This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101069732

D2.2 – Use cases manual, requirements, legal and regulatory analysis (1)

Deliverable No.	D2.2	Due Date	31-MAY-2023
Type	Report	Dissemination Level	Public (PU)
Version	1.0	WP	WP1
Description	Initial version of requirements elicitation, use cases and scenarios definition and legal and regulatory analysis.		

The aerOS consortium consists of the following 27 partners:

UNIVERSITAT POLITÈCNICA DE VALÈNCIA	ES
NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS"	EL
ASOCIACION DE EMPRESAS TECNOLOGICAS INNOVALIA	ES
TTCONTROL GMBH	AT
TTTECH COMPUTERTECHNIK AG (*third linked party*)	AT
SIEMENS AKTIENGESELLSCHAFT	DE
FIWARE FOUNDATION EV	DE
TELEFONICA INVESTIGACION Y DESARROLLO SA	ES
COSMOTE KINITES TILEPIKOINONIES AE	EL
EIGHT BELLS LTD	CY
INQBIT INNOVATIONS SRL	RO
FOGUS INNOVATIONS & SERVICES P.C.	EL
L.M. ERICSSON LIMITED	IE
SYSTEMS RESEARCH INSTITUTE OF THE POLISH ACADEMY OF SCIENCES IBS PAN	PL
ICTFICIAL OY	FI
INFOLYSIS P.C.	EL
PRODEVELOP SL	ES
EUROGATE CONTAINER TERMINAL LIMASSOL LIMITED	CY
TECHNOLOGIKO PANEPISTIMIO KYPROU	CY
DS TECH SRL	IT
GRUPO S 21SEC GESTION SA	ES
JOHN DEERE GMBH & CO. KG*JD	DE
CLOUDFERRO SP ZOO	PL
ELECTRUM SP ZOO	PL
POLITECNICO DI MILANO	IT
MADE SCARL	IT
NAVARRA DE SERVICIOS Y TECNOLOGIAS SA	ES
SWITZERLAND INNOVATION PARK BIEL/BIENNE AG	CH

Authors

Name	Partner	e-mail
Ignacio Lacalle	P01 UPV	iglaub@upv.es
Andreu Belsa	P01 UPV	anbelpel@upv.es
Rafael Vañó	P01 UPV	ravagar2@upv.es
Raúl San Julián	P01 UPV	rausanga@upv.es
Harilaos Koumaras	P02 NCSRD	koumaras@iit.demokritos.gr
Vasilis Pitsilis	P02 NCSRD	vpitsilis@dat.demokritos.gr
Constantinos Vasilakis	P02 NCSRD	cvassilakis@iit.demokritos.gr
Anastasios Gogos	P02 NCSRD	angogos@iit.demokritos.gr
Thanos Papakyriakou	P02 NCSRD	thpap@iit.demokritos.gr
George Makropoulos	P02 NCSRD	gmakropoulos@iit.demokritos.gr
Eneko Rada	P03 INNOV	erada@innovalia.org
Anna Ryabokon	P04 TTC	anna.ryabokon@tttech.com
Philippe Buschmann	P05 SIEMENS	philippe.buschmann@siemens.com
Korbinian Pfab	P05 SIEMENS	korbinian.pfab@siemens.com
Florian Gramss	P05 SIEMENS	florian.gramss@siemens.com
Foteini Setaki	P08 COSM	fsetaki@cosmote.gr
George Lyberopoulos	P08 COSM	glimperop@cosmote.gr
Eleni Theodoropoulou	P08 COSM	etheodorop@cosmote.gr
Ioanna Mesogiti	P08 COSM	imesogiti@cosmote.gr
Dimitra Siaili	P09 8BELLS	dimitra.siaili@8bellsresearch.com
Dimitris Tsolkas	P11 FOGUS	dtsolkas@fogus.gr
Christos Milarokostas	P11 FOGUS	milarokostas@fogus.gr
Manolis Marinos	P11 FOGUS	marinos@fogus.gr
Katarzyna Wasielewska-Michniewska	P13 IBSPAN	katarzyna.wasiliewska@ibspan.waw.pl
Nikolaos Gkatzios	P15 INF	ngkatzios@infolysis.gr
Vaios Koumaras	P15 INF	vkoumaras@infolysis.gr
Eduardo Garro	P16 PRO	egarro@prodevelop.es
Mª Ángeles Burgos	P16 PRO	mburgos@prodevelop.es
Alvaro Martínez-Romero	P16 PRO	amromero@prodevelop.es
Petros Dias	P17 EGCT	petros.dias@eurogate-limassol.com
Alessandro Cassera	P17 EGCT	alessandro.cassera@eurogate-limassol.com
Michalis Michaelides	P18 CUT	michalis.michaelides@cut.ac.cy
Herodotos Herodotou	P18 CUT	herodotos.herodotou@cut.ac.cy

Sheraz Aslam	P18 CUT	sheraazaslam@gmail.com
Shaden Baradie	P21 JD	BaradieShaden@johndeere.com
Stanisław Krzyżanowski	P22 CF	skrzyzanowski@cloudferro.com
Marcin Michel	P23 ELECTRUM	mmichel@electrum.pl
Walter Quadrini	P24 POLIMI	walter.quadrini@polimi.it
Dario La Carrubba	P25 MADE	dario.lacarrubba@made-cc.eu
Pablo Patús	P26 NASERTIC	ppatusdi@nasertic.es
Charly Gerber	P27 SIPBB	Charly.Gerber@sipbb.ch
Michael Wendling	P27 SIPBB	Michael.Wendling@sipbb.ch

History

Date	Version	Change
6-MAR-2023	0.0	ToC created and announced in WP2 telco
10-APR-2023	0.1	First content included in the document
-	0.2-0.6	Intermediate versions during content creation/integration
26-MAY-2023	0.6	Version submitted to internal review
2-JUN-2023	1.0	Version submitted (Pilot 3 information removed)
13-JUN-2023	1.1	Version sent including reviewed Pilot 3 content

Key Data

Keywords	Use cases, pilots, trial, requirement, KPI, scenario.
Lead Editor	P01 UPV (Ignacio Lacalle)
Internal Reviewer(s)	P20 S21Sec (Jon Egaña), P06 FIWARE (José Ignacio Carretero)

Executive Summary

This document is written in the framework of *WP2 - aerOS reference architecture for the IoT-edge-cloud continuum* of the Horizon Europe project aerOS (GA No 10106932).

The HE-funded project aerOS aims at transparently utilising the computing resources on the edge-to-cloud continuum for enabling applications in an effective manner while incorporating multiple services. The overarching goal of aerOS is to design and build a virtualised, platform-agnostic meta operating system for the IoT edge-cloud continuum. In the action, the technical provisions must be first described and analysed to be later developed. In addition, all results will be validated in relevant environments (use cases) to prove the usefulness and validity of the proposed meta Operating System.

This document depicts the efforts devoted to the elicitation of requirements and the description of the 5 use cases (*P1 - Data-Driven Cognitive Production Lines*, *P2 - Containerised Edge Computing near Renewable Energy Sources, P3 - High Performance Computing Platform for Connected and Cooperative Agricultural Mobile Machinery to Enable CO2 Neutral Farming (HPCP-F), P4 – Smart edge services for the Port Continuum and P5 - Energy Efficient, Health Safe & Sustainable Smart Buildings*), that will be executed later in the project.

Starting by the use cases, aerOS is following a methodology based on Trial Handbooks, as suggested by the Digital Factory Alliance. There, every use case (becoming a trial) uses a series of templated documents (Chapters) to describe their nature, goals, equipment, data sources, planning, etc. Those consist of live documents, that will be changing along the duration of the project, and that feed directly various tracks of it. Chapter 1 concentrates on giving an overview of the pilot, Chapter 2 delves deeper into the description of the particular scenarios of each use case, detailing the role of aerOS to solve specific issues and outlines the legal, social and economic framework of the trial. Meanwhile, Chapter 3 thoroughly lists the data sources, IT equipment (software and hardware) and all necessary infrastructure considerations. Chapter 4 contains the planning of the pilots, in terms of procurement, development, integration and deployment activities. Chapter 5 will include the demonstration evidences, and, finally, Chapter 6 will gather all the evaluation and assessment results out of it.

The application of this methodology in the first 9 months of aerOS has provided already very valuable insights out of all 5 pilots that is feeding the different technical and architectural developments.

The first use case (**pilot P1**) represents the Industry 4.0 (I4.0) vertical through the intention to deploy and validate MAL4 cognitive production processes in 4 public-private Pilot Lines (PL). This use case is divided in **three different scenarios**, which share among them the final goal of creating a highly flexible, sustainable (green) modular digital production lines and manufacturing of a new product in a low-volume production via the implementation of smart rapid response features in connection with self-optimization, reconfigurations ramp-up, adaptation of production line and operations, while the corresponding lines are located in: (1) INNO Didactic Factory at AIC - Automotive Intelligence Center (Bilbao, Spain), (2) MADE Competence Centre & POLIMI Industry 4.0 Lab facilities (Milano, Italy); (3) SSF open factory lab at SIPBB (Biel, Switzerland), and (4) SIEMENS INNOVATION CAMPUS in factory automation headquarter (Nuremberg, Germany). These sites provide access to state-of-the-art I4.0 production systems spanning 5000m2 and bring together over 500 companies.

aerOS is expected to provide a decentralized architecture across the continuum to effectively mitigate expenses, diminish energy consumption, minimize idle time of components, and alleviate bottlenecks. These three scenarios are: (1) Green manufacturing (zero net-energy) and CO2 footprint monitoring, (2) Automotive Smart Factory Zero Defect Manufacturing, and (3) AGV swarm zero break-down logistics & zero ramp-up safe PLC reconfiguration for lot-size-1 production.

Four main outcomes are expected at the end of the pilot: (1) Smart management services for zero-touch ZDM, (2) Metrology solution which leverages underlying meta Operating System (aerOS), (3) Assembly systems in the line with new software installed (aerOS), and (4) Digital Twin fed by aerOS features.

The **second use case (P2)** will be driven by partners CloudFerro (CF) and Electrum supported by SRIPAS as technical partner targeting applicability of aerOS for carbon aware computing. It will determine impact project's results can have on the carbon emissions generated by the European cloud industry and will also verify aerOS ability to set up and manage dynamic federation of heterogeneous infrastructure resources. The pilot will proof applicability of aerOS for set up and management of cloud-edge architectures distributed between "big" central clouds and small edge nodes located directly at energy producing locations, gathering information and events from the deployed smart devices.

The pilot is composed of two scenarios. The first focuses on deploying two federated edge nodes and a private cloud located directly at renewable energy premises, and connected to different smart devices and data sources from wind and PhV farms. The goal is for the computation to be performed in energy, network and self-conscious manner, measuring the reductions provided. The second scenario extends the federation beyond infrastructure owned by a single actor. Simultaneously, it will on-board multiple, independent tenants and execute unmoderated (thus, not trusted) workload provided by these tenants. It means that the main challenges of this scenario are in security and data and information management domains. Data to be used will range from Earth Observation data (Copernicus and Sentinel) to energy consumption of computing machines, relying on an (already in place) Kubernetes-based OpenStack infrastructure.

Three main outcomes are expected at the end of the pilot: (1) Reduction in energy consumption due to the transfer of AI and real-time analytics to the edge nodes, (2) Flexibility and scalability of the aerOS concept portability in the IoT edge-cloud continuum and (3) Definition and implementation of energy and network conscious management tools and procedures.

The **third use case (P3)** will be driven by partners **John Deere** and **TTControl** targeting to develop a High-Performance Computing Platform (HPCP) for Connected and Cooperative Mobile Machinery which has the potential to reduce the CO2 footprint in areas like agriculture, construction, or forestry. The HPCP use case will be deployed and validated in John Deere's European Technology Innovation Center in Kaiserslautern. The target of the HPCP use case is to develop a proof-of-concept of a High-Performance Computing Platform providing a machine-to-machine connectivity from everywhere for a large-scale agricultural production system on one side, but also delivering certain real-time performance still navigating the overall system remotely and controlling (i.e., supervising) execution of the agricultural work process.

The pilot is composed of two scenarios. The first of those (Cooperative large-scale producing) aims at leveraging the traits of the meta Operating System (aerOS) to optimize a large-scale production harvesting process system based on mobile machines, to be demonstrated with a mobile machinery unit to extend to a future swarm of vehicles. The second scenario digs deeper into the monitoring of machinery via edge and cloud calculations to achieve a for CO2 neutral intelligent operation (e.g., farming, construction, forestry). The benefit is also related with the energy consumption when transferring AI and real-time embedded analytics, what may reduce the CO2 impact.

Three main outcomes are expected at the end of the pilot: (1) Fully automated safe and secure execution at the edge node of the vehicles swarm, (2) IoT edge-cloud continuum. And (3) -IoT edge-cloud continuum.

The **use case number 4** is oriented to provide a metaOS to transform maritime port container terminal operations, improving scalability through decentralization. The Industrial partner, EUROGATE, manages the container terminal located in the Port of Limassol (EGCTL). At technical level, EGCTL will be supported by partner Prodevelop (PRO) and the Cyprus University of Technology (CUT). The pilot pursues the achievement of four objectives: (i) to improve the traceability of port assets, (ii) to allow the use in the terminal of heterogeneous Infrastructure Elements (IE), ranging from small IoT devices to big servers, (iii) to offer a predictive maintenance service integrated into the system and based on Frugal AI and (iv) to provide a computer vision solution that can be inferred from the edge without requiring very high bandwidths.

The use case is **divided into two scenarios**, being the first focused on predictive maintenance of container handling equipment (via the execution of ML algorithms through edge technology to improve the speed and performance of predictive analytics, reducing latency times compared to centralised cloud servers, leveraging data collected from sensors and PLCs in the machines) and the second one concentrating on risk prevention via computer vision in the edge. (having AI allow to optimize the allocation of resources through automated visual inspection and quality control). aerOS will enable the development, integration and validation of different CV Frugal AI algorithms at the edge. Customizable IPTV cameras will be used to enable (using edge processing to perform local ML training and inference) the automatic identification of damaged containers and verification of the existence of seals on the containers without the need for human intervention. Cloud resources will be used for more intensive ML training and testing, and the data will be transmitted through the aerOS communication infrastructure.

Eight main outcomes are expected at the end of the pilot: (1) Integration of live data from the container terminal, (2) Integration of assets for predictive maintenance, (3) Data collection supporting AI, (4) Predictive maintenance, (5) Edge models, (6) Recording of containers, (7) Computer Vision and (8) CV services.

The **fifth use case (P5)** will be driven by partners COSMOTE (COSM), NCSRD, FOGUS, INF and UPV, aims to demonstrate gains of the aerOS architecture in an edge deployment for energy efficient, sustainable, flexible and health-safe smart buildings. The use case considers deployment and validation in an office enterprise building of COSMOTE (Athens, Greece). The main goal behind the use case is (i) to achieve swarm intelligence among the aerOS capable sensors shall allow them to cooperate in a decentralized manner and collectively manage each room’s condition, so that the office becomes self-organized in terms of health and efficiency, as well as to (ii) demonstrate energy efficiency of the large buildings using real-time processing and (frugal) AI and to (iii) use 5G and smart network components like NFV and NetApps to extend aerOS capabilities.

The pilot is divided into two scenarios. The first one focuses on the definition and implementation of latency controlled distributed smart networking components to deliver a dashboard monitoring and controlling the energy consumption of the building, allowing automation of office seats allocation. The second scenario relates to cybersecurity and data privacy in building automation, with the goal of enhancing the security approach in Smart Buildings based on aerOS novel propositions.

Four main outcomes are expected at the end of the pilot: (1) Interoperabilty in a Smart Building, (2) Interoperabilty in a Smart Building, (3) Decentralised intelligence and (4) Orchestration.

With regards to the **requirements elicitation**, a two-headed approach has been taken, resulting in a thorough procedure for establishing technical, user and system requirements in aerOS. This procedure is drilled down in (a) Technical Requirements and (b) Requirements coming from pilots (user and system requirements). The first track (technical requirements) has been conducted using a specific template covering the domain, category and type of requisite, specifying the technological area of the project that those refer to.

In the first 9 months of the project, a number of 67 technical requirements were recorded, corresponding 23% to data management, 18% to infrastructure virtualization and handling, 15% to security and/or privacy, 12% to characteristics of a meta Operating System, 8% to network features, 8% to AI, 7% to code development, 6% to high-level applications and 3% to global services.

Coming from pilots, a total of 54 user and system requirements (combined) have been identified. Out of those, 28 were considered functional requirements and 26 non-functional requirements. In addition, the distribution per pilot was as follows: 8 requirements of P1, 5 requirements of P2, 5 requirements of P3, 20 requirements of P3 and 16 requirements of P5.

Measurement of aerOS performance and progress will be actually done via the usage of Key Performance Indicators (KPIs). However, the evaluation duty of the project is assigned to WP8, and more specifically to “T5.2 - KPIs definition and setup of evaluation framework”, along with “T5.3 - Continuous use cases analysis, evaluation and assessment”, which will start their execution in month M12. Therefore, this deliverable serves as the first step for the identification of KPIs. This section is divided into (a) Overall KPIs of the project, where is outlined a general introduction to the KPIs definition in the project, and (b) KPIs from pilots, where is provided a table with 38 KPIs associated to them identified by M9.

.

Table of contents

List of tables

List of figures

List of acronyms

Acronym	Explanation
AGV	Automated Guided Vehicle
AI/ML	Artificial Intelligence / Machine Learning
APC	Alternative Power Creator
API	Application Programming Interface
AU	aerOS Application User
CPS	Cyberphysical System
CEI	CloudEdgeIoT
CHE	Container Handling Equipment
CMM	Coordinate-Measuring Machines
CMMS	Computerized Maintenance Management System
COTS	Commercial-Off-The-Shelf
CV	Computer Vision
DFA	Digital Factory Alliance
DI FA	Digital Industry Factory Automation
DoA	Description of Action
DPP	Digital Product Passport
EC	European Commission
ECU	Electronic Control Unit
ERP	Enterprise Resource Planning
ETIC	European Technology Innovation Center
EU	European Union
FaaS	Function as a Service
GUI	Graphic User Interface
HPCP	High Performance Computing Platform
HVAC	Heating, Ventilation and Air Conditioning
IAM	Identity and Access Management
ICT	Information and Communications Technologies
IE	Infrastructure Element
IoT	Internet of Things
IP	IoT Infrastructure Provider
IPTV	Internet Protocol Television
ISO	International Standards Organisation
KPI	Key Performance Indicator

KVI	Key Validation Indicator
LCM	Lifecycle Management
M2M	Machine-to-Machine
MES	Manufacturing Execution System
NDI	Non-Destructive Inspection
NEF	Network Exposure Functions
NP	Network Provider
OPC-UA	OPC Unified Architecture
PCS	Port Community System
PdM	Predictive Maintenance
PhV	Photovoltaic
PIR	Passive Infrared Sensor
PLC	Programmable Logic Controller
PMI	Project Management Institute
R+D+i	Research and Development and Innovation
RFID	Radiofrequency Identification
RTG	Rubber-Tired Gantry
RUL	Remaining Useful Lifetime
SDK	Software Development Kit
SLA	Service Level Agreement
SP	Service Provider
TEU	Twenty-foot Equivalent Unit
TH	Trial Handbook
TOS	Terminal Operating System
VNF	Virtualized Network Function
ZDM	Zero-Defect Manufacturing

1. About this document

The main objective of this document is to provide the initial version of requirements elicitation, use cases and scenarios definition and legal and regulatory analysis. More specifically, the document offers a formal definition of use cases associated with the five vertical domains will encompass: (i) identification of actors involved and their participation; (ii) specification of requirements and assumptions to be fulfilled; (iii) description of event flow and actor interactions, highlighting differences from current operations; and (iv) determination of expected outcomes after use case execution. The document highlights how the continuous results obtained from the KPI definition and setup evaluation framework from aerOS and integration of third parties through the Open Call will enable the monitoring and redefinition of use cases. The deliverable aims to disclose both functional and non-functional requirements, ensuring their clarity, completeness, and consistency. Through analysis of technical and business requirements, initial assessment will be conducted using relevant Key Performance Indicators (KPIs). This analysis will help identify existing gaps (technical, functional, and organizational) that need to be addressed to fulfil the operational concept, approach, and goals. The requirements provided in this document will be reviewed throughout the project to validate, evolve, and prioritize them. This process will follow agile methodologies such as Volere and MosCoW to ensure overall coherence across all technical stages.

1.1. Deliverable context

Table 1. Deliverable context

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Objectives</td><td>This deliverable is directly related with all objectives of aerOS. The deliverable will elicit functional and non-functional requirements verifying whether they are clear, complete, and consistent (related to O1-O5). They will be focused on the use cases and scenarios addressed in the project (related to O6). In addition, the deliverable provides the basis to the integration of the Open Call third parties to allow a follow-up and redefinition of use cases (related to O7).</td></tr>
<tr><td>Work plan</td><td>Deliverable D2.2 is the second technical deliverable of the project. It is the second deliverable of WP2. It will be delivered at the same time as the D2.4 DevPrivSecOps methodology specification. It will be followed by the document related with the architecture of the project. More specifically, D2.2 identified requirements will drive architecture building (D2.6) and identifying necessary components and interactions among them, with particular attention paid to the defined use cases. The identification of requirements and use cases will serve as the driving force behind constructing the different tasks of WP2, WP3, WP4 and WP5.</td></tr>
<tr><td>Milestones</td><td>The submission of deliverable D2.2 is directly related to the completion of milestone MS2: First iteration of use cases and requirements. With D2.2, MS2 is fully achieved, as D2.2 was already submitted by M9.
<table>
<tr><th>Milestone No</th><th>Milestone Name</th><th>Work Package No</th><th>Lead Beneficiary</th><th>Means of Verification</th><th>Due Date (month)</th></tr>
<tr><td>2</td><td>Use cases and requirements defined</td><td>WP2</td><td>1-UPV</td><td>First iteration of use cases and requirements (D2.2a)</td><td>9</td></tr>
</table></td></tr>
<tr><td>Deliverables</td><td>D2.2 is not directly feed from any other previous deliverables. This document is part of an iteration of living deliverables. This is the first version (D2.2), which is due to M9. The second and final variant (D2.3) is planned for M18. They correspondingly provide the initial and final version of requirements elicitation, use cases and scenarios definition and legal and regulatory analysis. It is expected to serve as baselines for the forthcoming technical deliverables: D2.3, D2.6, D3.1, D4.1, D5.1, D5.3 and D5.5.</td></tr>
<tr><td>Risks</td><td>#5 Failure providing a reference architecture specification for the IoT edge-cloud</td></tr>
</table>

	continuum, getting low acceptance by the market and other projects. D2.2 establishes a first iteration to ensure that use cases and technical, system and user requirements are properly defined in an early stage of aerOS. The process of identifying requirements will play a pivotal role in shaping the architecture, as it involves establishing the necessary components and their interactions. Significant focus will be placed on the defined use cases to ensure their specific needs are met.

1.2. The rationale behind the structure

The content of the deliverable is organised in six main sections, aligned with the scope of the task T2.2:

- Section 1. This sections provides the overview, context and structure of the deliverable.
- Section 2. This section includes an introduction to aerOS project and its scope. It defines the terminology used throughout the document. It also provides an overview of the methodology used for describing use cases and capturing requirements.
- Section 3. This section illustrates an explanation of each of the five aerOS use cases, including its general description, current problems/barriers area, participant partners, data sources, existing software, and available hardware. The section also discusses the objectives, benefits, and expected results of the trial, as well as its specific measurable outcomes and KPIs. Additionally, the legal and social frameworks surrounding the trial are examined.
- Section 4. This section reports the elicitation of the requirements focusing in the technical requirements and the requirements coming from pilots (user and system requirements). This chapter provides an overall explanation of the results. In addition, the actual list of requirements can be found in Appendix A and Appendix B.
- Section 5. This section outlines a general introduction to the aerOS KPIs definition and the list of the KPIs designed to assess the success of the pilot deployments.
- Section 6. The document concludes with a conclusion and future work section.
- Appendix A. This appendix includes the table with the technical requirements.
- Appendix B. This appendix includes the table with the user and system requirements.

2. Introduction

This section provides a brief overview of aerOS project and the scope of work that will be covered during the project. The terminology used throughout the document is explained, and the methodology for use cases description and requirements capture is detailed.

2.1. Scope of aerOS

The HE-funded project aerOS aims at transparently utilising the computing resources on the edge-to-cloud continuum for enabling applications in an effective manner while incorporating multiple services. The overarching goal of aerOS is to design and build a virtualised, platform-agnostic meta operating system for the IoT edge-cloud continuum.

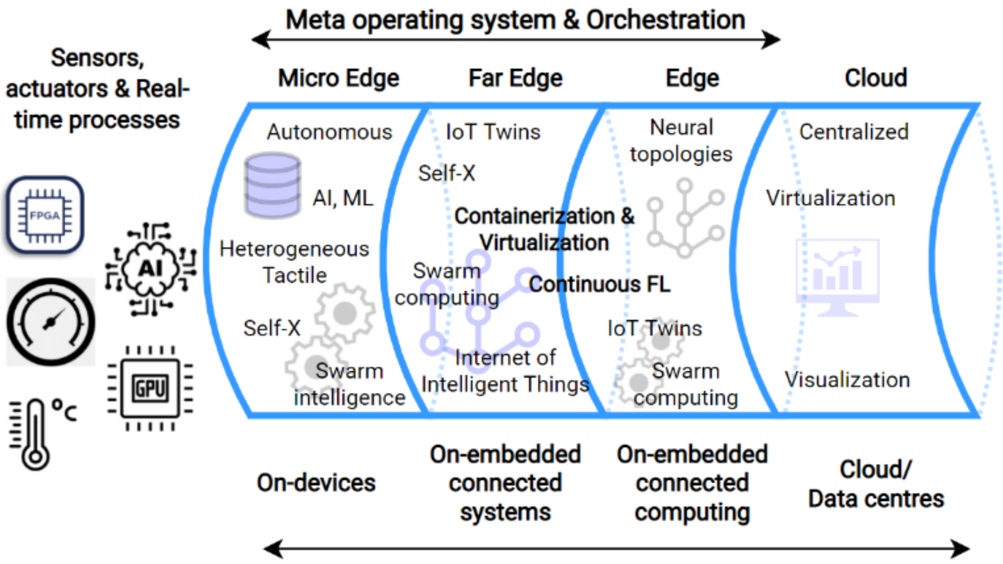


Figure 1. aerOS continuum

As a solution, to be executed on any Infrastructure Element within the IoT-edge-cloud continuum – hence, independent from underlying hardware and operating system(s) – aerOS will: (i) deliver common virtualised services to enable orchestration, virtual communication (network-related programmable functions), and efficient support for frugal, explainable AI and creation of distributed data-driven applications; (ii) expose an API to be available anywhere and anytime (location-time independent), flexible, resilient and platform-agnostic; and (iii) include a set of infrastructural services and features addressing cybersecurity, trustworthiness and manageability. aerOS will: (a) use context-awareness to distribute software task (application) execution requests; (b) support intelligence as close to the events as possible; (c) support execution of services using "abstract resources" (e.g., virtual machines, containers) connected through a smart network infrastructure; (d) allocate and orchestrate abstract resources, responsible for executing service chain(s) and (e) support for scalable data autonomy.

Moreover, aerOS will leverage European leadership in automation systems in industry (where edge resides) and pointedly prove how European industry can benefit from decentralised, platform-agnostic IoT edge-cloud continuum data-processing ecosystem, to build competitive advantages e.g., reduced time to decisions; cost and time efficient, secure, trustworthy data sharing and control; semi-autonomous action taking; agile operations; sustainable, human-centric data processing, governance, and interoperability; reduced external traffic; and improved latency. The aerOS approach will be generic and directly applicable to any vertical, cross-vertical business process, and several different physical or virtual platforms. It will answer the urgent need for a trustworthy, decentralised, autonomous, orchestrated solution, enabling bottom-up formation of compute continuum ecosystems, where hyper-distributed applications will be efficiently executed, within any selected "fragment" of heterogeneous physical infrastructure.

aerOS is part of the community of EUCloudEdgeIoT.eu initiative. EUCloudEdgeIoT aims to realise a pathway for the understanding and development of the Cloud, Edge and IoT (CEI) Continuum by promoting cooperation between a wide range of research projects, developers and suppliers, business users and potential adopters of this new technological paradigm.

The aerOS concept will be validated by means of realistic trials in five use cases (deployed in multiple sites). Evaluation will be done with regard to the technical assessment, stakeholders' acceptance and exploitation, in association with the DevPrivSecOps agile approach used in the project. In accordance to the previous, and to achieve its ambitious goals, aerOS will follow a clear methodology to define those use-cases and deliver the requirements that will guide the technical assessment and acceptance.

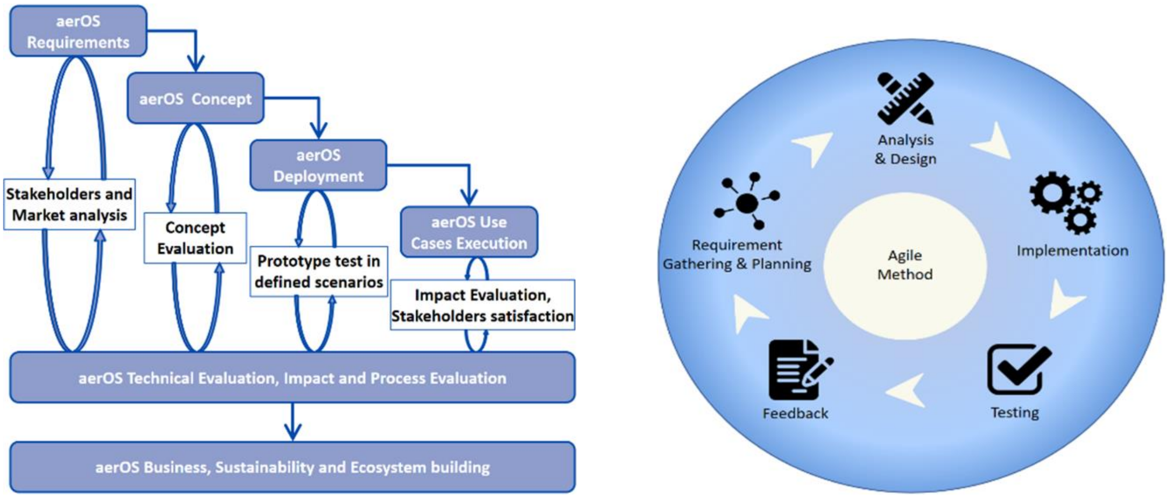


Figure 2. aerOS concept assessment and validation approach

This document aims at reporting the first version of those activities, detailing both the requirements and the use cases of the project.

2.2. Terminology of the document

Along this document (and the whole activity of aerOS), a series of terms are being used that require explanation. Those might be used in different contexts and may have different acceptations, therefore it was considered necessary to clarify their meaning from this point on.

The definitions in the table below do not come from formal, standardized manuals (e.g., from PMI), but rather from the natural explanation by aerOS partners that have decided to adopt this terminology.

Table 2. Terminology

Term	Definition
Use case	The global perspective of a usage of the developed technology in which aerOS' features are used to provide: (i) solution to a specific problem in a sector, (ii) validation of those developments, ensuring appropriateness and usefulness.
Use case site	The logical and physical space where a pilot takes place. Also mentioned as: *deployment site.*
Stakeholder	Those entities that are involved to some extent in a use case. In general terms, *stakeholder* refers to aerOS partner that act as owner of the pilot; bringing the challenge/issue to be solved by aerOS and putting the physical means (premises, equipment, machinery, etc.) for the trial to happen. The term can also be used to refer to a generic figure that could be targeted by aerOS (e.g., manufacturing sector stakeholders).
Expected benefit	From an operational/business angle, the benefits than can be extracted by the execution of a use case of aerOS. Understood as the positive throughput obtained by the entities involved

	in such a use case.
Pilot / Trial	The materialisation of a use case. The words *pilot* and *trial* are complementary in aerOS and can be used interchangeably. Their actual meaning refers to the execution actions leading to a realisation of a use case. Pragmatically, a pilot/trial consists of a small-scale demonstration of a use case in a use case site that is used to prove the viability of a project idea. aerOS pilots represent: (i) Industry 4.0, (ii) utilities (renewable energy), (iii) smart agriculture, (iv) port transportation and logistics, and (v) smart buildings. From a broader perspective, a trial/pilot tests the implementation approach of a product (aerOS meta operating system) and the risks associated with potential rollout or wider pilots.
Scenario	A sub-partition of a use case. Considering a vertical domain (e.g., smart buildings), there may be several areas, issues or challenges within it that can be tackled through aerOS' traits. Each of those areas would conform to a single scenario, that would require a specific strategic and technological approach (although always framed within a global purpose). Every aerOS' use case includes different scenarios, in which different technological pillars will be executed and validated. Also mentioned as: *use case scenario.*
Actor	Person or profile of person that will intervene in the pilot, either actively participating on it (e.g., truck driver in a maritime port pilot) or directly benefitting from the achievement of the goals of the use case (e.g., Operations Director or Office Manager).
Trial Handbook	The Trial Handbook is a complete document defining in full detail the whole process carried out throughout each trial/pilot and the outcomes and results of the developed activities. Each Trial Handbook is an internal a confidential document, owned by the Trial Owner, and it's the only trustfully source of information for that trial. The Trial Handbook methodology will be used in the requirement and use cases definition process. In aerOS, the Trial Handbook is used as the main source of truth of the description of every pilot, including activities performed, objectives, planning, etc.
Objective	An objective defines the targeted change that is pursued when initiating an action (in the case of aerOS and this document, when initiating a use case). It represents what is to be achieved that was not available before and that involves impactful modifications in the adopting organization. Also mentioned as: *goal.*
Requirement	"A requirement is Statement that identifies a product (includes product, service, or enterprise) or process operational, functional, or design characteristic or constraint, which is unambiguous, testable or measurable, and necessary for product or process acceptability." (ISO/IEC 2007) As an alternative, the following definition has also been considered valid: "A requirement is a statement that identifies a system, product or process characteristic or constraint, which is unambiguous, clear, unique, consistent, stand-alone (not grouped), and verifiable, and is deemed necessary for stakeholder acceptability." (INCOSE 2010)
Outcome	In aerOS' use cases, an outcome represents a tangible asset or a gained knowledge that objectively has been acquired/obtained after the execution of the pilot. Also mentioned as: *result.*
KPI	Key Performance Indicators (KPI) is a set of quantifiable measures that either a stakeholder or a technician of an aerOS use case employs to gauge and compare performance in terms of meeting their particular strategic and operational goals. KPIs were initially defined in the proposal stage and are being refined and enhanced during this stage of the project. The main difference between KPIs and objectives is that the former are much more concrete, are measurable and that have the intention to compare final status versus initial status of a specific performance measurement.

2.3. Methodology of use cases description and requirements capture

aerOS has planned a specific task to deal with the description and formalization of the use cases and requirements in aerOS. As formally declared, such task – T2.2- aims to "*[…] formally define use cases associated with the five vertical domains, including: (i) Actors that interact and participate in each use case; (ii) Requirements and assumptions to be satisfied for the use case; (iii) Flow of events between actors, and sequences of interactions focusing on differences from current operations, and (iv) Expected outcomes after the use case execution. Continuous results gathered in T5.3 and integration of the Open Call third parties will allow a follow-up and redefinition of use cases. The task will elicit functional and non-functional requirements, verifying whether they are clear, complete, and consistent. Technical and business requirements analysis will allow to initially assess by means of related KPIs, and refine action coverage, identifying existing gaps (technical, functional and organisational) to fulfil the operational concept, approach and goals. Requirements will also be revisited within the project, in order to validate, evolve and prioritise them, following agile methodological approaches (i.e., Volere and MosCoW) to ensure general coherence for all the technical stag*es."

Drawing from these objectives, a concrete plan has been designed to streamline such actions and to deliver the advances that are depicted in this document.

To start with, the task is clearly divided in two main activities[1]:.

- On the one hand, the definition of use cases is a crucial activity in aerOS that will have a major influence during the project. The validity of the solution will be observed via the implementation of five pilots, thus a correct definition, planning and structuration of those becomes crucial. In addition to the previous sentences, it was agreed early that use cases description should include, at least:
    - Context explanation (with pictures)
    - Issues/problems to solve explanation and current solutions tackling similar scenarios
    - Actors intervening and diagrams (sequence, interaction)
    - Goals and expected outcomes (including mockup visualisations)
    - Associated requirements
    - Initial/final status (A/B analysis)
    - Data available (including examples, format, expected size...)
    - Data to be acquired
    - Computing –and other- equipment (existing and to be acquired)
    - Other systems to interact with (e.g., SCADA, PCS)
    - KPIs
    - Tentative timeline
    - Risks
- On the other hand, the elicitation of requirements to govern the technical developments and the use cases alike. A proper, clear and concise description of requirements will ensure a proper execution of the research across work packages in aerOS. Among these, the following aspects were decided:
    - Requirements are catalogued as *functional* or *non-functional*.
    - A prioritization mechanism based on Volere should be followed.

In addition, based on the experience of aerOS partners in similar activities in the past, an overall methodology was designed in order how to merge both actions together and how to structure the teams to advance in the definition of use cases and requirements:

[1] Note that technical KPIs are not included in the lists below. As per the design of the work plan, those are not under the scope of T2.2 but on WP5 (T5.3). Therefore, in order to keep consistency with the whole coverage of use cases, the only KPIs that were included in this methodology (and, thus, reported in this document) are those associated to use cases.

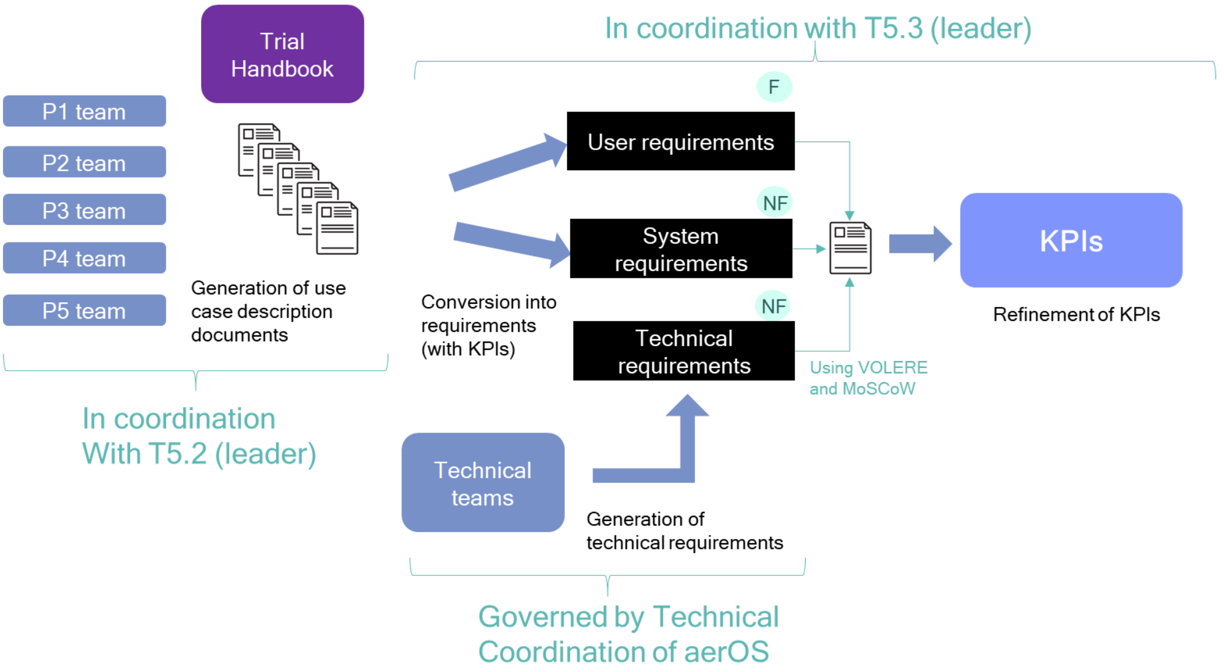


Figure 3. Methodology for use cases and requirements definition in aerOS

The methodology started by the creation of specific teams devoted to deliver content that is then glued together as indicated in the previous figure.

- The description of use-cases has decided to be done **using the Trial Handbook methodology**[23]**.** The TH is divided in various chapters that gather relevant information about a trial. TH Chapters are living documents that will be regularly updated by the partners involved in the corresponding use cases. For doing so, different teams have been established, one per each pilot in aerOS (P1, P2, P3, P4 and P5). These teams work together with the **joint goal of generating the use case description documents** (Chapters of the TH methodology).
- The technical partners in aerOS (UPV, NCSRD, PRO, DST, SIEMENS, SRIPAS, S21SEC, IQB, ICT-FI, LMI-ERICSSON, FOGUS, TTC, INNOVALIA) were called to form a team to identify the requirements associated to their corresponding tasks and roles, adjusted to the results that must be provided in aerOS. For this action, the Technical Coordinator of the project is selected to oversee the procedure and descriptions, ensuring alignment with the goals of the action and the reality of the advances across the work plan.
- In parallel, a sub-team has been created to merge both actions together (to some extent). This team, led by the coordinator of KPIs in the project (T5.3 leader – PRO) is in charge of gathering the requirements expressed by the stakeholders in the Trial Handbook Chapters, curate and list them and classify them into User requirements and System requirements. Those, together with the technical requirements result in the global list of requirements of aerOS. At the same time, KPI analysis from stakeholders is also controlled by this task force.

The next sub-sections are devoted to detail the methodology and considerations that are being put in place in aerOS towards a successful description of use cases and elicitation of requirements.

[2] This is a methodology coined and invented by the Digital Factory Alliance (DFA) – of which the coordinator of pilot in aerOS (INNOVALIA) is founding member. chrome-
[3] extension://efaidnbmnnnibpcajpcglclefindmkaj/https://digitalfactoryalliance.eu/wp-content/uploads/2021/12/Digital-Factory-eBook-reviewed_v1.5_graficas.pdf

2.3.1. Use cases description

As mentioned, in order to fulfil the description of use cases in aerOS, the methodology of Trial Handbook has been selected to be used. According to this methodology, the creation of a TH is "**a complete document defining in full detail the whole process carried out throughout each trial and the outcomes and results of the developed activities**". The establishment can be beneficial for the following reasons (illustrated in):

- Creating a sole source of truth simplifies communication and links to update.
- By being able to select confidentiality rules per chapter (or section) eases the online cooperation without fear of information disclosure.
- Improves coordination, enabling quick and reliable access to the most updated documentation.
- Prevents duplication of efforts and shows progress in real time.
- Inconsistencies are avoided, as all the information is on a single point (here, proper backup techniques must be put in place to avoid single point of failure).
- Ensure to meet the deadlines.
- For documenting deliverables, instead of repeating over the information in several places, the content is directly extracted by document leaders from the TH and transferred into each proper document.

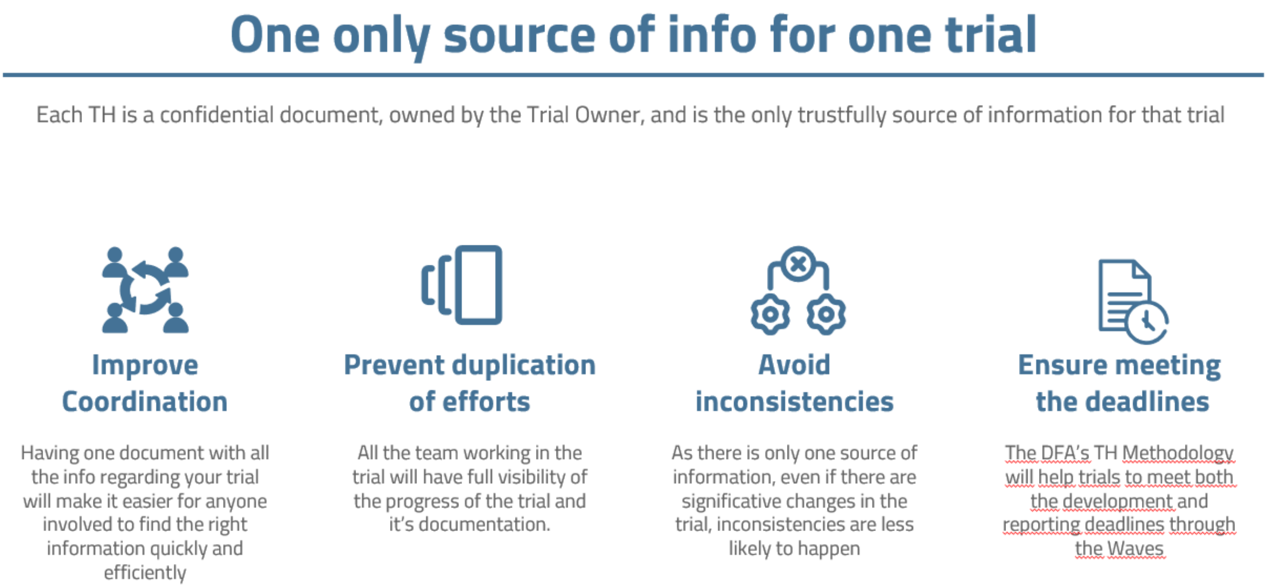


Figure 4. Methodology for use cases and requirements definition in aerOS

Therefore, in aerOS it has been decided to employ the TH not only as a useful tool to meet the goals of task T2.2 (use case description and requirements elicitation). The idea is to use the Chapters as a source and sink of information for/from all WPs where use cases are touched upon.

This way, everything related to use cases will be dealt with using the TH of each pilot, that will be always the main source of truth and represent a live document to be continuously updated. Thus, this methodology will be cross-WP.

Later in this section, a handy file mapping the sections of the chapters to the different WPs, tasks and deliverables of the project is illustrated.

