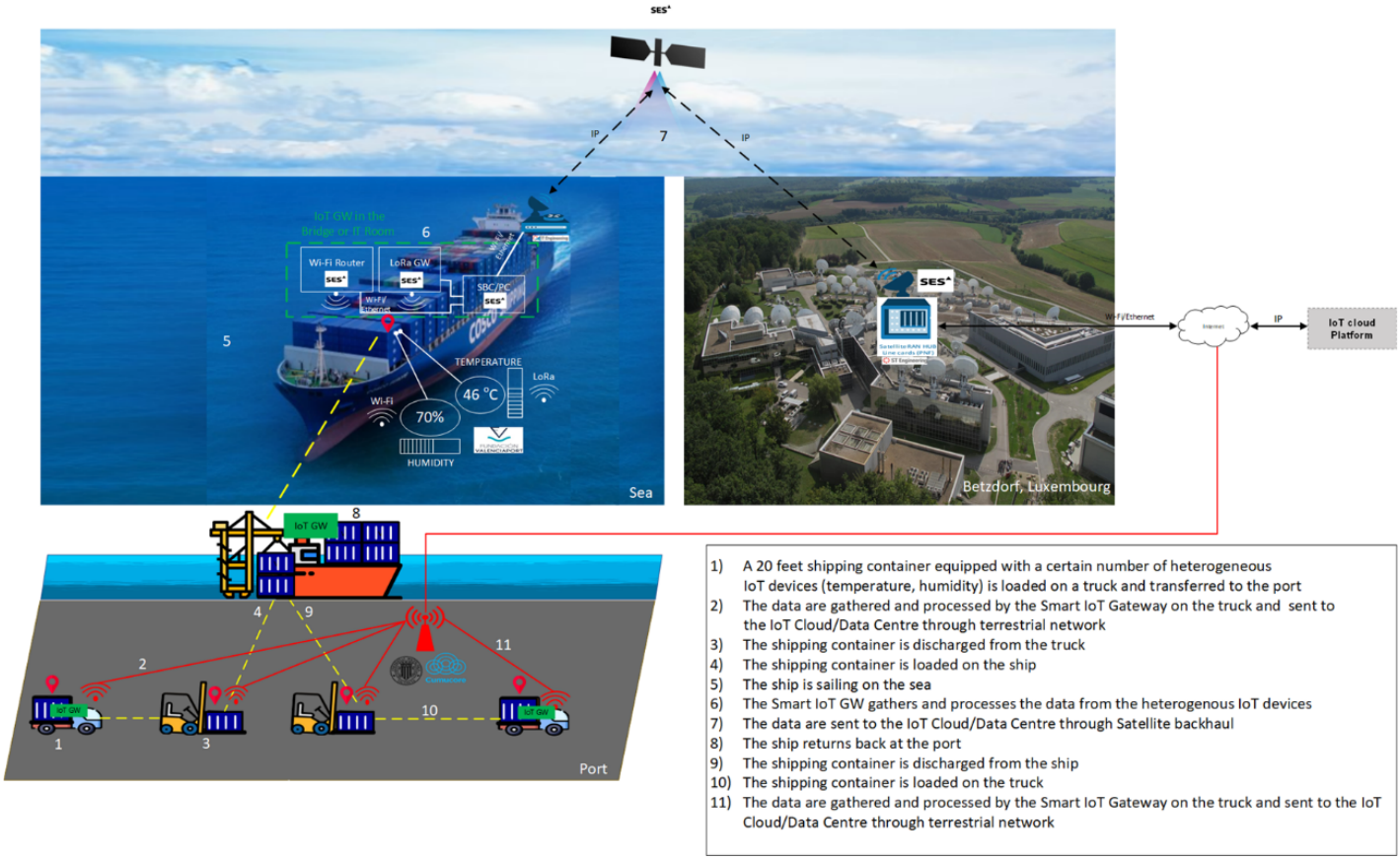


Figure 24: Scenario of the use case with satellite terminal and smart IoT gateway installed on the ship

7.2 Expected Innovation

This use case aims at providing E2E intermodal asset tracking via satellite and IoT technologies. It also targets to optimise real-time data interchange along the whole supply chain, improving customer satisfaction and increasing transparency and collaboration. The use case will develop a Smart IoT Gateway allowing interoperability between heterogeneous IoT devices; and it will provide intelligent real-time connectivity solutions for enabling asset tracking and monitoring from the originating point to the final destination. Regarding the Smart IoT Gateway, the following core technologies will be used:

- OneM2M standard such as openMTC.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- Secure Data Storage such as Distributed Ledger Technology (e.g., Hyperledger Fabric).
- Time Series Storage such as influxdb.
- Protocol bridging such as Ponte.
- Flow Management / User Interface such as NodeRED.
- IoT Protocols such as MQTT, MQTT-SN, CoAP, HTTP(s).
- Data visualization such as Grafana.
- Persistent Storage such as MongoDB.
- Software Architecture (Microservices) such as Docker.
- Communication Interfaces such as LoRa, WiFi, Ethernet, RFID, BLE, Bluetooth, 4G/5G IoT.

7.3 End User and Environment

Shipping agencies (COSCO Shipping Lines Spain S.A) and other actors belonging to the port community (e.g., port authorities, port terminals, hauliers and freight forwarders) that are interested in the data collected.

7.4 Actors

Port Authorities will give access to the port infrastructure.

Port Terminals will give access to the port terminal infrastructure where trucks will enter and exit for the loading or unloading of cargo.

Hauliers will transport the cargo for performing loading or unloading operations inside the port and terminal facilities.

Ship Providers will transport the cargo when the ship is sailing on the sea.

Sensor and IoT Providers will deploy sensors and IoT devices in the shipping container for collecting information on cargo tracking, cargo conditions, safety conditions, etc.

Communication and Network Management entities will provide the satellite, wireless and IoT connectivity when the ship is sailing on the sea and also inside the port facilities and the inland for enabling the real-time tracking and the transmission of the data collected by the IoT sensors.

Big Data Analytics Providers will analyse and exploit the data collected by the different sensors and IoT devices in order to model and develop situational understanding and predictive models. This data will be made available on cloud-based platforms where data will be stored and made accessible through the use of APIs.

7.5 Data and Service(s)

The data used to define the focus of the use case and the demonstration are:

- COSCO Service lines from Valencia to Piraeus: (i) BSM service with 10 days of duration and four intermediate port calls (Algeciras, Casablanca, Algeciras and Malta); (ii) AEM1 service with 4 days of voyage duration and with no intermediate port calls or (iii) any other new service in the moment of loading the container operation.
- COSCO Service lines from Piraeus to Valencia: (i) BSM service with 5 days of voyage duration and with one intermediate port call (Malta) or (ii) AEM1 service with 10 days of voyage duration and three intermediate port calls (La Spezia, Genoa and FOS).

The data to be obtained by the IoT sensor are:

Co-funded by the Horizon 2020 Framework Programme of the European Union

- Real-time location of the cargo: Real-time tracking of cargo will be especially relevant at the land and terminal sides (not so relevant at the seaside). This data stream will be provided in real time by an IoT tracking sensor.
- Cargo conditions: Three different IoT sensors will provide information on cargo conditions related to: (i) temperature - measured every 10 minutes; (ii) humidity - measured every 10 minutes; (iii) movement - measured constantly for detecting movement occurs; and vibration - measured constantly for detecting when vibration occurs.
- Safety conditions: Data related to the container safety will be provided by two different sensors: (i) stop and bump detection - measured constantly for detecting when stops or bumps occur, and (ii) container door opening - measured constantly for detecting when the door is opened.

The data to validate the use case results are:

- Vessel's Estimated Time of Arrival and Estimated Time of Departure (Proforma and updates).
- Transport orders from inland to Valencia port and related acceptance and release orders.

7.6 Asset(s)

The assets to be used for the realization of this use case are the following:

- Ship with current devices on board: i) Automatic Identification System (AIS) for navigation data exchange, ii) Inmarsat for communication via satellite, and iii) VHF radio connection for information exchange when ship is approaching the port.
- A truck to transport the container in the terrestrial segment and a 20 feet empty shipping container.
- IoT sensors: Up to six different sensors and actuators will be installed in the container for measuring real-time location, cargo and safety conditions of the container. All IoT sensors will be standalone in terms of energy consumption thanks to the use of power supply batteries. Sensors will be installed and attached to the 20 feet container for General Purpose (20GP) by using magnetic elements. The set of IoT sensors installed in the container is composed of: (i) real-time tracking sensor, (ii) temperature and humidity sensor, (iii) accelerometer sensor for measuring movement and vibration, (iv) bump and stop detection sensor, and (v) container door opening sensor.
- The Port of Valencia and Port of Piraeus facilities to load and unload the container to the ship.
- Wireless IoT communication modems (LoRa, Wi-Fi, 4G/5G IoT) and mobile core network.
- Smart IoT Gateway, Satellite Terminal, GEO satellite, Ku-band, Satellite uplink/downlink facilities and 5G Satellite Hub.