<u>Steps of the methodology:</u>

As per its definition by DFA, the Trial Handbook methodology defines several steps towards the completion of the document. The steps are as follows:

- 00: Definition of the chapters of the TH
- 01: Definition of the teams

- 02: Map deliverables to TH Chapters
- 03: Adapt the inner sections of TH chapters to the project (aerOS)
- 04: Set the general timeline of waves
- 05: Continuous fulfilment and update of the Chapters

In the next pages, the methodological decisions taken in each step in aerOS are documented:

00- <u>Definition of the chapters of TH:</u>

Originally, there are 5 chapters defined to conform the TH. However, those chapters are interchangeable and extendable. In, aerOS, it was decided to create a structure with 6 different chapters responding to the following structure:

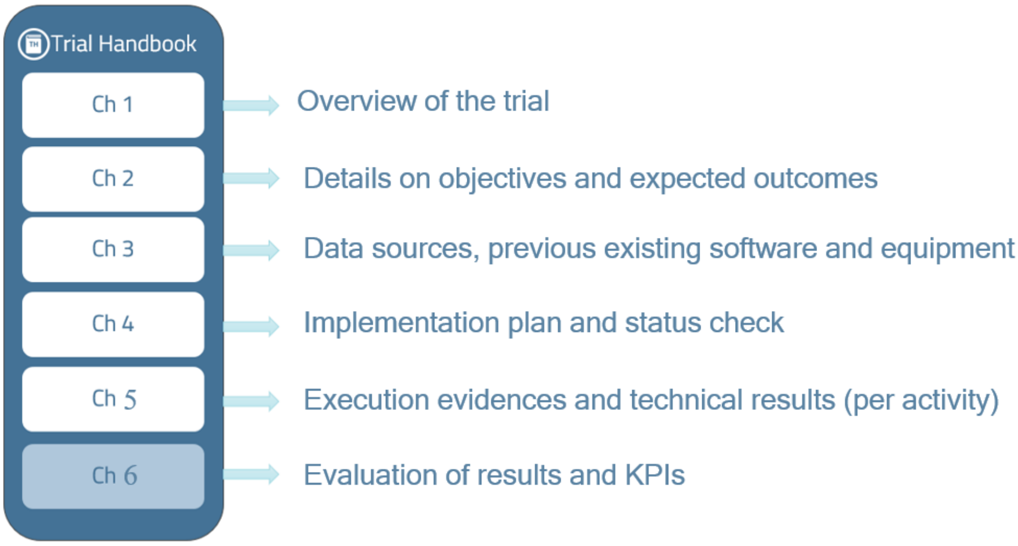


Figure 5. TH Chapters definition in aerOS

01. <u>Definition of the teams</u>

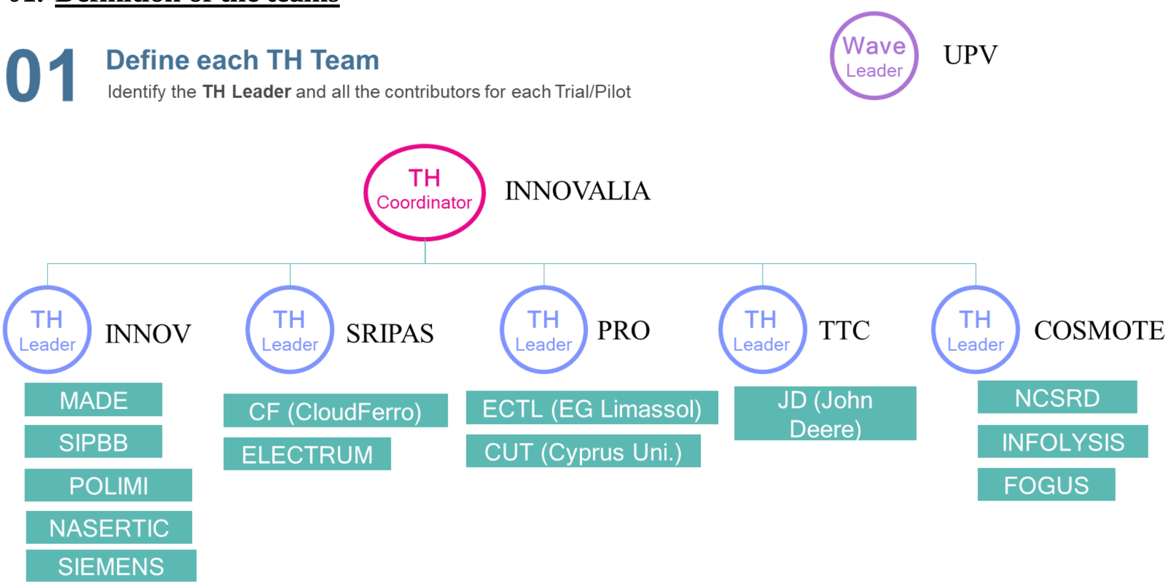


Figure 6. TH Chapters definition in aerOS

02. Map the deliverables into the TH

First, a global mapping was made. The figure below does not go deep into the section-to-deliverable mapping, but rather expresses the relevance of each chapter to every deliverable in aerOS directly related to use cases. This was devised at the beginning of the TH methodology application in aerOS.

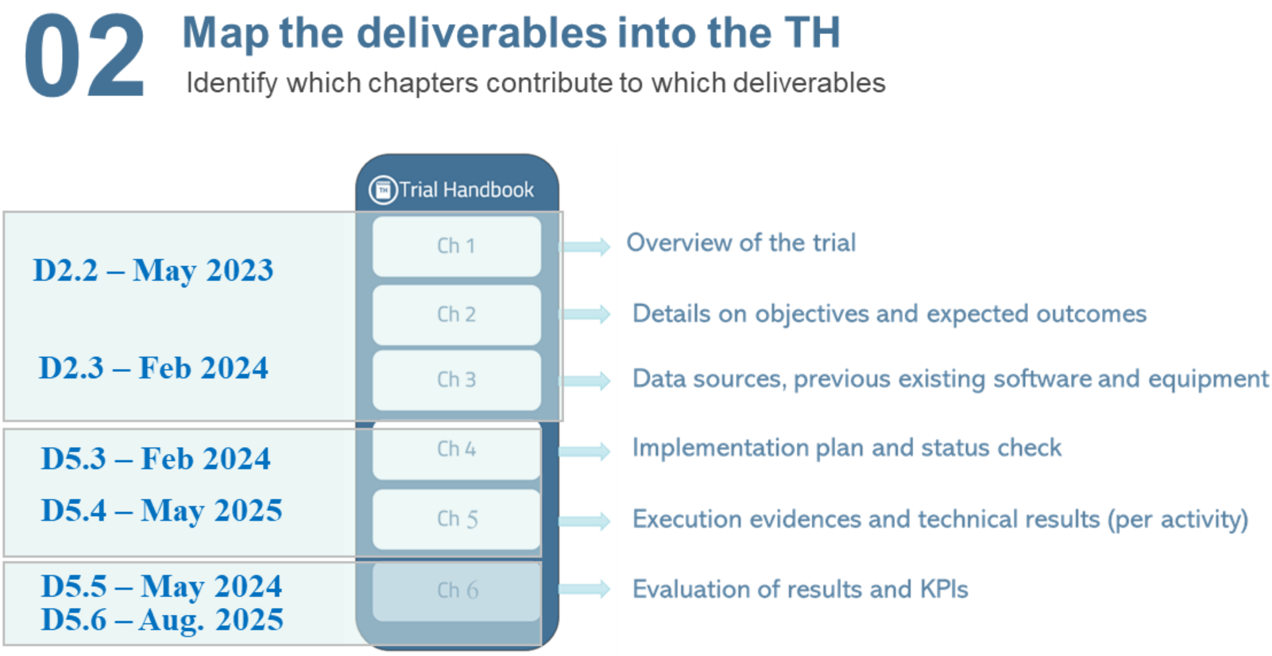
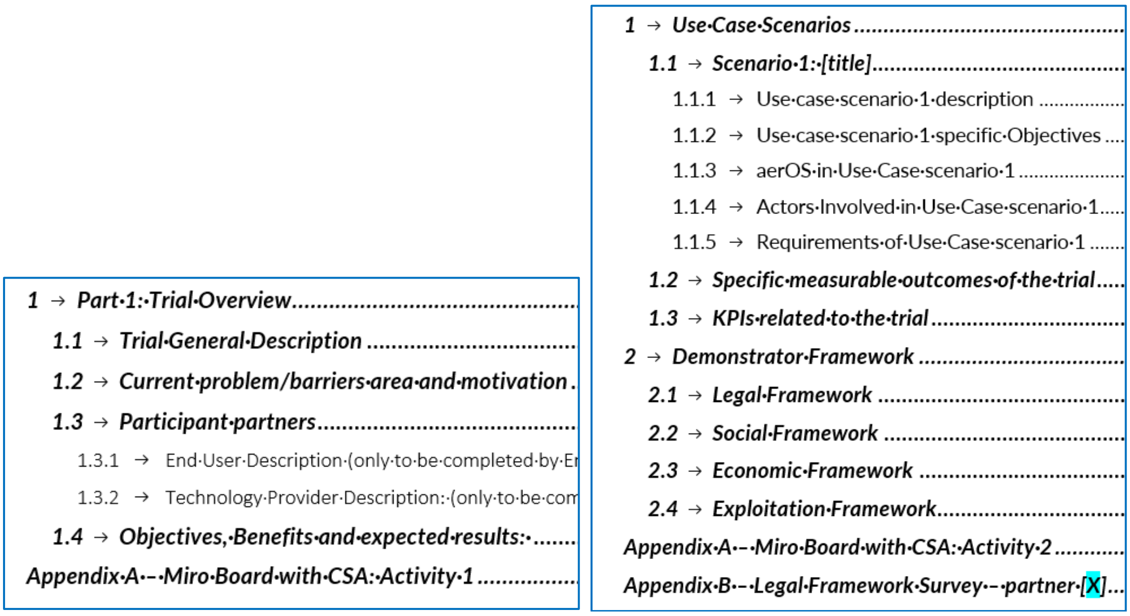


Figure 7. TH Chapters to deliverables mapping in aerOS

03- Adapt the inner sections of the TH Chapters to the project (aerOS).

Here, the final documents that materialise each chapter were defined. Those consist of text documents with a established table of contents to respond to the needs of aerOS respecting the decision taken in 00. The following images represent those ToCs:



1 → Part·1:·Trial·Overview
1.1 → Trial·General·Description
1.2 → Current·problem/barriers·area·and·motivation
1.3 → Participant·partners
1.3.1 → End·User·Description·(only·to·be·completed·by·E
1.3.2 → Technology·Provider·Description:·(only·to·be·com
1.4 → Objectives,·Benefits·and·expected·results:·
Appendix·A·-·Miro·Board·with·CSA:·Activity·1

1 → Use·Case·Scenarios
1.1 → Scenario·1:·[title]
1.1.1 → Use·case·scenario·1·description
1.1.2 → Use·case·scenario·1·specific·Objectives
1.1.3 → aerOS·in·Use·Case·scenario·1
1.1.4 → Actors·Involved·in·Use·Case·scenario·1
1.1.5 → Requirements·of·Use·Case·scenario·1
1.2 → Specific·measurable·outcomes·of·the·trial
1.3 → KPIs·related·to·the·trial
2 → Demonstrator·Framework
2.1 → Legal·Framework
2.2 → Social·Framework
2.3 → Economic·Framework
2.4 → Exploitation·Framework
Appendix·A·-·Miro·Board·with·CSA:·Activity·2
Appendix·B·-·Legal·Framework·Survey·-·partner·[X]

Figure 8. TH Chapters ToC in aeros (CH1 and CH2)

Figure 9. TH Chapters ToC in aeros (CH3 and CH4)

Figure 10. TH Chapters ToC in aeros (CH5 and CH6)

In addition, in the methodology defined in aerOS, one step beyond was performed: deliver an advanced mapping between TH and the deliverables of aerOS.

In essence, the goal was to achieve a correlation between the sub-sections between the inner sections of the chapters (see table of contents above) to the deliverables committed to be delivered in the project. This is facilitating the proper completion in time of the sections to ensure fulfilling the duties and keeping a pace in the advancement on the chapters.

This is also helping to conduct periodic updates to the material included in the TH and, at the same time, keeps a synchronization between the stakeholders of the use cases with the technical partners of the project (that lead, concoct and edit those deliverables).

In that regard, the established procedure is that, whenever deliverables submission dates are approaching, a team is defined to check with the stakeholders the current content, identifying which part (and how much) of it needs to be transferred into the deliverable. Afterwards, this transfer of information is performed. This advanced mapping tool is illustrated in Figure 11.

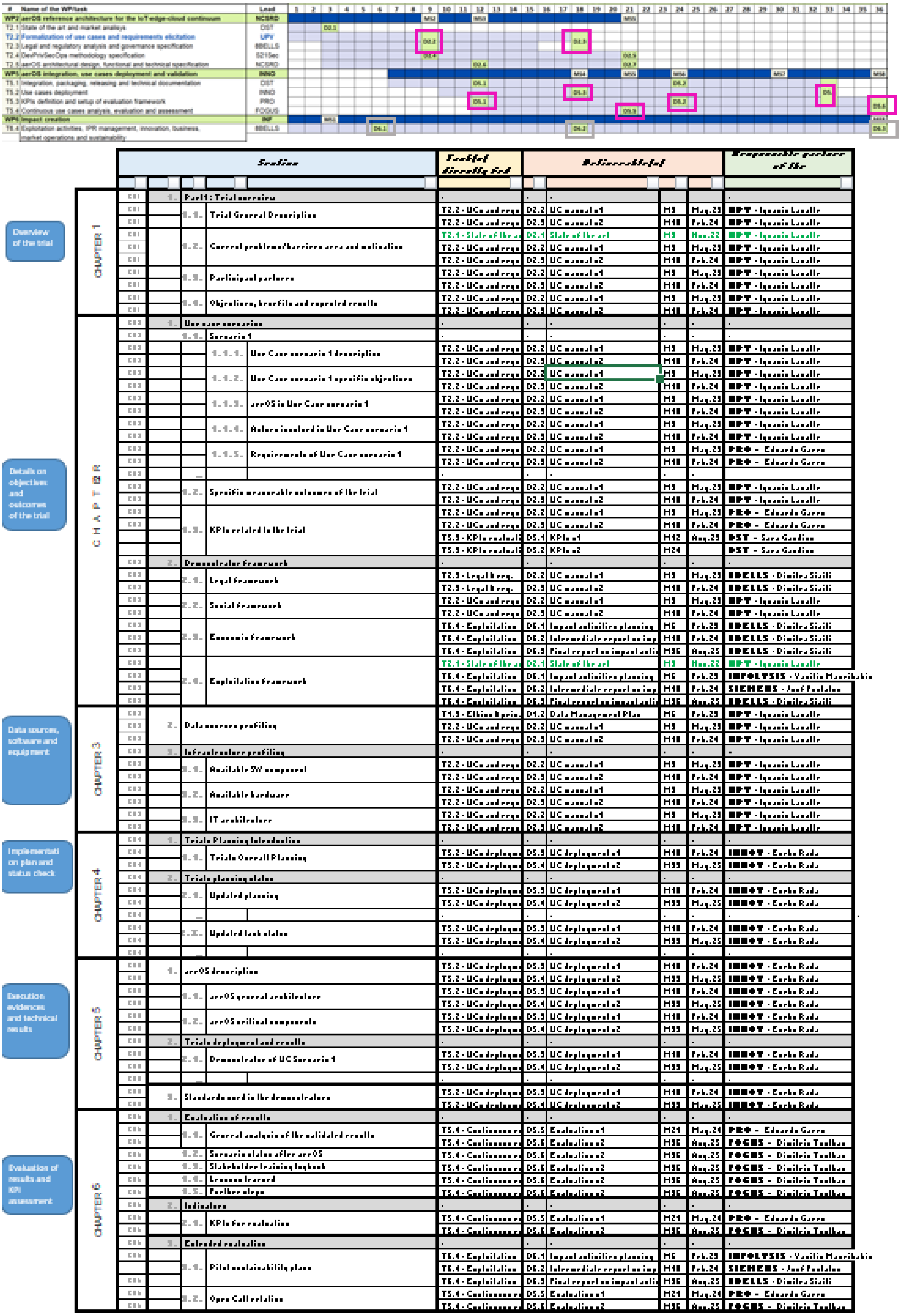


Figure 11. Advanced mapping between Chapter sections and aerOS deliverables

04. <u>Set the general timeline of waves</u>

Based on the strategy defined above, the establishment of the 4th step of the methodology came straightforward. The concept of waves relate to "those sub-periods that are selected ending in a completion of a set of chapters".

In aerOS, the meaning of a wave has been adopted as follows: "*a wave is a sprint action that finalises in a moment of time when the update of the Chapters is frozen and the content in the TH Chapters is transferred into the corresponding deliverables that are due to that date*".

The table in Figure 11 establishes such a pace, that is depicted as a timeline in the Gantt represented by the next figure:

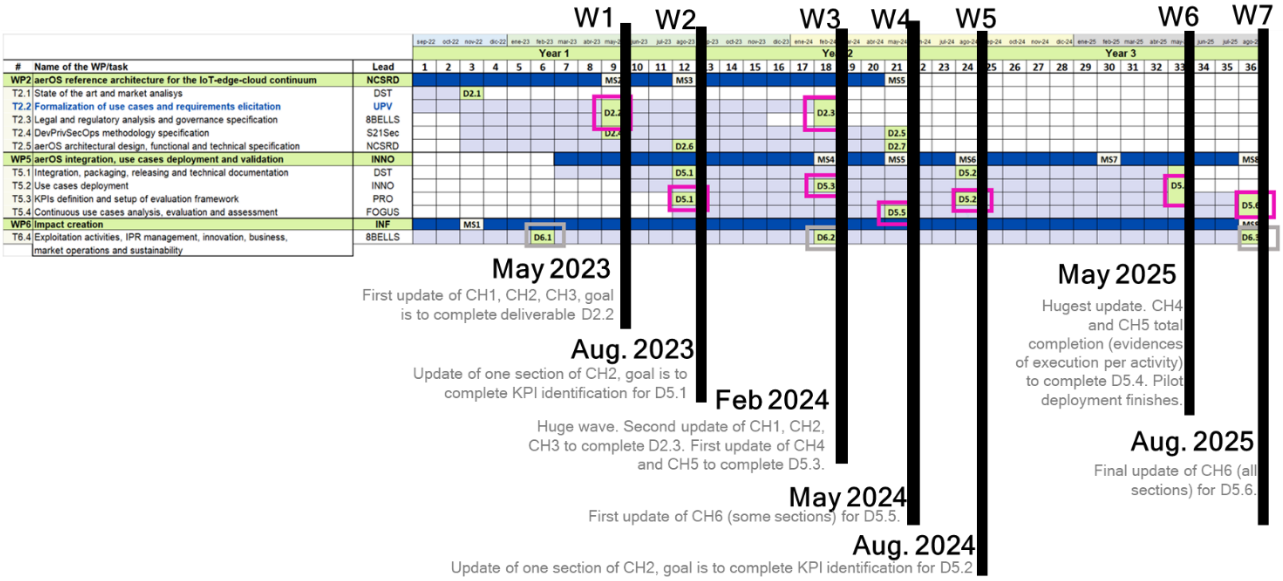


Figure 12. Timeline of waves in aerOS' TH methodology

2.3.2. Requirements elicitation

For any project it is necessary to establish from the beginning what should be achieved, i.e., set the scope of the project. To that aim, a thorough analysis to understand the use case scenarios that will be addressed in the project (described in previous chapters) has been performed. Based on that, features and functionalities of corresponding use case scenarios are now identified and formalised as requirements. It is worth noting that this effort will be strengthened during the following months, and that **a new, ultimate version of the requirements must be expected by M18 (February 2024), materialised in the deliverable D2.3**.

While various definitions exist of what is a requirement, in this study, aerOS partners agreed to use the ISO definition: "*A requirement is Statement that identifies a product (includes product, service, or enterprise) or process operational, functional, or design characteristic or constraint, which is unambiguous, testable or measurable, and necessary for product or process acceptability.*" [4].

Once the definition was clarified, the ***<u>following guiding principles</u>*** were also agreed by partners of the project:

- Requirements in aerOS can be of three main **<u>types:</u>**

4 ISO/IEC. 2007. Systems and Software Engineering -- Recommended Practice for Architectural Description of Software-Intensive Systems. Geneva, Switzerland: International Organization for Standards (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 42010:2007

- *Technical requirements*: identify how the eventual product must fit into the world (i.e., the product might have to interface with or use some existing hardware, software, or business practice).
- *User requirements:* describe what the user needs and wants from the system, in terms of functionality, expected response, actuation capacity, visualization, etc. while system requirements
- *System requirements*: describe the specifications and constraints that the system must have in order to fulfil the user requirements. In aerOS, system requirements are directly coming from what is expressed by stakeholders in terms of what a meta-OS must bring to them.

- Independently of the type of requirement (tech., user, service), those can be **classified in three categories**, being the first two the most prominent, and the third one less common:
  - *Functional requirements*: are the fundamental subject matter of the system and are measured by concrete means like data values, decision-making logic, and algorithms.
  - *Non-functional requirements:* are the behavioural properties that the specified functions must have, such as performance, usability, etc. Non-functional requirements can be assigned to a specific measurement.
  - *Constraints for design*: are those aspects that do not come imposed by the needs of the users or the meta-OS, but for the contextual circumstances. These are relevant as they must be considered when designing the technology.

- Requirements must follow the principles proposed by Volere methodology[5]:
  - *Necessary:* The requirement defines an essential capability, characteristic, constraint, and/or quality factor. If it is not included in the set of requirements, a deficiency in capability or characteristic will exist, which cannot be fulfilled by implementing other requirements.
  - *Appropriate:* The specific intent and amount of detail of the requirement is appropriate to the level of the entity to which it refers (level of abstraction). This includes avoiding unnecessary constraints on the architecture or design to help ensure implementation independence to the extent possible.
  - *Unambiguous*: The requirement is concisely stated. It expresses objective facts, not subjective opinions. It is subject to one and only one interpretation.
  - *Complete*: The requirement sufficiently describes the necessary capability, characteristic, constraint, or quality factor to meet the entity need without needing other information to understand the requirement.
  - *Singular:* The requirement should state a single capability, characteristic, constraint, or quality factor.
  - *Feasible:* The requirement can be realized within entity constraints (e.g., cost, schedule, technical, legal, or regulatory) with acceptable risk.
  - *Verifiable*: The requirement is structured and worded in such a way that it is possible to verify its accomplishment, as well as the degree of customer's satisfaction regarding its realization.
  - *Correct:* The requirement must be an accurate representation of the entity need from which it was transformed.
  - *Consistent:* The requirement does not contradict any other requirement and is fully consistent with all authoritative external documentation.
  - *Comprehensible*: The set of requirements must be written such that it is clear as to what is expected by the entity and its relation to the system of which it is a part.

5 Volere Requirements Specification Template:
https://www.st.cs.uni- saarland.de/edu/se/2009/slides/volere_specification_template_v6.pdf

- In addition, a common requirement definition criterion adopted in aerOS was the **prioritization**. Project partners decided to follow the requirements prioritization proposed by the MoSCoW[6] methodology, that details as follow:
    - *Must have*: requirements labelled as MUST have to be included as mandatory to be delivered in order for it to be a complete success. It is good to have clarity on this before a project begins, as this is the minimum scope for the product to be useful.
    - *Should have*: SHOULD have requirements are also critical to the success of the project, but are not necessary for delivery in the final form. SHOULD requirements may be as important as MUST, although SHOULD requirements are often not as time-critical or there may be another way to satisfy the requirement.
    - *Could have*: requirements labelled as COULD are desirable but not necessary, and could improve user experience or customer satisfaction for little development cost.
    - *Would like to have*: requirements labelled as WOULD have been agreed by stakeholders as the least-critical, lowest-payback items, or not appropriate. As a result, WOULD requirements may be either dropped or reconsidered for inclusion in later phases or projects.

- As the last agreement made in the requirement elicitation methodology, the division of the work was structured. In order to follow a pragmatical approach, it was determined to break down the requirement gathering process in two separate branches (see Figure 3). In each of those, a slightly different methodology (including timing and templates) was followed, even though considering always all the above bullet points as guiding principles. Next figure represents this breakdown, and the two following sub-sections describe the actions performed in each of them.

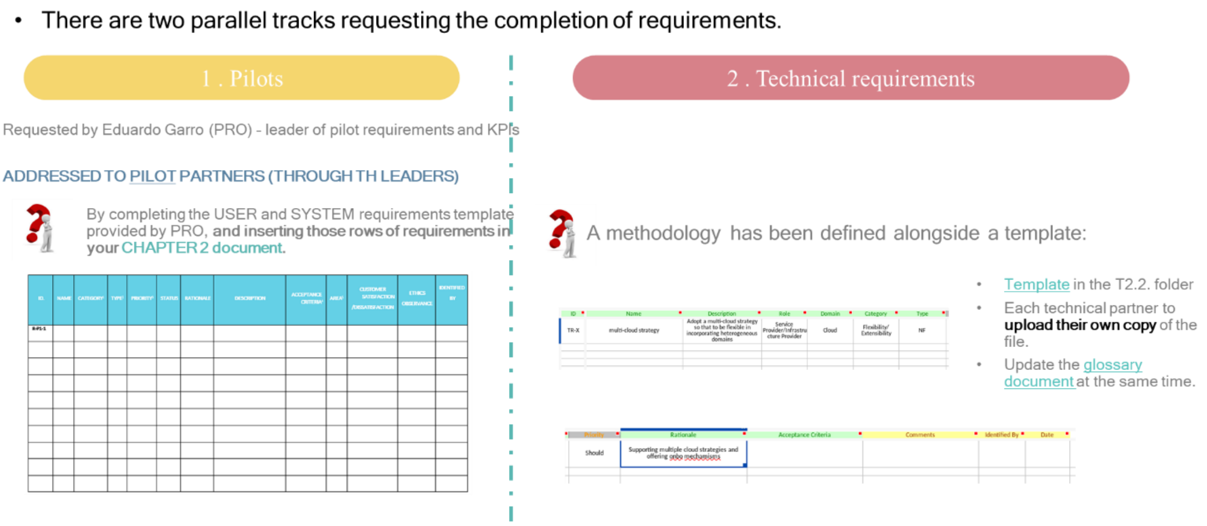


Figure 13. Parallel requirement gathering tracks in aerOS methodology

- Finally, planning-wise, depending on the advancement of project works through time the collection process follows subsequent phases.
    - In Phase 1 the first recording of technical requirements happens in parallel with the recording of requirements for the Pilot use cases while in…

[6] https://www.agilebusiness.org/dsdm-project-framework/moscow-prioririsation.html

- Phase 2 a translation of the Pilot use cases requirements into technical ones provides an update. An analysis of the outcomes from these initial two phases is documented in this deliverable and provides valuable input to the initial design of the aerOS architecture.
- In Phase 3 to come, technical requirements are reflected to the aerOS architecture design and updated as a deeper understanding is gained while they drive the definition of the KPIs.
- Phase 4 which will last until the end of the project technical requirements are updated as developments and trials proceed while KPIs are monitored and actual needs become clear.

2.3.2.1. Technical requirements elicitation methodology

Technical requirements are those factors required to deliver desired functions or behaviour from a system to satisfy users' standards and needs. Indicative types of required factors addressed are accessibility, adaptability, usability, maintainability and performance. A proper technical requirements elicitation process provides most valuable input to drive a successful system's design and implementation, The methodology followed in recording the technical requirements helps and drives the analysis to provide valuable input to other project processes.

The recording process of a technical requirement follows principles defined in the Volere requirements specification methodology considered to lead to a more well thought and precise recording. Indicatively, for each technical requirement defined, a fit criterion must also be defined which specifies at this early stage the way the requirement should be tested if it is covered.

Furthermore, apart from functional and non-functional known types of requirements other types are introduced, among them that of design Constraint requirement which refers to restrictions on how the product must be designed. Each recorded requirement is prioritized according to the MoSCoW (Must have, Should have, Could have, Won't have this time) popular prioritization scheme.

In the methodology selected for this sub-track of requirements gathering, the following aspects were agreed:

- The Technical Coordinator led this action, that involved all technical partners of the project.
- A technical requirement consists of a set of fields each of them adding valuable information to its definition by answering a specific question.
- A specific template was created, materialized in an spreadsheet, with the head columns as illustrated below:

ID	Refers to	Name	Description	Role	Domain	Category	Type	**Priority**	Rationale	Acceptance Criteria

Table 3. Technical requirement template explanation

Field	Question answered	Field definition
ID	How it is uniquely identifiable with an id?	A unique ID, following the naming: TR-*X*
Refers to	Which area of the project is it directly related to? (can be more than one)	In order to further ease the extraction of valuable input to the various areas of developments, technical requirements are classified according to the area they refer to. The main areas identified in the context of the aerOS project are: Infrastructure, Network, Meta-OS, Applications, Services, Development, Security, Data, AI … each one reflecting a major development area in the scope of the project
Name	How it is uniquely identifiable with a highly representative name?	A representative name for the technical requirement
Description	What does it concern?	A description of the technical requirement

Rationale	How it is justified?	A justification of the requirement
Role	Who does it concern?	The specific role it concerns: - (AP) Application programmer - (IP) IoT infrastructure provider - (CP) Cloud infrastructure provider - (NP) Network provider - (SP) Service provider - (AU) aerOS application user There may be more than one roles specified or (ALL) in the case the requirement concerns all roles.
Domain	Where it applies?	The domain the requirement applies to: Continuum, IoT, Edge, Cloud, Network, App… There may be more than one domains a specific requirement applies to.
Category	How is it categorized?	Specification of how this technical requirement could be categorized according to the area it addresses: - General - Accessibility - Performance - Throughput - Availability - Reliability - Maintainability - Security - Privacy - Standards - Data quality - Extensibility Others may appear along the process of requirements gathering.
Type	What's its type? (Functional / Non-functional / Constraint)	Definition of the type of requirement: (F) Functional requirements. (NF) Nonfunctional requirements (C) Constraints for design
Priority	How is it prioritized? (following MoSCoW prioritization)	Definition of the priority of the requirement regarding the necessity of its illustration: • (M) "Must" • (S) "Should" • (C) "Could". • (W) "Would"
Acceptance criteria)	How is it tested?	Specification of how the requirement is tested once illustrated

The technical requirements recording process is continuous throughout the lifetime of the project and technical requirements document is considered live. In practical terms, the collection of technical requirements is done through an online spreadsheet that lives in the cloud document repository of the project.

2.3.2.2. Pilot requirements elicitation methodology

In the second track of requirements gathering, the activity has focused on the requirements coming from the use cases, as expressed by the involved stakeholders. The goal has been to identify the requisites classified as "user" and "system".

For doing so, several considerations have been made:

- There is a common spreadsheet in the repository of the project that collects this information. This sheet is filled by the TH leaders (of each pilot). In addition, per each pilot, a replica of the content of that file is inserted, included only the requirements associated to that pilot. This is done once per wave. This procedure follows the ideas of the TH methodology described in Section 2.3.1.
- The gathering has been done using the following template. Meaning of every field is described in the table below.

ID	Name	Cate gory	Type	**Prio rity**	Status	Ration ale	Descri ption	Acceptance Criteria	Customer satisfaction	Customer Dissatisfaction	Ethics Observance	Identifie d By

Table 4. User and system requirement template explanation

Field	Field definition
ID	A unique ID, following the naming: TR-P*X*-*Y* , being *X* the number of the pilot (P1-manufacturing, P2-containerised edge data center, P3-HPCP agriculture, P4-maritime port and P5-smart building) angd *Y* the unique identifier (sequential) of the requirement in that pilot.
Name	A representative name for the requirement
Category	Definition of the category of the requirement as indicated in the methodology above: (F) Functional requirements. (NF) Nonfunctional requirements (C) Constraints for design
Type	A specification of the type of requirement based on the first guiding principle: (U) User requirement (S) System requirement
Priority	Definition of the priority of the requirement regarding the necessity of its illustration: • (M) "Must" • (S) "Should" • (C) "Could". • (W) "Would"
Rationale	A justification of the requirement
Description	A description of the requirement
Acceptance criteria	This fit criterion measures the requirement, making it possible to determine whether a given solution fits the requirement. If a fit criterion cannot be found for a requirement, then the requirement is either ambiguous or poorly understood. All requirements can be measured, and all should carry a fit criterion. In any event, the fit criterion is the benchmark to allow the tester to determine whether the implemented product has met the requirement.
Customer satisfaction	Degree of stakeholder happiness if this requirement is successfully implemented. Scale from 1 = uninterested to 5 = extremely pleased
Customer dissatisfaction	Measure of stakeholder unhappiness if this requirement is not part of the final product. Scale from 1 = hardly matters to 5 = extremely displeased.
Ethics Observance	Whether or not this requirement must be tagged as Ethics-prone for observance.
Identified by	Internal field to ensure proper tracking and identification of the partner that created or last modified the requirement.

3. Use cases description

aerOS validates its results in five use cases, representing: (i) Industry 4.0, (ii) utilities (renewable energy), (iii) smart agriculture, (iv) port transportation and logistics, and (v) smart buildings. The following subsection presents a description of each use case that is currently underway, including its general description, current problems/barriers area, participant partners, data sources, existing software, and available hardware. The section also discusses the objectives, benefits, and expected results of the trial, as well as its specific outcomes and KPIs. Additionally, the legal and social frameworks surrounding the trial are examined.

3.1. Pilot 1: Data-Driven Cognitive Production Lines

3.1.1. Trial general description

The use case aims to deploy and validate **Manufacturing Autonomy Level 4** (MAL4) **cognitive production processes** in **4 public-private Pilot Lines (PL)** located in: (1) INNO Didactic Factory at AIC - Automotive Intelligence Center (Bilbao, Spain), (2) MADE Competence Centre & POLIMI Industry 4.0 Lab facilities (Milano, Italy); (3) SSF open factory lab at SIPBB (Biel, Switzerland), and (4) SIEMENS INNOVATION CAMPUS in factory automation headquarter (Nuremberg, Germany). The sites offer 5000 m^2 of cutting-edge I4.0 production systems and bring together over 500 companies. Therefore, and responding to the structure that was designed since the proposal stage, the trial is divided in four clearly differentiated scenarios. This is very relevant in Pilot 1 of aerOS, as varying groups of partners and stakeholder in the Consortium are devoted to the different scenarios. However, all of them pursue the goal of **creating a highly flexible, sustainable (green) modular digital production lines** and manufacturing of a new product in a low-volume production via the implementation of smart rapid response features in connection with self-optimisation, reconfigurations ramp-up, adaptation of production line and operations.

The four scenarios are as follows. A more thorough description of each of them, together with their objectives, benefits and expected results are described in Section 3.1.5:

- ***Scenario 1 – Green manufacturing (zero net-energy) and CO_2 footprint monitoring*** product life cycle digital thread and sustainability (CO_2 footprint) data models, in connection with the implementation of Digital Product Passport (DPP), enabling a systemic shift towards circular economy, supporting de-manufacturing operations, optimisation of reverse logistics infrastructure and more sustainable product design. It will experiment Gaia-X and **aerOS** services at PL3 (CH) to implement edge intelligence services (and analytics) to optimise impact and footprint of lines.
- ***Scenario 2 – Automotive Smart Factory Zero Defect Manufacturing.*** A ZDM approach, ensuring robustness and stability of the process, deploying inline quality control among the manufacturing workflow. Remote tactile human-CMM interaction (where resilience policies and SLAs must be reached); energy efficiency monitoring and real-time machine error compensation extending 5GROWTH set-up to ensure accuracy of product quality dimensional inspection will be showcased at PL1 (ES). The **aerOS** system will enable the seamless interaction of quality control intelligence engine with a wide range of dimensional instrumentation equipment, hybrid Coordinate-Measuring Machines (CMM), arm robots or in machine-tool metrology. Considering that an Industrial IE down in a manufacturing line can have major negative economic impacts, self-features are needed.
- ***Scenario 3 – AGV swarm zero break-down logistics & zero ramp-up safe PLC reconfiguration for lot-size-1 production.*** The business process incorporates process specific information (MES) with context information about what needs to be done, which is feed to the edge-cloud continuum by means of SIMATIC Industrial edge apps (pub/sub schemas) to feed **aerOS**. Production flexibility (reconfigurability) is realised by on-the-fly Automated Guided Vehicles (AGVs) decision making and robot path calculations. **aerOS** automatic transport and safe placement of robotic arms is safely realised with safety enabled PLCs that enrich the process with critical device data and communicate with stationary safety devices like light fences via edge. PL2 (IT) will showcase advanced logistic processes (real-time benchmarking); whereas PL4 (DE) will showcase safe and secure automation of production. Diverse IE nodes will co-exist and collaborate, orchestrated by a master node.

3.1.2. Current problems/barriers area and motivation

In order to illustrate the problems/barriers that have motivated this use case in aerOS, and according to the personalized templates of Trial Handbook devised for the project, it was decided to utilise the following table:

First, about metrology that is required for Scenario 1, it was concluded that the current problem/barriers existing in the sector, and that will also mean a hindrance to overcome during aerOS trial were:

Table 5. Current problems and barriers in UC1 related to metrology

CHALLENGES or BARRIERS	DESCRIPTION	AREA	IMPACT IN THE COMPANY
Experienced metrologists are needed	Currently only highly experienced metrologists are able to adequately define the measurement strategy in the software, that is, define the point sets. Based on their great experience, they have the ability to know which regions of the piece are the most relevant.	Technical support	Lack of experienced workforce. Loss of operational efficiency. High quantity of resources and time must be consumed for training. Loss of operational efficiency in the processes.
There is no possibility of reusing information	When the metrologists start to define the measurement strategy of a part, none of the previously performed jobs are used, the strategy is defined from scratch for each job.	Technical support	Time consuming tasks for the staff and loss of operational efficiency.
On-site operation of CMM	The operation of dimensional equipments requires a metrologist expert to be physically in the facility.	Technical support	Time consuming for metrologists. Operational inefficiencies Increased costs. Exposure to additional risks in industrial facilities.
Extrapolation of data from scratch	In the case of reuse values from another measurement, the data to program the machine is entered by hand, and this supposes a considerable loss of time.	Technical support	Time consuming tasks for the staff. Loss of operational efficiency.
Standardization	Need for standardized measurements and units of measurement	Technical support	Inefficient business and operational process. Inconsistencies in the quality of the service.
Maintenance and calibration	The equipment must maintain the accuracy of measurements over time. It requires regular calibrations and maintenance.	Technical support	Loss of efficiency. It consumes human and economic resources.
Data management/security	The security, accuracy, reliability and accessibility of the generated metrological data must be ensured.	Technical support	Data loss and breaches and exposure of confidential or sensitive information. Reputation damage and difficulties to access data.

In addition, reflecting about data management in edge, distributed, decentralized production lines in manufacturing, the problems and barriers must be analysed from another perspective. There, the current way to perform edge computing is to have independent systems inside the company that cooperates to achieve the best results possible, the current strategy to optimize the plant is utilizing a digital twin that is able to estimate some of the critical parameters changing the configuration of the devices inside the plant.

The objectives are improving the current status of the technological area introducing: (i) a more distributed (towards the edge-layers) computing power architecture that will enable real-time computing and permit to avoid transmission of huge amount of data to the cloud; (ii) introducing a Decentralized intelligence by Frugal AI/ML system that will contribute to increase network and orchestration efficiency; (iii) enable data interoperability and standardization for data coming from different third-party components and (iv) introducing ease of use and implementation of these applications by ad-hoc APIs that enable flexibility, scalability and versatility of the whole solution.

The integration of the platform should be able to increase efficiency of the technology area, reducing costs, reducing energy consumption, reducing idle time of the components, improve interoperability and communication from different components, optimizing bottlenecks.

Table 6. Current problems and barriers in UC1 related to data and edge management in production lines

CHALLENGES or BARRIERS	DESCRIPTION	AREA	IMPACT IN THE COMPANY
Improve current data management	introducing a more distributed (towards the edge-layers) computing power architecture that will enable real-time computing and permit to avoid transmission of huge amount of data to the cloud	Manufacturing	The technology will support the **reduction of waste of energy** because of the optimization of AGV travels and buffer managing. The AGV power consumption could be reduced even of 50% if the aerOS solution is able to make the system avoid some travels. Optimizing AGVs, the assembly line and quality control line buffers would lead to a **reduction of lead time**. This would lead to **Increase efficiency of production line, Decrease of idle time and costs**. Finally installing such type of solution in a production plant would lead to an high level of digitalization that would lead to a huge **Increase of awareness of the production processes.**
Barrier: poor data availability	Introducing such a data dependent solution will require great amount of data. Currently the AREA in MADE has the important barrier that it is not always working, to work it needs an operator that constantly operates in the area. So generating hystorical data could be a barrier to develop the use case. It could be necessary to simulate some data	Manufacturing	Poor data available will affect general reliability of AI/ML algorithms and general efficiency of the solution

Challenge: asset interoperability	The introduction of aerOS platform will imply several iteration of system integration activities, as analogue assets part of the pilot come from different vendors, with consequent different interfaces with respect to the information systems logically displaced in the upper levels	Manufacturing	Possible lacks of useful information due to the conversion of raw data formats into different ones. Possible “a posteriori” data patches could be also implemented to patch missing information from the original source

On the other hand, one of the aspects where this use case of aerOS is focusing is on drone production lines. This is a field where several challenges can be addressed by aerOS, still posing challenges for its implementation. In the current drone production line, several machines and demonstrators are already working together and are dependent on each other. For this, they are already exchanging data from machine to machine to guarantee a seamless production of the drones. Some of the demonstrators are already equipped with power measurement devices and condition monitoring devices. One current barrier is that this data is not processed and analyzed in a common way to have a good understanding about the overall production line. To be able to calculate and predict the CO2 emissions of the line, the data must be collected and analyzed on a common solution. One further barrier is the availability of data from external suppliers.

Broadening the scope to public entities wishing to enlarge their capacities toward production lines (and other sectors) in their regions, there are several challenges related to sustainability of digitalization strategies of large-scale cloud-to-edge deployments. Tackling the lack of proper infrastructure for cloud-edge continuum with the deployment of aerOS will broaden the technological framework that serves as the foundations for the development of the technologies that those governments could bring.

Table 7. Current problems and barriers in UC1 related to managing large edge-cloud infrastructures by public entities

CHALLENGES or BARRIERS	DESCRIPTION	AREA	IMPACT IN THE COMPANY
Public cloud-edge infrastructure	As a public IT provider, NASERTIC desires to deploy public aerOS infrastructure for it to be exploited and leveraged by local agents that look forward to the implementation technological solutions in line with Navarre’s current sustainability & digitalization strategies.	Infrastructure	Since NASERTIC does not have any industrial activity, aerOS’ impact within the company is entirely related to the creation of a public infrastructure for it to be put at the disposal of Navarre’s society.

Finally, some of the main challenges/barriers in the manufacturing field are those that emerge from shifting from mass production to more personalized and customized production methods, which prioritize variety and flexibility while still demanding the high efficiency of mass production. With the increasing demand for personalized production, there is a growing need to produce variable products in high volumes to meet customer demands. This requires new technological solutions that can help streamline the production process and make it more efficient while still allowing for a high level of customization. As a leader in the field of factory automation, SIEMENS (partners of aerOS) is well-positioned to develop innovative solutions that can help organizations adapt to these changing manufacturing trends and stay ahead of the competition outside of Europe.

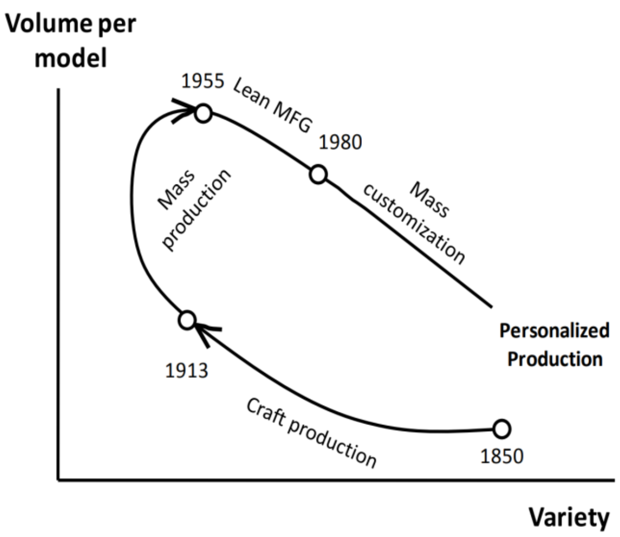


Figure 14. The evolution of production types in relation between volume per model and variety through the past 150 years[7]

One of the significant challenges in achieving flexible production facilities is the issue of siloed solutions provided by individual machine builders. Often, different systems within a factory operate on different proprietary protocols, making it challenging to integrate these systems into a cohesive production environment. As factories strive to increase their flexibility and adaptability, this lack of standardization can be a significant barrier to expansion.

To address these challenges, there must be standardization efforts across the industry, which would require machine builders and technology providers to work towards common standards that allow their systems to comgmunicate and integrate more effectively. This would help to create more unified, interoperable production environments that can adapt more quickly and efficiently to changing market demands.

This is where the aerOS platform comes in, providing a solution that enables standardization and continuity research across different manufacturing processes. It supports an open interface architecture that facilitates communication and data exchange between different machines, systems, and software. The platform is designed to help factories rapidly expand their production capabilities while maintaining flexibility and agility, allowing them to adapt quickly to changing market demands.

In conclusion, the challenges posed by siloed solutions provided by individual machine builders can be a significant barrier to the expansion of flexible production facilities. Standardization efforts and continuity research, as provided by aerOS, can help to lower these barriers, enabling more rapid expansion

[7] http://www-personal.umich.edu/~ykoren/uploads/Assembly_System_Design_and_Operations.pdf

and greater adaptability in manufacturing processes. By providing an open interface architecture and enabling seamless data exchange, aerOS is helping to create a more unified, integrated production environment that can meet the demands of a rapidly changing manufacturing landscape.

It is worth noting that aerOS is not only operating in manufacturing processes, but it operates as a middleware across different branches of data-generating assets. By providing a seamless and unified platform for data management and analysis, aerOS enables organizations to optimize their operations and gain insights into their performance across a range of industries, from energy and utilities to transportation and logistics. This broader applicability makes aerOS an even more valuable tool for organizations looking to improve their operations and gain a competitive advantage in their respective markets. With its focus on standardization and continuity research, aerOS is at the forefront of innovation in the data management and analysis space, providing organizations with a powerful tool to unlock new insights and drive growth across multiple industries

Table 8. Current problems and barriers in UC1 related to data and edge management in production lines

CHALLENGES or BARRIERS	DESCRIPTION	AREA	IMPACT IN THE COMPANY
Transition from a static production to a flexible production	Reconfiguration and reallocation of production assets is non-trivial. A lot of Engineering with different tools must be used and automated while maintaining the same level of performance as static production assets	Engineering	Addressing new customer segments. Diverging from machine builders towards end customers and empowerment of those.
On-demand orchestration of apps in dynamic, changing environments	Applications that use physical hardware need to be orchestrated to devices that have access to the hardware. In changing production lines, this hardware can move around which should then change the existing orchestration.	Manufacturing	Zero touch configuration
Dynamic plant layout optimization and reconfiguration	Dynamic plant layout optimization and reconfiguration	Production Planning, Manufacturing	Less manual interaction needed, faster response times, less workforce needed
Heterogeneous and integrated communication infrastructures	Flexible and modular production systems require the sporadic relocation of resources grouped in modules, because of that, those modules are best served by wireless communication networks for their connection to the factory management or other resources. This means that networks must be built integrating wired and wireless infrastructures. Additionally, those networks must fulfil the requirements on bounded latency or packet loss often found in industrial networks.	Engineering, Manufacturing	New business opportunities for network integration solutions. Usability of current networking technology based on wired infrastructure in the future flexible factory.

3.1.3. Participant partners

INNOVALIA:

The Innovalia Association is an R+D+i Business Unit belonging to the Basque Science and Technology Network founded in 2002 by a group of small and medium-sized technology-based companies, with an international presence and highly aware of the need for continuous innovation in products and services to maintain and improve competitiveness at the international level. The Innovalia Association is a private research laboratory, which was created to articulate a critical mass capable of successfully undertaking its strategic long-term research ambitions and objectives. It has offices in the Basque Country, Community of Madrid, Catalonia, Canary Islands, as well as other points in Europe, Asia, the Middle East, Central America and South America.

The Innovalia Association provides a clear and structured emphasis on the strategic axes of technological innovation, business cooperation and market orientation. It represents the centre of excellence with the capacity to develop methodological procedures and tools and software, highly specialized, under the strictest quality standards, for systematic innovation. The digitization of manufacturing companies and advanced manufacturing systems represent two of the strategic areas of knowledge in which the Innovalia Association focuses its efforts and which are part of the reason for its existence. The R+D+i project described in this technical report falls within these areas. The Innovalia Association as a Business I+D Unit has an extensive network of infrastructures and equipment to be able to carry out its functions of managing and boosting the technological developments of its founding employers, focused on the different technological areas of interest to the Innovalia Association: (i) Metrology and Manufacturing Processes, (ii) Wireless communication and service platforms, (iii) Software engineering: verification, validation and quality and (iv) Safety, reliability and performance.

MADE:

MADE is a Competence Center for Industry 4.0 which has the mission of Leading Digital and Sustainable Manufacturing Industry transition towards Industry 4.0. To support the mission MADE implements Orientation, Training, and Finalization activities for technology transfer projects with companies on Industry 4.0 issues. A technical interlocutor that companies can rely on for support during the digital transition to a smart factory. Further, to simplify usability and facilitate the creation of in-depth paths, six technology areas have been implemented within the Competence Center. The six areas are developed in more than 2500m^2 and are covering almost all the cutting-edge technologies involved in industry 4.0 such as: Virtual Design and New Product Development; Digital Twin and Virtual Commissioning; Lean Manufacturing 4.0; Logistics 4.0; Collaborative robotics and intelligent worker assistance systems; Quality 4.0; Product traceability and additive manufacturing; Smart monitoring and control of industrial processes; Smart energy monitoring and control; Smart maintenance; Industrial Cyber Security and Big Data Analytics.

Further, MADE 4.0 empowers academic and industrial partners to participate in funded projects through the exploitation of installed assets and solutions, as well as the concept of the "Teaching and Learning Factory".MADE 4.0 offers partners access to European networks in which an international network of expertise can be developed by leveraging the know-how of consortium partners

SIPBB:

The work in this project is being carried out by the team of the Swiss Smart Factory (SSF) in Biel, which is part of the Switzerland Innovation Park Biel/Bienne (SIPBB). The Swiss Smart Factory is an extensive test and demo laboratory for Industry 4.0 on 1000 m2, which, among other things, consists of a large production line for the manufacture of quadcopter and hexacopter drones in batch size 1. The production line demonstrates innovative manufacturing concepts and is built and operated with more than 70 companies. It serves, among others, as an international test bench for data sharing in the POC-series with NTT and SIEMENS and in the EU-Project DIMOFAC.

NASERTIC:

NASERTIC participates in this use case as an IT provider and not as an industrial agent because it currently does not have any relation with edge computing-related activities, and even less relation with industrial manufacturing and logistics. In fact, NASERTIC is not the direct responsible in any of the demonstrators within the use case. NASERTIC is a public organization with expertise at managing its regional government's datacenter and delivering IT services to society. For all these reasons, this company cannot identify any challenge to face from the industrial standpoint, but is interested in boosting aerOS so that it can later be put at the disposal of Navarre's society. NASERTIC boosts all Telco projects commissioned by the Government of Navarre and is the reference partner for the Public Corporations in that Community for everything related with the deployment, assistance and maintenance of ad-hoc Telco services. This line of action has allowed our community to carry phone coverage, Digital TV and high-speed Internet connectivity (among other services) to 99.5% of our territory, which is possible thanks to our own telecommunication infrastructure and to the management of the Government of Navarre's data centres. Simply put, NASERTIC offers the infrastructure on top of which other entities deploy their own IT services, which add value to the society in Navarre.

SIEMENS:

Siemens is a well-known and reputable company in the field of factory automation, with a broad range of products and services that are designed to make the manufacturing process more efficient, productive, and flexible. One of the core divisions within Siemens that is responsible for these products and services is the Digital Industries Factory Automation (DI FA) division. The DI FA division's primary focus is on providing customers with automation solutions that are tailored to their specific needs, from product design to installation, implementation, and after-sales service.

An essential aspect of Siemens' approach is their emphasis on constantly getting real-world customer feedback and challenging new internal product developments with that experience. The DI FA division is continually working to improve their products and services by incorporating customer feedback into their design process. This allows Siemens to stay ahead of the curve by developing innovative solutions that are tailored to meet the needs of their customers.

Siemens has also established an innovation laboratory in Nuremberg, Germany, which is focused on exploring new technologies and approaches to factory automation. This facility serves as a pilot location for testing new concepts and products, including the trail of Pilot 1 in aerOS.

Collaborating with aerOS, the importance of flexible production facilities in an increasingly connected environment will be highlighted and further evaluated. The aerOS platform is designed to improve the efficiency and productivity of manufacturing processes while allowing for greater flexibility and customization. By working together, Siemens and aerOS aim to develop innovative solutions that will meet the demands of a rapidly changing manufacturing landscape. The focus on flexible production facilities will enable organizations to adapt to changing market demands and optimize their manufacturing processes to stay ahead of the competition.

3.1.4. Data sources, existing software and available hardware

The data sources, existing software and hardware that have been detected so far to be used in the Pilot 1 of aerOS are as follows. The next list reflects only a summary of the minimum aspects detected so far. A far more thorough description is included in the current stage of the Trial Handbook (online) of the pilot. In addition, it is worth noting that these descriptions will be fully disclosed in the next deliverable of this task (T2.2, deliverable D2.3):

Data sources

- Product related data (CO2-footprint, colours, size, type, etc.) accessible via API endpoint.
- Process data for calculating CO2 footprint reachable via OPC-UA, API endpoint and MQTT.
- Machinery data for calculating CO2 footprint reachable via OPC-UA, API endpoint and MQTT.
- Sensor data and 3D metrological data that are stored in a data lake of the pilot and can be accessed via API Endpoint, File Extract, SQL data access and OPC-UA SDK.
- Status of the machines through sensors accessible via API endpoints.
- Digital twin (of the production line) estimations.

Available software (that aerOS will somehow need to be aware of / interact with):

- ProAlpha ERP (Cloud-based ERP system)
- SETAGO App (Manual Assembly Workstation Software)
- Melkus AGV Navigation Software
- NODE-RED, that is used in the SSF Factory for several assets and tasks
- M3 platform, a platform for the total management of dimensional quality in the manufacturing sector. Composed of M3 Gage (for the capture), M3 Server (for storage) and M3 Tablet (for analysis).

Available hardware:

- Manual Workstation SETAGO
- Motor Production (Automated Production System)
- PCB THT-Assembly (Automated Production System)
- Melkus C4060 AGV
- Balluff Sensor for Ambient Temperature & Humidity

Figure 16. Hardware of Pilot 1: Manual Workstation SETAGO

Figure 15. Hardware of Pilot 1: • Motor Production

Figure 18. Hardware of Pilot 1: • PCB THT-Assembly

Figure 17. Hardware of Pilot 1: Melkus C4060 AGV

3.1.5. Objectives, benefits and expected results

In the following sub-sections there is a thorough description of each one of the scenarios in Pilot 1.

3.1.5.1. Use case Scenario 1: Green manufacturing (zero net-energy) and CO2 footprint monitoring

3.1.5.1.1. Description

Green manufacturing (zero net-energy) and CO_2 footprint monitoring product life cycle digital thread and sustainability (CO2 footprint) data models, in connection with the implementation of Digital Product Passport (DPP), enabling a systemic shift towards circular economy, supporting de-manufacturing operations, optimization of reverse logistics infrastructure and more sustainable product design. It will experiment Gaia-X and aerOS services at PL3 (CH) to implement edge intelligence services (and analytics) to optimize impact and footprint of modular production lines for drones.

This scenario will be built withing the test – and demonstration platform of the SSF. Based on the described equipment in the next paragraph, the goal is collecting data from the available equipment, which is used for the manufacturing of the lot-size one drone production. The customized configuration of the drones produced on the production line does have a direct impact on the CO2-footprint of the drone. Meant by this are for example the material selection of the single parts of the drone, the actual environment conditions of the production line, specific individual engravings and the delivery method selected. With aerOS the data generated by the demonstrators should be collected and processed to be able to measure the actual CO2 footprint of the production for each individualized produced product. With this a Digital Product Passport (DPP) can be implemented and enriched with this data. Based on the CO2 footprint measurement of the production for each individualized produced product, the next goal is to achieve a prediction of the CO2 footprint of the production for each individualized produced product. In a last step, the goal is to achieve a reduction of the CO2-emission through the calculation of an optimized production path. This could include, to calculate the most efficient path for the Melkus C4060 AGV which is responsible for the transportation of the drone and drone parts during production. Furthermore, the assembly and the motor production could be optimized by learning from the data measured and predicted through aerOS. This enables the SSF an comprehensive understanding of the CO2 generation of the production line. This knowledge and methodology can be transferred to other companies of the SSF network and can help them to reduce their CO2 footprint in their own production sites.

3.1.5.1.2. Specific objectives

The objectives of this use case are described using the table below, which aims at explaining their impact and their effect in value (being 1 no significant and 5 very significant).

Table 9. Specific objectives of Use case 1 – Scenario 1

OBJECTIVE	DESCRIPTION	IMPACT	EFFECT OF VALUE	
Real-time measuring of CO2 generated by the assets of the test – and demo platform	The assets of the drone production line in the Swiss Smart Factory are consuming energy and generating CO2 emissions. aerOS enable the constant measuring of the emissions by considering several factors such as energy source or amount of energy consumed	Transparent knowledge about the CO2-Footprint of every drone produced.	**Cost**	1
			Efficiency	4
			Quality	1
			Flexibility	2
			Innovation	3
			Sustainability	5
Real-time monitoring of CO2 generated by the assets of the test – and	With aerOS the measured CO2-emissions of the assets of the production line should be monitored in real-time in the factory. This monitoring could be also exchanged with the customer to keep him informed	Overview about the CO2-emissions of the production line and the footprint of the drones produced	**Cost**	1
			Efficiency	3
			Quality	1
			Flexibility	3

demo platform	about the current situation.	in the factory.	**Innovation**	3
			Sustainability	5
Predicting the CO2-footprint (production) for each individualized produced product.	By predicting the CO2-footprint for each individualized produced product, the customer can be informed in advance about the emissions generated by his choice and can adapt his choice accordingly. In addition, the prediction will help for a more sustainable production.	Reducing the CO2-emissions of the production line by considering the predicted CO2-Footprint.	**Cost**	1
			Efficiency	3
			Quality	1
			Flexibility	3
			Innovation	4
			Sustainability	5

3.1.5.1.3. aerOS in Scenario 1

aerOS will be used as a data exchange, dashboarding and processing tool in the first scenario of Use-Case1 (where the partner SIPBB is the main stakeholder). aerOS will enable to communicate among and collect between different kinds of assets and data in the drone production line This enables the measuring and calculation of the CO2-emissions generated by the production line for each individualized produced product. The big advantage of using aerOS for this is that aerOS has the ability to handle various kinds of devices with different levels of capabilities. This is exactly needed for the scenario 1 of this use case, since there are very various kinds of assets (AGV's, Manual Workstations, Motor production etc.) in the production line.

To process the collected data and make use of certain AI-capabilities for the prediction of the CO2 footprint for each individualized produced product and to enable the reduction of the CO2-emissions generated by each individualized produced product aerOS will be used. In addition to the provided functionalities, the possibility of deploying self-created AI-modules in aerOS will play an important role in this use-case.

Besides, aerOS will be used to display the generated CO2-emissions and the prediction of the CO2-footprint generated by the assets of the production-line for each individualized produced product. In the Swiss Smart Factory there are several screens, which are used to display several information about the production process of a drone.

For the next version of this deliverable, this section will be complemented with a full diagram with the presence of aerOS meta-Operating System in the process, machinery and software of this scenario in Pilot 1.

3.1.5.1.4. Actors involved in Scenario 1

The actors involved of this use case have been collected following the table below, representing the actors involved, business area impacted, together with the type of impact and what it consists of.

Table 10. Actors involved in Scenario 1 of Use case 1

ACTOR	B$ AREA	TYPE OF IMP.	IMPACT DESCRIPTION
Production line coordinator	Manufacturing	Direct	By predicting and dashboarding the CO2-footprint of the individualized product the coordinator of the production line can edit the line path and the production of the drones.
Salesperson	Sales	Direct	When sharing the CO2-Footprint of the drone produced within the production line, the salesperson is affected when interacting with customers.

3.1.5.2. Use case Scenario 2: Automotive Smart Factory Zero Defect Manufacturing

3.1.5.2.1. Description

For the use case scenario 2, a Zero-Defect Manufacturing (ZDM) approach will be addressed in order to deliver semi-autonomous orchestration via remote tactile human-CMM interaction in dimensional quality control processes. “Zero-Defects” concept has been around for decades aiming at avoiding all failures and imperfections. Regarding the definition of ZDM, one of the big mistakes is to believe that this concept pressures us to produce without waste, without emissions, without accidents, without losses and without unemployment, among others. An organization must work to achieve perfection at each stage of the process, quality must be caused not controlled and while the definition of quality must be defined by each organization, the quality system should be considered a method of prevention and not a final stage in the process that will help us determine if the quality of the production has been as good. The industry has always seen metrology as an expensive process that does not add value, but it is in fact an essential part of the production process and part of the added value of a company: *The price of quality measurement is the price of nonconformity.*

The real need to optimize the process is starting to gain weight in companies and after a lot of effort, quality control is, right now, part of the production process. To reach this point there has been a significant change thanks to the emerging technologies and the rise of Industry 4.0: optical sensors and new data processing systems have been incorporated to contribute to shorten the time dedicated to quality management. The incorporation of these optical sensors and new software solutions, with great capacity to analyze and store data, has facilitated the natural process of acceptance of the role of metrology. To reach this reality, there has been not only a conceptual change but a technological change that allows us to scan the parts in production and in the laboratory in an agile way. In addition, before we did not have capable systems of storing or processing as much data as we have now; Technological development has been crucial for metrology to be part of the added value of a process.

In that regard, metrological studies are used to test the tolerances of parts. The fundamental objective is the obtaining and expression of the values of the magnitude working with different instruments, methods and appropriate measurements, with the precision required in each case. Since there are many different types of measurements, **this demonstrator will focus on dimensional measurement of components (i.e., machinery)**. More specifically, new metrological solutions are increasingly located within the production line, because it is sometimes crucial to arrive at high quality products that enhance the competitiveness of the company in sectors close to ZDM, such as the automotive or the aeronautics.

The process for the metrological analysis of a manufacturer has 2 phases:

a) the planning of the strategy
b) the programming of the machine.

Before starting to program the part point tracking, one needs to plan a strategy that depends on numerous characteristics of the physical part and parameters that the manufacturer requires. Usually, it is necessary to develop a metrological strategy for each part, observing its characteristics and parameters, only tacitly taking advantage of the information that previous similar projects have with the object of study. It is not only a waste of information, due to the difficulty of preserving the "know-how", but also a waste of time, since it requires metrologists with relatively high experience, and this can be translated as a gap in the improvement of the process and suboptimal process performance.

In today's market there are various metrological software solutions for the processing of data acquired in dimensional control. Most metrological solutions focus on the processing of information, regardless of the source of the data. Some allow control with coordinate measuring machines, being able to design and launch the scanning programs from the same interface.

The demonstrator focuses on implementing aerOS components, aiming at the following goals:

- Interaction of quality control engine with dimensional equipment, arm robots or in machine-tool metrology.
- Real-time quality control monitoring and error compensation.
- Remote tactile low latency human interaction.
- Energy efficiency monitoring.

For achieving the previous, the scenario 2 of Use case 1 of aerOS targets the implementation of aerOS capabilities in dimensional measurement of components, with the aim of promoting the manufacturing autonomy Level 4 and remote operation of CMMs. To this end, aerOS technological components will be deployed and validated in Innovalia Didactic Factory at AIC – Automotive Intelligence Center (Bilbao, Spain). Innovalia´s facilities aim at developing the following competences and related technologies:

- Industrial IoT & CPPS
- Metrology
- Zero Defect manufacturing
- Business Digitalization
- Big Data & 3D Mobile Visualization
- Cybersecurity and Digital Trust

Figure 19. Innovalia Didactic Factory at AIC

Companies dedicated to the manufacture of parts and components for the automotive, aeronautical, energy, etc. sectors are receiving dimensional quality requirements and tolerances from large companies that cannot be achieved with traditional methods.

The technology that is currently being imposed for the realization of dimensional quality controls is optical technology, since it allows the acquisition of a large amount of information in a much shorter time than probing technology. As a consequence, the number of pieces controlled is much higher. On the other hand, the amount of information that is handled is much greater, a point cloud of a car door can have 15 million points; therefore, the management and calculation algorithms have to be optimized to the maximum.

Currently, the optical measurement system has its own information processing software parameterizable associated with it and depending on the operator, one result or another will be obtained, which the developers design as a “black box” making it difficult to verify how they process this information.

In the use case scenario 2, aerOS will be implemented in the dimensional measurement process, which implies the following steps:

- Set a measurement plan for the part to be measured.
- Execute the measurement machine to scan the part.
- Upload the point data to the cloud.
- Extract parameter values
- Extract measurement results to the database.
- Generation of visualization and reports.

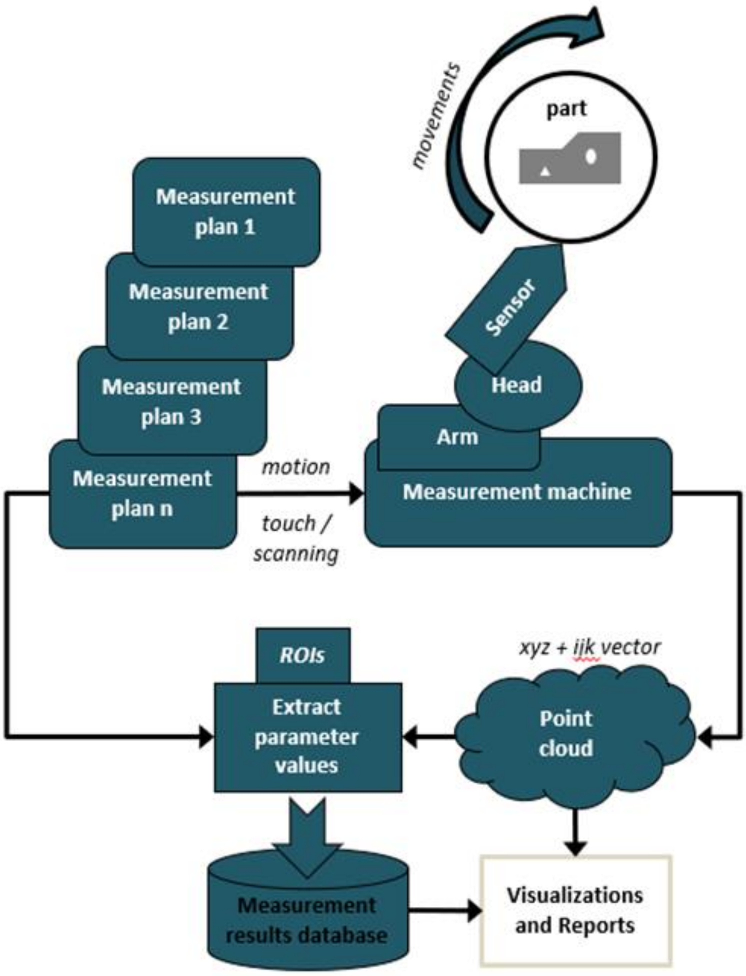


Figure 20. Actual measurement process of M3 SW

The dimensional measurement process in Innovalia involves the utilisation of M3MH work platform, which includes the components shown in the figure below. aerOS will enable the automation of the capture process, and will assist in the data management and connectivity of the work platform.

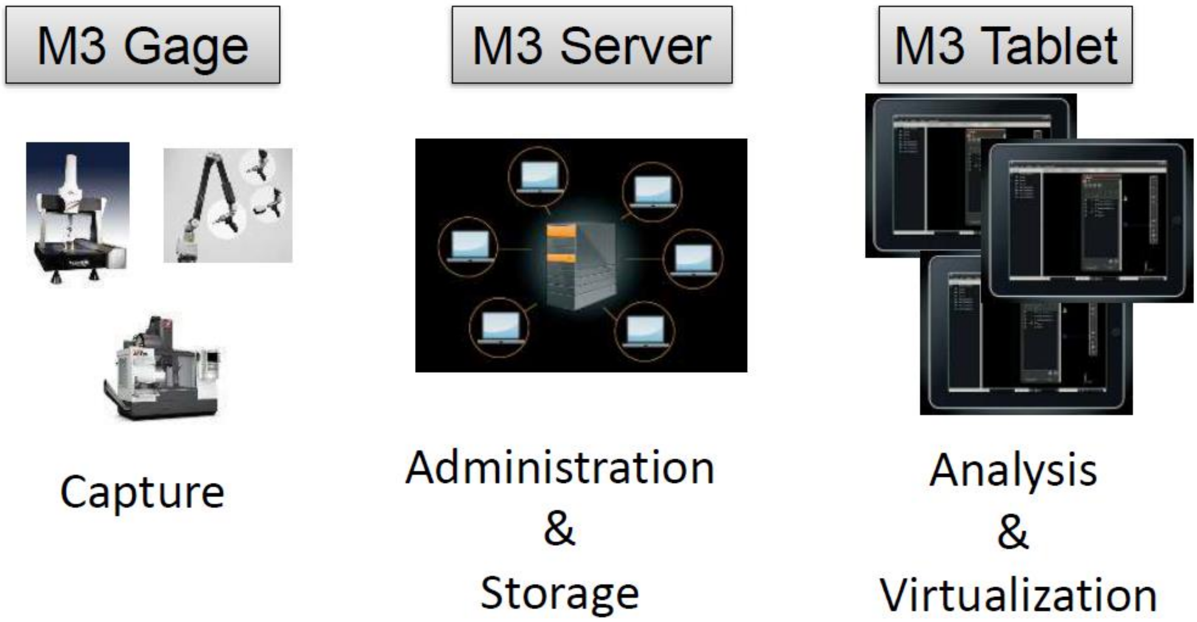


Figure 21. M3MH Work platform

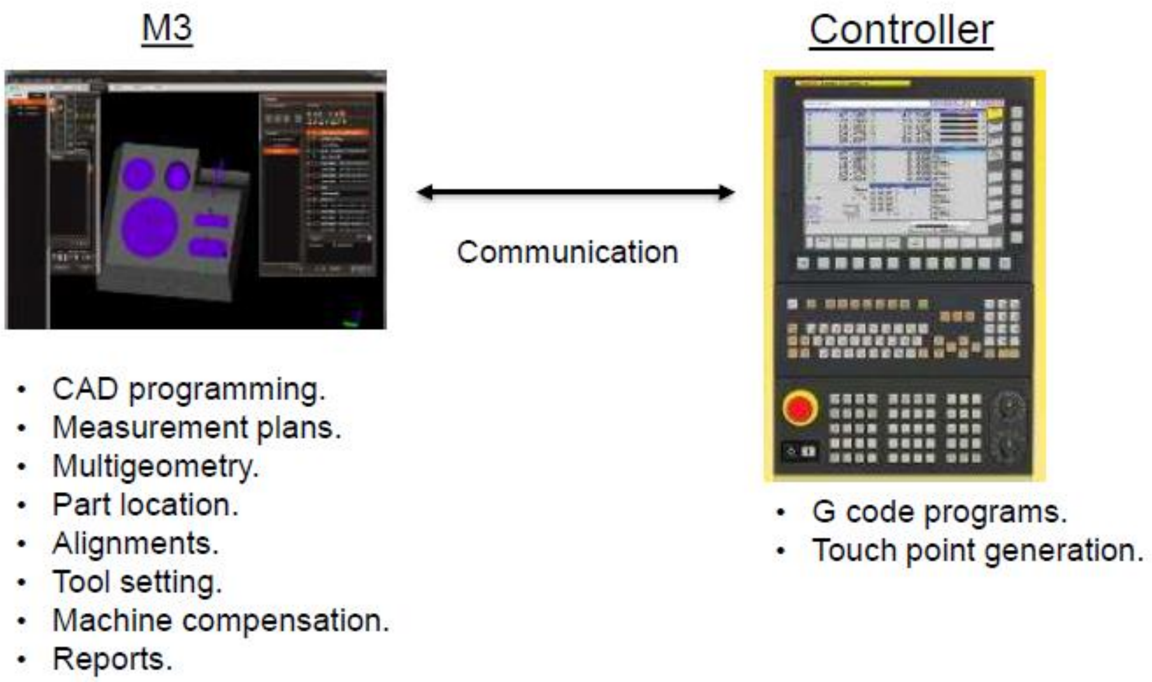


Figure 22. M3-Controller data communication

In addition, aerOS will assist and optimise the whole process of Digital Twin creation which is based on the following steps:

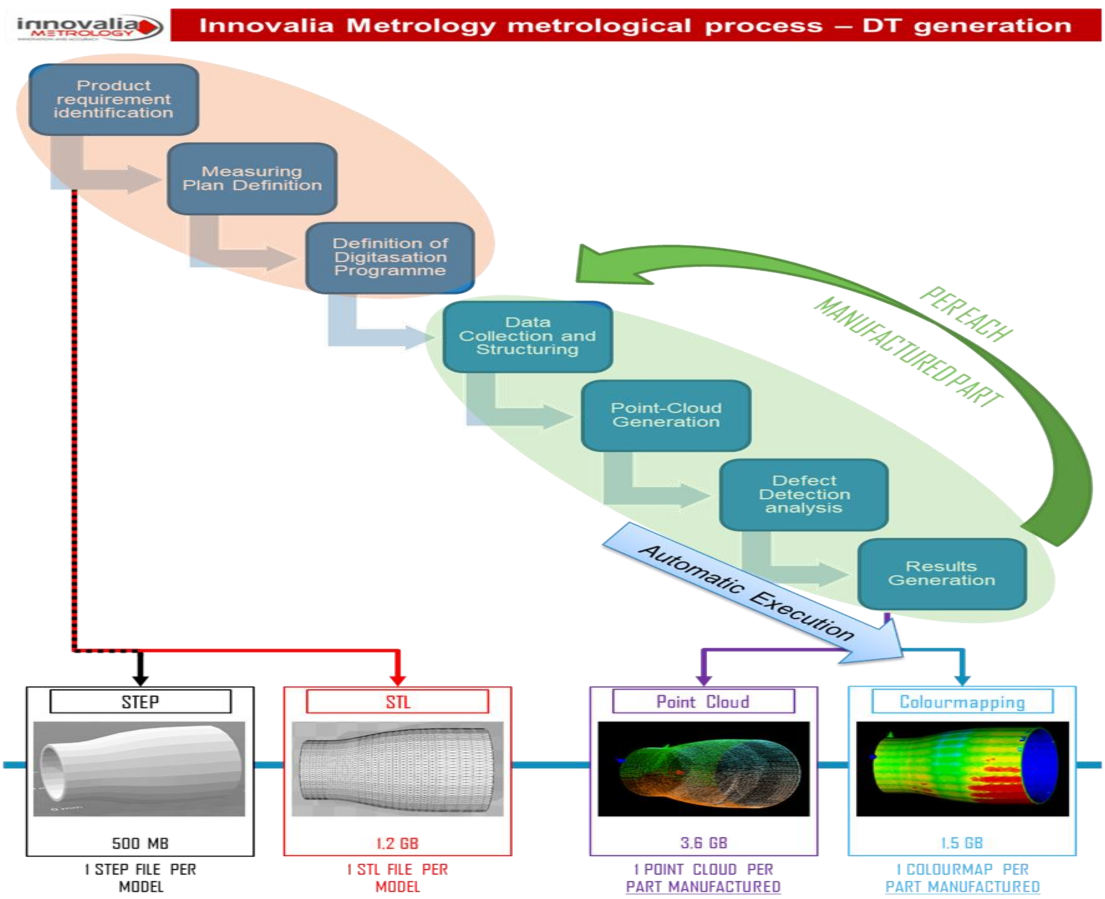
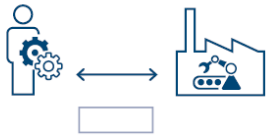
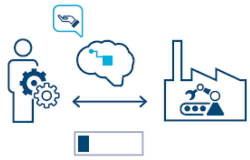
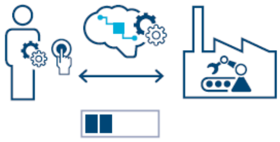
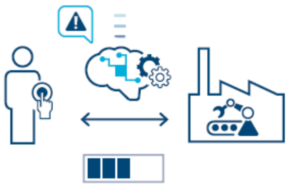
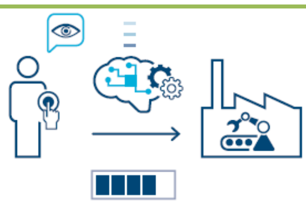
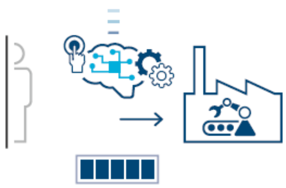


Figure 23. Digital Twin generation process

3.1.5.2.2. Specific objectives

The global objective of the use case scenario 2 is to promote the autonomy level 4 of manufacturing processes (**MAL4**). This is defined as an autonomous and adaptive manufacturing process, and different manufacturing autonomy levels can be differentiated as follows:

Table 11. Manufacturing autonomy levels

LEVEL 0		**No autonomy**, human beings have total control without any help.
LEVEL 1		**Assistance with respect to selected functions,** humans have full responsibility and make all decisions.
LEVEL 2		**Partial autonomy in clearly defined areas,** workers have full responsibility and define (some) objectives.
LEVEL 3	System-monitored environment 	**Autonomy delimited into larger sub-areas**, the system warns if problems occur, the workers confirm the solutions recommended by the system or operate at an alternative level.
LEVEL 4		**The system operates autonomously and adaptively,** within the defined limits of the system, workers can supervise or intervene in emergency situations.
LEVEL 5		**The system operates completely autonomously.**

With the aim of reaching the aforementioned global objective and promote cyber physical systems (CPS), the specific objectives of the implementation of the aerOS in ZDM use case are as follows:

- Remote tactile operation.

Currently, the operation of CMMs is mainly carried out on site. When it comes to the factory level, this implies that a metrologist expert must physically travel to the factory. As a consequence, there are operational inefficiencies and higher associated costs, as well as an increased risk to the operator working in hazardous areas. Aiming at the remote tactile, low latency operation, it would allow to face the aforementioned impact, requiring low latency communication protocols for reliable, fast and secure operation.

- Real-time monitoring and operation for machine error compensation, ensuring the accuracy of dimensional inspection.

The risk of false decision-making rises with higher measurement uncertainties. Since measuring is comparing, measurement is a physical process in which an iteration takes place between the object being measured and the instrument used for it. The result - the measurement - has to be collected and interpreted by the metrologist. Therefore, the ensemble will be subject to two types of influences: individual, inherent to the metrologist, and instrumental, arising from the method and the measuring device. Both will be the cause that exact knowledge of the magnitude is never possible, since the imperfection of the senses of the metrologist and the equipment used will always create an uncertainty in the value obtained and, consequently, a discrepancy between the exact value and the real, whose measure is the error interval.

The uncertainty associated with the instrument can be controlled through calibration; however, this is not the case for the uncertainty due to the metrologist.

- Avoidance of errors.

Error conditions often occur when one or more process parameters deviate significantly from the expected value and the quality of the process degrades. The sensitivity of the process to these variations in operating conditions depends on the point in the measurement process at which they occur, as well as the specific characteristics of a particular process disturbance.

Information from process parameters can be used to monitor the condition of a measurement operation, as well as to provide a process control signal to a feedback algorithm. If any of the key process parameters deviate, an error occurs.

- Promote the automation of measurement process

The achievement of MAL4 requires the automation of metrology process as part of manufacturing process. It involves the use of real-time, low latency orchestration of Infrastructure Elements (e.g., robotic arms, scanners…) to improve the accuracy and efficiency of measuring and recording physical dimensions and parameters. Automated metrology systems can help streamline and optimize various stages of the measurement process, from data collection and analysis to reporting and quality control.

One of the most important challenges related with the automation is related with the management of the large amounts of data that needs to be managed and processed in order to act upon physical elements.

A more particularised list of objectives of scenario 2 of Use case 1 is described using the table below, which aims at explaining their impact and their effect in value (being 1 no significant and 5 very significant).

Table 12. Specific objectives of Use case 1 – Scenario 2

OBJECTIVE	DESCRIPTION	IMPACT	EFFECT OF VALUE	
Remote tactile operation	Remote tactile, low latency operation, requiring fast response communication protocols for reliable, fast and secure operation.	High operational efficiency Improved safety for metrologists.	**Cost**	5
			Efficiency	4
			Quality	2
			Flexibility	5
			Innovation	3
			Sustainability	3
Real-time monitoring and operation for machine error compensation, ensuring the accuracy of dimensional inspection	Fast response compensation, real-time data analysis.	Consistence in the quality of the service. It saves human and economic resources	**Cost**	4
			Efficiency	4
			Quality	5
			Flexibility	5

			Innovation	5
			Sustainability	4
Avoidance of errors	Real time data monitoring and analytics will allow early detection of deviations and act upon them.	Consistence in the quality of the service. Higher reputation among customers.	**Cost**	4
			Efficiency	5
			Quality	5
			Flexibility	3
			Innovation	3
			Sustainability	4
Automation of measurement process	Promote MAL4 cognitive production lines by the automation of measurement process.	Higher productivity and manufacturing efficiency Consistence in the quality of the service Avoidance of human errors Improved safety	**Cost**	5
			Efficiency	5
			Quality	4
			Flexibility	5
			Innovation	5
			Sustainability	4

3.1.5.2.3. aerOS in Scenario 2

In the use case scenario 2, aerOS is expected to be used for the following purposes:

- Data management: aerOS will provide CMM metrological data management (point clouds…), providing interoperability and traceability.
- Networking: workload communication and load-balancing within CMMs, self-* capabilities during CMM operation.
- Hardware resources registry, CMM updates detection, registering of the status of CMM elements.
- Artificial Inteligence (AI): AI will be used to optimize the sequence of a CMM measurement process and the orchestration of its resources.
- Analytics: aerOS is expected to provide advanced analytics on the performance of CMM resources, anomaly detection and predictions.
- Cybersecurity: aerOS will provide the latest cybersecurity toolset to protect CMM machines and its operation.
- Privacy: provide privacy in CMM access to the network
- Trust and Data Sovereignty: aerOS will provide mechanisms and technologies to ensure trust in CMM communications and data transfer.
- Policy Services: providing remote access and authorisation control to the CMM equipment.
- Management toolset: aerOS will provide a management toolset to the CMM equipment, promoting its predictive maintenance and dynamic management of CMM components and resources.
- Master Database: the CMM equipment will provide metrological and CMM components performance data to the master Database of aerOS.
- Task Collector: aerOS will provide decomposed task requests to the CMM equipment.
- Task assignment: aerOS will assign tasks to the CMM equipment based on AI and ML techniques.

This will promote the improvement and the quality of the functionalities offered by the metrological software M3MH, which are shown in the figure below:

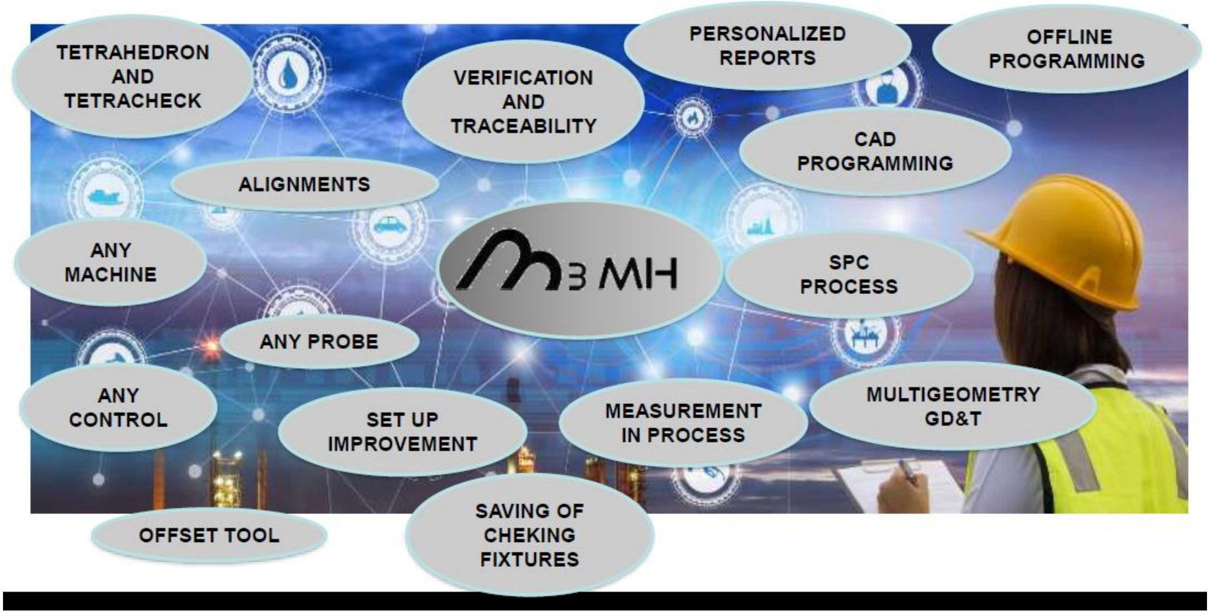


Figure 24. M3MH improved functionality with aerOS

3.1.5.2.4. Actors involved in Scenario 2

The actors involved of this use case have been collected following the table below, representing the actors involved, business area impacted, together with the type of impact and what it consists of.

Table 13. Actors involved in Scenario 2 of Use case 1

ACTOR	B$ AREA	TYPE OF IMP.	IMPACT DESCRIPTION
Metrologist	Manufacturing	Direct	The use case will enable the metrologist to balance their workload. Moreover, it will protect them from exposure to industrial facilities' hazards, as the remote operation will avoid the need for workers to travel to the site

3.1.5.3. Use case Scenario 3: AGV swarm zero break-down logistics & zero ramp-up safe PLC reconfiguration for lot-size-1 production

3.1.5.3.1. Description

Scenario 3 in Use case 1 is primarily conducted by partners SIEMENS, MADE and POLIMI. It represents a real Digital Factory where digital technologies are integrated with a Lean vision of logistics and production processes. The area exploits, in a real production line, the advantages deriving from the use of digital tools such as Industrial IoT, Cloud, Data Analytics, Collaborative Robotics, Virtual Commissioning, Product and Process Digital Twins. A concrete demonstration of how these new technologies are the enabling factors for the innovation of processes, products and the 4.0 operator, is expected, making it possible to create and sustain the company's competitive advantage.

The Digital Twin currently existing in the use case site allows to thoroughly analyze the characteristics of the production process and the product, prevent design errors and predict final performance. At the same time, it becomes an enabling technology for new methods of analysis and business models. The Lean 4.0 systematic approach defines a lean and agile factory where to implement several “4.0” technologies, tracking waste and reducing its generation. Logistics 4.0 solutions exploit IoT, RFID and advanced automation technologies to create an efficient, coordinated flow of material and a flow of information useful for the control and continuous improvement of the system.

Idea 1

The AGV results must be operatively efficient as much time as possible. One solution to optimize it could be introducing data-based analysis and AI/ML based orchestrator to optimize AGV travels based on the assembly capacity of the line and to the quality control area one. Here one of the problems is that the AGV leaves the loading area even for a single valve once the order has arrived. The problem is that if another order arrives immediately after there is no way to save a trip to the AGV and on the other hand the system does not consider the bottlenecks dictated by the assembly capacity and the testing capabilities. This theme is currently not managed, or rather it is simulated via the Digital Twin and the system should be manually reprogrammed to be more efficient. I could be interesting to try to introduce artificial intelligence which, using historical data on orders and the maximum capacity of the plant, estimates how many valves it makes sense to take on an AGV trip and try to get close to saturation in assembly and testing. aerOS would greatly help for this to happen.

Idea 2

It is conceived a scenario in which one of the internal supply chains is saturated, and it is decided to outsource production by loading it onto the other: the sharing of logistics data (position of the AGV and reference of the order in charge) would allow current-time tracking of the order. If it is possible to predict the saturation of the lines, we can implement a make-or-buy scenario.

Global description of the scenario:

The main goal is to explore how a production line can be flexibly adapted by modifying a specific process step for a particular task and seamlessly transitioning back to the previous production line using a decentral intelligent cloud system called EDGE. The Connectivity between all components can be achieved due to a fast, secure and modern 5G Network.

The production steps that could be modified and transitioned among are:

- *Step 1*: Automated Ground Vehicle (AGV) on a Specific Production Line an AGV is assigned to perform tasks on a specific production line, ensuring the smooth flow of operations. Step 2: AGV Receives Three New Packets from the Post Station. The AGV receives a notification to collect three new packets from the post station, which contain important components for an ongoing production task.
- *Step 3*: At this moment, the AGV downloads the associated software package from the cloud and is enriched with a functionality that enables the detection of physical packets on a pallet.
- *Step 4*: Thanks to the new software package, the AGV is now able to recognize the packages and their size through its integrated camera using AI algorithms. Since such algorithms are very GPU-intensive, they are calculated by outsourcing the algorithms in the cloud. Due to the fast 5G connectivity, cloud computing has hardly any latency.
- *Step 5*: AGV Identifies Interruption Point in its Production Line Using advanced sensors and visual recognition systems, the AGV locates an appropriate point in its production line where it can safely interrupt its current task.
- *Step 6*: AGV Drives to the Post Station and Collects the Packages with precise navigation and motion planning algorithms based on local resources on the device. The AGV autonomously drives to the post station, ensuring a safe and efficient path. It collects the three packages containing the required components.
- *Step 7*: AGV Utilizes Robotic Arm to Unpack the Payload Equipped with a versatile robotic arm, the AGV efficiently unpacks the payload from the packages, ensuring careful handling of delicate components and materials.
- *Step 8*: AGV Transports the Payload to the Target Destination Using its integrated mapping and path optimization algorithms, the AGV navigates through the production environment to deliver the payload to its designated target destination.

- *Step 9*: AGV Returns to its Primary Production Line and Resumes Work Upon successful delivery, the AGV retraces its path back to its primary production line. It carefully integrates itself back into the workflow and resumes its original tasks, ensuring minimal disruption to the overall production process.
- *Step 10*: The AGV can detach the robotic arm and all the other physical components to continue with different tasks, e.g. to charge its battery or picking and placing another object to another place, while the detached physical components proceed with its actions at their current station.

Aspects to Note: Safety, Motion, Non-Destructive Inspection (NDI), Security Throughout the entire process, the AGV prioritizes safety by adhering to predefined safety protocols and utilizing obstacle detection systems. The motion planning algorithms ensure smooth and efficient movement, minimizing any potential collision risks. Non-Destructive Inspection techniques may be employed during the payload unpacking process to ensure the integrity and quality of the components. Additionally, security measures such as authentication protocols and encrypted communication channels are implemented to protect sensitive data and prevent unauthorized access.

This use-case scenario showcases the benefits of incorporating robotics into flexible production lines, enabling efficient adaptation to changing tasks while ensuring safety, motion optimization, non-destructive inspection, and security throughout the entire process.

Figure 26. The AGV can detach itself and act similar to a pallet truck

Figure 25. Depending on the company and situation, the AGV can be configured with a wide variety of hardware

3.1.5.3.2. Specific objectives

TECHNICAL OBJECTIVES

Optimizing AGV travels and a smart make or buy scenario the company will for sure have decreased energy consumption, Reduction of lead time of the product, increase efficiency of production line, decrease of idle time and Increase awareness of the production processes that will for sure lead to Decrease of costs, reducing time to market, increase of reliability of the company due to a better performing production chain.

SOCIAL OBJECTIVES

The solution will allow for a better management of critical situations inside the plant, such as plant blocks due to exaggerated saturation, that would lead to better security and work life for employees, managers and operators.

1. Flexible usage of factory assets like a robot arm
2. Reduce the risk of workplace accidents by eliminating the need for manual lifting and handling of boxes.

3. Enhance agility and adaptability by using aerOS to seamlessly manage the software and hardware resources needed for the task.
4. Optimize network capabilities to ensure the uninterrupted operation of the AGV, robot arm, and AI vision software.

The use case scenario aligns with these objectives by automating a previously manual and potentially risky task. By using AI vision and automated machinery, the process becomes more consistent, and efficient. This aligns with the objective of improving efficiency. The use of machinery and automation also reduces the risk of workplace accidents. Ultimately, sustainability is enhanced by reusing existing production assets in multiple working areas while decreasing investment costs and ensuring flexibility.

The specific objectives of this use case are described using the table below, which aims at explaining their impact and their effect in value (being 1 no significant and 5 very significant).

Table 14. Specific objectives of Use case 1 – Scenario 3

OBJECTIVE	DESCRIPTION	IMPACT	EFFECT OF VALUE	
Optimizing AGV travels	The AGV results to be busy most of the time. One solution to optimize it could be introducing data based analysis and AI/ML based orchestrator to optimize AGV travels based on the assembly capacity of the line and to the quality control area one. Here one of the problems is that the AGV leaves the loading area even for a single valve once the order has arrived. The problem is that if another order arrives immediately after there is no way to save a trip to the AGV and on the other hand the system does not consider the bottlenecks dictated by the assembly capacity and the testing capabilities. This theme is currently not managed, or rather it is simulated via the Digital Twin and the system should be manually reprogrammed to be more efficient. I could be interesting to try to introduce artificial intelligence which, using historical data on orders and the maximum capacity of the plant, estimates how many valves it makes sense to take on an AGV trip and try to get close to saturation in assembly and testing.	Optimizing AGV travels and a smart make or buy scenario the company will for sure have decreased energy consumption, Reduction of lead time of the product, Increase efficiency of production line, Decrease of idle time and Increase awareness of the production processes that will for sure lead to Decrease of costs, reducing time to market, Increase of reliability of the company due to a better performing production chain.	**Cost**	4
			Efficiency	5
			Quality	3
			Flexibility	2
			Innovation	4
			Sustainability	4
Flexible usage of factory assets like a robot arm	The factory assets like a robotic arm has a specific task to do. Due to aerOS rescheduling capabilities, the factory gets instructed to free that asset for a short period. In this period the asset can be used in a complete new production use case scenario (e.g., box unpalletizing).	This saves cost and does not create the need to buy new resources that would not be used efficiently (long wait periods until next product arrives)	**Cost**	4
			Efficiency	3
			Quality	2
			Flexibility	5
			Innovation	4
			Sustainability	5
Enhance agility and adaptability by using aerOS to seamlessly manage the software and hardware resources needed for the task.	New Business Models can be achieved through the flexibility aerOS introduces. Hardware resources can be utilized most efficient based on the current task No one solution fits it all enables dedicated software for better quality	Changing software and rescheduling hardware resources does use resources most efficient	**Cost**	2
			Efficiency	1
			Quality	2
			Flexibility	0
			Innovation	0
			Sustainability	0

Optimize network capabilities to ensure the uninterrupted operation of the AGV, robot arm, and AI vision software.	The flexibility and modularity of the fac-tory design, requires the integration of wireless and wired infrastructure to build up the communication networks that the different resources require. Those integrated and heterogenous net-works must addition-ally provide guaran-tees of bounded latency and packet loss, needed for achieving high availability of the connect-ed resources.		**Cost**	5
			Efficiency	4
			Quality	4
			Flexibility	5
			Innovation	4
			Sustainability	5

3.1.5.3.3. aerOS in Scenario 3

aerOS is a decentralized system that provides the flexibility and adaptability to meet the changing needs and requirements of organizations. In some cases, these needs may require not only software, but also hardware solutions. For example, an automated guided vehicle (AGV) needs to pick up a mobile robot arm and deliver it to the operation area with the packages. Once the robot arm arrives, it needs to be reconfigured with new software through aerOS to perform an unpacking task.

To support this task, aerOS can seamlessly add the necessary hardware and software resources (skills) to the IEs. This includes not only the robot arm as an asset, but also the software needed to control it and enhance it through AI. aerOS can also provide the AGV with the capability to deliver the robot arm to the operation area, ensuring a seamless transition from one task to another.

Additionally, aerOS can retune the local 5G network capabilities to maintain service availability during this specific transition. By doing so, aerOS ensures that the network can support the increased demand for resources during the unpacking task. This helps to maintain a high level of service quality for users of the system.

Also interesting is the sub use case of aerOS equipping the AGV with AI technology utilizing onboard hardware accelerators to detect boxes and deliver to the operation:

1. The AGV is equipped with onboard hardware accelerators and cameras that allow for the detection of boxes through AI technology.
2. The aerOS software orchestrate the detection process by selecting the necessary hardware resources and providing the software resources.
3. The AI technology is trained to detect and classify boxes according to specific parameters, such as size, shape, or color; tailored for the specific box pickup use case.
4. Once the boxes are detected, the AGV picks them up and navigates to the operation site using the onboard AI technology and aerOS software.
5. At the operation site, the robot arm is now needed for the further succession of the complete task. This is done by the AGV and communicating with the respecting factory line providing the robot arm
6. In order to activate the skill of integrating the boxes into the factory line the robot arm needs different software skills orchestrated by the aerOS
7. After completion of the task, the robot arm is returned to its previous working slot by the AGV. Also, the software needed for the previous work of the robot arm is reallocated by aerOS disengaging further use of the specific box unloading software.

Overall, this process relies on the integration of onboard and external hardware accelerators, AI technology, and aerOS software to enable the AGV to detect, pick up, and deliver boxes to the operation site while seamlessly coordinating with the factory line equipment.