7.7 Requirements

User Requirement	Description
#1: User should be able to plug and play a diverse set of sensors in the container and automatically will be connected to the system and start reporting measurements.	User should be able to plug and play a diverse set of sensors (e.g., temperature, humidity) in the container and automatically will be connected to the system and start reporting measurements
#2: User should be able to choose the container number to be monitored and the set of monitoring parameters	Different type of users like shipping lines or freight-forwarders should be able to access (and possibly visualize)

Co-funded by the Horizon 2020 Framework Programme of the European Union

such as vibrations, door opening, temperature, humidity, will be shown depending on container type and goods transported.	information registered by the IoT sensors like vibrations, door opening, temperature, humidity etc.
#3: User should be able to set up a travel plan for the container depending on the level of service required. The travel plan combined with the container type will allow IoT devices to set up relevant parameters.	Different type of users like shipping lines or freight-forwarders should be able to easily setup relevant parameters to be registered by the IoT devices, also the users will receive in real time alarms detected by the devices.
#4: User should be able to monitor battery life of any individually powered IoT device(s) and/or sensors on container.	Different type of users like shipping lines or freight-forwarders should be able to access (and possibly visualize) information regarding battery life of any individually powered IoT devices, such as sensors, actuators, or communication devices installed in the container. In this way, they will be able to monitor the life status of the installed batteries and prepare for replacements if any is close to the end of its lifetime.
#5: User should be able to define critical events that can trigger an alarm to inform of such, as well as events that need to trigger status update. User should also be able to retrieve information about relative order of occurrence of critical events.	Different type of users like shipping lines or freight-forwarders should be able to receive (and possibly visualize) information about relevant events defined in the system like alarms (e.g., Container shock) or milestones (e.g., discharge in one port), this information must be kept in system and should be accessible for the user at any moment.
#6: User should be able to access all data gathered by IoT sensors and actuators from a web service-based application.	Different type of users like shipping lines, freight-forwarders or end-users must be able to access and visualize all data gathered by IoT sensors and actuators installed in the container. In this way, they will be able to monitor the status of cargo.
#7: User should be able to access all sensors data even if the IoT Gateway loses connectivity during a period of time.	The IoT Gateway should store the sensors data while it does not have connectivity to the internet in any way. Once the Gateway manages to re-connect, it should send all pending data so that the user can see it.
#8: A single graphical user interface is made available for tracking containers independent of the technology used for tracking.	Users will visualize IoT sensor data that comes from different containers, including tracking data. Normally, the different devices involved provide the own method of tracking and presenting the information. A unified graphical interface, with the data normalised and presented as one, will make the data easier to digest and analyse.
#9: User has secure access to events and sensor data for processing.	Different type of users like shipping lines, freight-forwarders or end-users must be able to access data gathered by IoT sensors and actuators installed in the container. They must only be able to access data that they are authorised to access.
#10: User should be able to query backhaul connectivity status via cloud-based API/UI.	A cloud-based API/UI should be made available to a user or user application, to indicate if there is a problem with the connection from the IoT sensors via the backhaul medium. The user can query the API/UI which will provide a positive response if the connection is ok and will provide a negative response if the connection has been lost. This will allow the user application to troubleshoot the backhaul connection as part of a troubleshooting process.

Co-funded by the Horizon 2020
Framework Programme of the European Union

System Requirement	Description
#1: Network connectivity both on maritime and inland segments is required. Hence, the data centre/cloud should be able to have real-time visibility and track the shipping containers reliably and accurately for the whole trip.	Network connectivity both on maritime and inland segments is required. Hence, the data centre/cloud should be able to have real-time visibility and track the shipping containers reliably and accurately for the whole trip.
#2: Data centre/cloud should have the ability to perform data analytics on collected data and should be able to analyse data on arrival to react as quickly as possible to events. To assist with analytics, the data centre / cloud may offload some of the analytics processing at the IoT Gateway, or edge cloud appliance, located on the ship or truck.	Data analytics functions are critical for the automation of systems that previously relied heavily on manual methods of analysis. Data analytics within the cloud will serve the purpose of analysing and responding quickly to both discrete events and to future events that are predicted from the data. A data analytics function at the edge cloud will serve the purpose of responding even quicker to some events, and because of its data processing function, it can optimise the backhaul connection by reducing the data that is backhauled to the cloud.
#3: Containers should include sensors to monitor environmental variables, such as temperature, pressure, humidity, sudden movement, breach, location.	IoT sensors must be installed into the containers that will be tracked and monitored.
#4: Battery-powered IoT device(s)/sensors should be able to operate for the entire lifetime of the tracked container without large capacity battery packs and without being replaced during this period of time.	Powered IoT devices should be able to operate for the entire lifetime of the tracked container without large capacity battery packs and without need of being replaced at all (or at least often) during this period of time.
#5: IoT sensors will send periodic status updates at a frequency that has been tuned for efficient use of bandwidth, and for providing up to date.	The IoT sensors should be configured to transmit data updates at a frequency that is relevant for each sensor type.
#6: Creation of a secure and resilient centralised repository for sensor information is required.	The centralised (or distributed) repository for sensor information must only be accessible to users that have the correct permission to access it.
#7: The IoT Gateway will backhaul data in a format and at a frequency that has been tuned for efficient use of bandwidth, and for providing up-to-date information.	The IoT Gateway should be configured to transmit bulk data across the backhaul connection at a frequency that is relevant for the IoT sensor data.
#8: The IoT GW should be able to receive and process multiple data streams coming simultaneously from multiple containers loaded on the ship and forward them to a data centre or cloud platform.	The IoT GW should be able to receive and process multiple data streams coming simultaneously from multiple containers loaded on the ship and forward them to a data centre or cloud platform.
#9: The IoT Gateway should be able to provide a remote management endpoint.	The IoT Gateway should be able to provide an interface to the external world that would allow basic and advanced management features on its configuration including deployments and upgrades.
#10: The IoT Gateway should be able to provide independent interfaces for different IoT protocols.	The IoT Gateway should be able to receive and send messages using at least the following messages, but not limited to: Physical and data link layer, LoRa, Wi-Fi, Ethernet, Network and transport layer, MQTT over IP, HTTP(S), Web sockets. And the system should be ready to incorporate other technologies.

Co-funded by the Horizon 2020 Framework Programme of the European Union

#11: The IoT Gateway should be able to optimize the traffic for satellite communications.	The system should sort and organize the traffic for optimum satellite communication. The system should setup a group of configurable rules for this. The users and administrators should be able to change them or even switch off one or more.
#12: The IoT Gateway should be able to report its status via an API and through its management dashboard.	The system should provide continuous status messages, including priorities and alerts messages, through a dedicated external endpoint for users (in the form of a GUI) and other systems (with a dedicated API).
#13: The IoT Gateway should be resilient to connectivity outages.	The system should be able to recover from connectivity outages, implementing features such as message re-routing, temporary store of received messages and buffering of outgoing traffic.
#14: The IoT Gateway should be able to provide a configurable limited storage to buffer the data.	The IoT Gateway should be able to provide a configurable limited storage to buffer the data.
#15: The IoT GW should forward (buffered) stored data as soon as possible when backhaul connectivity becomes available.	The IoT Gateway should detect when the backhaul connection availability has returned, in order to immediately transmit buffered data.
#16: The IoT Gateway, or a co-located appliance, should be able to detect, monitor, and report on availability of backhaul connectivity.	The IoT Gateway or a co-located appliance must detect the status of the backhaul connection. This will allow the appliance to troubleshoot the backhaul connection as part of a troubleshooting process.
#17: The IoT Gateway, or a co-located appliance, must be configurable to allow the operator to configure the connectivity decision process, e.g., choice of terrestrial or NTN connectivity.	The IoT Gateway, or a co-located appliance, runs a backhaul selection algorithm when required. The criteria used in the selection algorithm can be simple or complex.
#18: When the ship is out of range of terrestrial connectivity, the satellite network selected must meet the minimum connectivity requirements.	Any installation on-board the ship must meet minimum requirements for satellite connectivity to support this use case.
#19: The IoT Gateway should be able to route messages between its interfaces.	The IoT Gateway should be able to route messages between its interfaces.
#20: The IoT Gateway should be able to publish status, warnings and alert messages to external parties.	The IoT Gateway should be able to announce and push some high priority messages even if it has not an active connection to other system (i.e., the IoT Gateway should be able to initiate a communication channel to an external party).
#21: The IoT Gateway should be able to provide security for the communication through its interfaces.	Incoming and outgoing communications should be secured, external actors (sensors, clients and external systems) should be authenticated and authorized. Messages should be encrypted.
#22: The IoT Gateway should expose interfaces to allow the integration with other systems.	The system should provide documented external interfaces and APIs that should allow other system to interact with it, either as a recipient or the sender of the messages or as a management component that provides automatization.
#23: There will be a mechanism for a container to handover between the ship IoT Gateway and the onshore IoT Gateway.	The IoT Gateway should have a mechanism to facilitate the transfer of IoT sensor connectivity between ship and shore.
#24: There is an IP connection between	There is an IP connection between the radio access and

Co-funded by the Horizon 2020 Framework Programme of the European Union

the radio access and the mobile core for signalling from base stations and data from sensors.	the mobile core for signalling from base stations and data from sensors.
#25: The sensors will include nano-SIM or similar for authentication with the 5GC.	The sensors will include nano-SIM or similar for authentication with the 5GC.
#26: The IoT sensor information may be transferred over the satellite network without the need to establish a dedicated data path over the satellite network.	The IoT sensor information may be transferred over the satellite network without the need to establish a dedicated data path over the satellite network.
#27: Sensors and actuators should integrate a module for enabling cellular IoT connectivity in static and mobility conditions.	Sensors and actuators have to report the collected data in containers that will be transported in vessels and trucks. As a consequence, sensors and actuators must integrate a module for enabling IoT connectivity in static and mobility conditions.
#28: Sensors should be able to communicate at low power from within the container to communicate with the IoT Gateway.	The IoT Gateway should have a standard mechanism of pairing with the container IoT sensors when the container is within range of the IoT Gateway. The IoT Gateway can be located on-board a ship or onshore.
#29: Satellite communication should not interfere with existing radio communication systems in the vicinity and should be tolerant of their presence.	The satellite network selected for backhaul connectivity should cause minimal interference with co-located communication networks and should tolerate their presence.