Underlying software assets and functionalities are provided either by Siemens proprietary software solutions or open source software assets from ROS.

The strength of aerOS lies in its ability to be tailored to specific requirements. As new tasks arise, aerOS can modify the installed apps to meet them, ensuring that the system stays up-to-date with the latest needs and requirements. To effectively manage these changes, SIEMENS is utilizing aerOS optimization algorithms. These handle the allocation of new and the re-allocation of existing tasks over a changing infrastructure automatically using e.g., Mixed Integer Programming and Deep Reinforcement Learning.

3.1.5.3.4. Actors involved in Scenario 3

The actors involved of this use case have been collected following the table below, representing the actors involved, business area impacted, together with the type of impact and what it consists of.

Table 15. Actors involved in Scenario 3 of Use case 1

ACTOR	B$ AREA	TYPE OF IMP.	IMPACT DESCRIPTION
System integrator	Manufacturing	Direct	Deployment and configuration of aerOS tools and interfaces into the physical assets and ICT infrastructure of pilot plant
Blue Collar Workers	Unpalletizing	Direct - Less work	The work is replaced by a robot arm and the Blue Collar Worker can focus on other more sufficient tasks in the production
Manufacturing	Factory Engineering	Direct - Keep more flexibility in mind when designing production assets like robot arms and working areas (e.g. unpalletizing area)	Factory assets now can have multiple purposes. This introduces new challenges in engineering mechanical interfaces while lowering the number of overall assets to maintain
Management	Restructuring / adaptability	Direct	New possibilities to interact with existing factory assets

3.1.6. Requirements of the trial

Below there is a list of the specific requirements identified for this trial. A full list of all the requirements gathered (in M9) for Pilot 1 as a whole are available in Appendix B.

- Real time data management and response
- Computing resources (cloud & edge)
- Low latency communication between edge devices and with cloud
- Secure communications between edge devices and with the cloud
- Compatibility among heterogeneous devices and industrial machinery
- Interoperability of the technology, which enables a various kind of data, IoT-Devices and interfaces.
- Support for various types of devices, even at different levels
- Real time data management and response
- Computing resources (cloud & edge)
- Low latency communication between edge devices and with cloud

3.1.7. Outcomes of the trial

After the completion of the activities of the pilot, when fulfilling the objectives above by the partners of the use case, the expected outcomes of the trial are as follows:

- <u>Secure industrial edge management services for green manufacturing & logistics.</u>

Result: Meta Operating System running in a manufacturing production line.

The implementation of aerOS for green manufacturing and logistics will enable local data processing at the edge of the network, reducing latency, bandwidth and storage costs, and improving data security and privacy. It will allow centralized management of all connected edge devices and applications, which reduces maintenance and updating costs, enhances security patches, and enables scalability and flexibility, leveraging advanced analytics and AI to optimize environmental impact of production processes and their performance.

- Smart management services for zero-touch ZDM

Result: Metrology solution which leverages underlying meta Operating System (aerOS).

The implementation of aerOS will enable the use of advanced metrology solutions and inspection tools to monitor and control the quality of products and processes in real time. This will allow the integration of big data analytics, artificial intelligence, and digital twins to detect and prevent defects, optimize production parameters, and reduce waste and rework, providing a platform for developing and deploying customized metrology applications and solutions for different industry types and use cases, based on state-of-the-art technologies and open-source software.

- Safe industrial edge automation services & self-optimisation reconfiguration services

Result: Assembly systems in the line with new software installed (aerOS)

aerOS will enable local and secure data processing at the edge of the network, which improves data security, privacy, and latency, thus allowing centralized management of all connected edge devices and applications, which enhances security patches, scalability, and flexibility. In addition, the self*- components of aerOS will enable the use of self-optimizing functions to monitor and control the quality of products and processes in real time, and to adapt to changing production targets and customer needs. Thus, it will allow the integration of reconfigurable tooling and fixtures to support flexible and versatile assembly systems for different products and variants.

- Increase the data processing capacity of the IoT edge-cloud continuum for smart manufacturing services.

Result: Digital Twin fed by aerOS features.

The implementation of aerOS will enable faster and more reliable data processing at the edge of the network, where IoT devices generate and consume data, reducing latency, bandwidth, and storage costs, thus allowing seamless integration and orchestration of edge and cloud computing resources, where users can leverage cloud-based services and platforms for advanced analytics, artificial intelligence, and digital twins to optimize production processes and performance. aerOS will provide a flexible and scalable computing continuum that can support workload mobility and adaptation to different industrial scenarios and requirements, such as security, privacy, reliability, and efficiency.

As expected benefits, aerOS will allow manufacturing lines (represented by MADE, POLIMI, INNOVALIA, NASERTIC and SIEMENS) to have:

- It will promote the reduction of carbon footprint and CO_2 emissions in manufacturing processes and logistics.
- It will improve the performance of CMM operation, reducing the time and costs for quality control processes.
- It will promote the industrial automation level, reducing the human intervention and allowing the self-monitoring of a process.
- Increased efficiency and productivity due to the use of on-demand AI technology that can detect and classify boxes.
- Reduced risk of workplace accidents since the AGV is equipped with onboard sensors and cameras that can detect and avoid potential hazards on its path.
- Enhanced flexibility and adaptability to changing factory line conditions, as the AI technology can be retrained to detect new types of boxes or handle different tasks as needed.
- Reduced labor costs as the AGV can perform tasks that would otherwise require human intervention, leading to a more cost-effective and efficient operation.

3.1.8. KPIs related to the trial

Same as for the requirements, it is only the goal in this section to make a bullet pointed list of the KPIs that have been identified. This exercise helps understand the relevant aspects of the pilot that the execution activities will be paying more attention to.

- Robustness of the production process.
- Accuracy of CO2 Footprint prediction.
- CO2 footprint measurement.
- CO2 emissions reduction.
- AGV use.
- AGV availability.

3.1.9. Legal framework

During the course of task T2.3 (Legal and regulatory analysis and governance specification), several actions have been performed in order to identify the legal framework surrounding activities in Pilot 1. As the main result of this action, find attached in Appendix C.1.

Besides that, a thorough analysis of the legal and regulatory aspects affecting the different scenarios of Use case 1 was performed, outputting the following results:

EU-wide regulations

- EU GDPR: European General Data Protection Regulation (2016). Data privacy law which applies to any organization that processes the personal data of EU residents, regardless of where the organization is located. The regulation aims to protect the fundamental right to privacy by setting out strict rules on how personal data must be collected, processed, stored, and deleted. The GDPR requires organizations to obtain explicit consent before collecting and processing personal data, provides individuals with the right to access and correct their data, and mandates that organizations report data breaches to authorities within 72 hours.
- EU Directive 2014/53: regulatory framework established to ensure the safety and compatibility of radio equipment placed on the EU market. It covers a wide range of radio equipment used for communication, broadcasting, remote control, and signal processing, as well as their accessories and components. The directive sets out essential requirements for conformity assessment, market surveillance, and the placing of CE marking on compliant equipment. It also includes provisions for the protection of privacy and personal data, as well as measures to ensure traceability of equipment to its manufacturer or importer. The main objective of the directive is to ensure that all radio equipment placed on the EU market is safe, does not cause interference with other equipment or networks, and meets the necessary standards for health and safety. Since this is a directive, each country transposed it into national laws, which will later be covered for each demonstrator.
- EU NIS Directive 2016: cybersecurity law that aims to increase the security and resilience of network and information systems across the European Union. As it is a directive, it requires EU member states to establish their own national framework for the security of network and information systems, and to designate competent authorities to oversee and enforce these frameworks. The directive also requires operators of essential services and digital service providers to take appropriate measures to manage the risks to the security of their networks and information systems. Again, due to this regulation being a directive, each country transposed it into its national legislation system.

National-wide regulations

Scenario 1: Green manufacturing (zero net-energy) and CO2 footprint monitoring

Since use case site of Scenario 1 takes place in Switzerland, the following regulations apply:

- Ordinance on Telecommunications Installations (OTI) and "Radiocommunication Ordinance": these laws are homologue to EU Directive 2014/53, but since Switzerland is not a member of the EU it did not directly transpose it. Instead, Switzerland adopted these two ordinances, issued by OFCOM (Swiss Federal Office of Communications), which set out the requirements for the placing on the market and the use of radio equipment in Switzerland.
- About data regulation: Switzerland has its own data protection law (FADP - Federal Act on Data Protection), which regulates the processing of personal data by setting out rules for the collection, use, and disclosure of personal data by both private and public sector organizations. Of course, if a Swiss organization should process personal data of EU individuals, the EU GDPR applies, as it has extraterritorial effect.
- Federal Act on the Protection of Critical Infrastructure: law that aims to protect critical infrastructure and essential services in Switzerland from cyber threats and other risks. It is homologue to EU NIS Directive 2016.

Demonstrator 2: Automotive Smart Factory Zero Defect Manufacturing

Since Use case site of scenario 2 2 takes place in Spain, the following regulations apply:

- General Telecommunications Law: regulates telecommunications services and networks. It sets out rules for the management, operation, and use of telecommunications networks and establishes the regulatory framework for the Spanish telecommunications sector. The law defines the roles and responsibilities of various public and private entities involved in the provision of telecommunications services and includes provisions related to the allocation and use of radio frequencies, the protection of consumers' rights, and the promotion of competition in the telecommunications sector.
- Royal Decree-Law 188/2016: implementation of EU Directive 2014/53. The decree establishes the regulatory framework for the placing on the market of radio equipment in Spain and sets out requirements for the conformity assessment, labeling, and market surveillance of radio equipment. It also includes provisions related to the use of radio frequencies and electromagnetic compatibility to ensure the efficient functioning of the internal market for radio equipment and the protection of public health and safety.
- Royal Decree-Law 12/2018: implementation of EU NIS Directive 2016.

Demonstrator 3: AGV swarm zero break-down logistics & zero ramp-up safe PLC reconfiguration for lot-size-1

Since Use case site of Scenario 3 takes place in 2 production lines, one in Italy and another in Germany, the following regulations apply:

Germany

- German Radio Equipment Act (FTEG): implementation of EU Directive 2014/53.
- Act on the Federal Office for Information Security and on Information Technology in Federal Administration (BSIG): implementation of EU NIS Directive 2016.
- Telecommunications Act (TKG): regulates the provision of telecommunications services and networks, the allocation of radio frequencies, the protection of personal data and privacy, and the consumer rights of telecommunications users.

Italy

- Legislative Decree No. 128 of 2016: implementation of EU Directive 2014/53.
- Legislative Decree No. 65 of 2018: implementation of EU NIS Directive 2016.
- Codice delle comunicazioni elettroniche: regulates the provision of electronic communications services and networks, including fixed and mobile telephony, internet access, and broadcasting. It sets out the rules on access to and use of network infrastructure, interconnection, numbering, spectrum management, and radio frequency allocation.

3.2. Pilot 2: Containerised Edge Computing near Renewable Energy Sources

3.2.1. Trial general description

Use case 2 will be driven by partners CloudFerro (CF) and Electrum supported by SRIPAS as technical partner targeting applicability of **aerOS for carbon aware computing**. It will determine impact project's results can have on the carbon emissions generated by the European cloud industry. It will also verify aerOS ability to set up and manage dynamic federation of heterogeneous infrastructure resources.

This pilot will address the management of containerized edge data centres developed by CF and located directly at energy sources, connected to the smart infrastructure and providing cloud continuity. It will be deployed and validated at renewable energy centres operated by ELECT, in Poland.

The pilot will proof applicability of aerOS for set up and management of cloud-edge architectures distributed between "big" central clouds and small edge nodes located directly at energy producing locations, gathering information and events from the deployed smart devices. The edge nodes will have connectivity to the private cloud infrastructure of CF.

By pursuing these goals, we will verify how aerOS answers needs highlighted by EU in European Green Deal and Europe fit for the digital age priorities. Both initiatives signify growing need for sustainable solutions in edge-cloud industry. Energy intensive nature of traditional data centres makes it less and less feasible to expand operations by buying, or building, more space, as indicated by DAIRO. Traditionally, resource-demanding services (e.g., AI) have been deployed in the cloud. Thus, approaches based in decentralized edge devices, such aerOS, may improve performance. By leveraging aerOS cloud industry will be able to take advantage of potential benefits for including numerous far and near edge nodes located at renewal energy producing locations, (thus, rapidly scaling operations), while keeping computing/storage capacity due to orchestration capabilities.

The trial will require deployment of hardware and software components at multiple locations. For efficiency, there is the intention to leverage existing "big" traditional cloud infrastructure operated by CloudFerro and compliment it with containerized edge nodes. While CF's traditional clouds are a mature technology, that undergoes incremental changes, the containerized edge nodes are still in development. Their architecture may change substantially overtime.

Clouds to hold part of the trial are located in TIER 3 complaint data centers with PUE (power usage effectiveness) between 1.5 and 1.7. Exact efficiency will depend on cloud selected. On the component level, CF's infrastructure is built using state-of-the-art, industry leading parts and solutions. From server grade GPUs (A6000s and A100s) to Supermicro motherboards to power supplies.

Current vision for the **containerized edge node** architecture involves singular UPS (uninterruptible power supply – energy container to support 15 minutes of operation) per 6 physical server racks in a single edge node. Within these 6 racks we will install between 20 and 40 compute nodes and several storage nodes.

On the **system level** planned cloud edge system will range from **OpenStack** that manages traditional clouds with CEPH for storage to **bare metal Kubernetes** deployments in the edge nodes. It is yet to be decided what storage solution will be applied in the distributed edge nodes.

The trials will take place at the hybrid or single source DER installation (two locations), where the case of containerized data center and its power management system will be tested. Electrum will design and install the required power connection infrastructure with the hybrid power management controller for the data center (Grid, ESS and PV/Wind generators).

The data sources include energy meters, weather sensors and data concentrators that collect multiple power parameters from all electronics devices installed at given facility. Electrum will provide the Renedium Master Power Controller - responsible for calculations of active and reactive power of whole plant. Renedium 1.0 is a regulator certified to meet NC RfG requirements, used to regulate active and reactive power of the entire facility according to various criteria. Additionally, Electrum will provide the industrial edge computer with neural network accelerator to test the Company's distributed architecture platform – EMACS2.0 - Virtual Power Plant.

3.2.2. Current problems/barriers area and motivation

aerOS Consortium, represented in this use case by CloudFerro and ELECTRUM, see emergence of edge computing as a way of building more sustainable and optimized cloud computing services. There is the plan of the cloud provider in the Consortium (CF) to geographically and topologically distribute computing resources in a network of edge nodes. In our vision a single node will have a power consumption between 50 and 100 kW (what translates to 5 to 10 server racks), that can be powered by a single windmill or PV farm. It will allow CF to enforce a new paradigm: instead of moving Watts of Power, we will move Bits of Data. With this approach, CF can lower the carbon footprint of certain Infrastructure and platform services and offer a solution for the problem of energy grid congestion/overload.

At the moment CloudFerro is in the process of developing and building its cloud-edge system. MVP (minimal viable product) of the service that leverages edge computing is to be launched in the Q1 2024. It has been defined as a serverless data processing engine, dedicated to batch-type of applications. At first, CloudFerro will be the main customer of this service. CF's satellite Earth Observation data repository and related workload will be able to saturate initial set of edge nodes. In next steps, there is the plan to introduce more stakeholders from the European space industry, followed by customers representing other domains.

Although, in preparatory activities there haver been identified a number of risks and barriers in regulatory, technical and managerial domains. However, it is believed that with the support of the innovations by aerOS, all these will be successfully overcome.

- Supply Chain disruptions
    - Key Driver: Current and Future supply chain disruptions can slow down technology development and deployment of the pilot.
    - Mitigation: Established relations with providers, long-term procurement plans, reusing the existing hardware.
- Shortage in Professional Competencies
    - Key Driver: A shortage of competent professional personnel and competition with industry leaders in this regard can slow the development and deployment of the system and drive costs up.
    - Mitigation: Leveraging existing European initiatives (e.g.: HiPEAC), creating attractive work environment and benefit systems, assuring knowledge retention and redistribution in the organization.
- Interoperability
    - Key Driver: Interoperability between technology stacks owned by different stakeholders is a must to enable operations on a large scale.
    - Mitigation: Maximize use of existing, well-established technologies and protocols (e.g.: K8S API or Liqo). Creation and adoption of industry de-facto standards.
- Regulatory Landscape and Cross-Territorial Consistency
    - Key Driver: Deployment of services in a geographically distributed edge-cloud system can be limited by specific national/regional norms and laws. Localized rules or regulations could slow down or prevent deployment of the system.
    - Mitigation: Analysis of the current landscape and interaction with stakeholders. Collaboration across European actors, including MS, industry leaders and policy makers to establish common norms and regulatory standards.

Table 16. Current problems and barriers in UC2

CHALLENGES or BARRIERS	DESCRIPTION	AREA	IMPACT IN THE COMPANY
Procurement	Long delivery times for IT components	Purchasing	Risk mitigated by updating milestone dates
Supply chain disruption	Current and Future supply chain disruptions can slow down technology development and deployment of the pilot	Purchasing	Risk of reduced adoption
Shortage in Professional Competencies	A shortage of competent professional personnel and competition with industry leaders in this regard can slow the development and deployment of the system and drive costs up.	Technical support	Lower production capacities and outdate of skills and competences
Interoperability	Interoperability between technology stacks owned by different stakeholders is a must to enable operations on a large scale.	Manufacturing	Integration issues resulting in diminished turnover.
Regulatory Landscape and Cross-Territorial Consistency	Deployment of services in a geographically distributed edge-cloud system can be limited by specific national/regional norms and laws. Localized rules or regulations could slow down or prevent deployment of the system.	Manufacturing	Adjustment to regulation prevents from expanding.

3.2.3. Participant partners

CloudFerro (CF):

CF provides next generation cloud services dedicated to specific domains and industries. CF delivers and operates cloud computing platforms for specialized markets such as the European space sector, climate research and science. CF offers flexible, open source based, cost effective cloud solutions in a public, private or hybrid model, customized to meet user needs. CF will be the early adopter and first user of the service that leverages the aerOS federation capability. It will deploy Earth Observation data processing on the created cloud-edge system.

ELECTRUM:

ELECTRUM is an APC (Alternative Power Creator) offering creative engineering solutions at every stage of the investment for the renewable energy sector. ELECTR carries out projects along the entire value chain and throughout the life cycle of the project and assets: Development – EPCM – Asset Management & ESCO – Reinvestment & Repowering.

The aerOS project's exploitable outcome for Electrum are two test field locations where the implementation of the IoT-Edge-Cloud operating system is to be deployed and tested across Micro Edge & Far Edge IoT sensors installed across PV and Wind power generating installations with initial data processing on-premises running on Industrial AI Edge Computers as well as Cloud High Performance Computing operations in the distributed container-based data centers provided by Consortium Partner - CloudFerro. The result type of the outcome is a demonstrator (Outcome Category - Research Achievement), where the power management system designed by Electrum for the distributed on-premises data centers can be tested, validated and certified. The demonstrator will allow autonomous management of the power balance between grid connection and local renewable energy generation capacity across two power park locations being under Operating & Maintenance service by Electrum. The aerOS objectives are in-line with the goals of a major internal R&D project at Electrum - the development of the Virtual Power Plant Solution. The VPP solution was designed to manage the distributed energy mix with the highest possible economical and energy efficiency. Based on microservices and supported by Machine Learning Operations, all of it enabled by an underlying meta

Operating System (aerOS), the VPP solution is a completed software + hardware package delivered as Infrastructure as a Service and / or Software as a Service, offering ultimate data security and new autonomous features highly increasing the efficiency of the renewable energy mix. The platform architecture features data integration across Micro Edge - Far Edge IoT devices, Edge AI Computing and distributed Cloud / HPC data centers, providing virtually unlimited scalability.

SRIPAS

Systems Research Institute of the Polish Academy of Sciences (SRI PAS) conducts studies in broadly understood systems analysis, encompassing analysis, modelling, optimization and decision making concerning complex – composite, multi-aspect and multicriteria problems. It has experience in the area of distributed systems and AI/ML. SRIPAS expectations is to increase rankings in the academic areas through publications, participations in the conferences, to gain recognition in the areas of research covered by aerOS and to build collaboration with the industry.

3.2.4. Data sources, existing software and available hardware

The data sources, existing software and hardware that have been detected so far to be used in the Pilot 1 of aerOS are as follows. The next list reflects only a summary of the minimum aspects detected so far. A far more thorough description is included in the current stage of the Trial Handbook (online) of the pilot. In addition, it is worth noting that these descriptions will be fully disclosed in the next deliverable of this task (T2.2, deliverable D2.3):

Data sources

- Earth Observation data from Copernicus and Sentinel (JSON and XML in an access to be selected)
- Energy consumption data of computing machines received via MQTT.

Available software (that aerOS will somehow need to be aware of / interact with):

- OpenStack Ironic (Bare metal provisioning software)
- Kubernetes container orchestrator
- Ceph (storage cluster in a distributed cluster foundation)
- OpenStack

Available hardware:

The use case deployment edge-cloud infrastructure (i.e., WAW 2-1 and, potentially, FRA 1-1), monitoring and administration tools, data repositories and processing chains, front end portals and dashboards for processing disposition. CF cloud infrastructure is federated in the framework of the Gaia-X project. The deployment will make use also use the Everything Monitoring and Control System software for energy source and throughput monitoring and reporting tool, already in use in ELECT premises.

Hardware infrastructure already available:

In order to retain as much control as possible over the entire production cycle, CloudFerro’s practice is to assemble infrastructure internally and to restrain from leveraging ready to use server nodes. Thus, it is not possible to provide an exhaustive list of hardware components that can be used for the AerOS project. Fluctuating prices and availability – or lack thereof – of certain brands and configurations necessitate flexibility in hardware building. However, our team's experience and established connections with providers guarantee optimal selection. Projected equipment costs are based on the current state of the market and projected changes in the costs of hardware components required for building and maintaining operational cloud infrastructure. Following types of components are required: CPUs, HDD storage drives, SSD storage drives, Server chassis, Network interfaces, Power supplies, RAMs and GPUs.

Infrastructure and technology to be acquired during the project:

CloudFerro – Servers and racks assembled from COTS, according to current state-of-the-art in the industry.

Electrum – Industrial Computer with Nvidia Orin Nano NX 16GB SoM; AC160Amp Power Connection; Fiberoptics network connection.

3.2.5. Objectives, benefits and expected results

In the following sub-sections there is a thorough description of each one of the scenarios in Pilot 2.

3.2.5.1. Use case Scenario 1: Green Edge Processing

3.2.5.1.1. Description

Green Edge Processing scenario aims to deploy two federated edge nodes and a private CF cloud located directly at renewable energy premises, and connected to different smart devices and data sources from wind and PhV farms operated by ELECTRUM. Managing the system shall be performed in energy, network and self-conscious manner, measuring the reductions provided (benchmarking of parameters based on real-time own analytics in the IE) in the orchestration of tasks deployed in the edge instead than in the cloud (e.g., AI). With the changes in requirements for computing resources, available energy or network throughput, aerOS will facilitate rapid changes (self-scalability, self-automation) in task distribution though orchestration (managing topology, tasks and services).

Primary goal of this use case, apart from creating and managing cloud-edge continuum, is to **test aerOS capacity for carbon-aware computing**. By shifting movable compute tasks between different locations, based on current and projected energy availability, we want to manage carbon footprint of our services. This includes edge nodes powered by windmills or photovoltaic farms and traditional "big" data centers powered by energy from the grid with green certificates. To do it, scheduling with real-time adjustments that can take into account changing circumstances every hour or so is required. Another logical step to do is shifting computing tasks across time. There is the aim of having aerOS using predictions about how heavy workload will be and what type of energy will be available to create task queues.

Of course, not every type of computing job can be managed this flexibly. Fortunately, CloudFerro as the operator of the biggest Earth Observation data storage and management platform in Europe, deals on every-day basis with abundance of batch-type of processing tasks.

At the moment, CF offers its users "*DataGeneration-as-a-Service"* that allows them to process satellite images/measurements using any of the pre-selected applications. This processing is performed in two modes:

- Vest-effort: free of charge service with a limited pool of resources allocated to it. New orders are placed in a queue based only on time, no SLA are provided.
- On-demand: Commercial service, that gives user the ability to set the desired time for execution of the processing

Both modes are deployed on Kubernetes cluster in CF's traditional cloud.

For the **Green Edge Processing** scenario, there is the aim of defining and deploying a new service. It will allow users to execute their own applications (delivered as docker images) for batch processing of Earth Observation data. There will be no moderation in the application content. As in the case of VMs of other container-based services, there will not be direct access to it. In their requirements, user will be able to define how fast they need the results, where (topologically and geographically) processing should be performed and what should be the renewable energy usage rate for their processing. Depending on these factors, price will be automatically determined.

Most important characteristic of a task in this service is its limited execution time. In order to efficiently populate the system, there is the need of having workload that is movable and in batches. It comes with an additional advantage and requirement: efficient usage of available cloud resources. This kind of service does not allow for over commitment of resources, typical for big clouds. To keep it commercially viable, there is the need of utilizing (thus, selling) resources at a much higher rate. Our current estimations suggest that the desired level of consumption is north of 80%.

3.2.5.1.2. Specific objectives

The objectives of this use case are described using the table below, which aims at explaining their impact and their effect in value (being 1 no significant and 5 very significant).

Table 17. Specific objectives of Use case 2 – Scenario 1

OBJECTIVE	DESCRIPTION	IMPACT	EFFECT OF VALUE	
Carbon footptrint reduction and increased CPU utilization	Ability to process data when and where the carbon footprint of the activity is the lowest.	Mitigation of carbon emissions generated by cloud&edge services. Positive environmental impact that mitigates the risk of slowing down the deployment of European ICT resources, due to new regulations. Decreased costs of operations for service providers, by maximizing use of cheaper, renewable energy.	**Cost**	1
			Efficiency	1
			Quality	1
			Flexibility	2
			Innovation	2
			Sustainability	2

3.2.5.1.3. aerOS in Scenario 1

aerOS will support the management and utilization of IoT-edge-cloud infrastructure by introducing the concept of computational continuum and smart orchestration. It will enable to deploy applications in the continuum and execute computational jobs in a reliable and adaptable manner. The aerOS Server would be reading data from our SCADA database table (lakehouse architecture) and managing access permissions for any data recipient or sharing client.

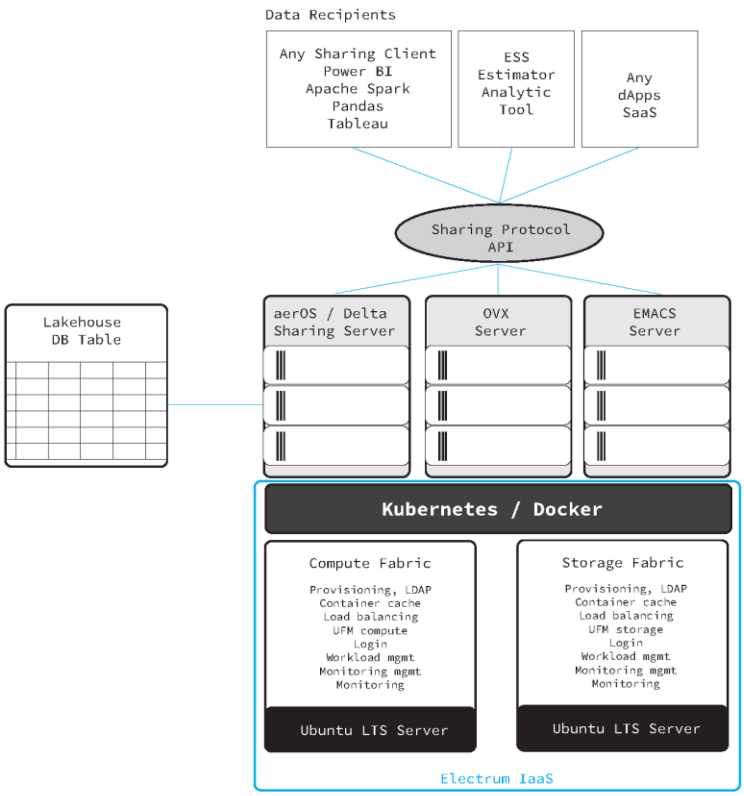


Figure 27. aerOS in scenario 1 of Use case 2

It will allow specific applications to benefit from frugal techniques in improve energy efficiency

- aerOS will be used for distributing, monitoring and relaying tasks of stateless processing allowing execution of batch or FaaS-like activities among a pool of near and far-edge nodes located at ELECT renewable energy premises (e.g., wind/photovoltaic farms, hydro energy or high capacity batteries).
- aerOS will make use of heterogeneous information in the orchestration and scheduling model (master DB and registry will be needed along the task collector and distributor), boosting the energy and resource optimization. aerOS will allow for definition and implementation of energy and network conscious management tools and procedures.

- aerOS capability to manage dynamically changing infrastructure environment will be tested.
- Proposed application shall also result in lower capital intensity of the system, allowing the operator to abandon redundancy at a node level and assuring it on system wide level, as tasks of a failing node can be transferred to an operational one.
- aerOS will enable managing the system in energy, network and self-conscious manner allowing for reductions in real-time analytics efficiency.

3.2.5.1.4. Actors involved in Scenario 1

The actors involved of this use case have been collected following the table below, representing the actors involved, business area impacted, together with the type of impact and what it consists of.

Table 18. Actors involved in Scenario 1 of Use case 2

ACTOR	B$ AREA	TYPE OF IMP.	IMPACT DESCRIPTION
Clients/End-user	Any	Direct	Must align his/her workload to specific requirements of aerOs managed processing.
Data Providers	Management	Indirect	Must enable data source for aerOS workload to interaction with.
Business Development	Marketing&Sales	Direct	Must define aerOS-related product/service and include it in its offering.
SysAdmin	Engineering	Direct	Must implement and maintain aerOS capabilities
Developer/Integrator	Engineering	Direct	Must implement aerOS across the continuum
User support	Support	Direct	Must incorporate aerOS functionalities into its practices, prepare and perform relevant staff training.
Energy source owner	Management	Indirect	Must review its business model and align it with aerOS consumption mode.

3.2.5.2. Use case Scenario 2: Secure federation of edge/cloud

3.2.5.2.1. Description

This use case considers the aerOS capability to create secure ad-hoc resource federations composed from heterogeneous edge nodes and traditional “big” clouds. It will build on top of the use case scenario 1 and extend the federation beyond infrastructure owned by a single actor. Simultaneously, it will on-board multiple, independent tenants and execute unmoderated (thus, not trusted) workload provided by these tenants. It means that the main challenges of this scenario are in security and data and information management domains. Secure federation scenario will leverage aerOS functionalities that will be developed within work packages 3 and 4 – WPs that tackle cybersecurity and data privacy. Additionally, integrating 3rd party-owned resources will verify aerOS’ interoperability.

3.2.5.2.2. Specific objectives

The objectives of this use case are described using the table below, which aims at explaining their impact and their effect in value (being 1 no significant and 5 very significant).

Table 19. Specific objectives of Use case 2 – Scenario 2

OBJECTIVE	DESCRIPTION	IMPACT	EFFECT OF VALUE	
Security across	Resilience of the	Introduction of new providers to the	**Cost**	3

the federation	cloud-edge federation against breaches	federation is easier, thus limits the cost of operations. It also increases the trust of stakeholders in the system. Streamlining activities.	**Efficiency**	1
			Quality	5
			Flexibility	2
			Innovation	2
			Sustainability	1
Separation between tenants / security of users	Measures of digital separation of physical infrastructure to accommodate multiple tenant	Better management of users, access control and less risk of threats and vulnerabilities	**Cost**	3
			Efficiency	1
			Quality	5
			Flexibility	2
			Innovation	2
			Sustainability	1

3.2.5.2.3. aerOS in Scenario 2

The main focus of this use case scenario will be on testing and verifying aerOS meta-operating system's basic unit capabilities - IE. Infrastructure Element will be the building block that provides virtualization layer, over heterogeneous infrastructure resources. It will provide runtimes environment for the remaining elements of the systems as well as for the user applications. Crucial requirement in this scenario (comparing to scenario 1) is tenant separation. We understand it as an ability of Infrastructure Element (or wider aerOS) to create secure, individual environments for multiple users within common infrastructure nodes. These environments should be able to accommodate un-moderated workload – user can provide application docker images without supervision of the system administrator.

Additionally, we expect IE to be interoperable in their deployments. Scenario 2 foresees federation of varied infrastructure resources, especially at the edge. Moreover, aerOS will be used not only to virtualize bare metal servers. It will also be used to connect big clouds – managed with established cloud software – or edge nodes with a virtualization layer already existing (e.g.: Kubernetes on Ironic).

- A preliminary list of aerOS components to be used in the scenario 2 is:
- IAM – identity and role management
- Autonomous management
- Federated Orchestration
- Traceability
- Security, Privacy and Trust

In the second iteration of the use case planning, a detailed deployment description of these components will be provided.

3.2.5.2.4. Actors involved in Scenario 2

The actors involved of this use case have been collected following the table below, representing the actors involved, business area impacted, together with the type of impact and what it consists of.

Table 20. Actors involved in Scenario 2 of Use case 2

ACTOR	B$ AREA	TYPE OF IMP.	IMPACT DESCRIPTION
Technical Support	Maintenance	Direct	Must prepare and conduct workshops for staff
Management	Administration/strategy	Indirect	Must include use of aerOS in the strategic planning

System architect	Technical Development	Direct	Must include aerOS capabilites in the system architecture
Sales	Marketing & Sales	Direct	Must devise new product/service aimed at edge node providers
System administrator	Maintenance	Direct	Must learn aerOS capabilites and prepare relevant monitoring practices
Security expert	Security & Compliance	Direct	Must review aerOS security approach and synchronize with company practices accordingly

3.2.6. Requirements of the trial

Below there is a list of the specific requirements identified for this trial. A full list of all the requirements gathered (in M9) for Pilot 1 as a whole are available in Appendix B.

- Scheduling with real-time adjustments support
- Shifting computing tasks across time
- Support for execution of user applications/jobs
- Application/job conditions definable by the user
- Support for movable workload in batches

3.2.7. Specific measurable outcome of the trial

After the completion of the activities of the pilot, when fulfilling the objectives above by the partners of the use case, the expected outcomes of the trial are as follows:

- Reduction in energy consumption due to the transfer of AI and real-time analytics to the edge nodes. And
- Flexibility and scalability of the aerOS concept portability in the IoT edge-cloud continuum.

Result: Meta Operating System running in the edge data centers of a cloud provider company.

- Definition and implementation of energy and network conscious management tools and procedures.

Result: Tools that can be used by Energy Operators.

As expected benefits, aerOS will stakeholders and partners involved in the Use case 2 (SRIPAS, CF and ELECTRUM) will have:

- It will promote the reduction of carbon footprint and CO_2 emissions in containerized data centres.
- Technological expertiseExperience in real environment deployment will be a learning opportunity and possibility to evaluate lab tested solutions for the team and company.
- Collaboration on an up-to-date problem coming from developing industrial area

3.2.8. KPIs related to the trial

Same as for the requirements, it is only the goal in this section to make a bullet pointed list of the KPIs that have been identified. This exercise helps understand the relevant aspects of the pilot that the execution activities will be paying more attention to.

- CPU utilization.
- Carbon awareness.

- Number of edge nodes.
- Total workload distributed and executed.

3.2.9. Legal framework

During the course of task T2.3 (Legal and regulatory analysis and governance specification), several actions have been performed in order to identify the legal framework surrounding activities in Pilot 1. As the main result of this action, find attached in Appendix C.2.

In addition, as part of the legal framework to be considered as requirement for Pilot 2, some local requirements were identified and are documented in the next paragraphs:

Electrical engineering, design, construction and testing performed in this Use case 2 shall comply with the latest applicable laws, decrees, administrative regulations, standards and technical regulations. All the installations shall be realized in accordance with the standards of professional practice and in respect of the specifications and local standards.

Monitoring and Control System should be manufactured, tested and shall be operated in accordance with the latest edition of the corresponding standards listed below:

- IEC 61000 Electromagnetic compatibility (EMC)
- IEC 60068-2 TC 104 - Environmental conditions, classification and methods of test
- IEC 61724 Photovoltaic system performance - Part 1: Monitoring
- IEC 60529 IP ratings
- IEC 62262 Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)
- IEEE 1379-2000 Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation
- IEC 60870-5-series Telecontrol equipment and systems - Part 5: Transmission protocols
- IEC 61850 Communication networks and systems for power utility automation IEC 61400-26-1 Time based Availability for Wind Turbines
- IEC 61400-26-2 Production based Availability for Wind Turbines

Listed in this chapter standards and specific codes should be treated as minimum requirements, but should not be limited to (this statement will be bear in mind by pilot partners during all the execution of the trial). Monitoring and Control system should be manufactured and tested to comply with national and local regulations, and should fulfil requirements of the local Grid Operator. In case of any discrepancies between the specifications and other documents, the more stringent specification requirements should be applied. The proposed solution should be given in good time to the Owner or Engineer for review.

3.3. Pilot 3: High Performance Computing Platform for Connected and Cooperative Agricultural Mobile Machinery (e.g. in Agriculture, Construction, Forestry) to improve Enable CO2 footprintNeutral Farming (HPCP-F)

3.3.1. Trial general description

Use case 3 will beis driven by partners **John Deere** and **TTControl** targeting to develop a High-Performance Computing Platform (HPCP) for Connected and Cooperative Mobile Machinery which has the potential to reduce the CO_2 footprint in areas like agriculture, construction, or forestry. The HPCP use case will be deployed and validated in John Deere's European Technology Innovation Center in Kaiserslautern.

The target of the HPCP use case is to develop a proof-of-concept of a High-Performance Computing Platform providing a machine-to-machine connectivity from everywhere for a large-scale agricultural production system on one side, but also delivering certain real-time performance stillwhile navigating the overall system remotely and controlling (i.e., supervising) execution of the agricultural work process. The required network connectivity everywhere and always is still a challenge. Edge computing in connection with locally limited and temporary networks will be needed as enabler for autonomous machine fleets.

Connected and cooperative agricultural mobile machinery is a key to synchronize and optimize the mobile machinery work. This use case will contribute to enabling sustainable farming solutions for energy optimisation and noise reduction. The developed solution will be capable to e.g., perform computational tasks in support of demonstrating fully electric swarm of vehicles safely and securely operating e.g., in platooning or other swarm combinations. The solution will bring higher performance and connectivity capabilities vs. existing solutions brought to the mobile machinery. Usage of ing IoT services also edge computing is foreseen for more semi real-time control critical tasks like e.g., identifying field borders in during the operation of the overall system. to e.g., to enable real-time control.

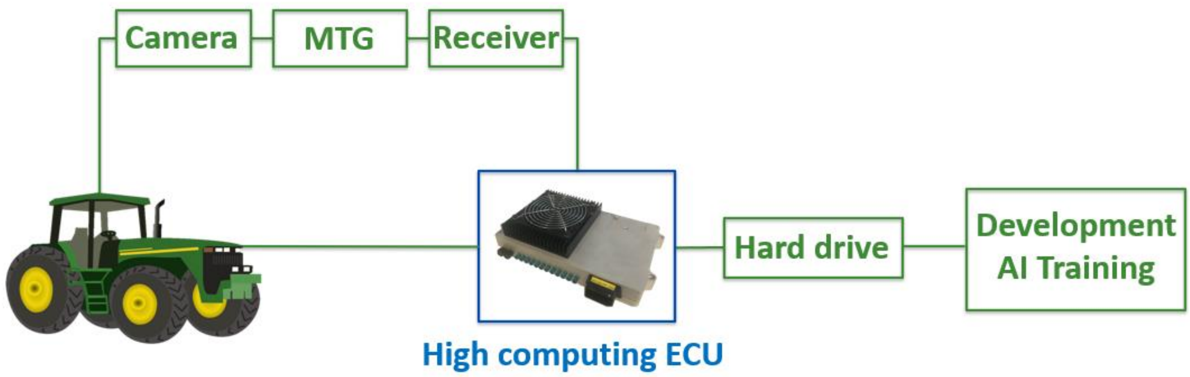


Figure 28. Preliminary setup of the demonstration of the HPCP Use Case (Pilot 3)

The main objective of the HPCP use case is to integrate, test and validate High-Performance Computing Platform for connected and cooperative mobile machinery e.g. farming, construction, and forestry. The proposed robust and flexible solutions need to provide M2M connectivity from everywhere for large-scale production systems; semi real-time performance with low latency networking; federated AI capabilities to improve performance in the edge and data management including autonomy (self-automation), ownership (trust for origin needed), storage and interoperability. This use case will contribute to enabling operation solutions for road building and sustainable farming with optimized energy input.

In particular, the pilot is for analyzing the already existing field work and find a room for improvement via the provided Electronic Control Unit (ECU) with high computing power from TTControl. Such tasks in agriculture and construction work that require collecting data from different components and analyzing it whether on-board or off-board, can highly benefit from an ECU with high computing power in its overall analysis of the field work aiming for optimization and performance enhancement.

Faster and optimized field work based on analyzing data that requires high computing power such as images with the help of the incorporated ECU with high computing power. This will help enabling elevation of the features of an existing field work that has been performed manually, such as, crop monitoring.

- Collecting and analyzing various types of data from different sources (components that are usually connected to the machine/vehicle), such as positioning and location information via the receiver, network status and type via a cellular modem, images via cameras. This will result in a detailed knowledge about the running system and make the end user's job easier, faster, and smoother.
- Shifting to semi-automated field monitoring will result in shorter completion times and less errors that can originate from the lack of concentration and exhaustion form performing repetitive tasks manually., while assuring quality standards at the same time.
- Giving a chance for the end user to focus on other tasks that require attentive observation and management, and prioritize their daily tasks.

For achieving the previous, it is expected that the pilot will carry out the next actions:

- Collecting data from different sources (images, location, network status).
- Connect to a display for convenient human machine interaction.
- Data from cameras as well as operating instructions from cloud must be processed in a semi real-time manner.
- Improving the quality of field work e.g. by automating some of the time-consuming tasks.
- Optimizing machine work and reducing the added error of manual tasks
- Improving the end-user's experience
- Impact of machine learning and artificial intelligence techniques to be analyzed.
- Semi real-time data analysis for large-scale mobile machinery system
- Proof-of-concept for a data monitoring system on board that analyses live data flow.
- Deployment and validation of the TTControl's prototype connecting to the John Deere's devices.
- Investigation of the applicability of the aerOS edge meta-operating system SW architecture and compatibility of the designed use case with the overall architecture of aerOS

3.3.2. Current problems/barriers area and motivation

Digital transformation in Agriculture, Construction, and Forestry is quickly progressing. Especially, Precision Operation (e.g. in farming known as "Precision Farming") offers a pathway towards reducing inputs, maximising quality of production and in farming also yields. Digitalisation allows integrated control of machines involved in production. At the same time, the operating mobile machines needs to interact with other production systems, sensors, and information services. Edge computing, in connection with limited / temporary networks (as connectivity in rural areas has current limitations), will enable the deployment of intelligence without permanent connectivity to the cloud (self-dependability).

A key enabler for optimized operation of machine fleets is synchronisation and optimisation of the work of all mobile machines (e.g. tractors, implements, combines in farming, pavers, rollers and trucks in road building, or forest harvesters and forwarders in forestry). Current systems, e.g., connected and cooperative mobile machinery, are pushed to resources limits, in tasks like data access and processing, ensure data privacy and security or provide continuity to the cloud. In-vehicle edge nodes (e.g., John Deere's Operations Center), interacting with smart devices, networking components and compute continuum, will benefit from the support provided by an IoT edge-cloud continuum solution. Applications of the aerOS system achievements can be applied in multiple business areas such as farming, construction, and forestry.

Especially but not exclusively, in farming aerOS can enable significant improvements of inputs through smart control and by this, the usage of the aerOS architectural concept might increase sustainability significantly.

Performing manually handled tasks in a semi-automated way with the help of AI training using images, or other form of data in the field and the help of the provided ECU with a high computing power, will significantly enhance user experience and will create an overall more sustainable solution than the ones present at the moment.

In order to further illustrate the problems/barriers that have motivated this use case in aerOS, and according to the personalized templates of Trial Handbook devised for the project, it was decided to utilise the following table:

Table 21. Current challenges and barriers in UC3

CHALLENGES or BARRIERS	DESCRIPTION	AREA	IMPACT IN THE COMPANY
Data collection	AI models require a large amount of data to be trained properly and perform in the way it is expected to.	Mobile machinery (e.g. farming machines, or construction machines)	More time required to obtain the information, larger resources and skills and efforts for labelling.
Live data analysis	Analysing data in real-time and comparing it to an existing trained model is a challenging task that require high processing capabilities	Mobile machinery (e.g. farming machines, or construction machines)	Huge investments, steep learning curve, time, resources and efforts. Challenging integration.

3.3.3. Participant partners

John Deere (JD):

John Deere is the brand of Deere & Company, the world's leading manufacturer of agricultural, forestry, construction, and turf and grounds care equipment, headquartered in the USA. Deere & Company employs approximately 79,000 people worldwide (2022) , has more than 100 plants , development and parts centers in 16 countries, and sells its products in more than 160 countries. As Germany's largest agricultural equipment manufacturer and a producer of road construction machinery, John Deere GmbH & Co. KG employs around 11,000 people at eleven locations in Germany.

The Intelligent Solutions Group at the European Technology Innovation Center (ETIC) investigates and develops future trends and technologies in the field of mobile agricultural and construction machinery in close cooperation with various research institutions. At the ETIC development center, engineers, IT, and marketing specialists are working on future technologies and "intelligent solutions" for precision agriculture and road construction. John Deere's contribution to aerOS will benefit the company itself in enabling further deployment of intelligence in mobile machines and optimizing the machinery work with the limited availability of resources. This contribution will also bring benefit to the project by allowing the aspired applications to be evaluated and validated using heavy machinery in different sectors (i.e., agriculture, construction, forestry), hence, examining the impact of the project in relation to important aspects nowadays, such as, sustainability in farming and the aspiration for reducing energy consumption nationally and globally. Which will help keeping the project up to date and diverse in terms of its impact application evaluation. In addition, John Deere is currently contributing to other European and national projects that are dealing with data on the edge, therefore, it can bring into aerOS the experience gained and lessons learned from previous projects.

TTControl (TTC):

TTControl GmbH (TTC), a joint-venture company of TTTech Computertechnik AG and HYDAC International, is headquartered in Vienna and belonging to TTTech Group, with an additional location site in Brixen, Italy. It supports its customers by offering consulting for application development, maintenance, and other support services. The company has a broad experience in commercial production projects within the area of electronic control systems in challenging conditions regarding their environment. The product portfolio comprises a range of Electronic Control Units (ECUs), electronic visualization units and human machine interface units.

With the nationally funded headquarter project MOBILE, TTControl was enabled to become an – also internationally – recognized centre in the area of mobile electronics, electronics control units and related software in particular in the Off-highway industrial domain. Furthermore, the development capacity has been raised significantly during the course of this project. Since several years, TTControl delivers reliable ECUs and display units to the off-highway community and in particular also to the farming machine, construction, municipal vehicles sectors which robustness and safety needs are especial.

Currently TTControl is involved in many research projects, standing out their participation in the H2020-ICT project called IntellIoT which aims at developing a framework for intelligent IoT environments that execute semi-autonomous IoT applications, which evolve by keeping the human-in-the-loop as an integral part of the system. TTControl also coordinates the Horizon Europe THEIA-XR project. THEIA-XR stands for Making The Invisible Visible for Off-Highway Machinery by Conveying Extended Reality Technologies at improving human-machine interaction in mobile machinery by enhancing user technology fit and extending reality technologies and functionalities. For more information about the research projects by TTTech group, and TTControl in particular, visit: www.tttech.com/innovation/research-projects

3.3.4. Data sources, existing software and available hardware

Overview of the hardware and infrastructure of the pilot:

From the side of the agricultural machinery stakeholder (JD – John Deere):

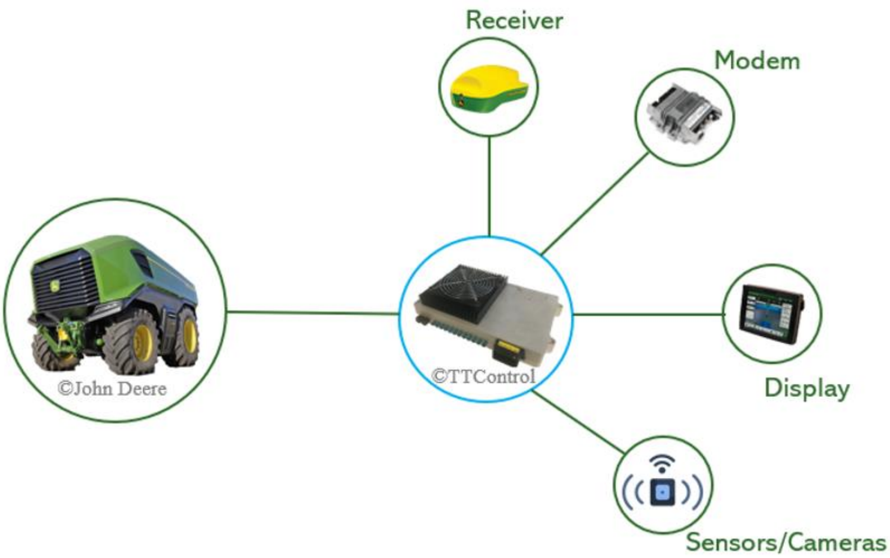


Figure 29. Pilot 3 preliminary hardware setup by agricultural machinery stakeholder

- GNSS receiver (Figure 29) providing location information and corrections for location accuracy (corrections are calculated upon communication with GPS). Information provided by the receiver can be viewed via the display and communicated to other connected vehicles depending on the running application.
- Modem providing cellular network connection to the vehicle and sending vehicle information to the cloud (fuel consumption, fuel level, location, engine state, working hours, etc).

- Display acting as an interface for user interaction, allowing the user to run different tasks on the vehicle and display various information about tasks, vehicle, and connected vehicles.
- Camera collecting images to be used for designing/developing a training model for crop monitoring.
- External hard drive to extract the collected images and pass them for training in the initial phase of the use case.
- Vehicle of John Deere (to be defined) where the ECU would be mounted. Integration and mounting of the provided ECU into the vehicle is expected to run seamlessly, as power and CAN connections appear to be compatible according to initial observations.

From the side of the technological stakeholder (TTControl): mandatory for the pilot components and interfaces are shown in blue like e.g. HPCP unit, remaining ones will be configured in the second year of the project.

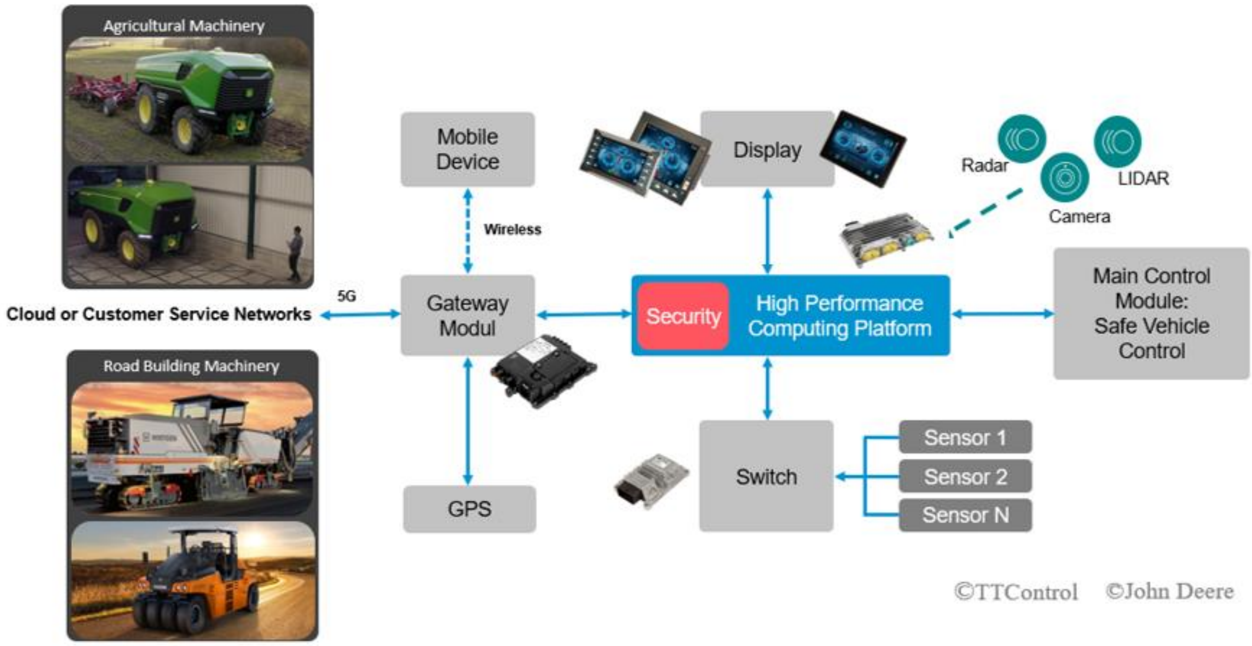


Figure 30. Pilot 3 preliminary hardware setup by technological stakeholder

- ECU platform (called High Performance Computing Platform in Figure 30 by TTControl incl. high-performance host containing a multi-core processor with hardware acceleration for AI and Machine Vision tasks, deliver extremely high computer performance and plentiful memory bandwidth (Jetson AGX Xavier-based Performance Host, Aurix TC3xx Safety Host, automotive connectors e.g. CAN-FD, data connectors, camera/video connectors, HDMI OUT, etc.)
- HW shall carry vehicle connectors and allow system wake-up via minimum one out of four CAN interfaces (Rationale: To reduce the complexity connecting multiple components together the connect is preferred to be used, as well as to eliminate a factor of human error)
- HW shall carry an ethernet switch with a minimum one 1000Base interface and dedicated high-speed connectors (Rationale: To satisfy the requirement for higher bandwidth, the HW shall support Ethernet interface)
- Mixed-criticality traffic for combination of fail-operational functionality with other communication
- Application hosting: the platform shall allow hosting applications (Linux as OS is possible for application hosting and orchestration)

The data sources, existing software and hardware that have been detected so far to be used in the Pilot 3 of aerOS are as follows. The next list reflects only a summary of the minimum aspects detected so far. In The deliverable D2.3 will provide an update regarding the HW and SW setup.

Data sources

- Data monitoring (e.g. JPG images processing on board based of trained AI model)- to be analysed in batch and semi real time
- Vehicle data monitoring (e.g. location, etc.)

Available software:

- Image processing tool to be defined by John Deere for image processing that enables detection of specific features/objects in the image.

Available hardware:

- High Performance Computing Platform (HPCP) prototype by TTControl to provide a connectivity and monitor vehicle subsystems.

3.3.5. Objectives, benefits and expected results

In the following sub-sections there is a thorough description of each one of the scenarios in Pilot 3.

3.3.5.1. Scenario 1: Cooperative large-scale producing

3.3.5.1.1. Description

The first scenario of Use Case 3 will optimize a large-scale production harvesting system based on mobile machines. Data from sensors (e.g., machine sensors, geo-positioning, cameras, radar) as well as operating instructions from cloud will be safely and securely processed. The basic development will be done on a sophistically selected machine fleet. A demonstration will be carried out with a mobile machinery vehicle. An IoT edge-cloud continuum approach will be adopted for the orchestration of services (AI/ML-based assignment), optimisation of data autonomy (with semantics) of a swarm of vehicles, each equipped with own far edge node executing aerOS (IE registry will play a key role here) and connected to the smart devices and sensors of the vehicle. The developed solution will be capable to e.g., perform computational tasks in support of demonstrating in the future swarm of vehicles safely and securely operating in platooning (up to TRL5), governed by a robust policy engine, which will be integrated and validated in the John Deere's functional **prototype** vehicle.

3.3.5.1.2. Specific objectives

The objectives of this use case are described using the table below, which aims at explaining their impact and their effect in value (being 1 not significant and 5 very significant).

Table 22. Specific objectives of Use case 1 – Scenario 1

OBJECTIVE	DESCRIPTION	IMPACT	EFFECT OF VALUE	
Optimizing field work[8]	Analyzing data that requires high computing power such as images with the help of the incorporated ECU with high	Elevation of field work that has been performed manually.	**Cost**	3
			Efficiency	5
			Quality	5

[8] The assessment of impact and effect value is performed for a single vehicle. In case of platooning (i.e. a swarm of vehicles operating with a joint goal), these positive effects might be at least multiplied by a number of vehicles or more (semi-automated operation with a supervising a driver for each of the vehicle has also a large impact which is, however, hard to calculate precisely).

	computing power		**Flexibility**	5
			Innovation	5
			Sustainability	5

The main objective of this scenario is to analyze the already existing field work and find a room for improvement using the Electronic Control Unit (ECU) with high computing power from TTControl, empowered by aerOS traits and provided to John Deere to realize the outcomes and KPIs established for the trial. Such tasks in agriculture and construction work that require collecting data from different components and analyzing it whether on-board or off-board, can highly benefit from an ECU with high computing power in its overall analysis of the field work aiming for optimization and performance enhancement.

3.3.5.1.3. aerOS in Scenario 1

In order to understand the role of aerOS to realize this scenario, a series of steps were analysed.

First, the TTControl's prototype of HPCP must be deployed in the John Deere experimental vehicle to ensure a proper connectivity and functioning of interfaces. The execution of the SW and sensor or camera data from John Deere would be essential to validate the performance, and if needed, necessary adaptations to be implemented. The subset of the tasks of this scenario described above require semi real-time execution and finding of proper allocation of tasks to optimize data communication latencies. Several parameters will be utilized to monitor e.g., energy consumption, resource allocation while performing data communication, or similar. The exact parameters for the evaluation, i.e., KPIs, are defined for two integration phases (Alpha and Beta).

Second, aerOS meta Operating System will be leveraged across edge (vehicles) and HPCP platform in order to allow the innovative applications sought for the scenario. Initially (current view by M9 of the project), there have been identified three potential areas of the benefits from the usage of the aerOS architecture concept (see Figure 31): (i) usage of common APIs to enable seamless application hosting and supporting the functional allocation, (ii) monitoring and real-time control or capabilities of the system in support of the time-aware execution of the tasks, and (iii) improvement of trustworthiness via implementation of a chain of trust on embedded software level which is needed for the future certification of TTC's products with regards to security measures (ISO/SAE 21434 standard to be considered). These are only few currently defined benefits from the usage of aerOS, however it becomes clear that a whole new world of computing possibilities will open up after aerOS successful deployment in the scenario. The incorporation of Linux-based approach for e.g., the monitoring of tasks / services will allow to investigation of further relevant services or functionalities from the project which could be potentially integrated or used in Pilot 3.

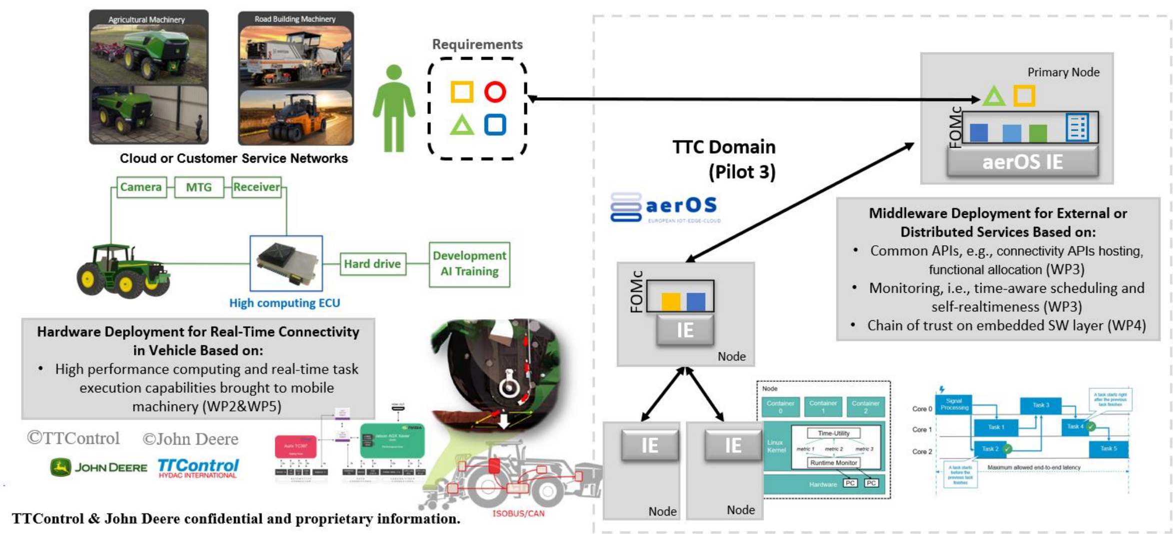


Figure 31. aerOS in scenario 1 of Use case 3

3.3.5.1.4. Actors involved in Scenario 1

The actors involved in this use case have been collected in the following table below, representing the actors involved, business area impacted, together with the type of impact and what it consists of.

Table 23. Actors involved in Scenario 1 of Use case 3

ACTOR[9]	B$ AREA	TYPE OF IMP.	IMPACT DESCRIPTION
Blue Collar workers (Farmers)	Agriculture	Direct	Potential shorter completion time of field work
Clients (Farm owners)	Agriculture	Direct	Potential shorter completion time of field work

3.3.5.2. Scenario 2: Basis for CO2 neutral intelligent operation (e.g., farming, construction, forestry)

3.3.5.2.1. Description

Basis for CO2 neutral intelligent operation (e.g. farming, construction, forestry): deploying of tasks in the edge, it is possible to reduce the latency and reaction time, by using low-latency networks like e.g. 5G. The benefit is also related with the energy consumption when transferring AI and real-time embedded analytics, what may reduce the CO2 impact. The scenario will measure in a collaborative swarm of vehicles the energy consumption reduction due to the use of aerOS and different federation topologies, considering how AI-supported approaches affect performance.

Figure 32. Example of data analysis in John Deere's operations Center

Other relevant considerations for describing scenario 2 of Use case 3 are the following:

- Data from sensors as well as operating instructions from cloud must be safely and securely processed

[9] It is important to note that the actors who are being referred to here (both inputs) are not directly affected by this use case unless it is implemented in a real-world scenario, which is not relevant for the course of the project. The collected data, held tests, and final demonstration would be carried out in a testing environment where no real clients are being involved or affected.

- Deploying of tasks in the edge
- Reducing the latency and reaction time, by using low-latency networks (e.g 5G), the benefit is also related to the energy consumption w0hen transferring AI and real-time embedded analytics, what may reduce the CO2 impact.
- The scenario will measure in a collaborative swarm of vehicles the energy consumption reduction due to the use of aerOS and different federation topologies
- Analyzing impact of AI-supported approaches for this scenario.

3.3.5.2.2. Specific objectives

Data and information from multiple devices and at least one autonomous or semi-autonomous mobile machines are processed on-the-go. aerOS-technology can principally be deployed to conventional commercial vehicles as well as to electrified machinery. In case of electric machines CO2 emissions from direct energy consumption can be significantly reduced. Further energetic improvements can be achieved by more precise operation and coordination with regard to optimized trajectories, positioning, and speed of one or more machines. Applications can be carried out at higher accuracies positively impacting overrunning surfaces and reducing outputs.

The objectives of this specific scenario are described using the table below, which aims at explaining their impact and their effect in value (being 1 no significant and 5 very significant).

Table 24. Specific objectives of Use case 3 – Scenario 2

OBJECTIVE	DESCRIPTION	IMPACT	EFFECT OF VALUE	
Connected machine and sensor/device data.	Massive data transfer and handling between mobile machinery and infrastructure for highly precise off-board operation	Reduced number of cabs: (i) Lower weight, and (ii) Reduced workload (1 operator of multiple machine). Path/trajectory planning optimized	**Cost**	3
			Efficiency	4
			Quality	3
			Flexibility	3
			Innovation	5
			Sustainability	4

3.3.5.2.3. aerOS in Scenario 2

The deployment of aerOS in this scenario is envisaged same as in scenario 1 (Section 3.3.5.1.3). In the next deliverable (D2.3), an update of this reflection will be provided, if needed.

3.3.5.2.4. Actors involved in Scenario 2

The actors involved of this use case have been collected following the table below, representing the actors involved, business area impacted, together with the type of impact and what it consists of.

Table 25. Actors involved in Scenario 1 of Use case 3

ACTOR[10]	B$ AREA	IMPACT	IMPACT DESCRIPTION
Operator in the Operations Center at John Deere	Mobile machinery and agriculture in particular	Indirect	Optimizing the operation of a fleet for energy consumption and CO2 reduction
End users with access to e Operations Center at John Deere	Mobile machinery and agriculture in particular	Indirect	Optimizing the operation of a fleet for energy consumption and CO2 reduction

[10] It is important to note that the actors who are being referred to here (both inputs) are not directly affected by this use case unless it is implemented in a real-world scenario, which is not relevant for the course of the project. The collected data, held tests, and final demonstration would be carried out in a testing environment where no real operators or users are being involved or affected.

3.3.6. Requirements of the trial

Below there is a list of the specific requirements identified for this trial. A full list of all the requirements gathered (in M9) for Pilot 3 as a whole are available in Appendix B.

- (Semi) real-time data analysis
- Local processing of data flow

3.3.7. Outcomes of the trial

After the completion of the activities of the pilot, when fulfilling the objectives above by the partners of the use case, the expected outcomes of the trial are as follows:

- <u>Semi-automated (i.e. with supervision) safe and secure execution at the edge node of the vehicles swarm.</u>

Result: Vehicles equip new hardware and software – HPCP and aerOS.

The pilot will demonstrate the process optimization in a closed loop of control ("vertical integration") ensuring semi-automated (i.e., with supervision) safe and secure execution at the edge (e.g. being integrated in the vehicle leading the swarm).

- <u>IoT edge-cloud continuum.</u>

Result: Meta Operating System now exists, abstracting underlying computing resources.

Creation of a IoT-environment providing real time, high bandwidth, and low latency connectivity in temporary networks based on next generation electronic building blocks of a safe and secure platform for more the execution of advanced automation application to support a grid-connected electric tractor system and control the swarm machines.

- <u>Enlarged open edge ecosystem.</u>

Result: Standard API for managing the continuum and creating new functionalities upon.

Enlarge open edge ecosystem of the aerOS project the pilot consortium focuses on standard-based interfaces (e.g. GMSL2) and widely available software elements (e.g. Linux-based) by integrating and orchestrating several applications for demand as services to enable the uptake of midcaps, SMEs and start-ups developing the relevant functions or services.

As expected benefits, aerOS will allow stakeholders of the agricultural machine use case (represented by John Deere and TTControl) to have, at least (but not limited to):

- Faster and optimized field work based on analyzing data that requires high computing power for processing e.g. images with the help of the incorporated ECU with high computing power. This will help enabling elevation of the features of an existing field work that has been performed manually.
- Collecting and analyzing various types of data from different data sources (components that are usually connected to the machine/vehicle), for exmaple positioning and location information via the receiver, network status and type via a cellular modem, images via cameras. This will result in a detailed knowledge about the running system and make the end user's job easier, faster, and smoother.
- Shifting to (semi-)automated field monitoring will result in shorter completion times and less errors that can originate from the lack of concentration and exhaustion from performing repetitive tasks manually, while assuring quality standards at the same time.
- Giving a chance for the end user to focus on other tasks that require attentive observation and management, and prioritize their daily tasks

3.3.8. KPIs related to the trial

Same as for the requirements, it is only the goal in this section to make a bullet pointed list of the KPIs that have been identified. This exercise helps understand the relevant aspects of the pilot that the execution activities will be paying more attention to.

- Performance with temporary network infrastructure
- Performance without using AI-supported application(s)
- Performance using AI-supported application(s)
- CO2 indicators

3.3.9. Legal framework

During the course of task T2.3 (Legal and regulatory analysis and governance specification), several actions have been performed in order to identify the legal framework surrounding activities in Pilot 3. Germany, where the use case will take place, is aligned with all relevant European directives.

The content of this analysis, as it includes information protected by companies' policies, is not delivered in this document. Further analysis will take place later, where it will be evaluated a proper summary of data to be potentially provided in deliverable D2.3.

.

3.4. Pilot 4: Smart edge services for the Port Continuum

3.4.1. Trial general description

The Smart edge services for the Port Continuum Use case (pilot 4) will be driven by the Industrial partner EUROGATE and the scenarios will be deployed and validated in the container terminal located in the Port of Limassol (EGCTL), the largest port in Cyprus, handling more than 90% of the container volume of the island, reaching approximately 300.000 TEUs per year. The terminal operates 24/7, servicing almost all container vessels of the island. Technically, EGCTL will be supported by partner Prodevelop (PRO) and the Cyprus University of Technology (CUT).

The equipment of the terminal consists of more than 35 rubber gantry cranes (straddle carriers), 5 empty container handling equipment, 10 terminal tractors and 5 Ship-To-Shore (STS) cranes. Two of the cranes were commissioned in 2019, are of type Super Post Panamax and have the capacity to handle two containers at a time (twin mode).

The Eurogate group develops and operates an in-house Terminal Operating System (TOS) which covers all operating aspects of the terminal, including vessel planning, cargo handling, cargo moves and machinery instructions, customs and Port Community System (PCS) interface and handling of dangerous goods. EGTL also operates a third-party maintenance management system.

Figure 33. Eurogate Container Terminal in the Port of Limassol – aerOS Use case 4

EGCTL has since starting operations, pioneered in the upgrade of the connectivity of the port systems, achieving a reduction of container clearance time from 24 hours to 15 minutes and an average import container delivery time of 20 minutes. Both of these achievements are a testament to the commitment of EGCTL to optimizing terminal operations and target of further improving the resilience of the terminal and the speed of operations.

In the above context, EGCTL is in the process of digitizing and automating more operations processes, such as creating an automated truck gate process. aerOS will be the starting point in creating scalable IoT infrastructure that the Terminal can build and expand in the future, as it is expected to connect more than two hundred devices in the next 5 years. The trial aims to generate the necessary knowhow in deploying scalable IoT systems and create a testing ground for AI technologies which can then be deployed both terminal wide and group wide (i.e., in one of the other twelve Eurogate terminals).

The Use case 4 has been divided in 2 scenarios (that will be described below) that, jointly, pursue the achievement of four objectives:

- Objective 1: To provide a digital platform for the port which can improve the traceability of assets in the terminal yard. To do so, proper data acquisition, transmission, and storage services should be guaranteed by aerOS.
- Objective 2: To support a heterogeneous set of Infrastructure Elements compliant with aerOS, from the lightweight IoT gateways such as RPis, up to the most-capable cloud servers (either private or public ones). Therefore, the minimum requirements for running aerOS operating system should not be very high.

- Objective 3: To provide a very accurate predictive maintenance service based on frugal AI models that are embedded in the aerOS stack.
- Objective 4: To provide a computer vision solution that can be inferred from the edge without requiring very high bandwidths. The aerOS orchestration should be smart enough to manage when these functionalities can be carried out in the edge devices dynamically, according to the actual IEs' capabilities.

3.4.2. Current problems/barriers area and motivation

Port container terminals and their logistic infrastructures are essential to keep the world-developed areas. At present it is considered that more than 90% of the world's trade is carried by sea[11]. Hence, the impact of this strategic sector in the quality of life of worldwide citizens is crucial, as freight transport is a powerful key driver for job creation and economic growth. Promoting innovation on efficiency, sustainability and safety of the port-container industry is a fundamental issue. In particular, the significant economic growth before and after the global COVID-19 pandemic crisis, as well as the increase of cargo volumes, have driven maritime ports into developing their capacities in unexpected ways. Shipping lines have always been the main stakeholders pressing for continuous port efficiencies, with new challenges arising coming from the strengthened ocean carrier alliances and the increased ship dimensions. On the one hand, shipping alliances, as a means of capacity rationalization, lead to further concentration and to decreased number of ports to call. Therefore, less ports are being required to serve more ships. On the other hand, those pressures are to intensify more as the dimensions of ships are continuously increasing. The average size of new containerships delivered has increased from an average of 1k TEUs (Twenty-feet Equivalent Units) in the 1970s to 7.7k TEUs ordered today[12]. As bigger ships mean also bigger volumes to be loaded/unloaded within small time-windows, this is also consequently impacting transferring congestion pressures towards container terminals[13]. Thus, this evolution has provided remarkable needs for the appropriate performance of container handling and logistics. However, operational missing links and bottlenecks remain, including among others performance inefficiencies, labor accidents, increased energy consumption as well as pollutant and Greenhouse gas emissions[14].

In parallel, the advancement of new digitization paradigms such as Cloud-Edge Computing, Internet of Things (IoT), Big Data, and Machine Learning (ML), have created new possibilities for the industry, leading to the well-known concept of Industry 4.0. In regards of the cargo handling industry, Industry 4.0 services, also known as Port 4.0, could improve processes by connecting all equipment and systems in real time, thus enabling seamless data exchanges. Under these new conditions, more automated and interoperable solutions could be achieved by the sector with less risk, at a lower cost, and faster lead-time. The aim of aerOS Pilot 4 is to provide and successfully test a cloud-edge continuum distributed system for container terminals that will efficiently tackle the mentioned challenges. aerOS shall provide an intelligent meta-OS for transforming container terminals' operations, using real data as a mechanism to support decision making and the generation of new incomes. Whereas the low latency applications, timely decisions and human-centric interaction are not possible with the cloud-centric architectures, aerOS will provide a cloud-edge continuum approach with secure services, allowing the industrial companies to alleviate the recurrent need to send the data to a central node, react faster to certain critical events deploying AI/ML close to the point of interest, extreme scale data governance and services, and improve scalability through decentralization.

In order to further illustrate the problems/barriers that have motivated this use case in aerOS, and according to the personalized templates of Trial Handbook devised for the project, it was decided to utilise the following table:

[11] International Maritime Organization, 2019. IMO profile
[12] M. Wackett, Global fleet capacity to bulge as more containerships are delivered in 2018, 2018.
[13] L.Nightingale, Tesco raises concern over bigger boxships, 2015.
[14] O. Merk, and T.T. Dang, Efficiency of World Ports in Container and Bulk Cargo (oil, coal, ores and grain), Paris, OECD Publishing, 2012.

Table 26. Current problems and barriers in UC4

CHALLENGES or BARRIERS	DESCRIPTION	AREA	IMPACT IN THE COMPANY
Poor data and telemetry digitization and analytics	Ports have a lot of equipment which provides sensor data, but these data are not stored and further used for decision making	Management/ Technical support	The lack of digitalization does not allow to gather insights for either better operational efficiency or reducing risky working situations
Fixed preventive maintenance periods	Cranes have a predefined maintenance time measured in hours (1000h), but sometimes there is a failure before period elapsed, and the port stops operations until crane's component is fixed.	Management / Technical support / Accounting / Warehousing	A larger time required to repair the equipment because the spares might not be available.
No computer vision features	There are several cameras installed across the port, but their video streams are not sufficiently exploited.	Management / Sales / Technical support / Customer relationships	Ports do not provide an automated quality check form about containers' status to their customers. If it is done manually, the required time for it is very high

3.4.3. Participant partners

EGCTL:

EUROGATE is Europe's leading shipping line-independent container terminal operator. EUROGATE actively address different challenges like globalisation and ever tougher competition among ports, continuous commitment and one hundred percent customer orientation. The handling of containers at seaports is the core business of EUROGATE. In 2020, EUROGATE handled 11 million TEUs at their different terminal locations. As a shipping line-independent container terminal group, EUROGATE operates sea terminals jointly with its sister company Contship Italia on the North Sea, in the Mediterranean region as well as on the Atlantic, with excellent connections to the European hinterland.

In addition to container handling, EUROGATE also offers a full range of "box"-related operations, from seaworthy packaging to container depot services, container servicing and container repair. EUROGATE's intermodal transport network links sea terminals in northern and southern Europe with the major European economic areas. EUROGATE Group has its head office in the Free and Hanseatic City of Bremen. In April, the Cypriot Transport Ministry and EUROGATE signed the contract for the takeover of Limassol Container Terminal. During this time, Eurogate has significantly upgraded the infrastructure and services offered at the terminal by reducing processing time and offering safe cargo storage and management until it is delivered to the recipient. The investment includes the purchase of two state-of-the-art "Super post Panamax" cranes capable of serving the world's largest container vessels as the Ever Given, as well as 17 new straddle carriers and two empty container stackers. In addition, an innovative IT system is connected to the Customs Department, Cyprus Ports Authority and shipping offices, reducing the processing time for containers, and releasing them for collection in just 20 minutes instead of 12-24 hours previously. Additionally, customers are now informed about container arrivals and pickup times via an online platform. Eurogate obtained in 2021 a top certification from the Cyprus Customs & Excise Department, the Authorised Economic Operator – Full (AEOF) Certification being the highest level of the Institution "Customs Simplifications, Security & Protection". Despite the reduction due to the Pandemic, a workload growth of around 10% was recorded in the past four years.

PRO:

PRODEVELOP, S.L. (PRO) is an SME employing more than 100 engineers (most of them computing, telecommunication, and cartography engineers), located in Valencia, Spain. The company has more than 25 years of experience. PRO is specialized in consulting, development, and operating solutions for the port and public bodies sectors as well as for private container terminals. The research lines at PRO include Internet of Things, big data management and interoperability, sensor systems, Edge/HPCs architectures, AI, as well as geospatial technologies, Web and service environments, and Digital Twins. PRO is a leader of Port Management Solutions at an international level.

During the last years, PRO has participated in several H2020 & HE projects like DICE, INTER-IoT, ASSIST-IoT, PIACERE, AIDOART, PIONEERS or MULTIRELOAD. Due to its participation in the aforementioned R&D and commercial projects, PRO has wide experience in data ETLs and representation techniques/tools, working with most the popular technologies and data formats in these areas: MQTT, Apache Kafka, WSO2, ELK stack, Qlik Sense or Power BI, StreamSets, NodeRed, etc., PRO has an interest on aerOS to enlarge the features and expertise around IoT, edge computing, and AI/ML in order to transform its outcomes in business. In particular, it is expected that the project will enable advanced frugal AI services to the POSIDONIA Terminal 4.0, our IoT and Big Data solution for Smart Ports, including ML-based predictive maintenance services for terminal CHEs, as well as improve our computer vision capabilities for different use cases such as detecting container IDs, or surface damages. her enhanced with in the field of predictive maintenance and computer vision.

Cyprus University of Technology (CUT):

CUT is a newly established public university founded by law in December 2004 and with its orientation towards applied research, the University aspires to establish for itself a role in support of the state and society in their efforts to confront problems, which cover all areas of science and technology. CUT has as its strategic target the design and development of research activities both within the University and in cooperation with other research Institutes in Cyprus and abroad. CUT has been ranked by the Times Higher Education among the top 301-350 universities in the world and among the 150-175 in Europe. In particular, according to the Times Higher Education World University Rankings,

CUT has established extensive experience coordinating and contributing to various projects related to maritime informatics and technologies, including the STM Validation Project (2014-EU-TM-0206-S), STEAM (INTEGRATED/0916/0063), and MARI-Sense (INTEGRATED/0918/0032). CUT will build on this experience and extend its knowledge towards the implementation of the "Smart Edge Services for the Port Continuum" use case of the aerOS project. The researchers from CUT aim to facilitate the digitalization of the container terminal, as well as develop machine learning models for predictive maintenance of quay cranes/straddle cariers and computer vision applications (e.g., detect container damage, distinguish sealed from non-sealed containers).

3.4.4. Data sources, existing software and available hardware

The data sources, existing software and hardware that have been detected so far to be used in the Pilot 4 of aerOS are as follows. The next list reflects only a summary of the minimum aspects detected so far. A far more thorough description is included in the current stage of the Trial Handbook (online) of the pilot. In addition, it is worth noting that these descriptions will be fully disclosed in the next deliverable of this task (T2.2, deliverable D2.3):

Data sources and associated software:

- Time-series data of the Quay cranes and Straddle Carriers of the EUROGATE Limassol port that will be stored every second, directly obtained from the PLC through MQTT or HTTP.
- Data from the tyre pressure monitoring system, vibration, hydraulic pressure, and acceleration sensors, road vibration sensors, oil and fuel levels, and power measurements. This data will be collected and handled at the far-edge (IoT Gateway) level.
- Terminal Operating System (TOS) data, to be used for feeding operational insights as well as training and validating predictive maintenance algorithms.
- Maintenance data from the Computerized Maintenance Management System (CMMS) exported as XLS and retrieved from APIs to gather information about the assets to be regularly maintained in the port, including equipment, materials, but also maintenance schedule and assigned workers.
- Video streams from yard IPTV cameras, including live video (via RTMP protocol) feed and file extracts (MPEG4-only for training purposes).

3.4.5. Objectives, benefits and expected results

In the following sub-sections there is a thorough description of each one of the scenarios in Pilot 4.

3.4.5.1. Scenario 1: Predictive maintenance of Container Handling Equipment

3.4.5.1.1. Description

Any industrial equipment wears out eventually, but if it is well-maintained, it would probably last longer. Originally, reactive maintenance was the regular process, which essentially addressed the repair of a piece of machinery only after it was broken down. However, it had many overhead costs that could be avoided. To name a few, the cost of unplanned maintenance due to equipment faults included a considerable amount of time wasted for responding to emergencies and diagnosing faults, so that would result in loss of production, as well as higher costs for parts commissioning and shipping. Preventive maintenance "looks ahead" to stop breakdowns before they occur by scheduling regular preventive maintenance cycles. With proper planning, technicians can ensure the best working conditions and prolong the expected life span for the equipment. In detail, preventive maintenance has traditionally been done using SCADA systems set up with human-coded thresholds, alert rules, and configurations about when machine conditions are at a state of needed repair or even replacement. However, either time-based or usage-based preventive maintenance may be addressing problems that do not exist, as maintenance is performed regardless of identified issues, leading to although planned, increased unnecessary downtimes. Furthermore, preventive maintenance requires a larger inventory management for replacement parts. Aiming at exploring options for improving maintenance strategies, and thanks to utilizing condition monitoring equipment and machine monitoring sensors, the performance assessment of assets can be realized with a more real-time, data-driven analytics approach. This new approach, namely predictive maintenance, utilises real-time health status knowledge and assessment, enabling the prediction of faults before they occur, thus not having to wait for equipment to breakdown (i.e., reactive maintenance), nor carrying out maintenance when it is not necessary (i.e., preventive maintenance).

With regards to the port continuum pilot, due to heavy loads, long periods of use, and a wide variety of weather conditions, Container Handling Equipment (CHE) (such as STS cranes, RTG cranes, Straddle carriers, or reach stackers) require an optimal maintenance process. However, the traditional preventive maintenance semi-manual approach does not consider more complex dynamic behaviours of CHEs, or the contextual data relating to the operational process at large. According to the previous needs, an accurate predictive maintenance system is pursued. Thanks to the latest advancements on Artificial Intelligence (AI), the implementation of machine learning (ML)-based solutions is seen as the next-step functionality that can lead predictive maintenance to major costs savings, higher predictability, and increased availability. The novelty of aerOS project becomes apparent when reviewing the state-of-the-art literature of AI predictive maintenance applied to the maritime sector. There is a current lack of scientific literature about AI in general, and ML models in particular, applied for the development of predictive maintenance solutions to container terminal machinery. Thus, while predictive maintenance as a tool is already being used in other sectors, terminal ports have still a long way to go into the digitalisation journey in order to benefit from implementing the proposed solutions to their machinery. The goal is that the trained ML algorithms will enable to detect anomalies and test correlations while searching for patterns across the various data feeds from OT (sensors, PLCs), and IT (TOS, CMMS, weather condition). But for that, like most ML works, sufficient historical data and expert knowledge will be needed to understand previous failures reasoning. This also includes general features, such as mechanical properties, average usage, and operating conditions.

The following components of the **STS cranes** will be used for the predictive maintenance tests on aerOS:

- <u>Trolley Wire Rope Enlargement Warning:</u> An early warning system will be put in place that monitors the discrepancy between the distance the limit switches of the trolley wire rope were positioned on the travel length of the boom with the distances that were stored in the first calibration of the machine. The warning system will predict in advance when it becomes faulty, allowing the Technical Department to plan for this issue before any undesired working condition.
- <u>Motor Filter Condition:</u> Currently, there is no analogue sensor measuring the temperature of the motor itself. Thus, a sensor monitoring ambient temperature and current load of the motor will be used to detect if the ventilation system is behaving adequately or requires replacement of the filter. The alerts

will be recorded by the CMMS software, and this will allow to use previous Dates/Times when the filters were replaced so that the system will be able to predict further replacements in advance.

- Motor Bearings Condition: Monitor motor speed as well as load and motor bearing housing temperature to determine if the bearings of the motor have degraded and require replacement (Sensor required).
- Motor load sharing from Hoist: Measure variability between the 2 motors, master and follower hoist motor to monitor that they share the load equally. This could indicate a misalignment of one of the motors, coupling degradation, motor degradation or closed loop control issue (Speed Encoder, Parameters, Inverter etc.).
- Tensioning Aux Cylinder Pressure Monitoring: This would check when the deviation between the 2 cylinders has increased greatly or avoid the disparity and notify personnel to check the wire ropes.

The following components of the **Straddle carriers** will be used for the predictive maintenance tests on aerOS:

- Generator engine efficiency: To calculate and monitor efficiency genset system by measuring power delivered to the engine in terms of fuel l/h and electrical energy produced. To do so, three main data inputs will be monitored: engine fuel consumption, generator output, and outdoor temperature.
- Genset vibrations: To monitor vibration on genset and predict if this is related to genset mounting failures, or engine injector issues. The main variables to be recorded are: genset vibration, generator output frequency, and generator output load.
- Inclination issues: To monitor the inclination of the straddle carrier during operation and send warnings if the system is behaving abnormally. The system should provide the main reason that could be due to e.g., suspension failing, tyres, etc. It will take into account not only machine inclination, but also load height, machine side frame speed difference, or if it is transporting a container or not.

Hydraulic system: Hydraulic Pressure Instability can indicate issues in the system, accumulator or pressure regulators that are faulty. Several pressure transducers will be placed on the machine to measure the system and alert if there is an anomaly based on the machine operation, including also parking brakes engaged or not, spreader motion ON/OFF and outdoor temperature.

3.4.5.1.2. Specific objectives

The general objective of use case scenario 1 is **to validate different frugal AI models[15] to (i) predict remaining useful lifetime (RUL) of assets with regression models, and (ii) to predict failure within a given time window with classification models** for **STS cranes** and **straddle carriers**. This can help to reduce downtime, increase efficiency, and save costs by reducing the need for regular manual inspections.

The system should also be able to provide real-time alerts to the users and system administrators when maintenance is needed. By using frugal AI models, the system can be more lightweight and less computationally intensive, which can be beneficial in situations where resources are limited. The envisioned frugal ML models of aerOS to be performed on the edge, would analyse the data on premise in real-time, reducing the amount of data to be transferred to the cloud, which in-turn would save businesses money on cloud storage costs.

Three frugal ML models[16] will be considered: “input frugality”, “learning process frugality” and “model frugality”. This general objective can be split into small specific objectives:

1. To retrieve telemetry data from 2 straddle carriers and 2 quay cranes every second. At the time of writing this handbook, tyre pressure, vibration, hydraulic pressure, acceleration, road vibrations, oil and fuel levels, and power measurements have been discussed.
2. To correlate the aforementioned telemetry data with the proprietary software solutions used in the terminal. In particular, the operational activities collected in the Terminal Operating System (TOS)

[15] Frugal AI refers to the use of simpler, more efficient models that can run on resource-constrained devices, such as those used in IoT gateways or embedded systems, which can learn with less data.
[16] M. Evchenko, J. Vanschoren, H. H. Hoos, M. Schoenauer, M. Sebag, "Frugal Machine Learning", Nov. 2021 https://arxiv.org/abs/2111.03731

and the Computerized Maintenance Management System (CMMS) will be properly integrated following an exchange of data with the secure, trusted aerOS services.

3. To develop, test, and validate different frugal AI models for providing advance insights of probable faults for the 4 CHEs being monitored. Both regression and classifications ML algorithms will be considered for the specific use case.

A more particularised list of objectives of scenario 1 of Use case 4 is described using the table below, which aims at explaining their impact and their effect in value (being 1 no significant and 5 very significant).

Table 27. Specific objectives of Use case 4 – Scenario 1

OBJECTIVE	DESCRIPTION	IMPACT	EFFECT OF VALUE	
CHE telemetry data acquisition	To retrieve telemetry data from 2 straddle carriers and 2 quay cranes every second	The access to real-time telemetry data of the CHEs in the port will allow terminal managers to carry out better and more informed choices, leading to a higher operational efficiency of the terminal.	**Cost**	2
			Efficiency	5
			Quality	3
			Flexibility	1
			Innovation	5
			Sustainability	1
Connection to TOS and CMMS	To collect work instruction data and maintenance tasks, warnings and faults data from the Terminal Operating System (TOS) and Computerized Maintenance Management System (CMMS), respectively.	The access to historical TOS and CMMS data will allow terminal managers to improve the decision-making process, leading to a higher operational efficiency of the terminal.	**Cost**	2
			Efficiency	3
			Quality	4
			Flexibility	1
			Innovation	5
			Sustainability	1
Frugal-AI models for predictive maintenance	To train, test, and validate frugal predictive maintenance AI-models (both, regression and classification) with the CHE telemetry data, and maintenance data.	The development and deployment of predictive maintenance solutions will allow to avoid unexpected machinery faults, which will reduce repair costs, as well as equipment downtime.	**Cost**	4
			Efficiency	5
			Quality	4
			Flexibility	1
			Innovation	5
			Sustainability	3

3.4.5.1.3. aerOS in Scenario 1

Even having enough data, the selection, training, and inference process of the most suitable ML model for the computing capabilities of the Infrastructure Elements (IEs) of the use case is critical. Edge technology is considered in aerOS as a key way of optimizing the speed and performance of predictive analytics by performing ML locally, since even though cloud computing can support predictive analytics solutions, carrying out these models on a remote server leads to potential latency issues, which may cause delayed response maintenance times.

The following diagram sketches the expected architectural deployment of Pilot 4 use case scenario 1. Far-edge devices will be used for collecting data from sensors and the machine's PLC, and performing basic pre-processing of the data. Edge processing will be performed for local ML training and inferencing for identifying the need for predictive maintenance.

Finally, Cloud resources will be used for more intense ML training and testing. Data will be exchanged using the aerOS communication infrastructure capabilities.

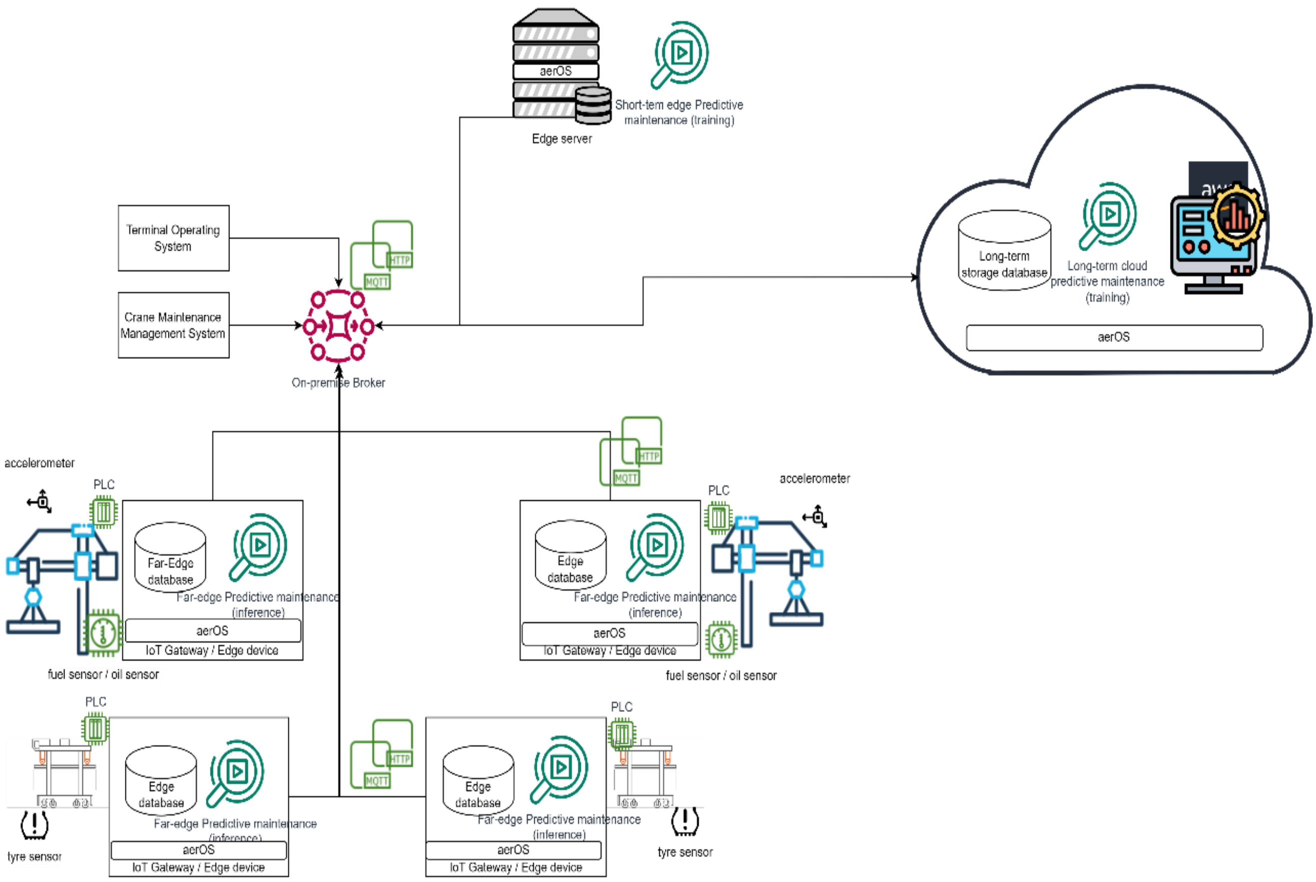


Figure 34. Predictive maintenance of Container Handling Equipment – scenario 1 of Use case 4 in aerOS

3.4.5.1.4. Actors involved in Scenario 1

The actors involved of this use case have been collected following the table below, representing the actors involved, business area impacted, together with the type of impact and what it consists of.

Table 28. Actors involved in Scenario 1 of Use case 4

ACTOR	B$ AREA	TYPE OF IMP.	IMPACT DESCRIPTION
Container terminal board	Management	Indirect	Extending lifespan of cranes will reduce capital expenditure on new CHEs, as well as increase terminal productivity
Container terminal maintenance dpt.	Maintenance	Direct	The predictive maintenance service will allow maintenance team to optimize their work, reducing unexpected faults
Crane drivers	Operations	Direct	The reduction of unexpected faults will increase cranes' lifespan and drivers' safety and satisfaction
Technology provider	IT	Direct	An accurate AI/ML service will be implemented, becoming part of the product portfolio

3.4.5.2. Scenario 2: Risk prevention via Computer Vision in the edge

3.4.5.2.1. Description

Influenced by the advancements and technologies generated by the well-known fourth industrial revolution (Industry 4.0)[17], maritime port digitalisation (also known as Port 4.0) is considered as one of the key pillars for addressing several operational efficiency challenges. Port 4.0 refers to the process by which digital technologies are integrated into the operations and management of ports and terminals. Therefore, cutting-edge technologies are employed to drive autonomous operations and assist humans to follow the right business and operational decisions. Among others, it involves the use of technologies such as Autonomous Systems, the Internet of Things (IoT), Computer Vision (CV), Big Data, or Artificial Intelligence (AI). Within this digitalization journey, AI has the potential to revolutionize the maritime industry. It will allow terminal operators to optimize resource allocation, reduce congestion, or improve turnaround times. Computer Vision (CV) is a rapidly growing field of AI that has many potential advantages in various industries[18]. One significant advantage of CV is its ability to automate visual inspection processes. With the help of CV algorithms, it is possible to automate quality control, defect detection, and inspection processes, resulting in increased accuracy, speed, and cost-effectiveness. This can be particularly useful in manufacturing and industrial settings, where visual inspections are critical to ensure product quality and safety. One of the main data sources for the terminal comes from the camera systems. Thanks to the explosion of customizable IPTV cameras, the captured video streams combined with CV can be used for improving different aspects in the port. In particular, it is crucial to keep track of the continuous flow of in-and-outgoing containers. Missing one container might lead to high costs. The second use case scenario of the pilot 4 is based on the development, integration and validation of different frugal-AI CV algorithms on the edge. IPTV cameras to be installed at the terminal yard or at the STS cranes when loading and unloading the vessels. This use case will allow the terminal to automatically identify containers with damages, and to check for the existence of container seals without the need of human intervention. These two features will be offered to container terminals' customers, providing an added value from the quality check point of view. In addition, the automated and low-latency analyses of those video streams on the edge will avoid human mistakes and at the same time reduce safety risks, achieving a secure, and trustable environment for workers.