7.8 Key Performance Indicators (KPIs)

KPI	Target Value	Verification Means
Availability	≥ 99.9%	Tested through over-the-air demonstrations, where satellite backhaul and IoT connectivity will enable monitoring of predetermined parameters (temperature, humidity, accelerometer, etc.) of shipping containers.
Reliability	≥ 99.9%	Tested through over-the-air demonstrations evaluating the probability that a certain amount of data from the IoT devices is successfully transmitted within a predefined time frame.
Battery life	> 12 years	A web service-based application will be able to show the battery life of IoT devices installed in the container
Coverage	GEO	During the over-the-air demonstrations the SES's GEO satellite fleet will be used as the baseline space segment
Typical message size	200 bytes	Tested through over-the-air demonstrations, where IoT devices installed in the shipping container will gather relevant data and send regular updates.
Maximum message size	2500 bytes	
Typical frequency (messages per day)	Maximum at every 10 minutes	Tested through over-the-air demonstrations, where up to six different sensors and actuators will be installed in the container for measuring real-time location, cargo and safety conditions of the container.
Connectivity of heterogeneous IoT devices	LoRa, Wi-Fi, Bluetooth and wired	The capability of the IoT GW to receive and process the data, which is sent simultaneously from several heterogeneous IoT devices will be tested via over-the-air demonstrations.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Latency	≤ 1 s	Tested through over-the-air demonstrations, where satellite backhaul and IoT connectivity will enable monitoring of predetermined parameters (temperature, humidity, accelerometer, etc.) of shipping containers.
Mobility	≤ 90 km/h(truck) 45 km/h (ship)	Maximum mobility conditions will be evaluated both in terrestrial and maritime segments by performing link-level simulations and real demonstrations.
Positioning accuracy	≤ 5 m	Positioning accuracy will be tested through real over-the-air demonstrations by installing IoT positioning sensors on the shipping container
Data Protection Impact Assessment (DPIA) prepared & approved	DPIA report approved	DPIA is available, shared with UC owners and approved by DPO (Data Protection Officer)
Privacy User Guide prepared & approved	Privacy User Guide approved	Privacy User Guide is available, shared with UC owners and approved by DPO (Data Protection Officer)
Confidentiality and integrity protection of sensitive data	100%	Controlling any sensitive data at rest, in transit and in use, it is never in clear text format

7.9 Operational, Business, Societal and Environmental Outcomes

The container tracking is an essential part of the supply chain and logistics to make them more efficient. By monitoring and tracking seamlessly the container in near real-time, it allows to provide all the supply chain players and stakeholders a full traceability and to optimize the transport and the storage of containerized goods. Any event related to a container is quickly notified and is allowing efficient analytics as well as taking related decision such as new sourcing plans if needed.

By tracking and tracing the cargo, the operator will monitor the asset movement, will record the actual routes, transit times, stationing in the facilities and congestions for every transport mode. By analysing the transit performance, the operator will take informed decisions by choosing preferred routes, carriers or even modes of transport.

By monitoring temperature, humidity, accelerometers, and even simple contact sensors the operator will assess additional states applicable for various goods. Temperature and humidity are relevant for perishable goods and abnormal variations in the values and they will indicate the immediate need for maintenance in order to avoid the loss of goods. Furthermore, the accelerometer output will provide real-time indication about the integrity of the goods and abnormal variations may trigger subsequent inquiries which may conclude that an accident occurred, and intervention is required.

Continuous contact sensors data may certify that the goods are transported securely in their containers and nobody attempted an unauthorized access. In eventuality of a door alarm the operator will alert appointed security entities to counteract a potential illegal action. Moreover, the IoT interoperability will enable the federation of different IoT platforms within heterogeneous domains, overcoming the compatibility issues between both standard and non-

Co-funded by the Horizon 2020 Framework Programme of the European Union

standard, proprietary, and custom M2M solutions. Also, it will enable the better exploitation of data in optimization and prediction, which provide the greatest business value.

7.10 Verification Means and Actors Involved

Real over-the-air demonstrations will be conducted for the validation of the relevant KPIs. In the section “Workflow”, the ideal scenario for this use case was described. However, there are several factors that need to be considered for performing a real demonstration of the inter-modal asset tracking scenario.

In the ideal scenario, it was assumed that a satellite terminal could be installed on the ship in order to enable through satellite backhaul, real-time/periodic tracking and monitoring of predetermined parameters (temperature, humidity, accelerometer, etc.) of shipping containers when they are sailing on the sea. Additionally, it was assumed that the Smart IoT Gateway responsible for collecting the data from the heterogeneous IoT device and passing them to the satellite terminal, will be also installed on the ship, outside the shipping container, in any place where it can be powered and can easily communicate with the IoT devices. However, the installation of a satellite terminal and the smart IoT Gateway on the ship is a very complicated process and needs the authorization of the owner of the ship and the captain. The physical installation may not take a lot of time, but a huge number of considerations (safety regulations, site survey to decide where to put the satellite terminal, opening holes and passing cables in the ship, etc.) should be considered in order to get the approval.

As mentioned, the Smart IoT Gateway should be placed outside the container for two reasons: i) it needs to be powered and ii) its battery is considered dangerous for the cargo. Therefore, for demonstrating the satellite backhaul connectivity three alternative scenarios can be considered:

- The authorisation can be obtained to install on the ship the Smart IoT GW but not the satellite terminal. In this case, when the shipping container was sailing on the sea, the heterogeneous IoT devices would send regular updates and their messages would be aggregated, processed and stored by the Smart IoT GW. Then, when the ship arrives at the port, the Smart IoT GW would communicate with the satellite terminal which is installed on the port and through satellite backhaul the data would be sent to the IoT Cloud/Data Centre.
- Both authorisations to install the satellite terminal and the Smart IoT GW on the ship are not obtained. In this case, when the shipping container was sailing on the sea, the heterogeneous IoT devices would send regular status update and their messages would be collected by a very small device, which would be placed inside the container. This small device has very low power consumption and its mission is to collect and store the data from the IoT devices without any further process. When the ship arrives at the port, this device communicates with the Smart IoT Gateway, which will be installed at the port next to the satellite terminal and through satellite backhaul the data will be sent to the IoT Cloud/Data Centre.
- The authorisations to install the satellite terminal and the Smart IoT GW on the ship cannot be obtained and the GW device cannot be placed inside the container. In this case, the ship would not be used and, the shipping container equipped with the heterogeneous IoT devices, the Smart IoT GW and the satellite terminal would be installed on the port.

In Figure 25 a more "realistic" scenario of this use case to be demonstrated is presented. In this setup, the Satellite terminal is installed on the port, while the Smart IoT GW is installed on the ship.

Co-funded by the Horizon 2020
Framework Programme of the European Union

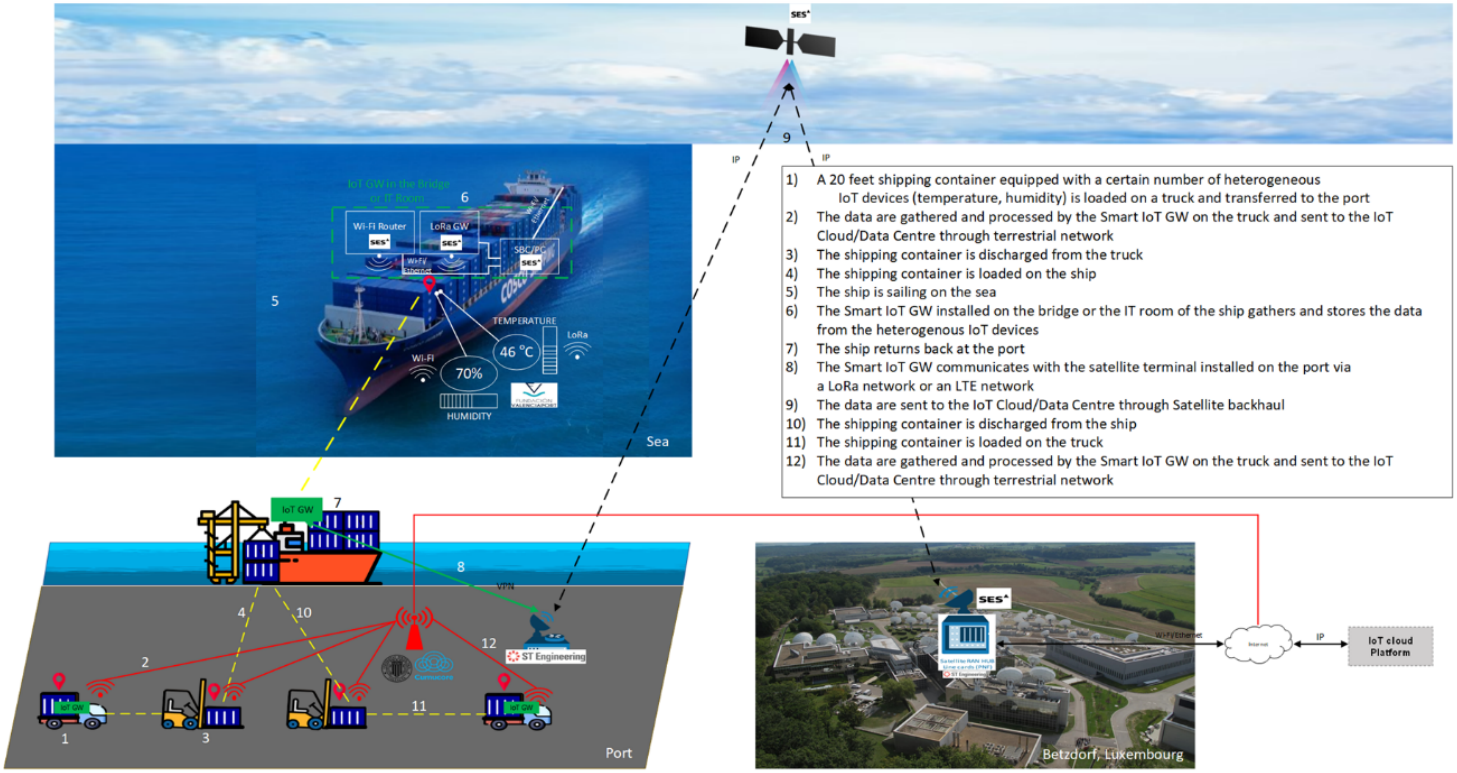


Figure 25: Scenario of the use case with satellite terminal on the port and smart IoT gateway on the ship

In addition to the identified risks related to the installation of the satellite and IoT Gateway on board of the ship, other aspects should be also considered for ensuring the ubiquitous connectivity over the inland segment.

- LTE-M connectivity over the whole inland segment needs to be ensured for enabling the real-time tracking of goods on board of the truck. For that purpose, the LTE-M coverage provided by different mobile network operators in Spanish inland segment will be explored. If LTE-M coverage cannot be assured across the considered inland segment, the use of traditional LTE networks will be assessed as a second option.
- Assuming that the Smart IoT gateway is installed at the ship, another IoT gateway will be required for collecting and transmitting all the data gathered by IoT sensors on board of the truck at the inland segment. The installation of this second gateway either at the container or at the truck will be explored and it will depend on the feedback provided by the haulier.
- All the limitations linked to the accomplishment of all regulations affecting the supply chain, like customs declarations, terminal working procedures, road and Maritime's safety regulations, etc., will have to be considered for performing real-time tracking demonstrations.

Several partners are involved in this use case and their role is described below:

- FV will be responsible for: (i) providing the IoT Sensors, (ii) providing the shipping container, (iii) installing the IoT sensors on the shipping container and (iv) ensuring the loading and unloading of the shipping container, in collaboration with COSCO, on the COSCO's ship or in the port of Valencia.
- COSSP will be responsible for: (i) coordinating, in collaboration with FV the loading and unloading of a container to be transported between Port of Piraeus and the Port of Valencia; (ii) obtaining the authorization to install on board IoT devices; (iii) providing a ship with route

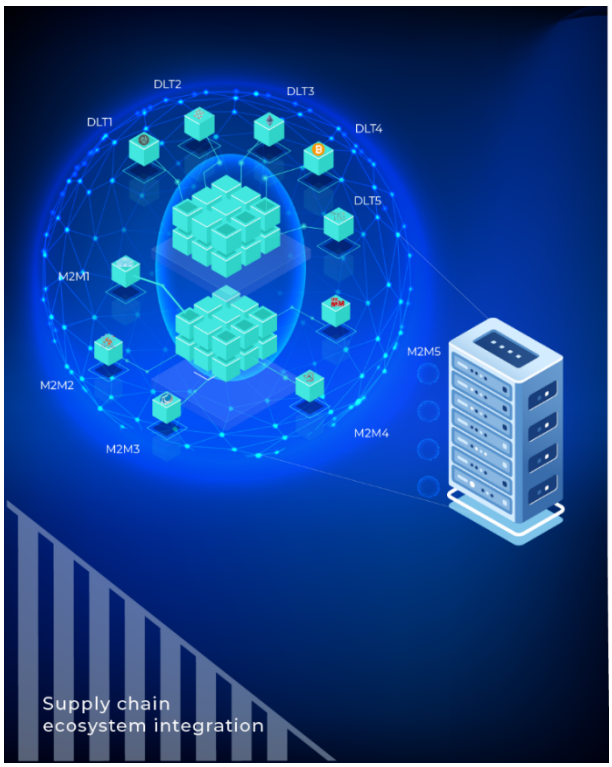
Co-funded by the Horizon 2020 Framework Programme of the European Union

from Valencia port to Piraeus port and vice versa and (iv) contacting hauliers for demonstrating ubiquitous connectivity over the terrestrial segment.

- SEQ will be responsible for providing low-power communication Cat-M/Cat-NB module/modem that can be attached to cellular network (thus, using LTE-M/NB-IoT cellular technologies), in order to provide real-time data from sensing of the shipping container, or as a possible alternative, if proved to be relevant to the requirements of this use case, to provide a standalone end user multi-sensor IoT device (powered by a Sequans Cat-M/Cat-NB solution) which can monitor and report on conditions such as temperature, humidity, atmospheric pressure, air quality/CO2, noise, light, and movement. They will also ensure the transmission of the data collected by the IoT devices to the Smart IoT Gateway. This will be obtained in collaboration with SES and FV.
- SES will be responsible for: (i) the development of a Smart IoT Gateway which will ensure the connectivity for a vast number of heterogeneous IoT devices, by harmonizing different IoT technologies and application protocols and formatting data to be transferred across the network, terrestrial either satellite; (ii) providing Occasional Use (OU) GEO satellite capacity; (iii) the installation and commissioning of the satellite terminals; (iv) providing access to GEO satellite hub platform; (v) providing access to SES teleport uplink facilities and to IP/MPLS global teleport access network; (vi) providing access to satellite 5G testbed node; and (vii) ensuring the transmission of the data collected by the IoT devices to the Smart IoT Gateway, in collaboration with SEQ and FV.
- iDR will be responsible for: (i) providing the satellite ground equipment – Hub and modems; (ii) providing E2E IP connectivity via SES GEO satellite, (iii) supporting SES in the development of the Smart IoT Gateway; and(iv) configure testbed and demonstration systems.
- CMC will provide 5GC for private network on-ship including support for NB-IoT and usage of satellite or VHF links for backend connection.
- UPV will be responsible for performing link-Level and system-level 5G/IoT SAT/NTN direct access; and providing support on field trials measurements.

Co-funded by the Horizon 2020
Framework Programme of the European Union

8 Supply Chain Ecosystem Integration



Standard approaches for efficient and secure data management from a single access point are still missing.

Full interoperability across M2M platforms still needs to be tackled on a case by case and platform by platform basis due to a wide number of possible applications, design choices, formats and configurations that can be adopted within IoT domain. Many of available M2M solutions have been developed in the form of application silos where interoperability is limited by the scope of the solution.

On the other hand, DLTs industry is completely fragmented with different alternatives: there is still lack of consistent standardization across different available DLT solutions that does not interoperate with each other. DLT's security capabilities are not fully exploited.

The use case is about interoperability between different M2M platforms as well as different DLT solutions. The main aim of this use case is to provide two different interoperable layers in order to abstract the complexity of the underlying M2M platforms and DLT solutions, guaranteeing at the same time data privacy and security by means of encoding and anonymization techniques.

8.1 Workflow

The following workflow is considered for this use case:

1. Input data set is used in order to feed different M2M platforms (Mobius OneM2M, Eclipse OM2M, Symphony, PI System OSIsoft and NB-IoT Platform). Each M2M platform stores raw data according to their own data management policies.
2. Data Virtualization layer interacts with all M2M platforms in order to retrieve raw data and aggregate them accordingly to a common and defined data model. Personal Data are automatically identified so that a pseudonymization (or anonymization) function can be applied when needed, fulfilling GDPR requirements.
3. Structured/aggregated data are generated by Data Virtualization Layer in order to make them available to the cross-DLT layer (Trust-OS) for storage, hash generation and trusted distribution over different DLT solutions (IOTA, Hyperledger Fabric, Ethereum, Tradelens and Bitcoin). Data are also shared with assisted-AI MANO system. The big amount of data coming from M2M platform, could be exploited by ML algorithm to collect information to improve and optimize the slice creation and lifecycle management.
4. DVL provides data according to a specific data model to Trust-OS through API (from DVL perspective, each M2M platform sends an agreed data set to DVL; data are aggregated following a common data model).

Co-funded by the Horizon 2020
Framework Programme of the European Union

5. Data coming from DVL are stored in Trust-OS that generates a hash associated to the received data, stores it within the dB (metadata) and distributes it over different DLTs through APIs.
6. Each available DLT can support either hash storage or raw data storage (it is up to specific DLT's implementation). Hash storage within a specific DLT should be sufficient to validate the Proof-of Existence concept: each hash stored within Trust-OS can be compared with the hash stored within a specific DLT at any time in order to prove data exists and that it has not been tampered.
7. Each DLT provides an acknowledgement to Trust-OS including positive/negative response to hash/data storage request made by Trust-OS. DLTs addresses are stored and associated to specific hash and data. Trust-OS knows from now what data are stored in each DLT, making them potentially available for the CONSUMER (any generic application that needs to check data integrity and immutability for any purpose).