The details of the two applications of CV are described next:

Broken seals / unsealed containers

One of the major applications of use case scenario 2 is to detect broken seals or absence of seals on containers, and differentiate between properly sealed and unsealed containers. Similar applications of computer vision have been applied to different projects, and their outputs are closely related to the main goal of the second use case. The objective is to discern sealed from non-sealed containers, which will enhance the quality control of the terminal yard operations.

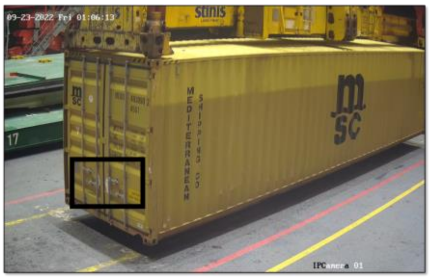


Figure 35. Example of detection of broken-sealed container for scenario 2 of Use case 4

[17] Fotios K Konstantinidis, Nikolaos Myrillas, Spyridon G Mouroutsos, Dimitrios Koulouriotis, and Antonios Gasteratos. 2022. Assessment of industry 4.0 for modern manufacturing ecosystem: A systematic survey of surveys. Machines 10, 9 (2022), 746

[18] Fotios K Konstantinidis, Spyridon G Mouroutsos, and Antonios Gasteratos. 2021. The role of machine vision in industry 4.0: an automotive manufacturing perspective. In 2021 IEEE International Conference on Imaging Systems and Techniques (IST). IEEE, 1–6.

The innovation proposed is, thus, the application of this technology to a different goal from the examples found in the literature, but in close relation with them. Furthermore, there is the plan to build a CV-based model for achieving higher accuracy in properly detecting the seals on the back side of containers, which can be a challenging task (as presented in Figure 35).

Container surfaces damages detection

Frequent use and stacking of containers can lead to various damages such as cracks, cuts, holes, deformations, and dents. The manual methods for early detection of damage have several weaknesses, such as low efficiency, slow speed, low accuracy, and high cost, which affect the efficiency of the port and cause economic losses. Therefore, the second major application of use case scenario 2 is to develop a CV-based method capable of detecting various damages of containers. The detection of damage to containers requires an efficient CV model instead of conventional detection models because they have some complexities. For example, there are multiple views of the container sample image, which leads to differences in the damage features for the same container. On the other hand, the difference in the damage features of different categories is not obvious, which makes training models difficult. Finally, weather, light, and other factors can cause interference during sampling.

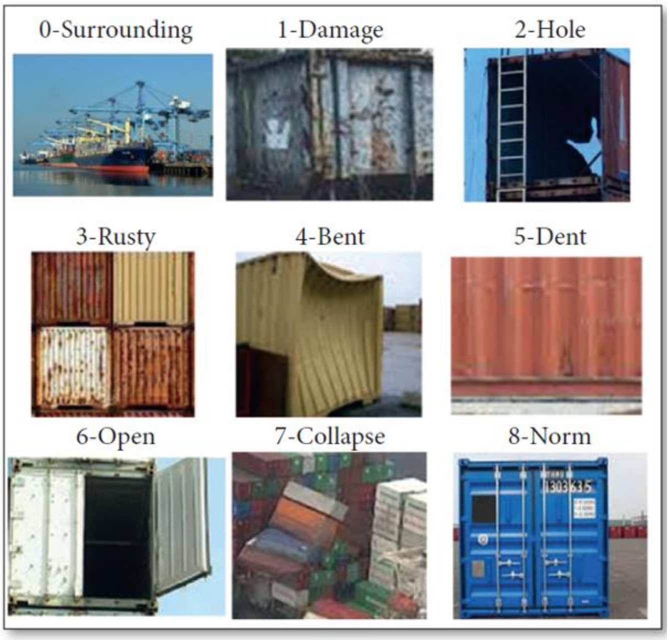


Figure 36. Different type of container surface scratches

3.4.5.2.2. Specific objectives

The general objective of use case scenario 2 is to provide a CV solution that can be inferred from the edge without requiring very high bandwidths. The aerOS orchestration will manage when these functionalities can be carried out in the edge devices dynamically, according to the actual IEs capabilities. This general objective can be split into small specific objectives:

Table 29. Specific objectives of Use case 4 – Scenario 2

OBJECTIVE	DESCRIPTION	IMPACT	EFFECT OF VALUE	
IPTV camera installation	To procure and install different IPTV cameras with enough resolution, local storage, and customization	The installation of IPTV cameras at the quay side of the port will allow to capture the processes of loading/discharging containers of vessels.	**Cost**	2
			Efficiency	2
			Quality	4
			Flexibility	1
			Innovation	3

	capabilities		**Sustainability**	2
Collect video streams from installed IPTV cameras	The video streams captured from the IPTV cameras should be properly collected for a long period of time in a sufficiently large storage service.	A large dataset is needed in order to allow AI practitioners to carry out the proper data annotation and ML training required for getting accurate ML algorithms	**Cost**	4
			Efficiency	3
			Quality	4
			Flexibility	2
			Innovation	3
			Sustainability	3
Frugal-AI models for object detection	To train, test, and validate frugal AI-models for detecting wrongly sealed containers, as well as containers' surfaces damages (classification NN are the main point of interest).	The development and deployment of CV solutions will provide an added value from the quality check point of view of the terminal SLAs. In addition, the automated and low-latency inspection of the containers will avoid human mistakes and at the same time reduce safety risks, achieving a secure, and trustable environment for workers.	**Cost**	2
			Efficiency	4
			Quality	5
			Flexibility	4
			Innovation	5
			Sustainability	4

3.4.5.2.3. aerOS in Scenario 2

Even having enough data, the selection, training, and inference process of the most suitable ML model for the computing capabilities of the Infrastructure Elements (IEs) of the use case is critical. Edge technology is considered in aerOS as the way of optimizing the speed and performance of CV analytics by performing ML locally, since despite cloud computing can support CV solutions, performing the inference process on a remote server may lead to potential latency issues, which may cause unsafe environment for terminal workers.

The following diagram sketches the expected architectural deployment of Pilot 4 use case scenario 2. Far-edge devices (i.e., IPTV customizable cameras) will be used for collecting video streams and performing basic pre-processing. Edge processing will be performed for local ML training and inferencing for identifying the presence of container damages or the absence of safety seals. Finally, Cloud resources will be used for more intense ML training and testing. Data will be exchanged using the aerOS communication infrastructure capabilities.

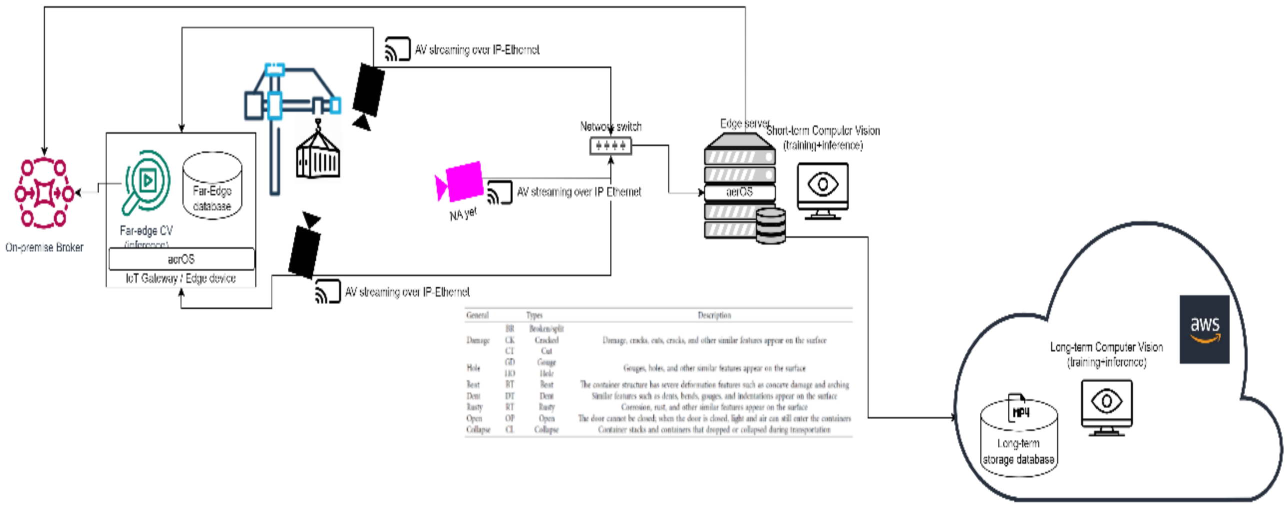


Figure 37. Container damage detection via CV – scenario 2 of Use case 4 in aerOS

3.4.5.2.4. Actors involved in Scenario 2

The actors involved of this use case have been collected following the table below, representing the actors involved, business area impacted, together with the type of impact and what it consists of.

Table 30. Actors involved in Scenario 2 of Use case 4

ACTOR	B$ AREA	TYPE OF IMP.	IMPACT DESCRIPTION
Container terminal board	Management	Indirect	Detection of sealed and non-sealed containers will help in making decisions; also, it helps in reducing human presence at an area with high safety risks. Eventually, it will help in enhancing the productivity of terminal, as humans need 30 seconds to 01 minute to check the seal but CV based system will do this task in couple of seconds (i.e., 2-5 seconds).
Container terminal maintenance department	Maintenance	Direct	Early detection of damages in containers can help to resolve the small issues before any big loss.
Crane drivers	Operations	Direct	Based of damage detection using computer vision-based models, they can carry damaged containers with more care to avoid any further loss of container contents.
Technology provider	IT	Direct	An efficient computer vision-based model will be implemented, becoming part of the product portfolio.

3.4.6. Requirements of the trial

Below there is a list of the specific requirements identified for this trial. A full list of all the requirements gathered (in M9) for Pilot 1 as a whole are available in Appendix B.

- Develop aerOS IE that integrates data telemetry from cranes into aerOS Data continuum
- Integration of TOS with aerOS
- Integration of CMMS into aerOS
- Monitor Trolley Wire Rope Enlargement
- Motor Filter Condition
- Motor Bearings Condition
- Motor load sharing from Hoist
- Tensioning Aux Cylinder Pressure Monitoring
- Generator engine efficiency
- Genset vibrations
- Inclination issues
- Hydraulic system
- AI models for Predictive Maintenance (PdM) should meet a minimum R2
- Integration of IPTV camera streams in aerOS
- Container plate identification
- Detection of damaged containers
- Detections of holes in containers
- Detection of wrongly sealed containers
- AI algorithms for CV should process at least 10 frames per second

- AI models for CV should meet a minimum R2

3.4.7. Outcome of the trial

After the completion of the activities of the pilot, when fulfilling the objectives above by the partners of the use case, the expected outcomes of the trial are as follows:

- Integration of live data from the container terminal.

Result: High-level meta-OS system up and running

- Integration of assets for predictive maintenance

Result: A tool (with GUI) provided to the Port Managers based on benefits provided by aerOS.

Real-time integration between HW and SW terminal assets for proper predictive maintenance.

- Data collection supporting AI

Result: Solid, robust, standardised, available, Big Data dataset

Dataset of telemetry data from quay cranes and straddle carriers that is big enough to support training, testing, and validation of Predictive Maintenance models.

- Predictive maintenance

Result: AI models for crane predictive maintenante

Frugal AI models for crane predictive maintenance alerting including classification and regression models such as decision trees, random forest, KNN, Binary recursive models, etc.

- Edge models

Result: PdM services properly working at the edge.

- Recording of containers

Result: Solid, robust, standardised, available, Big Data dataset

Dataset of images from IPTV cameras recording containers during load/unload operations (large enough to support training, testing, and validation of Computer Vision models).

- Computer Vision

Result: Computer Vision models working

Computer Vision models (YOLOV[19], Inception[20], ResNet50[21], EfficientNet[22]) for the detection of damaged containers, wrongly sealed containers, or other scratches needed for risk prevention purposes.

- CV services

Result: A set of CV services manageable via aerOS

Computer vision services properly working at the edge IEs.

As expected benefits, aerOS will allow stakeholders of maritime port use case (represented by EGCTL) to be able to:

- Achieve full end-to-end traceability of assets and procedures

[19] https://www.section.io/engineering-education/introduction-to-yolo-algorithm-for-object-detection/
[20] https://towardsdatascience.com/deep-learning-understand-the-inception-module-56146866e652
[21] https://datagen.tech/guides/computer-vision/resnet-50/
[22] https://roboflow.com/model/efficientnet

- Allow to take better decisions by improving the availability of the information and the way it is presented to the staff.
- Reduce manual interactions, automatizing as much as possible the input of traceability data in such a way that any service develop within the framework of aerOS may benefit from the insights that data can provide
- Increase efficiency and reduce costs by implementing real-time tracking and monitoring of assets in the terminal yard through the use of IoT and AI technologies
- Improve communication and collaboration between stakeholders
- Reducing idle periods due to unplanned maintenance operations of cranes and straddle carriers and the automatic detection of container IDs and structural checks to detect damages.
- Enhanced security services, guaranteeing overall customer satisfaction
- Enhance its ability to analyse and optimise its performance by collecting and analysing data on the usage and performance of equipment
- Implement security measures on the state of the containers
- Beneficial for security, as different organizations may have different requirements for data privacy and ownership
- Up-to-the-minute health status knowledge, enabling not to wait for equipment shutdown to occur (i.e., reactive maintenance), nor carrying out maintenance when it is not necessary (i.e., preventive maintenance).
- Help to prevent downtime, increase efficiency and save cost by reducing the need for regular manual inspections.

3.4.8. KPIs related to the trial

Same as for the requirements, it is only the goal in this section to make a bullet pointed list of the KPIs that have been identified. This exercise helps understand the relevant aspects of the pilot that the execution activities will be paying more attention to.

- Reduction of idle time caused by core equipment failure or unavailability
- Number of equipment malfunctions reduction: manually reported by the staff
- Number of automatically damaged containers being detected compared to manually reported by staff before aerOS
- Performance evaluation metrics of regression AI models (R2)
- Performance evaluation metrics of classification AI models (F1) for predictive maintenance of CHEs
- Performance evaluation metrics of classification AI models (F1) for damaged containers
- Performance evaluation metrics of classification AI models (F1) for damaged seals
- Number of models executed on edge nodes

3.4.9. Legal framework

During the course of task T2.3 (Legal and regulatory analysis and governance specification), several actions have been performed in order to identify the legal framework surrounding activities in Pilot 3. As the main result of this action, find attached in Appendix C.4.

Besides that, a thorough analysis of the legal and regulatory aspects affecting the different scenarios of Use case 1 was performed, outputting the following results:

Sectorial regulations (Maritime Ports):

- Maritime ports - REGULATION (EU) 2015/757, 29 April 2015 and amending Directive 2009/16/EC - monitoring, reporting and verification of carbon dioxide emissions from maritime transport. This legislation motivate the need of the presented solutions to reduce carbon dioxide emissions.

- Maritime transport - DIRECTIVE 2009/29/EC, April 2009 amending Directive 2003/87/EC - so as to improve and extend the greenhouse gas emission allowance trading scheme of the Community.

Technologies:

- Data - Data Act Document SEC(2022)81 (EU) - haring non-personal data that is generated through the use of connected product or related service by a user from the data holder to the user or a designated third-party data processor authorised by the user. Also relevant to prevent vendor lock-in with cloud and edge providers due to technical incapacity for switching limiting market growth and innovation.
- Platform services – Digital Markets Act {SEC(2020) 437 final} - Applies to core platform services provided or offered by gatekeepers to business users established in the Union or end users established or located in the Union, irrespective of the place of establishment or residence of the gatekeepers and of other law otherwise applicable to the provision of service. Aims to end unfair restrictions imposed by large-scale platforms, including cloud computing platforms, to reduce lock-in effects and increase innovation. Important for the implementation of services and analytics in the cloud-edge continuum developed in aerOS.
- Digital Services - Digital Services Act {SEC(2020) 432 final} - aims to contribute to the proper functioning of the internal market for intermediary services and set out uniform rules for a safe, predictable and trusted online environment, to protect fundamental human rights . Sets out obligations on intermediary information society services to ensure the proper functioning of the internal market and a safe, predictable and trusted online environment in which the fundamental rights enshrined in the Charter are duly protected
- Artificial Intelligence – Artificial Intelligence Act {SEC(2021) 167 final} - aims to provide clarity around what can and cannot be done with AI in the European Union. It established harmonised rules for the placing and using AI on the market, and prohibits certain practices. It outlines specific requirements and obligations for operators. It also provides harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content. Finally, it set out the rules on market monitoring and surveillance. Relevant implications for the implementation of computer vision applications

Products:

- Computer vision solutions - REGULATION (EU) 2016/679, and repealing Directive 95/46/EC (General Data Protection Regulation) - Any person recorded in the video streams needs to be anonymise protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- Computer vision solutions – Cypriot Data Portection Act. Law 125 (I)/2018 (Cyprus) - Any person recorded in the video streams needs to be anonymised. Protection of Natural Persons with regards to the processing of personal data and for the free movement of such data. The law states that the processing which is carried out by a controller or a processor for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be used for taking a decision which produces legal effects concerning the data subject or similarly significantly affects them.

3.5. Pilot 5: Energy Efficient, Health Safe & Sustainable Smart Buildings

3.5.1. Trial general description

This use case, driven by partners COSMOTE (COSM), NCSRD, FOGUS, INF and UPV, aims to demonstrate gains of the aerOS architecture in an edge deployment for energy efficient, sustainable, flexible and health-safe smart buildings. The use case considers deployment and validation in an office enterprise building of COSMOTE (Athens, Greece).

A wide number of sensors and actuators with the aerOS capabilities must be deployed to meter energy, luminosity, CO2, humidity, temperature, motion detection, and desk occupancy. The data collected by these sensors, together with the algorithmic criteria set to minimize energy consumption and maximize health measures is capable to determine the appropriate clustering of employees in the offices and deduce the recommended employees seating. Specifically, the system will run, supported by underlying aerOS meta Operating System by considering:

- The metrics received by the sensors;
- The employee's data, such as position in the organization's structure and team membership;
- Historical data on energy consumption, CO2 emissions per office segments;
- One's previous seating preferences;

Then, in the use case, the overall application (running over and making use of the traits of aerOS) selects the appropriate office and allocate the most suitable seat(s), and proceeds to direct the employee the use of a Mobile App with ChatBox capabilities. At the same time, the sensors data are to be exploited to actuate appropriately the ventilation, heating and air-condition systems as well as control luminosity. Swarm intelligence among the aerOS capable sensors shall allow them to cooperate in a decentralized manner and collectively manage each room's condition, so that the office becomes self-organized in terms of health and efficiency.

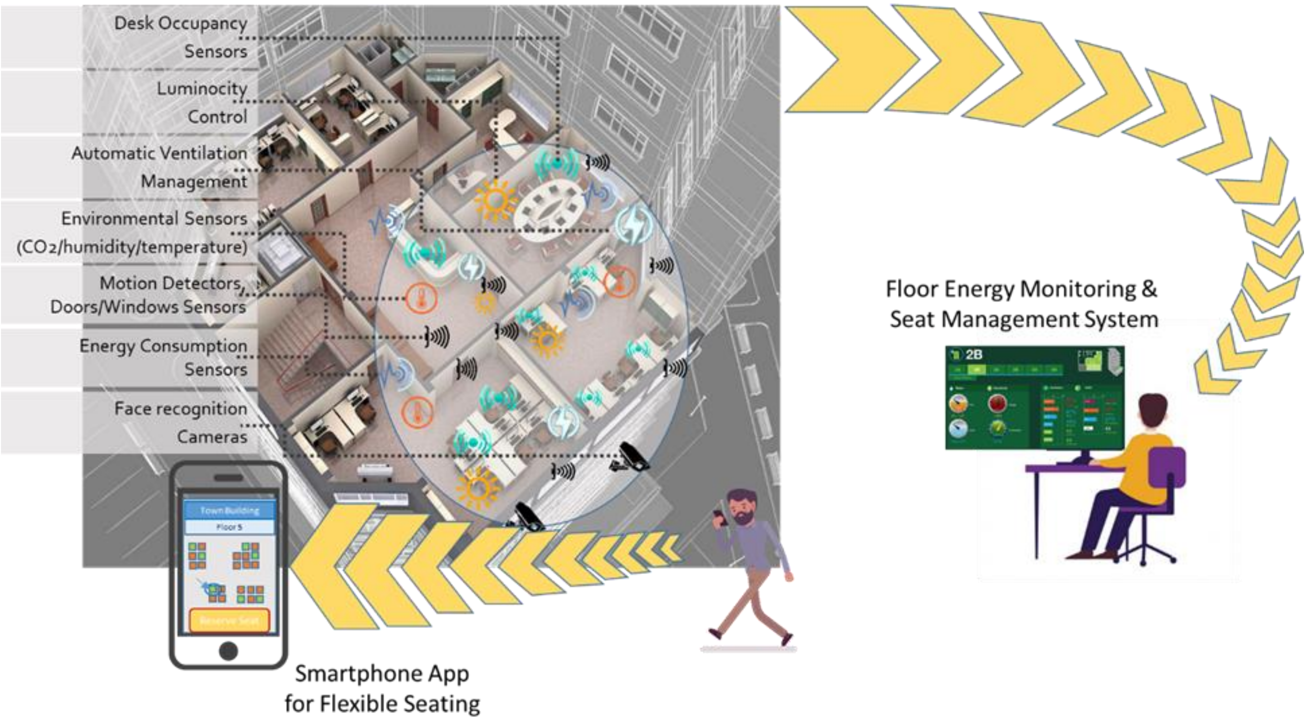


Figure 38. Overview of Use case 5

Finally, a user management interface available to the building facility managers, depicts monitoring dashboards presenting in real-time the energy consumption and health/safety KPIs set for each segment of the building and in total with flexible historical reference. In this way, the use case stands as a complete prototype of the target system envisaged for the aerOS paradigm.

The implementation shall leverage the IoT solution prototyped by COSMOTE R&D and already installed in residences and COSMOTE's telecom sites. The architectural layout of the solution is composed of: (a) A wide range of commercial (and custom) end-devices/sensors, (b) Multi-purpose IoT gateways for the support of a wide range of Use Cases, (c) A backend cloud infrastructure, enabling gateway/device management, data storage, data processing, (real-time and historical) data visualization, cloud-based dashboards (WebGUI). The solution is based on open source software and commercial HW and it offers an open API for data retrieval. The pilot also exploits INFOLYSIS chatbot system capabilities as the means to interact with the employees

The aerOS proposal for Energy Efficient, Health Safe & Sustainable Smart Buildings is unique and presents innovative solutions to business and IoT challenges: (i) An extensive number of IoT sensors are deployed in the Smart Buildings ecosystem, generating/processing huge amount of data that are only valid for the location they originate from, yielding their transmission and collection for central processing meaningless and wasteful. The distinctive infrastructure characteristics of each building rationalize the autonomous and decentralized decision-making at the edge with the use of the aerOS nodes intelligence, and the effects are instantaneous and tactile. (ii) With multiple IoT vendors and solutions, tech integration, so that sensors, systems, analytics work in sync, becomes a considerable obstacle. Applying the aerOS architecture that stands as a unique abstraction layer, the end-to-end integration can be achieved easily embracing the strategic IoT sourcing of each enterprise to offer an adaptable solution that can bridge heterogeneity.

With regards to the **global objectives of the Use case 5**, Energy Efficient, Health Safe & Sustainable Smart Buildings Use Case aims to exhibit how the aerOS platform agnostic meta-operating system for the IoT-cloud-edge continuum can be applied in the Smart Buildings applications domain. Three specific objectives are set:

- Objective 1: Implement the aerOS architecture in Smart Buildings market to optimize the efficiency and safety of enterprises based on process and data autonomy and self-orchestrated IoT ecosystems.
- Objective 2: Demonstrate energy efficiency of the large buildings using real-time processing and (frugal) AI.
- Objective 3: Use 5G and smart network components like NFV and NetApps to extend aerOS capabilities.

3.5.2. Current problems/barriers area and motivation

Enterprise buildings can save energy by using advanced sensors and automated controls in HVAC (Heating, Ventilation and Air Conditioning), plug loads, lighting, as well as advanced building automation and data analytics. Buildings that have advanced controls and sensors along with automation, communication, and analytic capabilities are known as smart buildings. In a fully-fledged smart building, the building systems are interconnected using information communications technologies (ICT) to communicate and share information about their operations. At the same time in the last years, the Coronavirus pandemic disruptively affected the traditional work norms, stranding previously crowded office buildings. Trying to ignite the economy recovery process, more and more companies have adopted a strategic return to the workplace, embracing flexible working and mobile workspaces. Rather than trying to fit as many people as possible into a workspace, so that to maximise utilisation of shared commodities and infrastructure in the quest of efficiency, companies seek to maximise the space between workers and perhaps rotate between a remote and in-office working model to facilitate a safer shared environment. Evidently, the post-pandemic workplaces have become large open spaces with no fixed seating per employee; and desks are to be allocated to employees on demand and on a daily basis. As such, proper employees' placement, social distancing and energy efficiency, along with business and personal preferences and work habits becomes a complex and dynamic task. In this transformation towards flexible, safe and sustainable workplaces, IoT technology and Analytics through the aerOS capabilities can offer a unique, autonomous solution towards safe and sustainable workplaces.

In order to illustrate the problems/barriers that have motivated this use case in aerOS, and according to the personalized templates of Trial Handbook devised for the project, it was decided to utilise the following table:

Table 31. Current problems and barriers in UC1 related to metrology

CHALLENGES or BARRIERS	DESCRIPTION	AREA	IMPACT IN THE COMPANY
Reduce operational costs by saving energy and space in a wide range of geographically dispersed buildings owned or rented.	COSM owns and need to maintain a lot of buildings, geographically dispersed and with a variety of use and occupancy, in the most cost-effective manner	Management	The distributed, orchestrated and dynamic nature of aerOS pilot 5 directly responds to the company's challenge to maintain in the most efficient manner the buildings occupied.
The solution must instantly integrate and incorporate SOTA components	Interoperability is a key issue for the smart building systems development process that leads to limiting options used to specific vendors products, that needs to be avoided. ..	Purchasing	By leveraging the openness and interoperability of the aerOS architecture, a lot of cost savings can be achieved as components can be plugged-in / integrated with minimum effort.
Data Privacy and Security	Collect and manipulate user data in a secure manner that protects personal information while enabling smart decision making and recommendations based on that data.	Management / Technical Support	Demonstration of aerOS nature in Pilot 5 through autonomous and decentralised decision-making at the edge.
The chatbot should be able to communicate with the aerOS elements	The chatbot needs to have access to information from the building sensors and the recommendation system in order to present them to the employees.	Product Development	A further development and an extension of the chatbot's capabilities will be achieved in order to be able to communicate with devices from aerOS ecosystem.
Test the aerOS IoT-cloud-edge computing continuum solution in real scenarios	UPV plays a key role in the development of the technical components of aerOS, specially with the ones related with the IoT-cloud-edge computing continuum. It is essential for the partner to deploy and test the developed solution in a real scenario with multiple challenges to be solved.	Technical support	By providing technical support in the deployment of the pilot, UPV will test the developed technological components in the project and enhance its knowledge regarding IoT-cloud-edge computing continuum scenarios and its capabilities to solve real-word challenges.

3.5.3. Participant partners

COSMOTE:

COSMOTE, the leading Mobile Network Operator of Greece launched in April 1998, is a member of OTE Group, and since March 2009 a member of Deutsche Telekom Group. COSMOTE holds the top market position in Greece since 2001, and today accounts for more than 50% of the Greek mobile network subscribers' base exceeding 7 million (Q4/2022). OTE Group is the largest telecommunications provider in Greece, offering a full range of telecommunications services: from fixed-line and mobile telephony, broadband services, to pay television and ICT solutions, while it is also involved in payment services, maritime communications, real estate, energy, insurance services and professional training. Furthermore, OTE Group has a strategic interest in supporting sustainability through many initiatives, both research and commercial.

As an obvious observation, the Smart & Health-Safe Buildings use case perfectly fits to the sustainability strategy of the company, and is considered if adopted, to directly contribute to maintaining OTE Group's superior performance in international sustainability indicators. COSMOTE as a telecom operator with 3000+ employees, located in many buildings geographically dispersed, seeks to validate the aerOS implementation from the perspective of a large-scale end-customer, in the quest to find a versatile, dynamic and distributed, intelligent solution to minimize the operational costs and energy consumption with minimum central management overheads. This interest is re-enforced considering that real-estate is part of the company's business portfolio. At the same time COSMOTE seeks to reorganise the placement of employees to buildings, on one hand moving towards shared mobile-office workplaces and one the other cutting down the number of buildings necessary for employees' placement, performing smarter facility management As such, COSMOTE offers the building of OTE Academy, for the installation, verification and demonstration of pilot 5 implementation.

COSMOTE, letting aside its main business as the top mobile operator of Greece, is a leading ICT provider not only in the Greek market but also at a European level. Understanding the wide-customer market potentials that the smart buildings business case offers, there is an active interest to explore the value proposition offering from the standpoint of a technology integrator. In this standpoint, COSMOTE brings in the project its "LeonR&Do" IoT testbed & energy monitoring system that has been developed internally for research purposes. The utilization of the "LeonR&Do" solution since 2014 in various R&D EU-funded innovative projects (e.g., INTERCONNECT, 5G-COMPLETE, LIFE-SAFE CROSSING, AEOLUS) as well as to own COSMOTE needs (for energy monitoring/management, physical security), has resulted in the development of a stable and complete IoT platform, that is constantly being evolved (i.e., expansions/upgrades, field trials towards higher TRL) with beyond state-of-the-art capabilities.

NCSRD:

The National Centre for Scientific Research Demokritos (NCSRD) is the biggest research centre in applied sciences and engineering in Greece and it is a self-governing research organization, under the supervision of the Greek Government. NCSRD consists of five Institutes spanning a broad range of activities, and of divisions responsible for administrative and technical support. Staff sums up to about 800 persons, including about 100 graduate students working towards a Ph.D. degree. It is the home of the Greek National Host and a major node in the Greek National Research and Technology Network (GR-Net). NCSRD participates in the project through the FutuRe COmmunication Networks (FRONT) Research Group of the Institute of Informatics and Telecommunications (IIT), which is actively involved in many areas of information technology and telecommunications, ranging from basic research, to goal oriented research, as well as development and application of processes and products. FRONT Research Group experience with compute and network virtualization techniques, including NFV/SDN & CNF, and its involvement with B5G network projects (EVOLVED-5G, 5GENESIS etc) and systems will be a valuable contribution for the UC5 scenarios implementations.

INFOLYSIS (INF):

INF has commercially available the INFOLYSiS Messaging Platform for engaging Viber users with messages using chatbots and the INFOLYSiS Chatbot platform for setting up custom made chatbots with Q&A

interoperability and statistical dashboards for monitoring and reporting purposes. Chatbots can combine the steps of complex processes to streamline and automate common and repetitive tasks through a few simple voice or text requests, reducing execution time and improving business efficiencies. INF bring in the project the Chatbot platform which has also been utilised in various EU-funded projects such as 5GENESIS, EVOLVED-5G, and SECANT

FOGUS:

FOGUS, a thriving SME in Greece, aims at integrating state-of-the-art technological advancements and cutting-edge research achievements, towards an immersive communication and computing experience. Founded by a group of industrial and academic experts covering a wide range of disciplines in the area of Information and Communication Technologies (ICT), FOGUS exhibits strong research record and vast experience in managing and implementing ICT Research & Innovation actions. It provides a comprehensive set of services, including: software development, simulation and experimentation set up, data analysis and tooling, and modelling and performance evaluation. FOGUS emphasizes on the optimization of core procedures and processes of network functions by integrating machine learning, big data analytics and cloud-empowered optimization. Holding experience that ranges from the design of mobile communication protocols to the development of custom-made software, FOGUS undertakes: i) end-to-end set-up of network simulation and emulation environments for IoT and User-centric services, ii) development of network functions end protocols for access and transport network domains, and iii) analysis of big data with expertise on mapping network and service performance parameters to user-experience metrics. FOGUS is currently operating an end-to-end deployment of LoRa/LoRaWAN IoT infrastructure with a cloud-enabled and modular application and network managers. This supports two key research and service lines of the company, namely network and service performance evaluation and campus/experimentation infrastructure development.

FOGUS supports the development and evaluation activities in aerOS pilot 5, by providing insights both to the communication infrastructure of the pilot and to all the data-related processes. For the communication part, FOGUS brings expertise in common protocols, such as MQTT, Webhooks, HTTP, and others. Regarding the data processes, FOGUS has experience with all the common data processes, i.e., data gathering, data storage, data cleaning, data processing, data analysis; using well-established practices in the IoT field, i.e., gathering via push and pull models, storage using timeseries formatting, processing and cleaning using well-known frameworks and libraries, and visualizing using de facto tools (e.g., Grafana).

UPV:

UPV (Universitat Politècnica de València) is a dynamic, innovative, public institution, dedicated to research and teaching that keeps strong ties with the social environment in which its activities are performed and, simultaneously, has an important presence abroad. Today, over 39,000 members integrate its academic community: 35,000 of these are students, 2,387 are teachers and 1,593 belong to administration. UPVLC includes 15 faculty centres: ten schools, three faculties, and two higher polytechnic schools (Alcoy and Gandia), and five associated institutions. UPV contribution to aerOS will come from the Distributed Real Time Systems Lab (DRTSL) which belongs to the Communications Department. DRTSL is specialized in IoT, interoperability, cloud and edge computing and Edge-to-Cloud computing continuum. This expertise has resulted in multiple publications in scientific journals along with the continuous participation in EC-funded R&D projects playing important roles, such as project coordination (INTER-IoT, ASSIST-IoT and aerOS itself), technical coordination and development and contribution to real pilots or scenarios.

3.5.4. Data sources, existing software and available hardware

The data sources, existing software and hardware that have been detected so far to be used in the Pilot 1 of aerOS are as follows. The next list reflects only a summary of the minimum aspects detected so far. A far more thorough description is included in the current stage of the Trial Handbook (online) of the pilot. In addition, it is worth noting that these descriptions will be fully disclosed in the next deliverable of this task (T2.2, deliverable D2.3):

Overview of the pilot infrastructure:

Pilot 5 will take place (and become) in an open, vendor and access technology/protocol agnostic, end-to-end, solution based on open-source tools environment. Its high-level architecture (Figure 39) is composed of.

a. The (wide range of commercial and custom) end-devices/sensors, utilizing various access technologies (WiFi, 2G/3G/4G/5G, NB-IoT, LoRa-WAN, Sigfox, ethernet, etc.).

b. The "LeonR&Do" IoT gateway.

c. A (common) backend cloud infrastructure enabling gateway/device management, data storage, data processing, (real-time and historical) data visualization, cloud-based Graphical User Interface, remote access from anywhere/anytime, security and command exchange

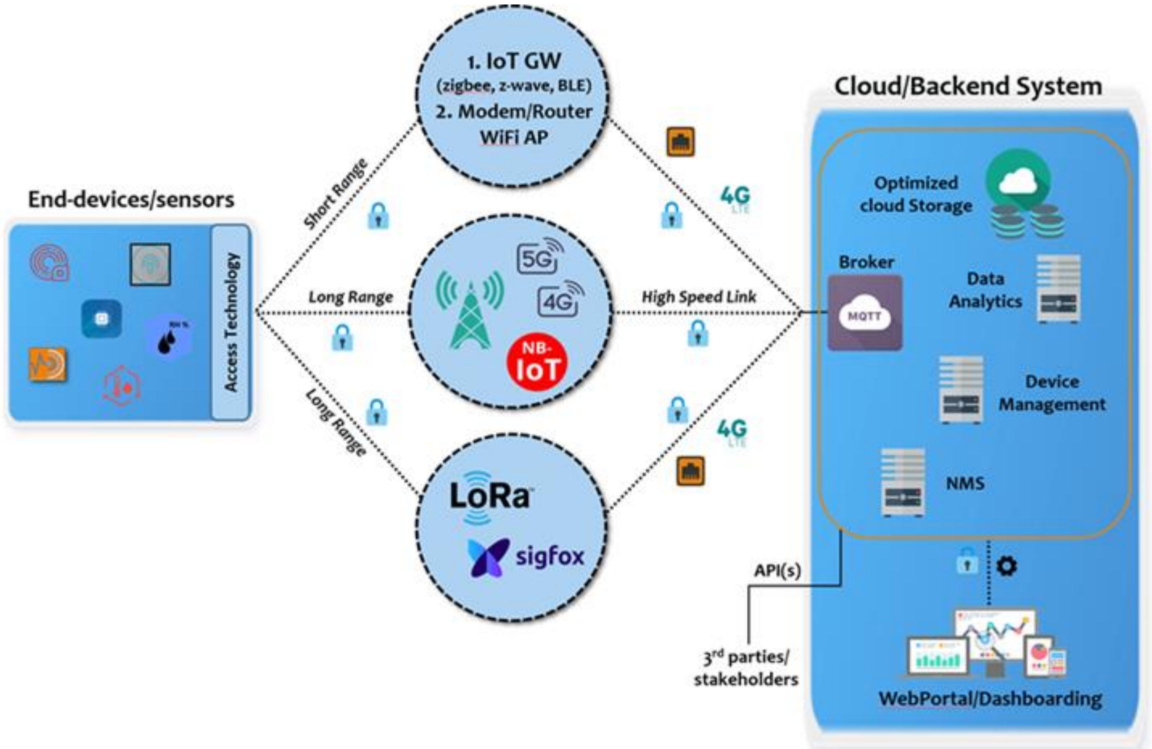


Figure 39. Pilot 5 infrastructure overview

Data sources

- Sensor-generated environment monitoring data (Temperature, luminosity, Air quality and gases, Motion, door sensor…) feeding an InfluxDB timeseries database (thus, accessible in JSON and SCV via API).
- Metadata of sensors' transmission (protocol-specific parameters, link quality parameters such as RSSI and SNR, app data transferred, availability, battery, name…) available through InfluxDB.
- Data and metadata of gateways' transmission (similar to the above).
- Configuration management and monitoring data (resource utilization data exposed by the K8s resources based on the usage of Prometheus, such as network latency, memory usage, CPU…). Both periodic and triggered by events, if needed.

Available software (that aerOS will somehow need to be aware of / interact with):

- Kubernetes and KubeEdge
- ESXi VMWare
- MQTT broker
- InfluxDB
- Grafana
- Home Assistant
- Chatbot

Available hardware:

- Backend system (HPE Proliant DL380 virtualized via VMWare, hosting various VMs that will be used as structural parts of the pilot).
- Chatbot Application Backend System

3.5.5. Objectives, benefits and expected results

In the following sub-sections there is a thorough description of each one of the scenarios in Pilot 5.

3.5.5.1. Scenario 1: Intelligent Occupational Safety and Health

3.5.5.1.1. Description

The global smart buildings market has been booming, with a growth rate of more than 32%[23], based on the promise of big cost reductions - 18% cut on the office energy costs- and improved operational efficiency –as smart sensors and data analytics automatically detect and instantaneously react to workspace alterations, equipment faults and environmental changes-. During the next couple of years, organizations will focus on the data enabled by IoT platforms to drive real results and commercial real estate will reach large-scale implementations of IoT applications[24], significantly transforming their **Operational Efficiency & Energy Management** processes.

At the same time, the Coronavirus pandemic disruptively affected the traditional work norms, stranding previously crowded office buildings. Trying to ignite the economy recovery process, more and more companies consider a strategic return to the workplace, embracing flexible working[25] and rotation between a remote and in-office working model, revolutionizing the **Human Resources Management** process through virtual, intelligent & mobile workplaces.

Addressing both aspects, the purpose of this scenario 1 of Use case 5 is to employ sensors that cooperate in a decentralized manner to collectively manage each building room's conditions in the working environment. Also, determine the appropriate clustering of employees in the offices and deduce the recommended employees seating keeping in mind that the goal is to minimize energy consumption and maximize health measures, considering the following aspects per business process:

- **Operational Efficiency & Energy Management**

In the business world operational efficiency is necessary to reduce costs, and energy consumption is put in the spotlight. While some measures are collectively adopted, the level of automation and intelligence in most buildings is still low. In an open space building, the first thing we currently do to minimize the energy consumption is to reduce the use of lighting. This can be achieved by turning on/off the lights at certain times (working hours) i.e., turn on/off the lights after 8am/8pm respectively, modified, though, to accommodate cleaning/security personnel. With the help of Passive Infrared Sensors (PIRs) the lights can be automatically turned on when motion is detected and off if there is no motion for i.e., 30 minutes or even keep the lights on only in corridors. Same rule can then be applied during working hours in empty rooms (in case of motion detection turn lights on). Moreover, during working hours lights can be turned on/off based on cloud coverage and ambient light levels: in case of adequate daylight there is no need for extra lights. Furthermore, with the use of switches we can control the heating in the common areas and the workspaces used based on automations. More specifically, the switches controlling the heating can turn on/off at certain times during cold and hot months. When the heating is on, the temperature can be set to 20-25 degrees Celsius, which according to ENERGY STAR is the ideal balance of comfort and energy efficiency.

- **Human Resources Management and Mobile Health-Safe Workspaces**

Following the Coronavirus pandemic, a key consideration in work environments becomes the social distancing and the concern for optimizing air quality conditions. The process up to now is rather arbitrary and fixed and is mainly agreed among the occupants of each room, thus not versatile, and optimum. The scenario assumes building a system for employees' placement, considering various environmental and energy related criteria as well as behavioral preferences and the employee's feedback. On top, the system could prioritize positioning same team members in the same space. The system can identify which desks are occupied through smart interpretation of motion sensors (PIRs) data.

[23]https://www.pwc.com/us/en/industries/capital-projects-infrastructure/library/scaling-up-smart-buildings.html
[24]https://www.rfidjournal.com/a-look-into-2019-smart-cities-and-smart-buildings
[25]https://www.workdesign.com/2020/12/2021-trends-the-mobile-workplace/

Notable indicators of air quality are CO2 and PM2.5 levels. High levels of these in a room should trigger actions. A smart light bulb can use different colors to depict the changes in the air quality of the room and an air purifier can be turned on to restore the gasses to normal levels. Moreover, pushover alerts to the facility managers can provide instructions to open a window taking into consideration indoor - outdoor environmental conditions (mainly temperature and/or humidity) and whether the A/C or heating is on. These measurements involve sensors located at certain zones and not the average measurements of all sensors located in a room and the recommendations/automations should refer to these specific zones. If there is no way to “fix” the air quality, then another room should be considered for the next employees to come, since moving the already stationed employees would affect the working conditions and is not recommended. We could monitor the room conditions and refer newcomers to other rooms before the conditions deteriorate.

Additional features include automation for the purpose of the system’s maintenance to guarantee the reliability of the overall solution. Such automation can include pushover/pushbullet alerts notifying for low battery levels if the sensor’s battery drops below a certain threshold (i.e. 30%). Dashboards depicting each room floor plan and the deployed sensors, as shown in Figure 40 can offer monitoring and visualization of the data in real time, as in the example of Figure 41. Finally, a time-series forecasting system can process the historical energy and environmental data, feed them to proper machine learning algorithms to predict and visualizing future energy and environmental data of each workspace/floor, including suggestions based on these. This service would interest both the employees, as they would acquire information fast and reliably, draw conclusions, gain consciousness by developing a better understanding of the workspace’s energy distribution and environmental conditions, and the facility managers, as they would have all the sensor information readily available and, on top of that, overview on a larger scale all the rooms/floors on the network. Having such a powerful tool for prognosis at their disposal, the facility managers could adjust, and act accordingly, and not only economize, but contribute to the overcoming of the energy crisis issue.

Figure 40. (WebGUI/Dashboard) | Interactive Floorplan

Figure 41. (WebGUI/Dashboard) Measurements Depiction Sample

3.5.5.1.2. Specific objectives

The objectives of this use case are described using the table below, which aims at explaining their impact and their effect in value (being 1 no significant and 5 very significant).

Table 32. Specific objectives of Use case 5 – Scenario 1

OBJECTIVE	DESCRIPTION	IMPACT	EFFECT OF VALUE	
Exhibit the portability and interoperability gains proposed by the aerOS concept in the heterogeneous IoT sensors market.	The IoT market is extremely diversified, with a wide range of heterogeneity both in protocols, data artefacts (attributes and values), as well management capabilities.	Through the implementation of the aerOS architecture, the components of the system become aerOS nodes and mask heterogeneity therefore allowing the instant (plug & play), automated deployment and expansion of the IoT solution.	**Cost**	5
			Efficiency	5
			Quality	4
			Flexibility	4
			Innovation	3
			Sustainability	4
Definition and implementation of latency controlled distributed smart networking components.	Mesh networking and 5G technologies shall be deployed in the IoT solution for the efficient communication among the aerOS nodes as well as the humans involved in the use case.	Reliable communication is critical in various layers (sensors, application components and users) and the aerOS architecture considers an all-encompassing efficient communication framework.	**Cost**	2
			Efficiency	5
			Quality	4
			Flexibility	4
			Innovation	3
			Sustainability	4
Definition and implementation of distributed explainable AI components for the aerOS	The pilot decentralizes the intelligence necessary to maintain a safe and sustainable working environment by implementing an edge solution to reduce heavy centralized processing and unnecessary data communication.	The solution can work autonomously to the level of granularity required (per room, floor, building, cluster of buildings) with analogous computational resources that can be scaled-in/out on demand as part of the aerOS node principles.	**Cost**	5
			Efficiency	4
			Quality	3
			Flexibility	5
			Innovation	5
			Sustainability	2
Definition and implementation of smart orchestration for the IoT-edge-cloud continuum	Smart orchestration is key to manage and maintain the environment, targeting the aerOS nodes deployment and provisioning coupled with necessary wireless network configurations, updates in distributed intelligence criteria and prioritization, as well as means to provide business critical monitoring information.	Automation and expandability are key to any IOT solution especially when targeting reliable autonomous operation. With the aerOS architecture, the most optimum deployment and utlilization of resources, as well as recovery in case of incidents is assured.	**Cost**	2
			Efficiency	5
			Quality	5
			Flexibility	5
			Innovation	4
			Sustainability	2

3.5.5.1.3. aerOS in Scenario 1

The use case aims to exhibit how the aerOS platform agnostic meta-operating system for the IoT-cloud-edge continuum shall be applied in the Smart Buildings market to optimize the efficiency and safety of enterprises through autonomous and self-organised IoT ecosystems.

The combination of the Energy Efficient, Health Safe & Sustainable Smart Buildings and aerOS concepts is unique and presents innovative solutions to business and IoT challenges:

- An extensive number of IoT sensors are deployed in the Smart Buildings ecosystem, generating/processing huge amount of data that are only valid for the location they originate from, yielding their transmission and collection for central processing meaningless and wasteful. The distinctive infrastructure characteristics of each building rationalize the autonomous and decentralized decision-making at the edge with the use of the aerOS nodes intelligence, and the effects are instantaneous and tactile.
- With multiple IoT vendors and solutions, tech integration, so that sensors, systems, analytics work in sync, becomes a considerable obstacle[26]. Applying the aerOS architecture that stands as a unique abstraction layer, the end-to-end integration can be achieved easily embracing the strategic IoT sourcing of each enterprise to offer an adaptable solution that can bridge heterogeneity.

The aerOS-enabled system developed as part of the use case will transform existing energy-efficiency IoT applications by:

- Deploying the aerOS architecture by bundling application components as aerOS nodes and identifying the appropriate placement and scaling of the application components for far-edge, edge or cloud processing. The use of configuration management and orchestration as well as self-* operations are fundamental enhancements.
- Investigating the AI principles and technologies (e.g., explainable AI and frugal AI) to implement the external, application-specific, AI requirements of the system
- Exploring the abstraction layer, and meta-data modelling techniques (e.g., FIWARE) as proposed by aerOS, to achieve interoperability and extensibility
- Incorporating the seamless integration of various communication types and network deployments (e.g. 5G and WIFI6) as envisaged by the aerOS network architecture.

The basic mapping of the envisaged use case implementation and placement of components within the aerOS model is depicted below:

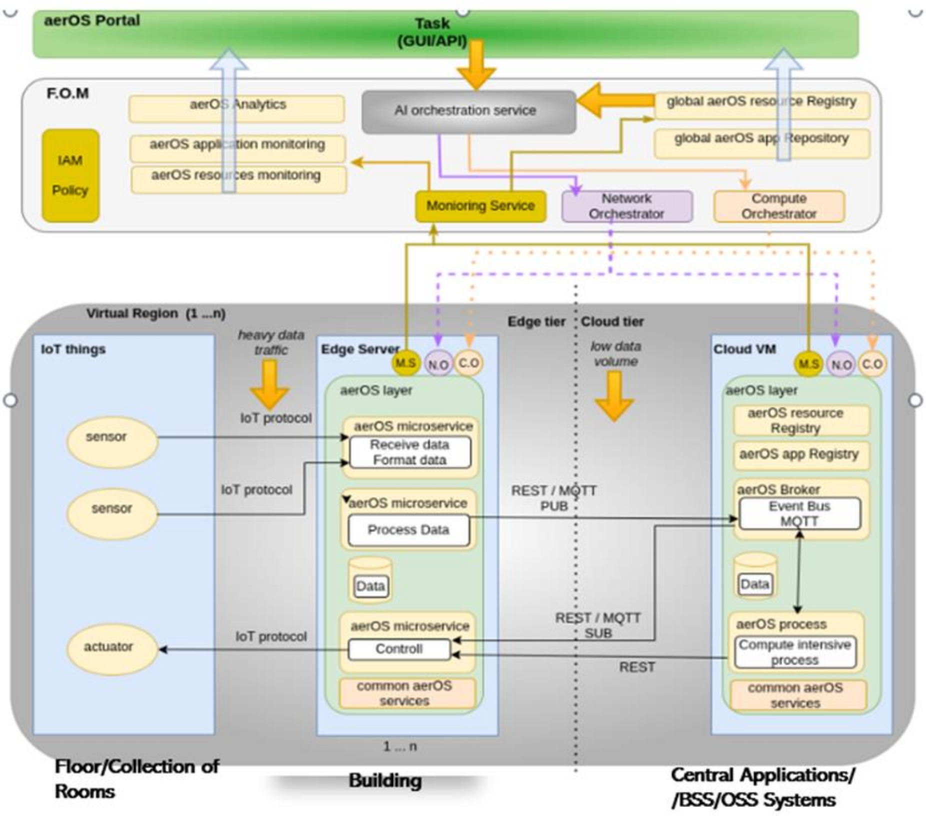


Figure 42. Blocks diagram of Use case 5 in sync with aerOS architecture

[26]https://www.pwc.com/us/en/industries/capital-projects-infrastructure/library/scaling-up-smart-buildings.html

3.5.5.1.4. Actors involved in Scenario 1

The actors involved of this use case have been collected following the table below, representing the actors involved, business area impacted, together with the type of impact and what it consists of.

Table 33. Actors involved in Scenario 1 of Use case 5

ACTOR	B$ AREA	TYPE OF IMP.	IMPACT DESCRIPTION
End-user/Employee	Any	Direct	Must approve to his/her smart workspace placement, and abide to the recommendations and instructions of the system
Customer/Property owner	Management	Indirect	Must invest in system intelligence to increase efficiency and reduce costs
IT Operations	Technical Support	Direct	Must implement & support aerOS capabilities
Facility Manager	Technical Support	Direct	Must comply with aerOS recommendations
System Provider (Developer/Integrator)	Engineering	Direct	Must implement aerOS nodes capabilities (e,g, AI, orchestration, interoperable semantic & syntactic data ontologies e.g.)
IOT Vendor	Manufacturing	Indirect	Must implement aerOS nodes capabilities (e,g, AI, orchestration, interoperable semantic & syntactic data ontologies e.g.)
Data Scientist	Engineering	Direct	Must explore explainable & frugal AI towards data models that are specific to each building needs

3.5.5.2. Scenario 2: Cybersecurity and data privacy in building automation

3.5.5.2.1. Description

The second scenario of Use Case 5 will build on top of use case scenario 1 and transfer and integrate aerOS components which will be developed within work packages WP3 and WP4 regarding Cybersecurity and data privacy with the goal of enhancing the security approach in Smart Buildings. Components that will support secure access to IoT processes deployed within building working areas, and governance procedures to enable supervised and authorized sharing of IoT generated data, will be deployed to frame with trust mechanisms the IoT, smart building solution, within COSMOTE premises. Beyond security mechanisms integration within smart buildings management system, the 5G network infrastructure, provided and deployed within COSMOTE area, will be used to demonstrate aerOS capabilities secure extension regarding user and third-party applications access to services and data from the core network.

Within use case 5 and in the process of optimizing energy efficiency and health safety and sustainability of smart buildings a multitude of heterogeneous sensors will be deployed within COSMOTE pilot smart buildings. These sensors will record a huge amount of data which will be transferred to edge cloud infrastructure not only to be stored but to also be analysed and used as input to AI models. Output of AI services will both guide decisions and actions to be transferred to other far-edge devices, the actuators, in order to further configure working space conditions, and will also provide recommendations to users regarding their working conditions and placement. Additionally, as data is the fuel of algorithms and decisions these data will also have the possibility to be shared among IEs that may submit requests to reuse these data or obtain trained models based on these data or get policies developed based on these data.

Reading carefully the above process it is obvious that IoT systems deployed, on top of aerOS infrastructure elements (IE), are increasingly interconnected and although they enable automation, optimization, and monitoring of building functions such as HVAC, lighting, security, this increased connectivity also creates new security risks and vulnerabilities. Insecure communication channels and weak authentication mechanisms make them vulnerable to data eavesdropping or even permit data poisoning. The inclusion of several devices and systems and multiple parties (owners, managers, applications etc) introduce the possibility of unauthorized access to data and processes that may produce critical decisions regarding the current working conditions and building operation. Unattended devices without the possibility to provide updates are left exposed to security exploits. Except from the possible risks coming from IoT data and processes exposure it is equally important to have in mind the risks that emerge due to the aerOS orchestration capabilities that are provided so that every aerOS IE (node) can be accessible for resources orchestration and monitoring. Every IE exposes some capabilities to either receive orchestration commands regarding deployments, connectivity etc or to provide resources that could support external processes. These exposed capabilities, provided as exposure API, if not properly secured can introduce obvious risks regarding third parties intervention both to aerOS IE environment but also to the hosting network segments too.

3.5.5.2.2. Specific objectives

In the ground of scenario 2 of use case 5, there is the goal to provide secure extension of aerOS capabilities with the integration of 5G network facilities, operating at COSMOTE premises, and the use of 5G and smart network components such as Network Exposure Functions (NEF) and network applications (NetApps). At the moment in 5G networks there is limited service exposure and although 5G networks have a wide range of services and capabilities, it is quite challenging for external applications to access and utilize these services effectively. Within the second scenario, the goal is to provide NEF (emulated) deployment, with the support of aerOS ecosystem, which should be able to provide standardized interfaces and make it easier for external applications to discover and access 5G network services. With the proliferation of devices and applications connected to 5G networks, security has become a critical concern and secure standards to access core network services information are critical. Finally, as vendors and operators involved in the 5G ecosystem, and new services and applications are emerging interoperability between network and flexibility to accommodate new use cases are a demand. The deployment of a NEF emulator, which can authenticate and authorize the requests according to the policies set by the network operator, of NetApps that will interact with NEF to request network resources and services on behalf vertical applications are planned within this second use case 5 scenario.

It is expected that a more refined description of the specific objectives of the scenario 2 of Use case 5 will be provided in the next iteration of the deliverable. As it is a scenario that will be built on top of scenario 1, most efforts have been put on the thorough description of specific objectives of the former.

3.5.5.2.3. aerOS in Scenario 2

The basic unit within the aerOS meta-operating system for the IoT edge-cloud continuum is the Infrastructure Element. Although this is not going to be extensively analyzed here, the basic principles of an IE element is that it provides the appropriate virtualization layer, which can operate over a variety of hardware resources, which provides the runtime environment where core components are deployed to enable the complete management and orchestration of underlying resources, providing thus network connectivity, processing and storage capabilities and supporting IoT applications deployment as close to the edge as needed. Although aerOS IE is much more than this, it is a prerequisite that all these operations regarding both meta-operating system resources orchestration and user IoT services management should be performed within a trusted environment where no one can tamper with the resources operating to form the edge-cloud continuum and user data and IoT services cannot be accessed without having the explicit permission from the owner. Thus Cybersecurity components designed and developed within WP3 and WP4 regarding data encryption, authentication and authorization will be deployed and their functionality will be tested in this, second, use case 5 scenario.

Certain techniques will be explored -always aligned with the global cybersecurity and trust approach of aerOS meta OS- like single sign-on technique based on OpenID, or others, to enable users and applications to authenticate and access IE resources and IoT services. Following diagram, Figure 43, is presenting a schematic diagram of the **proposed authentication and authorization process**. All entities requiring access to IE data and deployed services should first identify themselves, acquire some authorization enabling capability token and then permitted (or not) to specific services or data. Needless to say, all communications and data exchanges will be secure and private based on endpoints encryption enforcement. **<u>It is worth remarking that these diagrams are only an early, preliminary proposal. All this structure will be clarified when the global cybersecurity and trust approach in aerOS meta OS will be defined (tasks T3.4 and T4.5).</u>**

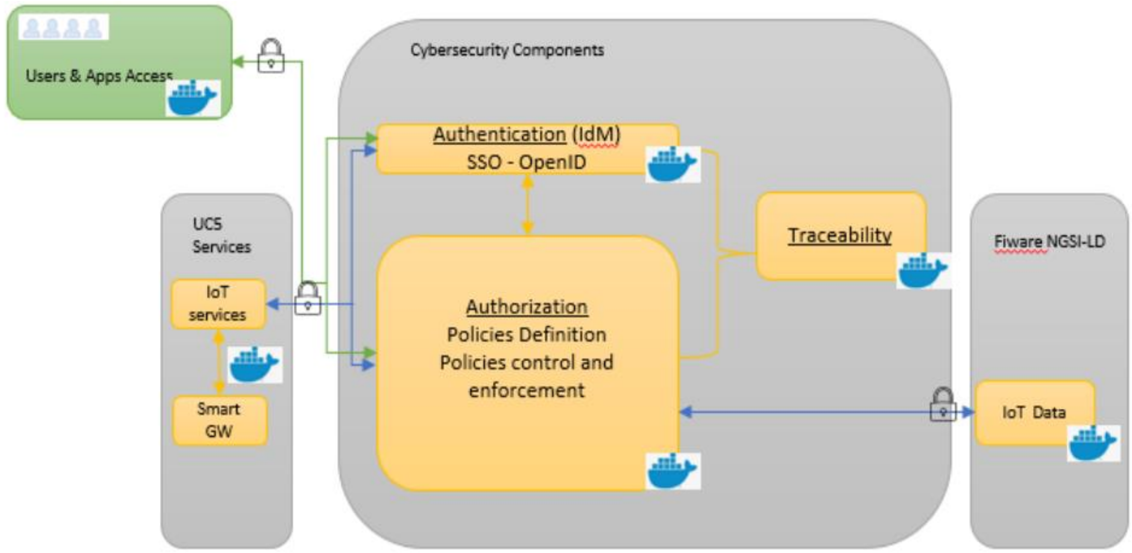


Figure 43. Authentication schema of aerOS in Use case 5, scenario 2

For the 5G deployment within this scenario, targeting to extend aerOS capabilities, which will integrate services regarding either deployments over radio connections or deployments exposing 5G core capabilities and data for the benefit of vertical applications a topology very similar to the following one will be deployed.

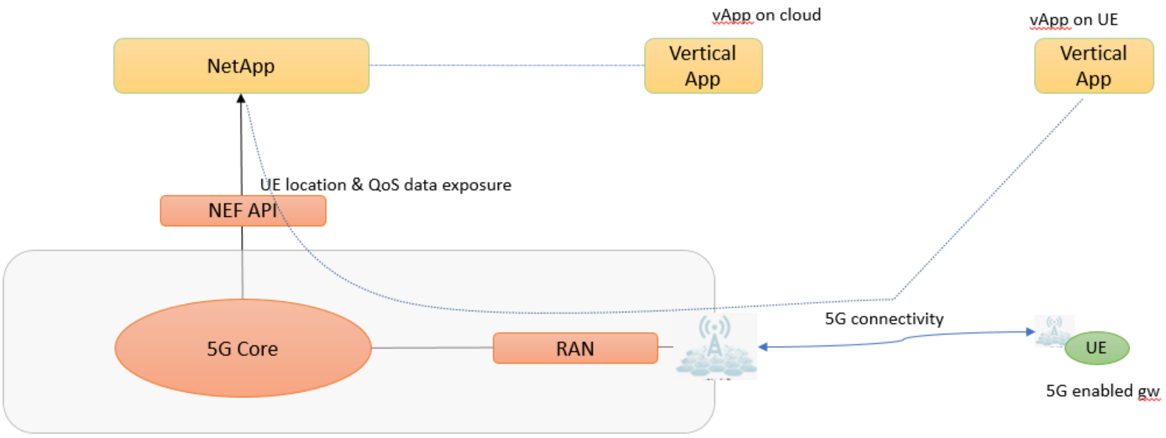


Figure 44. Tentative composition of 5G components deployments in scenario 2 of Use case 5 in aerOS

In this case a smart gateway is upgraded with 5G connectivity module and it will be connected to 5G network. The core components that will deployed and managed within aerOS ecosystem will be the NEF emulator, 2 Network Applications and 2 Vertical Applications. A brief description of the role and the deployment mode of these is provided in the next paragraphs.

The **Network Exposure Function (NEF) emulator** is a key component in the 5G core network architecture, ot will be deployed and managed (LCM) within the aerOS IE, and will be used to provide a secure and controlled interface for third-party applications that need to access services and data from the core network.

NEF will act as a safe intermediary between the core network and external applications, and will enable them to access network services and data while enforcing security and access controls.

Network applications (NetApp), deployed and managed (LCM) within aerOS IE, will abstract and streamline the communication of vertical applications (vAPPs) with the 5G Core (5GC). It will be deployed within IE either as a FaaS or a container workload and will operate as a wrapper of 5G/NEF Northbound APIs to expose services through Business APIs. The deployed NetApp will allow vertical applications to be developed/upgraded (and take advantage of the 5G exposure capabilities) without changing integral parts of their software, they will only consume the business APIs.

The **vertical application (vApp)** will either be deployed within the UE (i.e the 5H enhanced smart gw) or have a placement somewhere else within the Cosmote edge aerOS IE. It will consume the NetApp business interfaces making requests which will be translated to 3GPP specified API calls and when the necessary computations and data manipulation are completed these business APIs will transfer the information to the vertical application.

These components and a schematic of their, layered, interaction is presented in the following figure:

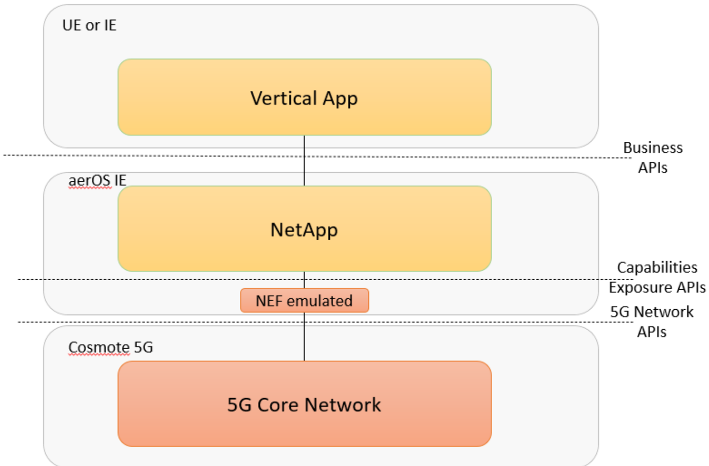


Figure 45. NEF-NetApp-vApp aerOS supported interaction

The scope of this implementation of 5G integration within the second scenario is to extend aerOS capabilities by providing standardized interface and make it easier for external applications to discover and access these 5G network services. This extension will "run" on a secure and controlled interface when accessing services and data from the core network as dictated by aerOS architecture.

3.5.5.2.4. Actors involved in Scenario 2

The actors involved of this use case have been collected following the table below, representing the actors involved, business area impacted, together with the type of impact and what it consists of.

Table 34. Actors involved in Scenario 2 of Use case 5

ACTOR	B$ AREA	TYPE OF IMP.	IMPACT DESCRIPTION
IT Operations	Technical Support	Direct	Must implement & support aerOS capabilities, specifically related to 5G actual connection and the NEF emulator
Facility Manager	Technical Support	Direct	Must comply with aerOS recommendations (in terms of privacy and cybersecurity).
System Provider (Developer/Integrator)	Engineering	Direct	Must implement aerOS nodes capabilities (in terms of privacy and cybersecurity).

3.5.6. Requirements of the trial

Below there is a list of the specific requirements identified for this trial. A full list of all the requirements gathered (in M9) for Pilot 5 as a whole are available in Appendix B.

- Far Edge and Edge storage capacity
- Cloud storage capacity
- Support any IoT sensor type and protocol
- Automatic service recovery upon system or network loss
- IoT Data Collection and processing fully automated, reliably transferred in a configurable manner
- IoT system automatic configuration management
- User-friendly monitoring of system health and remote management
- Scalability to Support Mass Deployments
- Data Analytics & Decision Making at the Edge
- APIs for 3rd Parties/Stakeholders
- Gateways and Base Stations Heterogeneity
- Web app / Mobile app for end user-system interaction
- Occupancy policy
- Message aggregation policy at gateway-level for lower overhead
- Gateway functionality for harmonizing heterogeneous data
- Distributed deployment of workloads/services along the continuum
- Meta-operating system deployment
- Portability
- Data privacy annotation
- Identity management
- Cybersecurity policies definition & enforcement
- Traceability

3.5.7. Outcomes of the trial

- Interoperabilty in a Smart Building.

Result: Smart Building solution with extension and interconnection capabilities

To exhibit portability and interoperability gains proposed by the aerOS concept, which stands as a unique solution to integration pains of existing heterogeneous IoT sensors market

- Advanced networking in a Smart Building

Result: Mesh network system governed by a meta Operating System

Outcome 2: Definition and implementation of latency controlled distributed smart networking components; Mesh networking and 5G technologies shall be deployed for efficient communication among the aerOS IE.

- Decentralised intelligence

Result: Platform where AI models run dynamically and execute all the way around the continuum

Outcome 3: To decentralise intelligence towards a safe and sustainable working environment. Federated learning at the edge, intelligence close to event and data sovereignty are integral characteristics of the use case definition.

- Orchestration

Result: Meta Operating System as the single point where orchestrator is ordered.

Outcome 4: Smart orchestration targeting wireless network configurations, updates in distributed intelligence criteria and prioritisation, and business critical monitoring information is a key enabler

As expected benefits, aerOS will allow Smart Building stakeholders (represented by COSMOTE in aerOS) to enjoy of the following:

- aerOS nodes intelligence, addressing distinctive infrastructure characteristics of buildings, through autonomous and decentralised decision-making at the edge.
- aerOS unique abstraction approach will offer an adaptable solution that can bridge heterogeneity (data and platforms), so that sensors, systems, and analytics can be orchestrated in the IoT edge-cloud continuum, and new elements or federation with new elements can be added.
- Smart building technologies can provide facilities operators with the tools to anticipate and proactively respond to maintenance, comfort, and energy performance issues, resulting in better equipment maintenance, higher occupant satisfaction, and reduced energy consumption and costs.
- The pilot proposes a unique combination of energy-efficient and health-safe buildings by utilizing a distributed AI approach for proper employees' placement, addressing social distancing and energy efficiency, along with business and personal preferences and work habits, a complex yet.

3.5.8. KPIs related to the trial

Same as for the requirements, it is only the goal in this section to make a bullet pointed list of the KPIs that have been identified. This exercise helps understand the relevant aspects of the pilot that the execution activities will be paying more attention to.

- Energy use reduction
- Performance gains
- Number of VNFs deployed
- Service Availability
- Service Creation/Scalability
- Services directly managed by the FOM
- Improvement of air quality
- Number of AI models used/adapted for the pilot

3.5.9. Legal framework

During the course of task T2.3 (Legal and regulatory analysis and governance specification), several actions have been performed in order to identify the legal framework surrounding activities in Pilot 1. As the main result of this action, find attached in Appendix 0.

Besides that, a thorough analysis of the legal and regulatory aspects affecting the different scenarios of Use case 1 was performed, outputting the following results:

Sectorial regulations (Telecommunications):

- HDPA (Greece) - By complying to the regulations fair access to services, and user/data protection is guaranteed.
- GDPR (EU) – Protection of user data.

Technological regulations:

- IoT – Law 4961/2022 (Greece) - Constitutes a primary, but high level endeavor in view of the forthcoming and more detailed EU legislation on new technologies.

- IoT – EU Connected Communities initiative (EU) - This initiative concerns the IoT development infrastructure, and aims to collect information from the market about existing public and private connectivity projects that seek to provide high speed broadband, more than 30 Mbps.
- IT Systems & Networks – HCA, Law 4727/2020 (Greece) – Cybersecurity and privacy.
- IT Systems & Networks – Directive (EU) 2019/1024, Directive (EU) 2018/1972, EU NIS Directive-2016 – Cybersecurity and privacy.
- 5G Technology – EETT (Greece) – Regulate the efficient use of spectrum, and ensures fair market competition.
- 5G Technology – 3GPP, ETSI, BEREC (EU) – Set the specifications for functional suitability and devices compliances to EC standards, facilitates interoperability among operators.

Usage of products:

- Open source software is used (MQTT, Home Assistant, K8s…). aerOS partners in Use case 5 will be sure to comply with proper licensing and noticing whenever making results public.

4. Requirements

As indicated in Section 2.3, the elicitation of requirements is key in a Research and Innovation Action to ensure the proper coverage of the goals set out for the project. In addition, a thorough procedure for establishing technical, user and system requirements will ensure a more efficient conduction of the technical and pilot activities across the WPs of aerOS. In this section are reported the main aspects related to those procedures, drilled down in (a) Technical Requirements and (b) Requirements coming from pilots (user and system requirements). While in this chapter an overall explanation of the results is provided, the actual list of requirements can be found in Appendix A and Appendix B.

4.1. Technical requirements

A number of 67 technical requirements were recorded following the methodology described in Section 2.3.2.1.

While the full list of technical requirements gathered till M9 of the project **is included in the Appendix A**, this section shows a statistical summary of the results obtained so far.

Summary of the technical requirements is the result of an initial recording, cross checking and updating, combined with an in-deep study of the different technical goals and tasks of aerOS. Through checking and filtering to provide a set of non-overlapping requirements, each of them has been classified as belonging to one or more areas of developments in the scope of the aerOS project.

In the following graphs, some statistics are shown regarding the recorded requirements; presented based on the area they refer to, the roles they concern, the domain they refer, the category they address, their type and priority. As it can be seen, the majority of requirements gathered are non-functional ones, prioritized as Must-have and mostly referring to Data, Infrastructure, AI, Security and Meta-OS areas of the aerOS project. However, there are recorded requirements for almost every area, role, domain and category within the scope of the project.

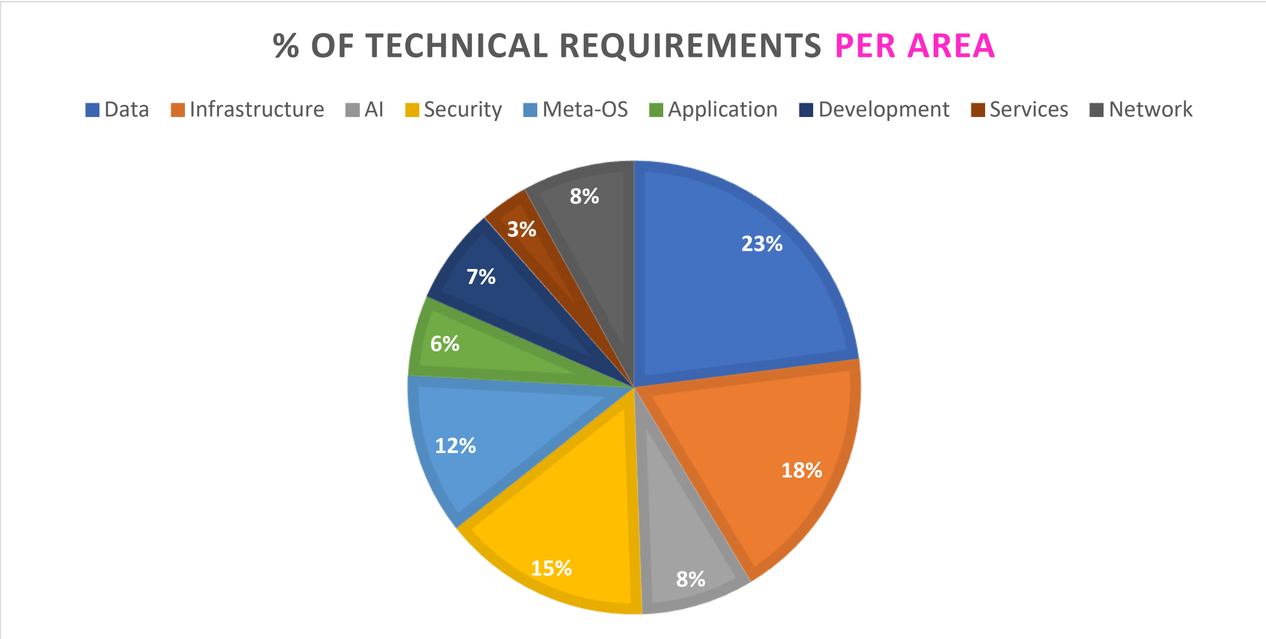


Figure 46. Graph representing the technical requirements per area

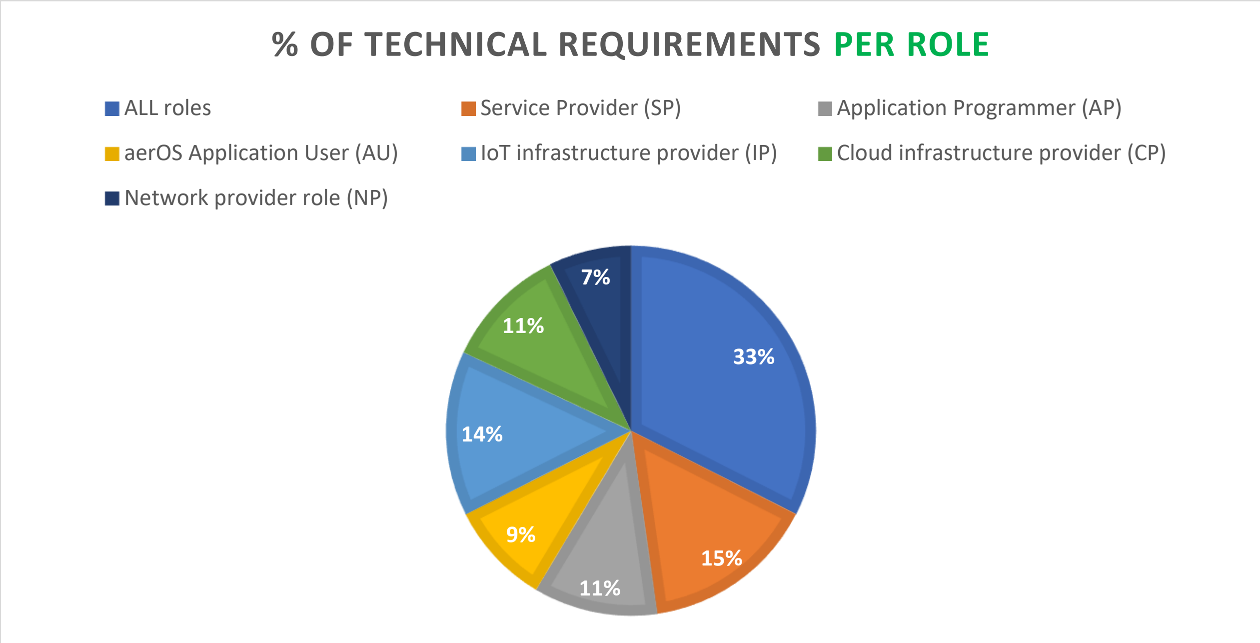


Figure 47. Graph representing the technical requirements per role

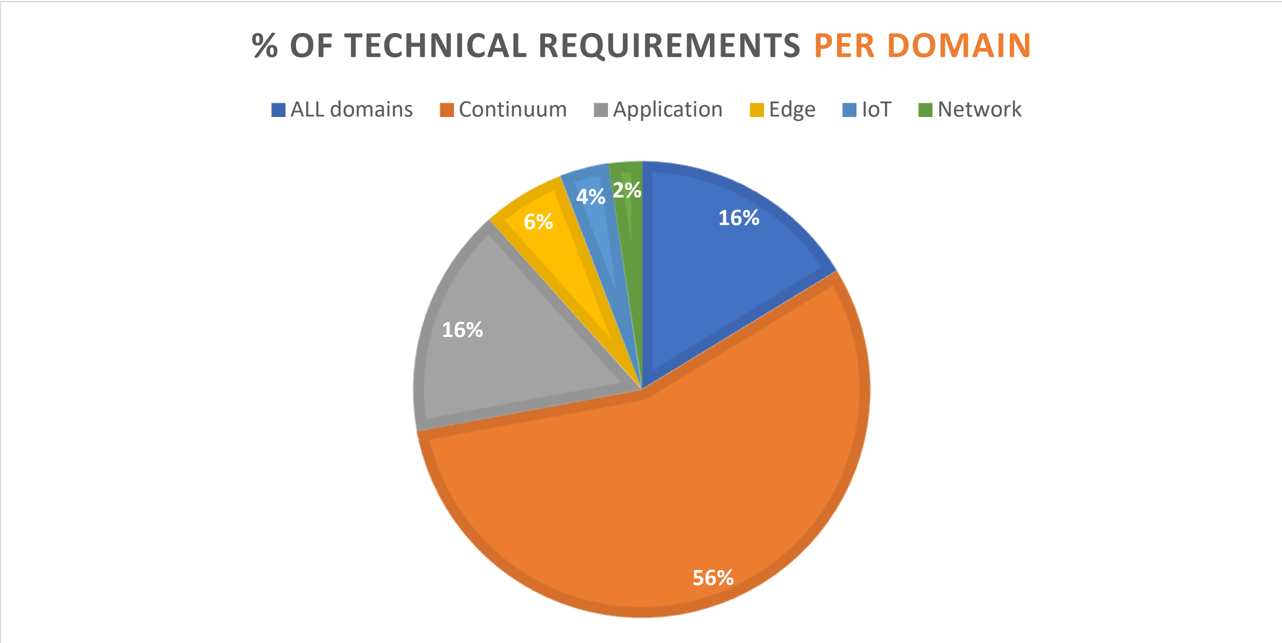


Figure 48. Graph representing the technical requirements per domain

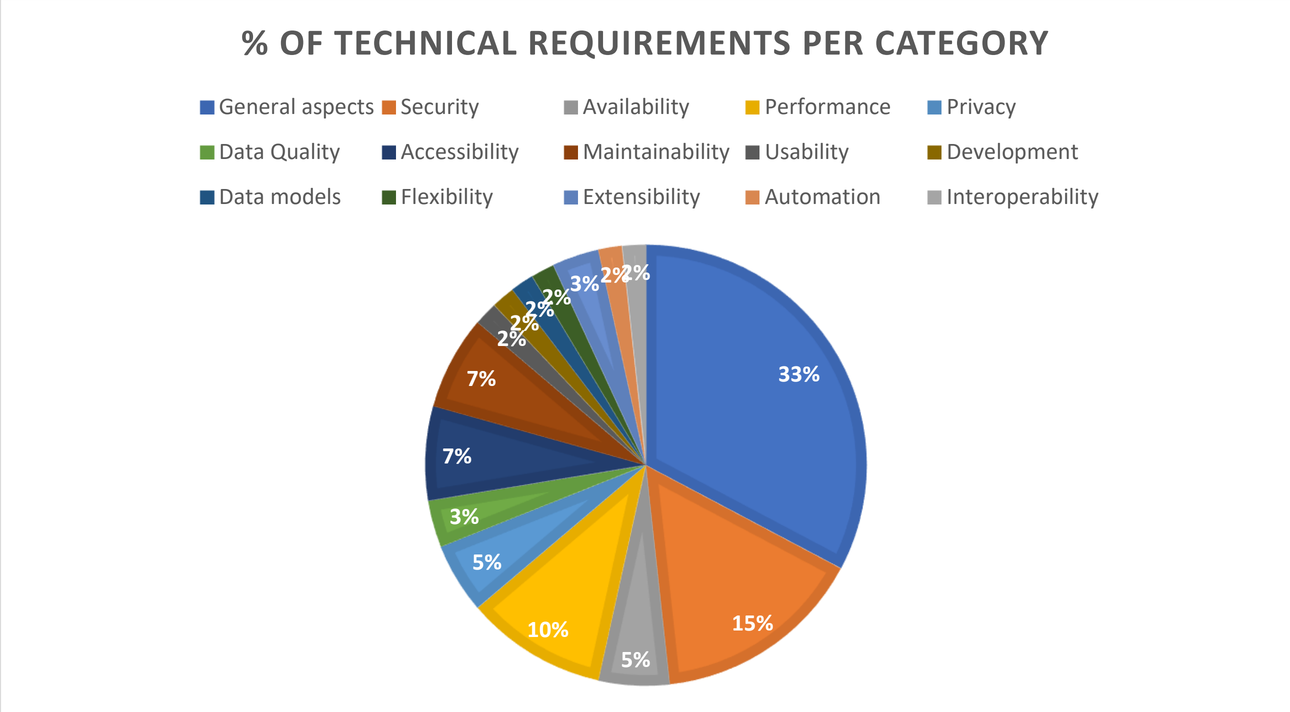


Figure 49. Graph representing the technical requirements per category

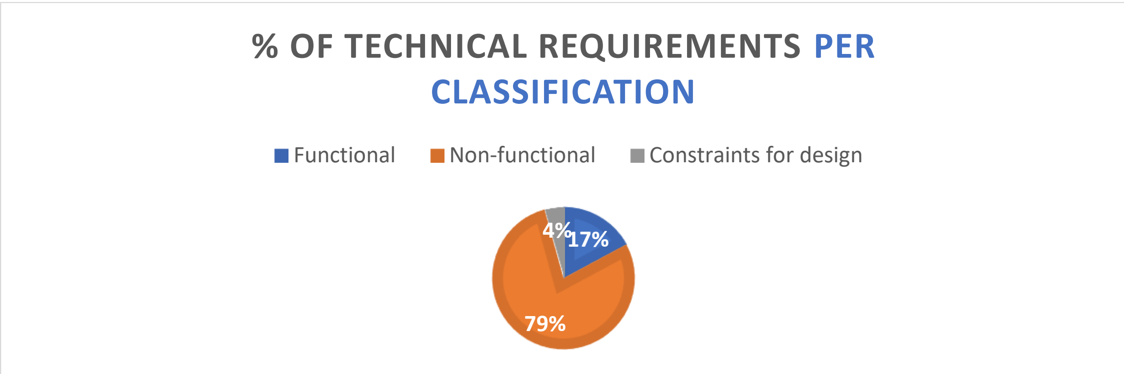


Figure 50. Graph representing the technical requirements per classification

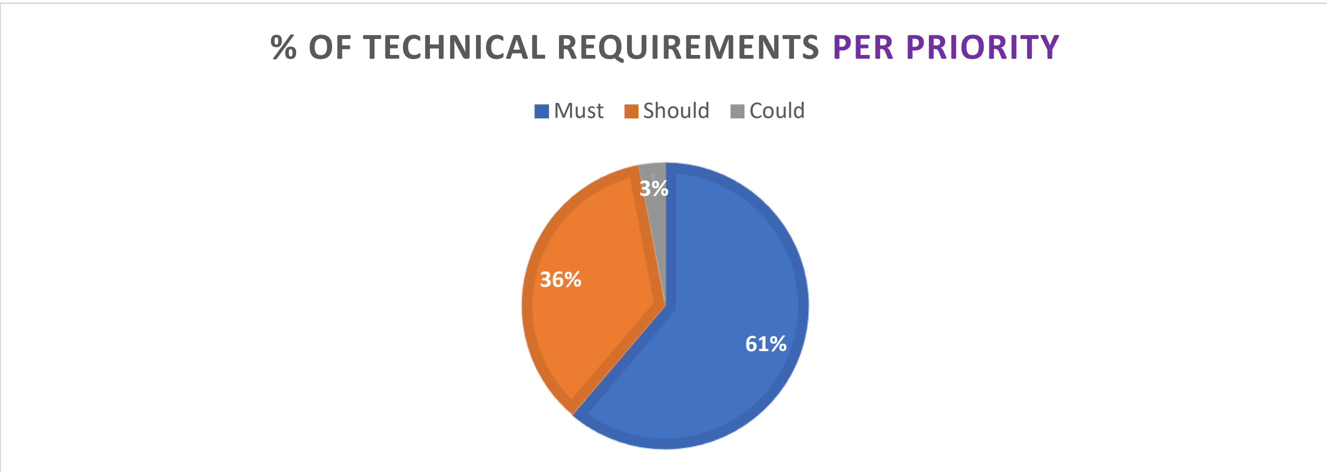


Figure 51. Graph representing the technical requirements per priority

As a written summary of those:

aerOS will seamlessly integrate various edge technologies into a homogeneous continuum. Computing and storage resources can be located anywhere in the network, defining an expanded network compute fabric that spans over (any fragment of) the entire path between (constrained) devices and cloud(s). Resources available in the compute continuum, are geo-distributed and migrate over time while some of them are part of a dynamic infrastructure. aerOS will leverage concept of services as a "unifying abstraction", across resources (i.e. any physical or virtual IoT edge-cloud continuum resource, from device to far-edge, edge or cloud); across multiple infrastructure domains and service levels, supporting federation. aerOS should efficiently orchestrate services in a heterogeneous continuum of resource federation, as opposed to single-domain orchestration (where the orchestrator has full control over resources; while multi-domain orchestration requires coordination across domains.

aerOS should support future hyper-distributed applications, delivering intelligence on demand. High level intents defined by users in a declarative way to specify applications and services needs, as well as consumed services, will be translated in an intelligent and automatic manner to permit efficient deployment and orchestration.

A common meta operating system for the IoT edge-cloud continuum will be developed, which will be able to orchestrate hyper-distributed applications over a heterogeneous and segmented/federated IoT edge-cloud continuum. The proposed aerOS meta-operating system will be hosted in a flexible and fully-orchestrated virtualisation/containerisation-based environment and will be deployable on different levels of the architecture, across the IoT edge-cloud continuum. It will consist of containerised S/W modules that can be executed on top of any operating system of any component of the architecture providing typical services of an operating system, e.g., abstractions, low-level element control, commonly-used functions or message-passing between processes.

aerOS will have ability to be executed in different infrastructural components of the IoT edge-cloud continuum enabling distributed AI and orchestration of services across IoT edge-cloud continuum. It should leverage the powerful toolset of openAPIs on network exposure and APIs for network management and orchestration to fully enable programmability feature in the IoT edge-cloud continuum. aerOS will allow for distributed data management to make user-side applications more intelligent and proactive, and to provide foundation for hyper-distributed applications and services, closer to data sources and event-generating processes without sacrificing aggregated data analysis and insights. Several aspects of aerOS will utilise the (semi)autonomous approaches, in particular these will include mechanisms for self-adaptation and self-healing of the Infrastructure Elements, based on self-observation.

aerOS should introduce a holistic cross-layer solution for cybersecurity, while supporting federated and distributed data governance. The management of the aerOS infrastructure should be as automated as possible, with minimum manual intervention. Security analysis and Privacy analysis will be an integral part of the Software Development Life Cycle.

Among jobs that can be executed in an aerOS deployment should be AI pipelines as a type of distributable services. aerOS components shall allow for execution of those, originating from internal use cases (supporting aerOS mechanisms) and external use cases (originating from applications). Users shall be able to specify requirements related to execution of AI pipelines according to a pre-established data model. Data models that shall support AI requirements and pipeline definitions should be extendable and adaptable to new cases. aerOS shall be able to process large amount of information at the edge and decide which information needs to be transmitted to a central cloud server for further storage and processing. aerOS shall support explainability of models and provide mechanisms for tackling data frugality.

aerOS will handle data generated by heterogeneous sources and support data processing tasks performed within the system towards supporting data autonomy. aerOS should offer mechanisms for defining (compound) data sources and creating data-flow topologies based on streams. Because of the high heterogeneity of aerOS deployments, it should use an interoperability solution based on semantics and semantically represented/annotated data and data flows. aerOS should be able to semantically annotate "raw" data to enable/empower its semantic interoperability mechanisms. Furthermore, aerOS syntactic interoperability solution should allow for user defined extensions; hence, it should have a modular and "parametrized" architecture.

4.2. User and system requirements

As indicated in the previous point, while functional requirements are defined to clarify the system's subject matter and thereby trigger requirements that have not yet been thought of, the non-functional requirements refer to the behavioural properties that the specified functions must have, such as performance, usability, etc.

Both functional and non-functional aerOS requirements listed below are result of intensive communication among stakeholders, as their analyses have been performed for all pilots separately. However, since requirements identifications is an iterative process that takes place throughout the duration of the project, existing requirements might be improved in the next deliverable D2.3, expected for month M18. Moreover, since an agile and iterative methodology is being used, new requirements without interfering current ones can be easily integrated.

Currently, the project has 54 requirements: 28 functional requirements, and 26 non-functional requirements. Concerning their priority, approximately three quarters are mandatory.

5. KPIs

Although several functional, non-functional, and technical requirements have been identified in previous sections of this deliverable, measurement of aerOS performance and progress will be done via the usage of Key Performance Indicators (KPIs). Technically, the definition of a KPI is "*a measurable value used to evaluate how successful a person or organization is at reaching a target*". For aerOS, the description indicated in 2.2 prevails (very aligned with the former statement). Their evaluation is done against a predefined set of values. While the evaluation duty of the project is assigned to WP8, and more specifically to "T5.2 - KPIs definition and setup of evaluation framework", and "T5.3 - Continuous use cases analysis, evaluation and assessment", which will start their execution in month M12, this deliverable serves as the first step for their identification.

It has been agreed that all KPIs will provide a quantitative assessment. This means that each KPI - value is going to be a number or a percentage over a baseline (i.e., if defined a KPI for users' satisfaction, a value from a set of numbers between 1 and 5 should be chosen, where 1 would represent complete dissatisfaction and 5 would represent complete satisfaction).

5.1. Overall KPIs of the project

The KPIs of the whole project are not targeted explicitly in this document, as the whole work of it is not under the scope of the task T2.2. Actually, task T5.3 (KPIs definition and setup of evaluation framework) is in charge of the definition of the KPIs of aerOS, which has not started at the time of writing this deliverable. Therefore, the first definition of the KPIs will be provided in the **deliverable D5.1** (due to M12) as an output of the task T5.3. Nevertheless, a general introduction to the KPIs definition of this research project can be outlined. In aerOS, it is envisioned to divide KPIs into four main dimensions or fields of measurement:

- Key Validation Indicators (KVI)
- Technological
- Assessment and impact
- Pilots (will be covered in the next 5.2 subsection).

The KVIs are defined in the Gran Agreement (GA) as tangible and more specific indicators with the final purpose of assessing the expected **result of the seven main objectives** to be achieved at the end of aerOS. Thus, the **KVIs** are **fixed (by DoA**) and directly **mapping to the global objectives of the project**. The vast majority of this KVIs, 18, belong to the first five main objectives, which are more related to technological aspects of the project. It is expected that, apart from being maintained as mandatory indicators to be tackled, the KVIs will spark the creation of now, related KPIs. For instance, KVI-1.1 (Orchestration of IoT applications with a maximum optimality gap of 15% for the response time) is a strong candidate for further technological KPIs definition due to its relevance and overall coverage of diverse fields of aerOS.

On the other hand, aerOS is a research project which one of its pillars is the contribution to the European IoT-edge-cloud continuum technology stack, so the technological KPIs will play a key role in the final evaluation stage. In this project, the technical and development related tasks (11 in total) have been divided into two work packages (WP3 and WP4) in the Gant Agreement.

Apart from that catalogation, it was considered interesting to clusterize some of those into more transversal "blocks or areas" that would take into consideration tasks intertwinning to achieve a better efficiency of the resources. This initiative has resulted in the creation of 5 working areas:

- Orchestration -resources, services and network- (T3.1, T3.2, T3.3)
- Data infrastructure (T4.1, T4.2)
- Cybersecurity and Trust infrastructure (T3.4, T4.5)
- AI and analytics (T4.3, T4.4), and
- Monitoring and configuration (T3.5, T4.6).

The previous is relevant for the KPIs definition, as it is expected that within the duties of these working groups will be, precisely, the identification and creation of technological KPIs. Furthermore, in the Gant Agreement are defined 19 technological contributions (TC) that aerOS is expected to provide as the outcome of the aforementioned tasks, so this TCs will also be taken into consideration for defining the technological KPIs.

Finally, the overall performance of the project, not only considering technological results, but taking the project as a whole, must also be evaluated. Here is where appears the last group of KPIs: Assessment and impact. This group involves KPIs related to exploitation (Open Calls, business models, product exploitation, …), impact (standardization, dissemination and communication), and ethical, societal, gender and legal aspects. Thus, this group is composed by a heterogeneous range of aspects, which could, in addition, be regrouped into more specific subgroups. As in the technological KPIs, the KVIs belonging to the objectives 6 and 7 of the GA are strong candidates to feed this group of KPIs.

5.2. List of KPIs from pilots

In this section the KPIs designed to assess the success of the pilot deployments are described. It is expected that by using the aerOS services, the efficiency and productivity of project's industrial stakeholders will be improved. Currently, up to 38 KPIs have been identified across the five pilots of the project.

It is worth noting that the KPIs associated to the pilots that have been gathered in this document are only preliminary. Moreover, those that directly come from the DoA are kept and detailed, while those that have been recently created might still be under definition (especially the target number, that requires a more advanced stated in the work in pilots).

The stakeholders of aerOS reserve the right to modify these along the course of tasks T2.2, T5.2 and, in general, during the project. A more thorough explanation will be provided in the subsequent version of this deliverable (D2.3) by M18 – February 2024.

The ID of the KPIs is constructed iteratively as follows: KPI X.Y.Z – being X the number of the pilot, Y the number of the scenario and Z the iterative, unique number identifier.