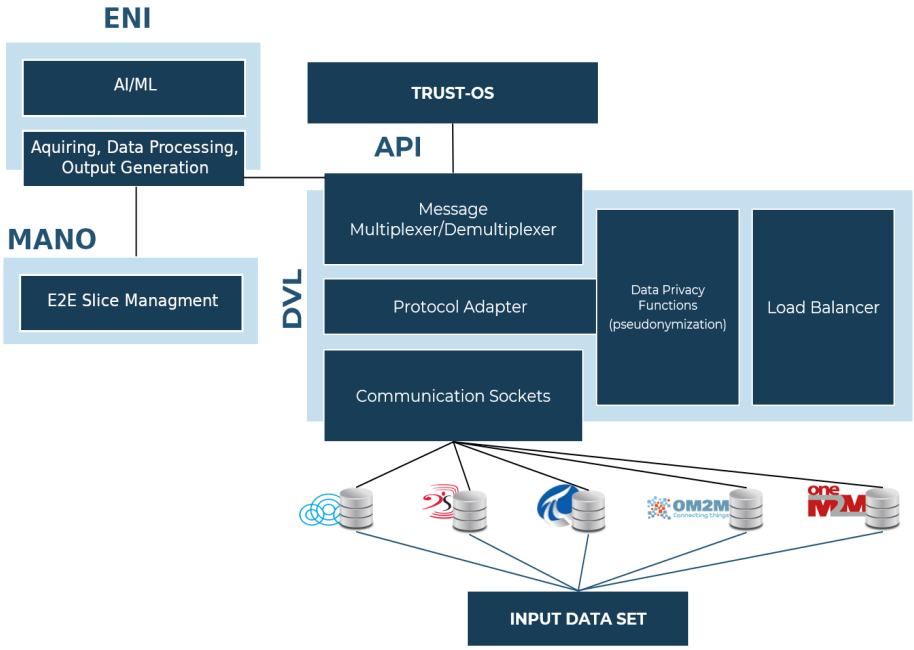


Figure 26: Cross-M2M layer architecture

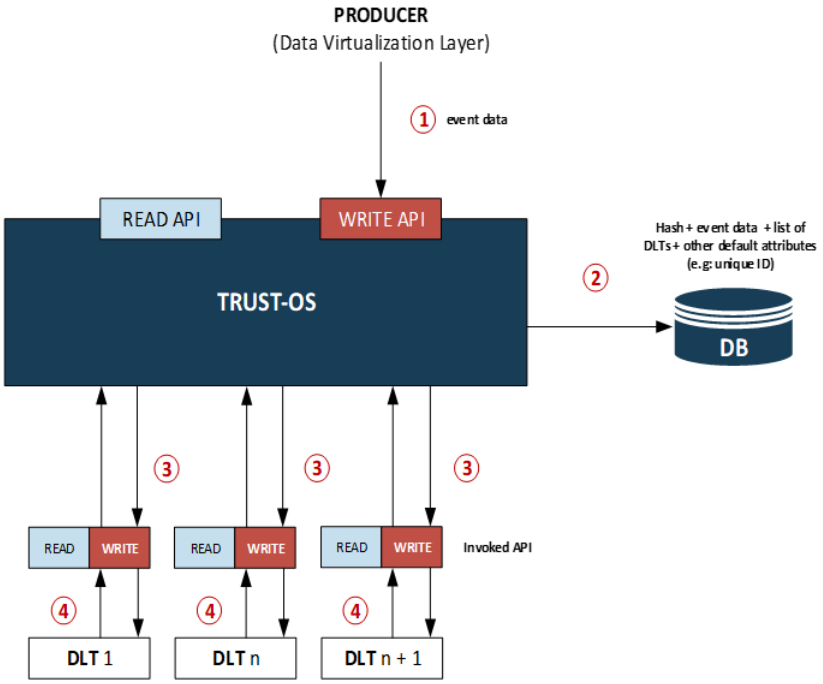


Figure 27: Data writing request flow

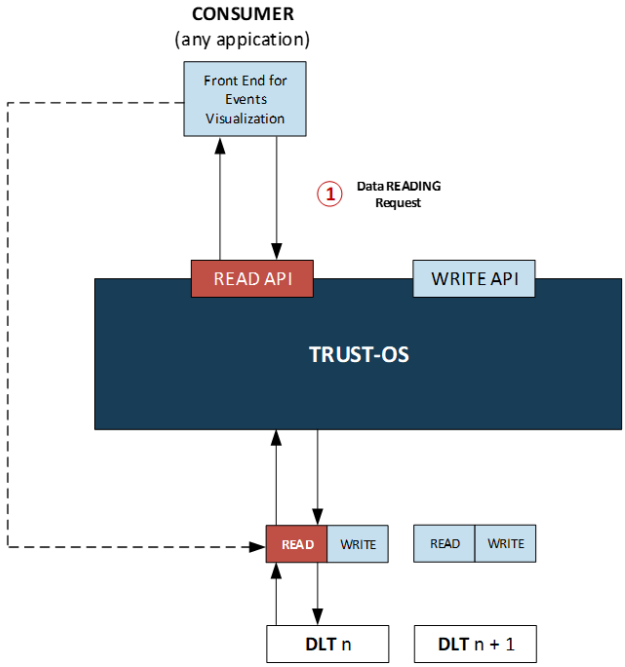


Figure 28: Data reading request flow

8.2 Expected Innovation

Different actors from the supply chain are starting to get advantages from the modern technologies that allow fast data communication, data sharing and secure data management. Blockchain-based applications are becoming more attractive in different industries, stakeholders are still suffering due to technological lock-in.

Co-funded by the Horizon 2020 Framework Programme of the European Union

While the current status of major M2M standardization activities is mainly related to the M2M device connectivity, technologies for access networks, identification and definition of data formats, standard approaches for data management and governance from a single access point are still missing. Development is limited to the system owners who understand the particular API, thus leading to high development costs and high costs for support. To overcome this challenge, it is essential to define more comprehensive standards, in particular regarding communication interfaces and data models. In addition, it is important to have a common platform for data governance that can be reused for multiple applications, avoiding the necessity to completely redesign solutions per application due to the lack of common capabilities. In order to overcome the above-mentioned barriers, the data virtualization layer is expected to be a good alternative for the cross-M2M interoperability. Data Virtualization approach is a common approach used for data management within companies in order to easily manage a huge amount of data coming from different heterogeneous data sources. Even if there are different commercial solutions on the market allowing data virtualization (from TIBCO, Denodo, IBM, Oracle, etc.), those solutions are not used for the M2M platforms harmonization and/or interoperability. By means of this approach it will be possible to hide technical details about different distributed M2M platform implementations, allowing interacting with them from a single access point, by defining a common data model for data exchange.

Moreover, projects such as Polkadot or Cosmos are actively developing protocols to enable the trustworthy exchange of data and digital assets between different DLT networks. They are both building proposals for the communication and interoperability between different DLT networks at a protocol level, mainly Comos' Inter-Blockchain Communication Protocol, and Polkadot's parachains. Both technologies are still under development, Polkadot's first PoC network has been recently released (Kusama), while there is no information about when Cosmos will be live. We can expect them to be ready in the next few years, however, no details have been disclosed about the specific dates, or the status of development of the future released networks (i.e., if they will represent production-ready networks, or just PoC testnet instances of the technology). Therefore, it would not be possible applying these technologies in the near future because of its development status. However, these technologies tackle the aforementioned challenge of the "exchange of data between DLT networks" and could be a future improvement to consider in the following years.

The use case proposes a proof-of-concept based on a centralized approach for data exchange and management (including privacy and security aspects) between heterogeneous M2M and DLT solutions, abstracting their complexity. A common layer for the interoperability could allow different stakeholders to manage and keep track of their own data coming from different M2M platforms, benefiting in the security capabilities provided by different DLTs. Stakeholders can take control over their own data flows: from the time data are produced by IoT devices and stored within different M2M platforms to the time data are secured thanks to different blockchain-based solutions.

8.3 End User and Environment

Considering the proposed interoperable solution is applied at the maritime sector in this use case the following actors could become potential users: Port Authority, Freight Forwarder, Container Terminal and Maritime Agency.

Co-funded by the Horizon 2020
Framework Programme of the European Union

8.4 Actors

M2M Platform Providers will bring into the use case different M2M solutions, supporting their integration with the cross-M2M layer.

DLT Solution Providers will bring into the project different available DLT solutions with different configurations to be used during the use case validation.

Cross-DLT Layer Provider will develop a Cross-DLT layer enabling the interoperability among different DLT solutions. Cross-DLT layer will be fed by data coming from DVL by means of APIs. Data will be stored, hashed and distributed among different DLTs (e.g.: Ethereum, Bitcoin, IoTA, Tradelens and Hyperledger Fabric) exploiting their security capabilities.

Cross-M2M Layer Provider will develop a Cross-M2M layer enabling the interoperability among different M2M solutions. Data virtualization approach will be used in order to collect raw data and aggregate them accordingly to a given data model, hiding technical details about underlying M2M platforms. Data will be then sent to the Cross-DLT layer.

Cybersecurity Expert will address the security and privacy aspects of the interoperable layers. The focus will be data protection and how well-proven technologies and standards can be exploited for data anonymization and encryption. By means of this, also GDPR requirements will be fulfilled.

NFV Orchestrator Provider will bring their solutions for NFV management and orchestration. The integration with the cross-M2M layer will allow to train ML algorithms based on available data set and improve the network slice usage within different use cases of the project.

8.5 Data and Service(s)

Based on the relationship between this UC and other UCs of the project, the following events have been identified as relevant for its validation:

- Gate In and Gate Out: terminal, voyage id, truck plate number, data and time of access, truck driver info, etc.
- Load and Discharge from Vessel: terminal, truck plate number, booking number, etc.
- Vessel Arrival and Departure: ETA, RTA, cargo type, terminal, port call berth, ETD, ATD, shipping line, vessel position, etc.
- Weather: wind speed, precipitation, average temperature, etc.

The final data set will be extracted from available data sources (OCR, meteorological station, PCS, AIS dispatcher) and used to feed different M2M platforms. Both DVL and cross-DLT layer will support a specific data model according to the identified data set.

8.6 Asset(s)

The assets to be used for the realization of this use case are the following:

- *Set of different M2M platforms:* Mobius OneM2M, Eclipse OM2M, Symphony, PI System OSIsoft and NB-IoT Platform.
- *Set of different DLT Platforms:* IOTA, Hyperledger Fabric, Ethereum, Tradelens and Bitcoin.
- *Data Virtualization Layer:* single access point for cross-M2M data governance.
- *TrustOS Framework:* single access point for cross-DLT interoperability.
- *MANO Platform:* will collect data from DVL in order to apply ML algorithms and enhance the network resources usage.

Co-funded by the Horizon 2020
Framework Programme of the European Union

8.7 Requirements

User Requirement	Description
#1: Gate-In, Gate-Out, Vessel Arrival and Vessel Departure events visualization.	Once data have been extracted (DVL), aggregated (DVL), stored (cross-DLT layer) and distributed across different DLTs in a form of events (cross-DLT layer), the users must be able to get access to their own events and visualize them in a human-readable form. Based on DLTs' capabilities, hash storage will be guaranteed for each DLT, while in other cases also data events storage can be possible.
#2: Extra user information visualization.	Once users get access to their own data/events they must also visualize extra information such as which DLT has been used for hash/data storage, hash string and the status of pending requests. This extra information is handled and stored by the cross-DLT layer.
#3: Data integrity and immutability.	The system must allow users to check and get back the proof of integrity and immutability of their own data. The system must also allow authorized users to interact directly with a DLT for which they have been authorized. Note: data hashes are aggregated in hash-trees, hash-tree roots are stored on the DLT and the user gets hash-tree root along with the derivation starting with the hash of his data.
#4: User Authentication.	Users must be able to access the cross-DLT layer visualization interface by means of a safe and secure authentication procedure able to distinguish between different user roles and user identities.

System Requirement	Description
#1: Interaction with M2M platforms	DVL must be able to retrieve data coming from different M2M platforms, supporting different communication protocols as well as different data formats
#2: Virtual data aggregation and events definition	Data Virtualization Layer should be able to virtually aggregate data coming from different M2M platforms accordingly to a given data-model for supported events. Collected data must be sufficient for the gate-in, gate-out, vessel arrival and vessel departure events definition.
#3: DVL's role-based data access policies	Data Virtualization Layer should provide data access by following a role-based policy. Roles should include data access privileges (based on writing, reading, deleting and updating capabilities)
#4: Views and queries caching	Data Virtualization Layer should provide a caching mechanism in order to store specific calls to queries and/or virtual procedures. This will yield significant performance gains if same queries or the same procedures are submitted often.
#5: Interaction between DVL and cross-DLT layer	DVL must allow cross-DLT layer to consume aggregated data by means of an interface so that data can be stored and managed according to DLTs' capabilities.
#6: DVL data provisioning to AI/ML assisted MANO	Data Virtualization Layer must allow the ML-based module of MANO to retrieve pseudo-anonymised data related to application and network usage by means of subscription mechanism.
#7: AI/ML assisted MANO stores the application data retrieved from DVL.	The AI/ML assisted MANO must be able to collect data from the DVL and store them to properly train slice optimization AI/ML algorithms.
#8: Cross-DLT data hashing capability	Cross-DLT layer should be able to generate a hash associated to the received data from the Data Virtualization Layer. This way, the data can be stored securely and anonymously in a public blockchain network using a limited amount of data (ideal for blockchains networks like Bitcoin).

Co-funded by the Horizon 2020 Framework Programme of the European Union

#9: Information accompanying data from the DVL storage	Cross-DLT layer should allocate a DBMS where data and generated hashes could be stored accordingly to a given data-model, including any other needed information (e.g., list of DLTs and stored hash address).
#10: APIs for writing in specific DLTs	Cross-DLT layer should be able to distribute hashes and/or data within different DLTs by means of WRITE APIs (writing operation). A positive/negative response should be received from different DLTs and managed by Cross-DLT layer, updating the DBMS accordingly.
#11: APIs for reading from specific DLTs.	Cross-DLT should integrate an API for exposing data and events to supply chain users, end users and applications in order to allow reading/writing operations. The proof-of-existence should be validated (data integrity and data immutability).
#12: ACL for Cross-DLT layer.	Cross-DLT layer should expect an authentication mechanism in order to manage and control users' access. This control is expected to affect users from upper layers and interactions with the Data Virtualization Layer, so identity is really important when storing data in DLTs.
#13: Data storage within DLTs and Cross-DLT layer.	Different DLTs should use a proper setup, according to their own capabilities, for hash and/or data storage across ledgers/network. Hash storage across different DLTs should be guaranteed as a minimum requirement. Cross-DLT layer will store events generated by DVL. As far as DLTs' is concerned, hash storage will be guaranteed for each available DLT as a minimum requirement. In some cases, it will be also possible to store data events (e.g., IOTA).
#14: DVL must act as a pseudonymization entity	Personal Data should be anonymized as soon as possible avoiding being exposed in clear text. As DVL is the closest point to M2M platforms (data generator from an Interoperable Layer point of view) it must also act as a Pseudonymization Entity.
#15: According to GDPR, any Personal Data must be stored in pseudonymized form (pseudonym).	Personal data is any information related to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also represents a personal data. According to GDPR, Personal Data can be pseudonymized to protect individual identity. Note: Personal Data should not be transferred across borders.
#16: Additional Information, used to reverse pseudonym, must be stored in a separated encrypted repository.	Pseudonymization is a reversible process. To do it "additional information" (e.g., encryption keys, conversion tables, etc.) are necessary. This information has to be protected.
#17: Supply Chain Users must only access the Personal Data for which they have been properly authorized.	Personal Data has to be accessible in clear format only by authorized entity. Note: Personal Data should not be transferred between partners.
#18: Storage of personal data must follow specific retention times which are aligned with the purposes of processing. In addition, "right to be forgotten" requests from Data Owner must be considered.	Personal Data are not forever; they have to be deleted according to data owner's agreements. Furthermore, the data owner has the right to request the deletion of his personal data.
#19: Collection, processing, and transfer of personal data must be limited to what is necessary for the purposes.	Personal data are retained only if strictly necessary.

Co-funded by the Horizon 2020 Framework Programme of the European Union

8.8 Key Performance Indicators (KPIs)

KPI	Target Value	Verification Means
Data Virtualization Layer scalability	≥5 heterogeneous and simultaneous M2M platforms as data sources.	DVL is able to interact with the given M2M platforms, retrieving identified data sets correctly.
Data Virtualization Layer data processing	Real-time	DVL is able to interact with the given M2M platforms, retrieving identified data sets in real-time.
Data Virtualization Layer access control	Role-based access	Defined roles for each entity are correctly used during data access procedures.
Cross-DLT layer access control	Role-based access	
Cross-DLT layer scalability	At least 4 simultaneous DLT technologies	Cross-DLT layer is able to interact with the given DLT technologies, sending transactions and reading from the ledgers.
Availability of the DLT connectivity layer	The DLT connectivity layer should be highly available	Measurement of actual value of availability on running system.
Data processing time in DLTs	Each request for the given DLT should be processed in less than one minute	*Benchmark.*
Cross-DLT concurrent requests.	At least 4 concurrent requests	*Cross-DLT layer is able to interact with the given DLT technologies sending up to five concurrent transactions. It will be possible to deploy multiple instances of the DLT connectivity layer.*
Data Protection Impact Assessment (DPIA) report prepared & approved.	DPIA report approved	*DPIA is available, shared with UC owners and approved by DPO (Data Protection Officer).*
Privacy User Guide prepared & approved	Privacy User Guide approved	*Privacy User Guide is available, shared with UC owners and approved by DPO (Data Protection Officer)*
Confidentiality and integrity protection of personal data	100%	*Controlling any personal data at rest, in transit and in use, it is never in clear text format.*
Logs of privacy events.	100%	*Analysis of whatever privacy event logs shall not contain clear text personal data.*

8.9 Operational, Business, Societal and Environmental Outcomes

Societal impact: IoT/DLTs interoperability will enable the communication and data exchange allowing users and companies with a way of governing their data in every network.

Business impact: Organizations and companies will spend less on building and managing data integration processes for connecting distributed data sources, benefiting in terms of costs and time savings.

Technological impact: The IoT/DLT interoperability layer will enable the federation of different IoT platforms overcoming compatibility issues between standard and non-standard solutions in industry 4.0 domain.

Co-funded by the Horizon 2020 Framework Programme of the European Union

8.10 Verification Means and Actors Involved

The PoC validation and verification will be based on the integration between different architectural components that will allow different data flows from M2M platforms to the targeted DLTs. Cross-DLT layer will be implemented by means of Trust-OS from Telefonica, a complete blockchain solution which abstracts all the complexity of blockchain technology enabling the interoperability between the different blockchain solutions provided by partners (Bitcoin – PJATK, CNIT – IOTA & Tradelens, Ethereum – TID, and Hyperledger – TID and FV). The interoperability between different M2M platforms provided by partners (Mobius oneM2M – CNIT, Symphony – NXW, PI System OSIsoft – FV, Eclipse OM2M – SES, and NB-IoT platform – CMC) , will be guaranteed by means of Teiid from CNIT, a data virtualization solution that sits in front of multiple data sources and allows them to be treated as a single source, delivering the right data, in the required format, at the right time to any application and/or user. Moreover, once data has been collected and aggregated based on a given data model, the NFV orchestrator will be able to consume these data by applying ML algorithms, optimizing network resources usage. The NFV orchestrator will be implemented by means of MANO platform from NXW and will be used in a real environment within different UCs of the project. For the PoC validation, different categories of end users have been identified:

- *Supply Chain Users* (users from the consortium that can get benefits in using interoperable layer: Port of Valencia, Port of Livorno).
- *End Users* (users that need to track their own assets status along the supply chain exploiting DLTs' capabilities. These users can interact with the interoperable layer but with less capabilities if compared with Supply Chain Users).
- *Applications* (any external system/application allowed to consume data from Trust-OS for other purposes).

To validate this use case, a user scenario and a set of KPIs will be defined. System Requirements will be derived and tests will be conducted to ensure they all have been properly covered. Test results will be benchmarked then against a defined set of KPIs, validating them accordingly. In particular, the PoC proof-of-concept will be validated in laboratory by means of (decentralized) computational resources with storage and hosting capabilities.

The proof-of-concept will be validated in laboratory by means of (decentralized) computational resources with storage and hosting capabilities.

Co-funded by the Horizon 2020
Framework Programme of the European Union

9 Analysis

Previous chapters described the main innovation required at the iNGENIOUS use cases together with the requirements and KPIs needed to evaluate the performance of the proposed technologies. According to the previous analysis, the technological solutions to be designed at the project will target an enhancement of the operative in different supply chain segments. In the following, the main technological components to be designed in each use case and its mapping to the technical WP of the project are analysed. Additionally, Key Performance Indicators are also analysed for each use case.

9.1 Analysis of Use Cases

9.1.1 Automated Robots with Heterogeneous Networks

First use case focuses on enabling an automated robot control in industrial environments thanks to the design of a smart distributed application that will leverage different types of sensors, actuators and parallel control loops for connecting machines and humans. To achieve this goal, the main technological modules affected in this use case are: (i) 5G IoT layer, with an special focus on software defined communications in PHY and MAC, NFV and time synchronization; (ii) MANO and Slicing Service for the automated deployment of slices for covering TSN requirements; and (iii) API layer for connecting the different components of the system and enabling the interaction with humans by means of graphical user interface (GUI) for monitoring and remote operation. Regarding the development of these components in the project, the developments of 5G IoT layer will be covered in WP3 and WP4; MANO and slicing services will be mainly covered in WP4; and APIs will be designed in WP5.

9.1.2 Transportation Platform Health Monitoring

This use case will enable the monitoring of health for transportation platforms with a particular focus on railway transportation. The monitoring of health conditions will reside in the design of neuromorphic sensors able to gather and process data on the edge of the network while bringing low cost and power and high life expectancy. For enabling the exchange of data between smart edge sensors and platforms, near continuous connectivity to the edge will be enabled by exploiting terrestrial and non-terrestrial networks. Based on these objectives, the main technological innovation of the project in this use case focuses on: (i) the design of neuromorphic edge sensors for data collection, (ii) enabling mobile edge connectivity and multi-model communication through the connection of sensors with a Smart IoT Gateway and, (iii) the design of new HW security communication concepts. The development of these components in the project will be mainly performed in WP3 for edge neuromorphic sensors and HW security, in WP4 for designing the Smart IoT GW and in WP5 for the data management and security.

9.1.3 Situational Understanding and Predictive Models in Smart Logistics

This use case aims at enhancing the situational understanding of events in maritime ports and terminals by means of collecting and aggregating data processing. By analysing the available data sources, the use case will optimize and predict processes for reducing the time that trucks spend inside the port and terminal facilities, i.e., truck turnaround times (TTT). The outcomes of the monitoring and optimization processes are expected to be visualized in a dashboard and map interface. As a consequence, the main technological innovation of the project in this use case focuses on: (i) the ingestion of data from existing data sources and external systems, (ii) the

Co-funded by the Horizon 2020
Framework Programme of the European Union

integration of data through the design of a DVL, (iii) the design of AI algorithms for the prediction and optimization of TTT, (iv) the execution of algorithms in a cloud-based infrastructure through the use of APIs, and (v) the installation of new IoT tracking devices on trucks as new data source. The development of these components in the project will be mainly performed in WP5 for the integration of data sources, the development of AI algorithms and the design of the cloud-based application; and residually in WP4 for setting the connectivity of IoT tracking devices.

9.1.4 Improve Driver's Safety with MR and Haptic Solutions

This UC aims at improving the safety conditions of workers in maritime ports and terminals by operating AGVs remotely thanks to the use of 5G communications, MR and haptic solutions, which will be integrated in an immersive remote indoor cockpit. 5G will ensure high throughput and low latency connectivity with the cockpit, while MR and haptic solutions will provide an immersive experience to the worker. Additionally, the project will also explore the deployment of a novel Time-Sensitive Networking Application Function (TSN-AF) that maps 5G network slicing with fixed TSN Central Network Controller (CNC) polices. Thus, the main technological components affected in this use case are: (i) 5G Infrastructure through the deployment of a 5G-based private network for enabling AGV remote connectivity; (ii) iNGENIOUS platform that will integrate the design of a remote indoor cockpit including MR and wearable devices; and (iii) TSN framework for enabling time sensitive communications. These components will be deployed in WP3 (MR and haptic devices) and WP4 (5G infrastructure deployment).

9.1.5 Inter-Modal Asset Tracking via IoT and Satellite

The fifth use case will allow the E2E asset tracking of shipping containers and cargo when they are transported through land and sea, i.e. inter-modal transportation. To do so, the project will explore communications via satellite backhaul and IoT terrestrial infrastructure, enabling real-time monitoring of cargo parameters when containers are sailing on the sea and when they approach earth. To enable the ubiquitous coverage, sensors and IoT tracking devices will be installed on the shipping containers transported by ships and trucks on both segments. The connectivity between sensors, satellite and IoT network will be provided by the Smart IoT GW. Therefore, the main technological modules affected in this use case are: (i) the Smart IoT GW for enabling satellite and IoT connectivity, (ii) the installation of smart sensors and IoT tracking devices, and (iii) the development of APIs for accessing the data. These components will be mainly deployed in WP3 (sensors and IoT tracking devices), WP4 (design of the Smart IoT GW and satellite connectivity) and WP5 (data management with APIs and visualization platform).

9.1.6 Supply Chain Ecosystem Integration:

The last use case targets interoperability between different M2M platforms and different DLT solutions that could be used in different segments of the supply chain as manufacturing, transportation or logistics. The project will provide two different interoperable layers in order to abstract the complexity of the underlying M2M platforms and DLT solutions, guaranteeing at the same time data privacy and security by means of encoding and anonymization techniques. As a consequence, the main technological innovations in this use case are: (i) DVL as data layer for retrieving raw data and aggregate them creating a common data model, (ii) Cross-DLT for enabling the exchange of data between public and private DLTs and (iii) a Cloud-based Application integrating APIs for enabling the exchange of data and events between platforms, DVL and the cross-DLT. All these components will be designed and implemented as part of WP5 work plan.

The summary of the influence of each technology in % on the different use cases is shown in Figure 29:

Co-funded by the Horizon 2020
Framework Programme of the European Union

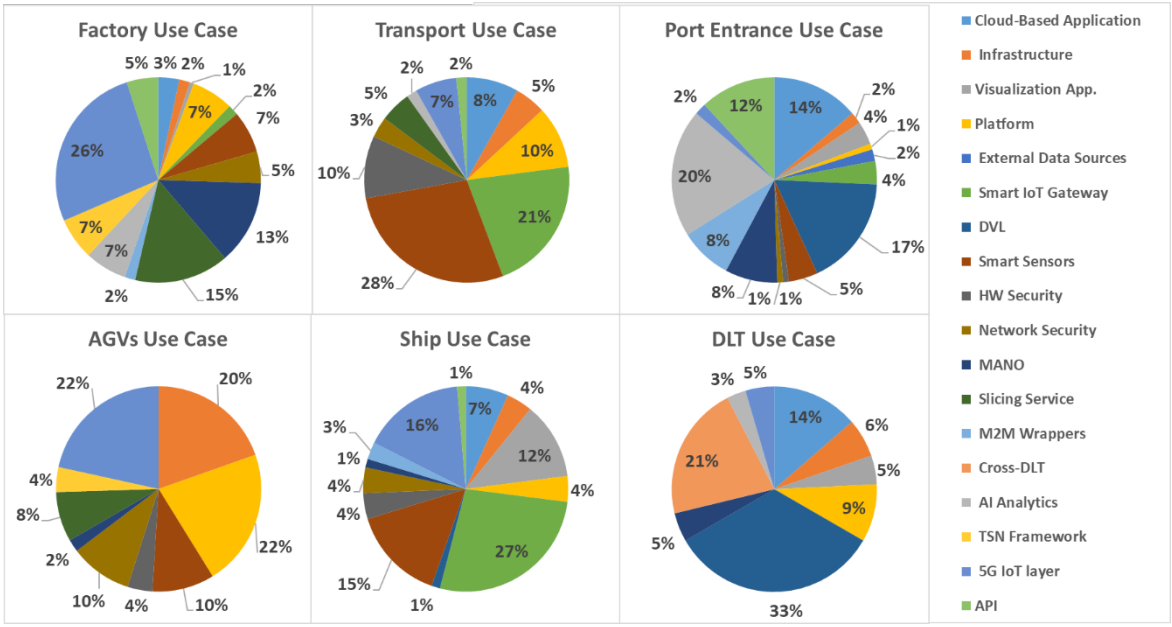


Figure 29: Influence of each technology per use case

Additionally, based on the analysis of the main technologies involved in the different use cases, the correlation between the technical work packages of the project and the use cases is quantified in Table 7:

	WP3: Forthcoming IoT devices	WP4: Future IoT network solutions	WP5: Smart data management analytics
Factory UC	Medium	High	Low
Transport UC	High	Medium	Medium
Port Entrance UC	Low	Medium	High
AGVs UC	Medium	High	Low
Ship UC	Medium	Medium	Medium
DLT UC	Low	Low	High

Table 7: Correlation between UC and Technical WPs based in technological innovation.

9.2 Analysis of KPIs

9.2.1 Automated Robots with Heterogeneous Networks - Factory Use Case

The automation applications involve different types of control loops mostly exchanging short packet of data for sensing feedback and actuation commands. In closed-loop control and cooperative machines, synchronization and deterministic data exchange is critical. This implies, that packets need to be exchanged reliably within timing constraints and low E2E latency. This corresponds to URLLC communications requirements in addition to precise timing. In particular, the cyclic time, and jitter time KPIs need to be guaranteed with very high probability. On the one hand, the network needs to provide precise timing and synchronization to all involved nodes during the running phase of the application. On the other hand, the E2E KPIs of data rate, latency and reliability need to be achieved within the provisioned connection density. In applications that employ mobile robots, seamless mobility support within the speed limit and positioning accuracy are essential. In addition, this use case encompasses also MBB and mMTC links with relaxed timing requirements. However, it is required to guarantee the data rate and latency KPIs w.r.t. the required connection density.

Co-funded by the Horizon 2020 Framework Programme of the European Union

9.2.2 Transportation Platform Health Monitoring - Transport Use Case

Transportation Platform Health Monitoring reduces critical safety incidents, and increases asset uptime, while reducing maintenance costs. This makes logistic services more reliable and cost effective. The principles of Asset Health Monitoring have been demonstrated before but applying this to a mobile cost driven commodity platform without power resources and in a sometimes bandwidths starved environment, with a net-cost benefit (maintenance cost reduction greater than monitoring investment) is the biggest KPI this use case can offer. Technology advances in machine learning data collection via neuromorphic networks, and end to end payload encrypted communication are noteworthy secondary KPIs.

9.2.3 Situational Understanding and Predictive Models in Smart Logistics - Port Entrance Use Case

This use case targets the optimization of truck turnaround times by analysing and exploiting existing and new data sources through the use of predictive AI-based algorithms. As a consequence, most of the relevant KPIs are related to data and predictive aspects.

In data domain, several indicators are defined to ensure that the ingested data adds the sufficient value for understanding and modelling the operational process related to truck turnaround times. Data source sufficiency is set to at least 5 data different sources considering PCS, AIS, M2M platforms, meteorological and gate access sensors as potential candidates to help understanding operational processes. Complementing this KPI, the use case targets the integration of a new data source related to the installation of IoT tracking devices on trucks. To ensure the effectiveness of these devices, positioning accuracy KPI is set to at least 5 meters for ensuring the quality of the tracking of trucks. Data availability is targeted to be higher than 99% uptime in order to ensure that data is obtained after performing queries to the different systems. Data quality will be assessed against the metrics defined by ISO/IEC 25012 where accuracy, completeness, consistency, credibility, correctness and accessibility aspects are considered. At the same time, security and privacy aspects are addressed by defining specific KPIs like the need for approving a Data Protection Impact Assessment (DPIA), the availability of a Privacy User Guide, the confidentiality and integrity of personal and sensitive data related to truck or vessel identities. Most of KPIs related to data aspects will be evaluated by inspecting the available data sets.

On the other hand, to ensure the quality of the time prediction performed by AI-based algorithms, an accuracy of 90% is targeted. The verification of this accuracy will be carried out by using common evaluation metrics used in regression problems like Minimum Sum of Absolute Errors (MSPE) or R Square, compared with the real values measured in demonstrations. Finally, the overall impact of the use case will be measured by targeting a reduction of TTTs and idling times of a 10%, leading the optimize the operative at the Port of Valencia and the Port of Livorno. The validation of these KPIs will be performed by means of analytical and real demonstration processes that will allow to cross-check the obtained predictions with the port reality.

9.2.4 Improve Driver's Safety with MR and Haptic Solutions - AGVs Use Case

This use case targets at satisfying E2E wireless communications over the proposed network infrastructure with good reasonable throughput at its lowest latency. This allows for live broadcasting of immersive experiences with volumetric video live streaming and experience an indoor remote driving of AGVs along the maritime port happening right in front of your eyes in real-time; 5G will enable this broadcasting and guarantee an available bandwidth (BW) for the provision. As a consequence, several KPIs embraced within those originally stated in the project proposal (availability, battery life, connection density, coverage, data rate, E2E latency, mobility,

Co-funded by the Horizon 2020
Framework Programme of the European Union

positioning accuracy, reliability and security), nevertheless, the most significant KPI is highlighted here, the throughput at its lowest latency. It Is this low latency requirement with high throughput the foremost for achieving reliable communications exchange between the involved parties that form this case scenario.

9.2.5 Inter-Model Asset Tracking Via IoT and Satellite - Ship Use Case

This use case targets at providing E2E intermodal asset tracking via satellite and IoT technologies, optimising real-time data interchange along the whole supply chain, improving customer satisfaction and increasing transparency and collaboration. As a consequence, most of the relevant Key Performance Indicators are related to data.

Up to six different sensors and actuators will be installed in the container for measuring real-time location, cargo and safety conditions of the container. The set of IoT sensors installed in the container is composed of: real-time tracking sensor which should provide the data constantly; temperature and humidity which should provide the data every 10 minutes; accelerometer sensor for measuring movement and vibration which should provide the data constantly; bump and stop detection sensor which should provide the data constantly; container door opening sensor which should provide the data constantly.

Then, a Smart IoT Gateway should be able to gather and process the data. The Smart IoT Gateway should be able to ensure the connectivity for a vast number of heterogeneous IoT devices, by harmonizing different IoT technologies and application protocols and formatting the data to be transferred across the network, optimized for satellite communications.

Data availability and reliability is targeted to be higher than 99% and the ubiquitous coverage is obtained though GEO satellite connectivity. At the same time, security and privacy aspects are addressed by defining specific KPIs like the need for approving a Data Protection Impact Assessment (DPIA), the availability of a Privacy User Guide, the confidentiality and integrity of personal and sensitive data related to truck or vessel identities.

9.2.6 Supply Chain Ecosystem Integration - DLT Use Case

This use case is focused on next generation supply chain supported by DLTs where the original data and events are collected from M2M layer and then made available to authorized actors using a desired DLT in order to share and store data in a secured manner. In order to enable this data flow between different technological components involved in this use case, integration activities will be performed accordingly: i) integration between DVL and M2M platforms, ii) integration between Cross-DLT layer and different DLTs, ii) integration between DVL and Cross-DLT layer for data exchange and iv) integration between DVL, MANO platform and AWAKE platform for predictive models. For this purpose, KPIs have been defined according to minimum set of functionalities of the interoperability layer.

In order to guarantee a proper level of scalability for both DVL and cross-DLT layer, a minimum number of available M2M platforms and DLTs has been set by means of related KPIs. Data access policies at DVL and cross-DLT layer are also considered just to make sure only authorized entities can get access. For this reason, two KPIs related to access control (role-based) have been introduced as well. Finally, data processing constraints both at DVL and cross-DLT layer have been considered to guarantee real-time capabilities as well as proper concurrent requests management.

Co-funded by the Horizon 2020
Framework Programme of the European Union

References

[1] I. 4. International Organization for Standards (ISO)/International Electrotechnical Commission (IEC), "Systems and Software Engineering -- Recommended Practice for Architectural Description of Software-Intensive Systems", ISO/IEC, Geneva, Switzerland, 2007.

[2] "Volere Requirements: How to Get Started", Available: https://www.volere.org/wp-content/uploads/2018/12/VolereGettingStarted.pdf.

[3] Available: http://www.tacnet40.com.

[4] LoRa. Alliance, "A technical overview of LoRa and LoRaWAN", November 2015.

[5] Awake.ai, "Awake platform is changing the maritime industry", Available: https://www.awake.ai/awake-platform.

[6] C. C. Aggarwal, "Neural Networks and Deep Learning: A Textbook", Springer International Publishing, September 2018.

[7] G. B. Team, "TensorFlow v2.1.0. An end-to-end open-source machine learning platform", October 2020. Available: https://www.tensorflow.org/versions/r2.1/api_docs/python/tf.

[8] N. Ketkar, "Introduction to PyTorch", de *Deep Learning with Python*, Berkeley, CA, Apress, 2017, p. pp. 195–208.

[9] "Scikit-learn. Machine Learning in Python", Available: https://scikit-learn.org/sTable/.

[10] "Jupyter Notebook", November 2020. Available: https://jupyter.org/documentation.

[11] "The fifth-generation automotive association 5GAA", Available: https://5gaa.org/.

[12] G. K. A. N. G. Z. S. Mangiante, "VR is on the Edge: How to Deliver 360° Videos in Mobile Networks", August 2017. Available: https://www.researchgate.net/publication/319049968_VR_is_on_the_Edge_How_to_Deliver_360_Videos_in_Mobile_Networks.

Co-funded by the Horizon 2020 Framework Programme of the European Union