KPIs (of pilots) identified by M9 are listed below:

Table 35. List of KPIs associated to pilots identified by M9

KPI id	Name	Description	Metric	Target
KPI 1.1.1	Production process robustness	Increase robustness of the production process	%	10%
KPI 1.2.1	CO^2-footprint production prediction accuracy	Prediction accuracy for each individualised produced product	%	90%
KPI 1.2.2	Actual CO^2-footprint production	Measure the CO^2-footprint production for each individualised produced product.	N/A	N/A
KPI 1.2.3	CO^2-emission reduction	Reduce the CO^2-emission through the calculation of an optimised production path	%	20%
KPI 1.3.2	AGV use	Use of AGV due to the aerOS components	%	>80%
KPI 1.3.3	AGV availability	Availaiblity of AGV due to the aerOS components	%	> 95%
KPI 2.1.1	Consumed renewable energy	Consumed renewable energy based on decision making process of aerOS	MWh per month	20
KPI 2.2.1	Task distribution effectiveness	Effectiveness of task executed on schedule through aerOS nodes	%	99.5%.
KPI 2.2.2	Task distribution scalability	Scalability of task distribution and management through aerOS	tasks executed per month	10k
KPI 2.3.1	CPU utilization	How efficiently the CPU in the system is used. Expressed in time of utilisation against total utilization time	%	>80%
KPI 2.3.2	Carbon awareness	Share of green energy in the consumed power over time	%	60%
KPI 2.3.3	Number of edge nodes	How many edge locations are connected in		2

		the continuum		
KPI 2.3.4	Total workload distributed and executed	Number of batch processing jobs successfully distributed and executed by the system	TBD	300k
KPI 3.1.1	Performance and connectivity capabilities improvement	Performance and connectivity capabilities improvement compared with existing solutions (single vehicle).	%	20%
KPI 3.1.2	Swarm of vehicles performance improvement	Improvement of performance using a swarm of vehicles and by means of (AI-supported) aerOS services deployed	%	20%
KPI 3.2.1	CO^2 emissions reduction by	Reduced noise emissions and CO^2 emissions using electric swarm in in a platooning association	%	80%
KPI 4.1.1	Core equipment idle time	Reduction of idle time caused by core equipment failure or unavailability	%	20-30%
KPI 4.1.2	Malfunctions reduction	Number of equipment malfunctions reduction versus manually reported by the staff	%	30-40%
KPI 4.1.3	Damaged containers reported	Decrease of the number of damaged containers manually reported by staff	%	30-40%
KPI 4.2.1	R^2 of regression models	Performance evaluation metrics of regression AI models (R2)	R^2	0.8
KPI 4.2.2	MAE / RMSE of regression models	Performance evaluation metrics of regression AI models (MAE / RMSE)	MAE	20%
KPI 4.2.3	Accuracy of classification models	Performance evaluation metrics of classification AI models (accuracy)	%	60%
KPI 4.2.4	Recall of classification models	Performance evaluation metrics of classification AI models (recall)	%	60%
KPI 4.2.5	Frugal AI predictive maintenance models	Number of frugal AI model trained for predictive maintenance use case scenario of pilot 4	Number	10
KPI 4.2.6	Frugal AI computer vision models	Number of frugal AI model trained for computer vision use case scenario of pilot 4	Number	3
KPI 4.2.7	Edge-AI performance	Number of models executed on edge nodes	Number	5
KPI 4.2.8	CHEs maintained predictively	Number of CHEs with predictive maintenance	Number	4
KPI 4.2.9	Container damage types	Number of damage types on container surfaces identified by CV AI models	Number	3
KPI 4.2.10	Connected CHEs	Number of CHEs connected to aerOS platform	Number	4
KPI 4.2.11	Video streams	Number of simultaneous video streams being managed by aerOS platform	Number	3
KPI 5.1.1	Energy use reduction	20% Energy use reduction, using frugal AI and real-time processing in aerOS instead than in the cloud.	%	80%
KPI 5.1.2	Edge processing performance	Edge processing and IoT performance gains, by evaluating the performance characteristics of the solution	TBD	TBD
KPI 5.1.3	5G VNFs integrated	Development of different VNFs in the 5G network that are fully integrated with aerOS ecosystem	Number	5
KPI 5.2.1	Service Availability	The aerOS automation responds to failures by instantly re-deploying failed nodes with minimum interruption time	%	99,99% in the service window
KPI 5.2.2	Service Creation/Scalability	Demonstrate the capability of dynamic provisioning of the service as well as scaling	Time (mins)	TBD

		in and out of buildings		
KPI 5.2.3	Services directly managed by the FOM	Number of services/workloads directly managed by the FOM and deployed along the IEs	Number	TBD
KPI 5.2.4	Improvement of air quality	Reduction of CO^2 levels (or other gasses) as a result of using frugal AI and real-time processing in aerOS to achieve an efficient distribution of workers in the office.	% or ppm	TBD
KPI 5.2.5	Number of AI models used/adapted for the pilot	Number of AI models which has been used in the pilot or specifically adapted to its requirements.	Number	TBD

6. Conclusions and future work

After the first months of analysis of requirements and description of the use cases, by M9 (May 2023), some conclusions may already be drawn.

- The usage of the Trial Handbook methodology is proving to be a successful tool to keep a healthy pace of fulfilment of all actions related to use cases. It has also proven to be valid for transferring information from the online, continuously updated document into this deliverable.
- Methodology for requirements gathering has created slight misalignments in timing and content, with the creation of two templates and the synchronization of various work teams has resulted challenging. However, this has served to bring the different perspectives to filling both technical and user and system requirements.
- A total of 121 requirements have been elicited, divided in 67 technical and 54 coming from the stakeholders of aerOS. It is expected that these will be reviewed and enhanced in the next phase of the task.
- A total of 38 KPIs (coming only from pilots) have been already identified. The actions related to KPI methodology, identification, planning and assessment do not fall under the scope of this task & deliverable.

Regarding the actions ahead, it is foreseen that the next period of task T2.2 will be intense in activity. From M9 (this point of time) till M18, the technical WPs will be advancing, thus more technical requirements will be identified/mapped/disregarded. In addition, WP5 (pilots) started only some months ago, and as it will advance in the execution, it will help clarify the scope of the pilots. Furthermore, the next period will be focused on the creation and submission of deliverable D2.3. It is expected that, by that document, all the propositions started in this deliverable will be enhanced.

D2.3 will be the final document describing use case definition and requirements gathering.

A. Technical Requirements table

ID	Refers to	Name	Description	Role	Domain	Category	Type	**Priority**	Rationale	Acceptance Criteria
TR-1	INFRASTRUCTURE	Homogeneous seamless integration of diverse edge technologies	Seamlessly integrate various edge technologies into a homogeneous continuum	ALL	Continuum	Interoperability Accessibility	NF	M	Seamless integration of different edge technologies achieving homogeneity across the continuum	Common homogenous access agnostic to the edge technology.
TR-2	INFRASTRUCTURE	IoT edge-cloud continuum resources	Computing and storage resources can be located across the network, defining an expanded network compute fabric that spans over (any fragment of) the entire path between (constrained) devices and cloud(s)	ALL	Continuum	Availability Accessibility	NF	M	Computing and storage resources can be located across the network; IoT, Edge, Cloud	Accessibility to orchestable resources at any domain.
TR-3	APPLICATIONS	Hyper-distributed applications support	Support future hyper-distributed applications, delivering intelligence on demand (when/where needed)	ALL	App Continuum	General	NF	M	Support of scalable distributed applications execution where parts of application run in different domains of the continuum delivering effectively required intelligence	Distributed application constructed as a service chain where each scalable component runs at the aggregated continuum.
TR-4	META-OS	Meta-operating system for the IoT edge-cloud continuum	Provide a common meta operating system for the IoT edge-cloud continuum, which will be able to orchestrate hyper-distributed applications over a heterogeneous and segmented/federated IoT edge-cloud continuum.	ALL	App Continuum	General	NF	M	Provide a meta-operating system to make possible scalable distributed applications constructed as service chains to effectively execute over offered resources across the continuum. This requires orchestration of distributed application execution over distributed continuum resources.	Scalable distributed applications constructed as service chains effectively execute over offered resources across the continuum.

ID	Refers to	Name	Description	Role	Domain	Category	Type	Priority	Rationale	Acceptance Criteria
TR-5	META-OS	Meta-operating system host environment	The proposed aerOS meta-operating system will be hosted in a flexible and fully-orchestrated virtualization/containerization-based environment	IP CP NP	Continuum	General	NF	M	A Virtualization/containerization environment provides the required flexibility to host a distributed meta-operating system where applications will be executed across the continuum.	Applications execute in a fully orchestrated virtualization/containerization environment hosting the distributed across the continuum meta-operating system.
TR-6	META-OS	Meta-operating system deployment - Portability	The envisioned meta operating system will be deployable, across the IoT edge-cloud continuum. It will consist of containerized S/W modules that can be executed over varying operating systems providing required services e.g., abstractions, low-level element control, commonly-used functions or message-passing between processes.	IP CP NP	Continuum	General	NF	M	Enable components at each part of the continuum to provide orchestrable resources for apps and services deployment.	aerOS can be executed on top of varying operating systems
TR-7	META-OS	Meta-operating system orchestration and AI enabler	aerOS will have the ability to be executed in different infrastructural components of the IoT edge-cloud continuum enabling distributed AI and orchestration of services across IoT edge-cloud continuum.	ALL	Continuum	Performance Availability Data quality	NF	M	Provide an environment for deploying distributed AI mechanisms as well as hyper distributed applications and services.	Distributed AI mechanisms as well as hyper distributed applications and services are efficiently deployed over the continuum.

ID	Refers to	Name	Description	Role	Domain	Category	Type	Priority	Rationale	Acceptance Criteria
TR-8	META-OS	Meta Operating System modulari-ty	aerOS will be modular in its implementation, allowing the deployment of different modules on the Infrastructure Elements (IE) conforming the IoT edge-cloud continuum, e.g., a smart device, IoT gateway, edge node or net-work component.	IP CP NP	Continuum	General	NF	M	Take advantage of virtualiza-tion technology for ease of deployment, isolation, per-formance, personalization and expandability.	aerOS will be modular in its implementation, allowing the deployment of different modules on the Infrastructure Elements (IE)
TR-9	NETWORK	Network pro-grammability in the IoT edge-cloud continuum	aerOS should leverage the powerful toolset of openAPIs on network exposure and APIs for network management and orchestration to fully enable programmability feature in the IoT edge-cloud continuum	NP	Continuum	General	NF	M	Enable smart networking capabilities for performance, availability, resilience, securi-ty.	Network parameters (e.g., throughput, bandwidth limita-tion) can be configured over a virtualized deployment.
TR-10	INFRASTRUCTURE	Dynamic re-sources	Resources available in the compute continuum, are geo-distributed and make part of a dynamic infrastructure	IP CP NP	Continuum	Availability	C	M	Support and exploit the dy-namicity of the environment.	Seamless access to resources belonging to different IEs within the continuum.

ID	Refers to	Name	Description	Role	Domain	Category	Type	**Priority**	Rationale	Acceptance Criteria
TR-11	DATA	Data autonomy	aerOS will handle data generated by heterogeneous sources and support data processing tasks performed within the system towards supporting data autonomy	ALL	Continuum	Security Privacy Availability Data quality	NF	M	Support the heterogeneity of the environment and the data sources to provide for data autonomy.	Data can be managed uniformly and following autonomy rules (to be defined).
TR-12	APPLICATIONS, SERVICES	Usage requirements	High level intents are defined by users (i.e., developers, service consumers, data providers, administrators) specifying needs, in terms of QoS and geo-scope. By leveraging these views, aerOS will orchestrate services in an intelligent and automatic manner	ALL	Continuum	General	NF	M	A way to provide an efficient and agnostic platform to handle the complexity of the operations while exploiting the benefits of the continuum.	High level intents are defined by users and efficiently reflected in deployments.
TR-13	DATA	Distributed data management	aerOS will allow for distributed data management to make user-side applications more intelligent and proactive, and to provide foundation for hyper-distributed applications and services, closer to data sources and **event-generating processes** without sacrificing aggregated data analysis and insights	ALL	Continuum	Performance Availability Data quality	NF	M	Efficiently support distributed data management to facilitate intelligent hyper-distributed applications and services.	Distributed data management is illustrated, and it is exploitable by applications and services.

ID	Refers to	Name	Description	Role	Domain	Category	Type	Priority	Rationale	Acceptance Criteria
TR-14	INFRASTRUCTURE	Federation	aerOS will leverage concept of services as a “unifying abstraction”, across resources (i.e. any physical or virtual IoT edge-cloud continuum resource, from device to far-edge, edge or cloud); across multiple infrastructure domains and service levels, supporting federation.	IP CP NP SP	Continuum	General	NF	M	Enable sharing of resources across multiple domains.	Resources across distinct administrative domains and from edge-to-cloud are accessible in a unified way.
TR-15	META-OS, INFRASTRUCTURE	Self-* mechanisms	Several aspects of aerOS will utilize the (semi)autonomous approaches, in particular these will include mechanisms for self-adaptation and self-healing of the Infrastructure Elements, based on self-observation.	IP CP NP SP	Continuum	Performance Availability Maintainability	NF	M	Support self-adaptation and self-healing of infrastructure elements to automate processes and reduce complexity.	Self-monitoring is existent in all IEs and the meta-OS is able to apply measures over itself.
TR-16	META-OS	Applicability	The aerOS approach will be generic and directly applicable to any vertical, cross-vertical business process, and several different physical or virtual platforms.	ALL	App Continuum	General	NF	M	Efficiently support a wide range of diverse vertical use cases.	Diverse use cases may be implemented using the aerOS solution.
TR-17	SECURITY, INFRASTRUCTURE	Cross-layer cybersecurity	aerOS will introduce a holistic cross-layer solution for cyber-security, while supporting federated and distributed data governance.	ALL	App Continuum	Security Privacy Availability Data quality	NF	M	Provide a holistic security solution across each continuum and along federated continuums.	Cybersecurity is covered by the software of the meta-OS.

ID	Refers to	Name	Description	Role	Domain	Category	Type	Priority	Rationale	Acceptance Criteria
TR-18	SERVICES, APPLICATIONS	Multi-domain services orchestration	aerOS must efficiently orchestrate services in a heterogeneous continuum of resource federation, as opposed to single-domain orchestration (where the orchestrator has full control over resources; while multi-domain orchestration requires coordination across domains	IP CP NP SP	Continuum	General	NF	M	Efficiently orchestrate services in a heterogeneous continuum of resources federation.	Services are efficiently orchestrated in a heterogeneous continuum of resources federation.
TR-19	INFRASTRUCTURE, NETWORK	Infrastructure resilience	aerOS should adapt to abrupt network changes, with the orchestrator re-allocating services allocation within IoT edge-cloud continuum	IP CP NP SP	Continuum	Availability Performance	NF	S	Efficiently adapt to the dynamicity of the environment to provide uninterruptible services deployed on the continuum.	Infrastructure proves resilient to the dynamicity of the environment.
TR-20	INFRASTRUCTURE, NETWORK	Resource availability	aerOS should make sure that there is always appropriate amount of resources available per infrastructural element.	IP CP NP SP	Continuum	Availability Performance	NF	S	Eliminate the possibility of resources starvation at each infrastructure element.	Scarcity of resources is efficiently avoided upon the establishment of thresholds.
TR-21	INFRASTRUCTURE, META-OS	Latency prioritization	aerOS should pursue delivering computing resources close to edge devices based on latencies	IP CP NP SP	IoT Edge	Performance Availability Data quality	NF	S	Maximize QoS and network efficiency.	Latency is given priority while deploying resources close to the edge services.
TR-22	DATA, INFRASTRUCTURE	Context awareness	aerOS must support the ability to provide information about heterogeneous IEs	IP	IoT Edge	General	NF	M	Enable context awareness as the ability of the heterogeneous IoT devices to gather information about their environment at any given time.	IEs across the continuum are able to expose their own information (thus, are aware of it).

ID	Refers to	Name	Description	Role	Domain	Category	Type	Priority	Rationale	Acceptance Criteria
TR-23	INFRASTRUCTURE, META-OS	Architecture expandability	aerOS architecture should be able to grow modularly, accepting the inclusion of new, encapsulated functionalities with ease.	ALL	Continuum	General, Extensibility	NF	S	Built a flexible and easily expandable architecture.	There is the possibility to add new structural traits.
TR-24	INFRASTRUCTURE	Hypervisor compatibility	It would be valuable for the aerOS system to be installed in virtualized computational environments and demonstrate integration support to most prevailing open source hypervisors	CP IP	Continuum	General	NF	C	The aerOS should be installed in enterprise-level computational infrastructures with minimum constraints	Demonstrate the installation of aerOS in several hypervisors.
TR-25	INFRASTRUCTURE	Policy configuration and compliance	The aerOS infrastructure must comply and execute centrally defined (enterprise-level) policies	CP IP	Continuum	General	NF	M	The aerOS system must follow well-defined policies for configuration management across the whole continuum	Demonstrate the infrastructure configuration policies definition and execution.
TR-26	INFRASTRUCTURE, NETWORK	aerOS Infrastructure Monitoring	The aerOS system must include enough monitoring infrastructure	ALL	Continuum	General	NF	M	Ability of the user to globally observe the meta-OS.	Existence of monitoring dashboard providing information about the meta-OS.
TR-27	INFRASTRUCTURE, NETWORK	Infrastructure management automation	The management of the aerOS infrastructure must be as automated as possible, with minimum manual intervention	ALL	Continuum	General	NF	M	With a huge number of infrastructure elements, manual actions are a prohibiting factor as they relate to an error-prone and time-consuming process	Depict the utilization of automation engines for management configuration support.
TR-28	APPLICATIONS	Declarative applications requirements	There must be a declarative way to specify the application's infrastructural requirements and other required information	IP SP	Continuum	Flexibility Extensibility	NF	M	Ensuring infrastructure and service specification consistency and simplicity across the continuum	A blueprint is provided to specify infrastructure and service requirements per application in the continuum.
TR-29	NETWORK, SERVICES	Services visibility across virtual network links	Once virtual links are established between infrastructure elements, services must be visible across the link	IP SP	Network	Accessibility	NF	M	Ensuring services visibility access across virtual networks	Interaction between services across the architecture should be possible and configurable.

ID	Refers to	Name	Description	Role	Domain	Category	Type	**Priority**	Rationale	Acceptance Criteria
TR-30	INFRASTRUCTURE, META-OS	Optimized configuration on IoT Devices	The architecture should allow automated setup and upgrade of IoT devices upon desired stated.	IP SP	IoT	Automation	NF	S	Ensuring automation in the configuration of farthest elements of the continuum.	The devices change their configuration dynamically based on continuum status.
TR-31	DATA	(semi) Real-time data analysis support	Support analysing live data in a timely manner and give a response back with the required/suggested action	ALL	Continuum Network	Performance Maintainability	NF	S	Depending on the situation: timely data analysis could improve the quality of work and allow better orchestration or automation of tasks	Data analysis /decision making through aerOS deployed continuum.
TR-32	NETWORK	aerOS network monitoring	System latency and other network parameters must be monitored.	NP	Edge	Performance Reliability	NF	M	Observing overall system latency	Ability to understand global latency in the deployed continuum.
TR-33	DATA	Syntactic interoperability	aerOS data infrastructure should provide support for the most commonly used data formats (JSON, XML, CSV) . In addition, syntactic interoperability solution should allow for user defined extensions. Hence, it should have a modular and “parametrized” architecture.	AP AU SP	App Continuum	Usability, Interoperability, Extensibility	F	S	To deal with large heterogeneity of formats, aerOS should be adaptable to support motley scenarios and to handle alternative formats.	Data pipelines support most commonly used data formats and the data-level interoperability mechanisms shall be extensible.
TR-34	DATA	Composable data topologies	aerOS should offer mechanisms for defining (compound) data sources and creating data-flow topologies based on streams.	AP AU SP	App Continuum	General	F	S	aerOS shall provide mechanisms for defining data sources and data flows	Mechanisms for defining data sources and data flows are provided.
TR-35	DATA	Data streams handling	Stream processing mechanisms should be created using tools and techniques allowing asynchronicity.	AP AU SP	Continuum	Usability	NF	S	aerOS stream processing should follow the asynchronous streams principles	aerOS interoperability tools support streaming data.
TR-36	DATA	Semantic data annotation	aerOS should be able to semantically annotate batch and streaming "raw" data to enable/empower its semantic interoperability mechanisms.	AP SP	App Continuum	Usability	F	S	In order to handling heterogeneous data without centralisation, a data homogenisation solution should be provided anchored in data annotation. aerOS shall provide mecha-	Mechanisms for semantic annotation of batch and streaming "raw" data are provided.

ID	Refers to	Name	Description	Role	Domain	Category	Type	Priority	Rationale	Acceptance Criteria
									nisms for semantic annotation of "raw" data	
TR-37	DATA	Semantic interop-erability	The aerOS data homogenisa-tion solution will be based on standardised ontologies and semantic interoperability mechanisms. To achieve interoperability, aerOS shall employ efficient semantic translation mechanisms.	AP SP AU	Continuum	Data quality	NF	M	Because of the high heteroge-neity of aerOS deployments, it should use an interoperability solution based on semantics and semantically represent-ed/annotated data and data flows.	Semantic interoperability is based on standardized ontol-ogies and utilizes semantic translation mechanisms.
TR-38	DATA	Core data mod-els/ontologies	aerOS Core data models design should be based on well-established ontologies whenever feasible and should ensure extensibility of defined data models.	AP SP AU	Continuum	Data quality, Extensibility	NF	S	aerOS Core data models, as the basis for the aerOS inter-nal data flow/exchange should be based on a set of carefully selected ontologies and should be prepared to be en-hanced/modified dynamically.	aerOS Core data models design is based on well-established ontologies.
TR-39	AI, APPLICATIONS, DATA	AI orchestration and pipelines realization	aerOS must be able to provide AI pipelines orchestration, including monitoring , re-source-requirements mapping and reliable execution in the continuum environment utilizing heterogenous IE.	AP SP AU	App Continuum	General	F	M	aerOS aims to enable the execution of AI pipelines in a distributed manner to increase system reliability. aerOS should provide means to check the status of long-running AI pipelines while matching them with the configurations and capabilities of the continuum resources to select the optimal pipeline realization,.	AI pipelines must be execut-ed in a distributed way in the continuum on the IE that matches the user-defined job-specific requirements and check their status. The AI pipeline that was commis-sioned to be execut-ed in aerOS-based system can be finished even if some unpredicted changes in the envi-ronment happened..
TR-40	AI	Support for non-centralised data processing	aerOS shall be able to process large amount of information at the edge and decide which information needs to be transmitted to a central cloud server for further storage and processing.	AP SP	App Continuum	General	C	M	aerOS shall support AI pipe-lines for training models without centralised data processing. Transmission of information to the cloud shall be kept to a minimum from the point of view of band-width, as well as security.	A selected AI service must be executed in such a way that training data does not leave a local device, e.g. federated learning implementation.

ID	Refers to	Name	Description	Role	Domain	Category	Type	**Priority**	Rationale	Acceptance Criteria
TR-41	AI	Distributed Models deployment in the continuum	aerOS shall support models deployed in different places in the continuum cooperating for doing predictions (Federated Learning).	AP SP	App Continuum	General	F	M	Distributed AI in aerOS can be envisioned as a process of model training and inferring using the available infrastructure or using ready models to support internal or pilot-related functionalities. Predictions may be done on IE "in different places" in the continuum including resource-restricted devices and these IEs can cooperate improve the performance of the whole process.	At least one IE has running service with deployed model that is used for prediction based on data sent to or available at this IE.
TR-42	AI, DATA	AI-related data models adaptability and extendibility	Data models that shall support AI requirements and pipeline definitions should be extendable and adaptable to new cases.	AP AU	App Continuum	Data models	NF	S	Large amount of possible use cases / algorithms / models / data may be utilized with aerOS architecture which requires the possibility to describe them using aerOS metadata.	There is a possibility to add new attributes to the existing data models without need to change the already implemented logic for the attributes that existed in the model before.
TR-43	AI	Support for data frugality and compliance with frugal AI paradigm	aerOS must provide mechanisms for tackling data frugality (small amount of training data and/or labels)and the execution of AI training services should be aligned with the concept of frugality.	AP SP AU	App Continuum Edge	General	NF	M	Due to the heterogeneity of the continuum, frugality (in data, model and labelling) must be considered when designing and implementing AI-based mechanisms especially close to the edge by applying frugality techniques where necessary.	For AI implemented in aerOS (internal or external) at least one frugal technique directed at limited data for AI shall be present.
TR-44	AI	Internal and external AI support	aerOS components must allow for execution of AI pipelines originating from internal needs (supporting aerOS mechanisms) and external services (originating from pilot applications).	ALL	App Continuum	General	C	M	aerOS shall allow to execute AI pipelines specific to pilot applications but may as well use AI to enhance its internal mechanisms.	There is at least one scenario for internal AI and one for external AI in aerOS that can be validated in trial execution.
TR-45	AI	Explainability support	aerOS must support explainability of models.	AP SP AU	App Continuum Edge	General	NF	M	To enhance the trustworthiness of the whole solutions selected AI should be explainable or interpretable.	At least one AI application scenario includes explainability or interpretability.

ID	Refers to	Name	Description	Role	Domain	Category	Type	Priority	Rationale	Acceptance Criteria
TR-46	DATA	Data cataloguing	Metadata about the available data sources and the data they provide	AU SP	Continuum	Data quality	F	M	Data consumers within aerOS (either users or aerOS internal services) need a way for discovering the data that are available in aerOS continuum	Standard interface that exposes the data catalog towards data consumers
TR-47	DATA	Data collection	Automated ingestion of data in the data infrastructure	ALL	Continuum	Accessibility	F	M	Data infrastructure must orchestrate and automate an on-demand collection of data from data sources on behalf of data consumers	Mechanisms for collecting data which will be implement based on the nature of the target data source.
TR-48	DATA	Data privacy labelling	Annotation of sensitive data such as Personal Identifiable Information (PII)	ALL	Continuum	Privacy Security	F	M	Definition of data governance policies for data access must consider sensitive data	Mechanism for annotation of data as sensitive.
TR-49	DATA	Data provenance	Metadata about history of data in a data pipeline	ALL	Continuum	Data quality Security	F	S	Tracing the history of data throughout its life cycle is needed for providing trust in the data	Mechanism for collecting provenance information about data.
TR-50	DATA	Context-aware data access	Definition of data access policies based on context information related to the target data and the data consumer	ALL	Continuum	Privacy Security	NF	M	Data access policies must be defined with a fine-grained level based on context information	Access control mechanism for defining data access policies based on the role of the consumer and the context of the target data.
TR-51	DATA	Distributed data management	Management of data across different data infrastructure instances	ALL	Continuum	General Performance Standards	NF	M	Distributed data management throughout the continuum is needed in order to scale and adapt in dynamic data exchange scenarios	Standard mechanisms and interfaces to enabled distributed data infrastructures.
TR-52	DATA	Data integration	Combination of data from different heterogenous data sources in a context intermediary	ALL	Continuum	Accessibility Standards	NF	M	Data consumers will greatly benefit from having a holistic view of data across the continuum	Leverage a consolidated, solid standard for data combination and cataloguing.
TR-53	DATA	Data-as-a-product	Management of data as a product that can be easily shared among consumers	ALL	Continuum	Accessibility Standards	NF	M	Exposing data following the Findable, Accessible, Interoperable, Reusable (FAIR) principles to enable interoperability among data consumers in the continuum	Standard interfaces and standard data models to facilitate interoperability.
TR-54	SECURITY	Cybersecurity tools	Cybersecurity tools to be implemented should comply with DevPrivSecOps procedures of aerOS	ALL	ALL	Security Privacy	NF	S	The cybersecurity tools are essential for DevPrivSecOps	All instructions and guidelines stated by DevPrivSecOps are kept in consideration in any cybersecurity flow.

ID	Refers to	Name	Description	Role	Domain	Category	Type	**Priority**	Rationale	Acceptance Criteria
TR-55	SECURITY	Privacy-preserving functions	Deployment of functions that aim at the protection of privacy by protecting sensitive data from unauthorized access	ALL	ALL	Privacy	NF	S	Protection of sensitive data from unauthorized access	Mechanisms for the protection of sensitive data from unauthorized access are realized.
TR-56	SECURITY	Trust establishment	Employment of mechanisms to establish trust within aerOS ecosystem	ALL	ALL	Security Trust	NF	S	Trust establishment in aerOS	Trust score calculation and trust management are realized.
TR-57	SECURITY	Cybersecurity policies	Establishment of cybersecurity policies to define who can do what and when	ALL	ALL	Security	NF	S	Cybersecurity policies to enhance and maintain the security of aerOS	Policies that define who can do what and when are realized.
TR-58	SECURITY	Identity Management	Self-Sovereign Identity Management Framework	ALL	ALL	Security Privacy	NF	S	Identity Management to establish access controls in aerOS ecosystem (T4.5).	Successful onboarding and authentication of users and devices on the aerOS platform.
TR-59	SECURITY	Self-Sovereign Identities	Implementation of SSI in the aerOS IdM	ALL	ALL	Security Privacy	NF	S	Digital IDs should be controlled by individuals based on Self-Sovereign Identity techniques (i.e., variable credentials, decentralized identifiers)	No identifiable information shared or leaked during onboarding and authentication.
TR-60	SECURITY	Distributed Trust Management	Dynamic Trust management for devices utilizing DLT technologies and MQTT protocol	ALL	ALL	Security Trust	NF	S	Distributed management of trust within aerOS	Continuous attestation of trust for all devices onboarding the system or roaming between different domains and revoking access to untrusted devices.
TR-61	SECURITY	Authentication and authorization accounting	Establishment of logs that record, based on the policies, who did what and when	ALL	ALL	Maintainability	NF	M	It is a must having an accounting system so as to register every single authentication and authorization within the aerOS continuum. This will help traceback and debug unexpected behaviours that pose conflict with the expected cybersecurity policies.	An accounting that registers every authentication and authorization grant and deny, is realized.

ID	Refers to	Name	Description	Role	Domain	Category	Type	Priority	Rationale	Acceptance Criteria
TR-62	SECURITY, DEVELOPMENT	User interface for cybersecurity control	GUI to set cybersecurity policies and to check the access logs	ALL	ALL	Maintainability Accessibility	NF	M	It is a must having a graphical user interface to easily adjust security and privacy policies; and also, to check whether incidents take place	Intuitive, user-friendly user interface that enables policy configuration and access log review.
TR-63	SECURITY, DEVELOPMENT	DevPrivSecOps coding environment	Recommendation of a set of plugins and guidelines for judiciously selected IDE that lead to the production of safe and clean code, while keeping general consistency.	ALL	ALL	Development	NF	C	Prior to taking any SAST/DAST testing, the coding environment should be aware of the security, privacy and efficiency constraints. Sets of plugins should guide the developer to the optimal code regarding security and efficiency.	Defined set of plugins and guidelines recommended during development.
TR-64	DEVELOPMENT	Continuous Integration and Continuous Delivery	Deployment of a Continuous Integration / Continuous Delivery (CI/CD) pipeline	ALL	ALL	Maintainability	NF	S	Deployment of the Continuous Integration / Continuous Delivery pipelines in the project repository	CI/CD pipelines are deployed resulting to production of a robust, secure aerOS services.
TR-65	DEVELOPMENT	Static and dynamic code test	SAST/DAST pipeline	ALL	ALL	Maintainability	NF	S	Implementation of automatic code testing in the development and operation phases	Static and dynamic code testing to identify vulnerabilities and ensure quality, design safety and functional code in aerOS services.
TR-66	DEVELOPMENT, SECURITY	Security analysis in Software Development Life Cycle	Security threat modelling	ALL	ALL	Security	NF	S	Security threat modelling to detect weaknesses in the aerOS platform and define mitigation actions	Security-preserving tools in application development and infrastructure to create security-by-design solutions and a secure aerOS platform.
TR-67	DEVELOPMENT, SECURITY	Privacy analysis in Software Development Life Cycle	Privacy Threat analysis	ALL	ALL	Privacy	NF	S	Privacy threat modelling to detect weaknesses in the meta-OS and to define mitigation actions.	Privacy-preserving tools in application development and infrastructure to create privacy-by-design solutions and a secure platform.

B. User and System Requirements table

Table 1. Functional (F) and non-functional (NF) requirements of Pilot 1.

ID	NAME	CATEGORY	TYPE	PRIORITY	RATIONALE	DESCRIPTION	ACCEPTANCE CRITERIA	SATISFACTION	ETHIC	IDENTIFY BY
R-P1-1	Real time data management and response	F	System	S	A real time data acquisition, processing and fast response is needed for actuators located in a manufacturing facility.	aerOS should be able to efficiently acquire and process data from a variety of devices (sensors…), in order to offer a fast response to actuators and rapidly act to avoid possible deviations.	aerOS must offer a real-time response when a parameter deviation is detected	5	NO	INNO
R-P1-2	Computing resources (cloud & edge)	NF	System	M	In order to fulfil R-P1-1 achieving real time data processing we need huge computing resources	aerOS should be able to host all the computational workload required in an industrial environment	aerOS must guarantee that all decisions are taken applied before it is too late on the production line, even faster than what the current scenario is able to deliver	5	NO	NASERTIC
R-P1-3	Low latency communication between edge devices and with cloud	NF	System	M	In order to fulfil R-P1-1, not only do we need high processing capabilities but also we need to access to the sources of information and to the sources of the intelligent decisions fast enough	aerOS should be able to guarantee a federated organization of devices while ensuring low latency communications among them. All on-field IoT devices must be able to intercommunicate rapidly, and they also must be able to communicate rapidly with the cloud or any other agent taking the intelligent decisions.		5	NO	NASERTIC
R-P1-4	Secure communications between edge devices and with the cloud	NF	System	M	Confidential information of industrial scope must remain confidential when transporting data from one device to another. Furthermore, no man in the middle should be able to intercept, alter or introduce any instructions to be taken by the industrial machinery. Any of these outcomes would lead to huge losses to the affected factory or enterprise.	aerOS should be able to guarantee secured communications, following the main cybersecurity standards in all communications between any given devices	At any given point in the communication of two devices, the information must be indecipherable and must remain integral (not modified by a third party).			
R-P1-5	Compatibility among heterogeneous devices and industrial machinery	NF	System	M	Production lines are made up of a variety of machinery which makes for a great heterogeneity of devices. This heterogeneity takes place within a given production line and accross different production lines in different factories. Making all different devices understand each other within the continuum would boost the productivity.	Production lines are made up of a variety of machinery which makes for a great heterogeneity of devices. This heterogeneity takes place within a given production line and accross different production lines in different factories. To really foster aerOS continuum, all those devices must be able to intercommunicate and understand each other in spite of its heterogeneity.		5	NO	NASERTIC
R-P1-6	Interoperability of the technology, which enables a various kind of data, IoT-Devices and interfaces.	NF	System	M	Same to R-P1-5	As a supplement to R-P1-5, aerOS should be built interoperability so that a wide variety of protocols, formats and interfaces are possible	Common Formats for Data echange industries are covered (OPCUA, REST-API etc.)	5	NO	SIPBB

ID	NAME	CATEGORY	TYPE	PRIORITY	RATIONALE	DESCRIPTION	ACCEPTANCE CRITERIA	SATISFACTION	ETHIC	IDENTIFY BY
R-P1-7	Support for various types of devices, even at different levels	NF	System	M	In production lines various types of devices at different levels are present. A continuum which is able to connect these on common platform enables completely new possibilities	In production lines various types of devices such as machine tools, AGV's, 3D-printers, senors, actuators, complete Systems etc. are present. A continuum which is able to connect these on common platform enables completely new possibilities	It must be possible to connect various types of devices on different levels. For example AGV's, 3D-printers and an ERP-system.	4	NO	SIPBB
R-P1-8	Real time dashboarding of processed and/or collected data	F	System	M	To display collected and processed data enables understanding possibilities for workers and also customer if data is shared with them	It is able to display processed and/or collected data in some kind of dashboarding tool.	Provision of Simple charts with the time on the X-Axis and the according value one Y-Axis. In Addition simple bar chart for comparisons would be great.	5	NO	SIPBB

Table 2. Functional (F) and non-functional (NF) requirements of Pilot 2.

ID	NAME	CATEGORY	TYPE	PRIORITY	RATIONALE	DESCRIPTION	ACCEPTANCE CRITERIA	SATISFACTION	ETHIC	IDENTIFY BY
R-P2-1	Scheduling with real-time adjustments support	F	System	M		aerOS should react to changing context and conditions and adopt application and job execution accordingly				
R-P2-2	Shifting computing tasks across time	F	System	M		aerOS should react to changing circumstances and use predictions of heavy the workload will be and what type of energy will be available to create task queues and adapt the execution environments for specific tasks				
R-P2-3	Support for execution of user applications/jobs	NF	System	M		aerOS should support execution of applications delivered by end user using the provided inrastructure				
R-P2-4	Application/job conditions definable by the user	F	System	S		User should be able to define how fast they need the results, where (topologically and geographically) processing should should be performed and what should be the renewable energy usage rate for their processing.				
R-P2-5	Support for movable workload in batches	F	System	M		Important characteristic of a task in this service is its limited execution time. In order to efficiently populate the system we need to have workload that is movable and in batches. It comes with an additional advantage and requirement: efficient usage of available cloud resources.				

Table 3. Functional (F) and non-functional (NF) requirements of Pilot 3.

ID	NAME	CATEGORY	TYPE	PRIORITY	RATIONALE	DESCRIPTION	ACCEPTANCE CRITERIA	SATISFACTION	ETHIC	IDENTIFY BY
R-P3-1	(semi) Real-time data analysis	F	System	S	Depending on the situation: timely data analysis would be beneficial in improving the quality of work and automate some of the tasks that are currently handled manually (reducing manual work).	Analysing a given data in a timely manner and give a response back with the required/suggested action.	TBD	5	NO	JD
R-P3-2	Low latency communication between system components	F	System	S	Monitoring the overall system latency	The main point of interest here is the integration of TTControl's HW (non-John Deere device) with all the other John Deere devices.	Defining a tolerable overall system latency	5	NO	JD / TTC
R-P3-3	Compatibility between different types of devices in the built system	NF	System	M	Compatibility of devices is important for the system to function properly	The main point of interest here is the integration of TTControl's HW (non-John Deere device) with all the other John Deere devices.	Achieving a system with components that can fully communicate with one another	5	NO	JD / TTC
R-P3-4	Compatibility between the built system and the overall architecture of aerOS	NF	System	S	How the pilot will fit into the overall architecture of aerOS, communicate with its different components, and use its available resources	The main point of interest here is the integration of TTControl's HW (non-John Deere device) with all the other John Deere devices.	TBD	5	NO	JD / TTC
R-P3-5	Local processing of data flow	F	System	S	Examining the processing capabilities and health monitoring of provided HW by TTControl	The main point of interest here is the integration of TTControl's HW (non-John Deere device) with all the other John Deere devices	Able to process the provided data in time and result in actions to take accordingly	4	NO	JD / TTC

Table 4. Functional (F) and non-functional (NF) requirements of Pilot 4.

ID	NAME	CATEGORY	TYPE	PRIORITY	RATIONALE	DESCRIPTION	ACCEPTANCE CRITERIA	SATISFACTION	ETHIC	IDENTIFY BY
R-P4-1	Develops aerOS IE that integrates data telemetry from cranes into aerOS Data continuum	F	User	M	Telemetry from cranes can be extracted using devices such as PLCs. That telemetry allows designing dashboards and execute algorithms and models to process trends in some specific parameters	In order to benefit from aerOS AI capabilities, it is necessary to feed aerOS with data from the cranes in being monitored in the port	Telemetry from cranes is stored in aerOS data stores	5	NO	PRO
R-P4-2	Integration of TOS with aerOS	F	User	M	TOS installed at ports usually provide alerts/notifications based on internal rules defined for the equipment/cranes available in the terminal. The use of such information provides added-value to aerOS since it can be used as an additional data source for algorithms	In order to exploit the data generated by the TOS, aerOS should implement the mechanisms to retrieve and storage these data	Alerts generated for configured cranes is available in aerOS data storage	4	NO	PRO
R-P4-3	Integration of CMMS into aerOS	F	User	M	The CMMS is the system used by the terminals to conduct the maintenance operations of the machinery available in the terminal. The use of maintenance logs can be used in the scenario of predictive maintenance as an additional data input for the algorithms	In order to enrich the predictive maintenance scenario, it is necessary that aerOS provides connectivity with the maintenance system used by the terminal to import relevant information for the AI models.	Maintenance jobs and logs are available in aerOS data storage	4	NO	PRO

ID	NAME	CATEGORY	TYPE	PRIORITY	RATIONALE	DESCRIPTION	ACCEPTANCE CRITERIA	SATISFACTION	ETHIC	IDENTIFY BY
R-P4-4	Integration of IPTV camera streams in aerOS	F	User	H	The risk prevention via computer vision scenario requires the feed of at least three video cameras to detect certain patterns in the video frames, and have a clear view of containers form their 6 sides while being handled	In order to scan containers from their 6 sides, it is necessary that aerOS integrates feeds from at least 3 video cameras placed at strategic places in the terminal. These cameras should use the IPTV protocol for a better compliance.	Video streams integrated in aerOS	5	YES	PRO
R-P4-5	Monitor Trolley Wire Rope Enlargement	F	User	M	An early warning system will be put in place that monitors the discrepancy between the distance the limit switches of the trolley wire rope were positioned on the travel length of the boom with the distances that were stored in the first calibration of the machine. The warning system will predict in advance when it becomes faulty, allowing the Technical Department to plan for this issue before any undesired working condition	In order to predict when the wires in a crane must be replaced due to wear out, it is necessary to develop an AI model that, using telemetry from the crane, can provide an alert on when the wire's elongation can lead to a failure.	Model trained and in execution for IEs in STS cranes	5	NO	PRO
R-P4-6	Motor Filter Condition	F	User	M	Monitor motor speed as well as load and motor bearing housing temperature to determine if the bearings of the motor have degraded and require replacement	In order to predict when bearings in the engine need replacement, aerOS will develop an AI model that, using engine telemetry, can generate an alert before the engine fails	Model trained and in execution for IEs in STS cranes	5	NO	PRO
R-P4-7	Motor Bearings Condition	F	User	M	Measure variability between the 2 motors, master and follower hoist motor to monitor that they share the load equally. This could indicate a misalignment of one of the motors, coupling degradation, motor degradation or closed loop control issue (Speed Encoder, Parameters, Inverter etc.).	In order to avoid engine load degradation, aerOS should provide an AI model that detects and predicts motor degradation by comparing the shared load between master and follower engines in the cranes	Model trained and in execution for IEs in STS cranes	4	NO	PRO
R-P4-8	Motor load sharing from Hoist	F	User	L	This would check when the deviation between the 2 cylinders has increased greatly or avoid the disparity and notify personnel to check the wire ropes	In order to predict wear out cables in straddle carriers, aerOS should provide an AI model that uses telemetry and detects disparity between the deviation of the 2 cylinders	Model trained and in execution for IEs in STS cranes	3	NO	PRO
R-P4-9	Tensioning Aux Cylinder Pressure Monitoring	F	User	L	To calculate and monitor efficiency genset system by measuring power delivered to the engine in terms of fuel l/h and electrical energy produced. To do so, three main data inputs will be monitored: engine fuel consumption, generator output, and outdoor temperature.	In order to predict the efficiency of the generator engine, aerOS will provide an AI model that uses telemetry to detect low efficiency and predict the required maintenance	Model trained and in execution for IEs in straddle carriers	4	NO	PRO
R-P4-10	Generator engine efficiency	F	User	M	Monitor motor speed as well as load and motor bearing housing temperature to determine if the bearings of the motor have degraded and require replacement	In order to predict when bearings in the engine need replacement, aerOS will develop an AI model that, using engine telemetry, can generate an alert before the engine fails	Model trained and in execution for IEs in STS cranes	4	NO	PRO

ID	NAME	CATEGORY	TYPE	PRIORITY	RATIONALE	DESCRIPTION	ACCEPTANCE CRITERIA	SATISFACTION	ETHIC	IDENTIFY BY
R-P4-11	Genset vibrations	F	User	L	To monitor vibration on genset and predict if this is related to genset mounting failures, or engine injector issues. The main variables to be recorded are: genset vibration, generator output frequency, and generator output load.	In order to discriminate the source of vibrations in the genset, aerOS will provide an AI model that uses telemetry from the straddle carrier and can discriminate whether the vibrations come from the genset or from the engine injectors due to wear out.	Model trained and in execution for IEs in straddle carriers	3	NO	PRO
R-P4-12	Inclination issues	F	User	M	To monitor the inclination of the straddle carrier during operation and send warnings if the system is behaving abnormally. The system should provide the main reason that could be due to e.g., suspension failing, tyres, etc. It will take into account not only machine inclination, but also load height, machine side frame speed difference, or if it is transporting a container or not	In order to prevent risky situations due to inclination of the straddle carrier, aerOS will provide an AI model that uses telemetry and detects dangerous situations, discriminating the source of the abnormal inclination	Model trained and in execution for IEs in straddle carriers	4	NO	PRO
R-P4-13	Hydraulic system	F	User	L	Hydraulic Pressure Instability can indicate issues in the system, accumulator or pressure regulators that are faulty. Several pressure transducers will be placed on the machine to measure the system and alert if there is an anomaly based on the machine operation, including also parking brakes engaged or not, spreader motion ON/OFF and outdoor temperature.	In order to prevent failures in the hydraulic system, aerOS will provide an AI model that monitors telemetry from straddle carriers and detects episodes of pressure instability that can lead to a malfunction	Model trained and in execution for IEs in straddle carriers	4	NO	PRO
R-P4-14	Container plate identification	F	User	M	Automatic identification of container plate numbers allows enhanced management of processes inside the cargo area	aerOS will provide frugal AI services based on computer vision that will identify the container plate number when the crane is handling the container in the cargo area	Plate numbers MUST be identified using computer vision independently of their location in the container	4	YES	PRO
R-P4-15	Detection of damaged containers	F	User	M	In order to ensure security on the load/unload operations, damaged containers that may lead to unsure operations (e.g., broken, split or cracked walls) should be detected and handled with special care.	In order to detect possible damaged containers while they are operated, aerOS should be able to detect different structural damages on the container's surfaces.	Algorithm trained and in execution	3	YES	PRO
R-P4-16	Detections of holes in containers	F	User	M	To ensure the security of the workers in the terminal, it is necessary to detect possible structural damages in containers that may lead to cargo being dropped through a hole into the working area	In order to ensure safety of workers and machinery, containers with severe damages and holes may be detected using video streams	Algorithm trained and in execution	3	YES	PRO
R-P4-17	Detection of wrongly sealed containers	F	User	M	Containers are sealed when they are shipped. If the sealed is broken, someone may have manipulated the cargo inside. To ensure that containers being departed from the terminal are correctly sealed, it is necessary a mechanism to automatically detect the seal at specific positions in the container's outside.	In order to have traceability of sealed containers, aerOS will develop a CV module that can detect when a container carries a seal or not	Algorithm trained and in execution	4	YES	PRO
R-P4-18	Frames per second processed by CV algorithms	NF	User	M	Algorithms should be fast enough to perform inference process in almost real-time	In order to reduce bandwidth and storage size, CV algorithms should be capable of performing inference training as fast as possible		4	NO	PRO

ID	NAME	CATEGORY	TYPE	PRIORITY	RATIONALE	DESCRIPTION	ACCEPTANCE CRITERIA	SATISFACTION	ETHIC	IDENTIFY BY
R-P4-19	Maximize evaluation metrics for AI models for PdM	NF	User	M	AI models should have a minimum quality of performance	In order to provide trustable data for final users, models will be evaluated with their corresponding metrics in order to assure trustable predictions	A quantitative analysis in terms of R2 and other evaluation metrics will be addressed in KPI evaluation task	4	NO	PRO
R-P4-20	Maximize evaluation metrics for AI models for CV	NF	User	M	CV models should have a minimum quality of performance	In order to provide trustable data for final users, models will be evaluated with their corresponding metrics in order to assure trustable predictions	A quantitative analysis in terms of accuracy and other evaluation metrics will be addressed in KPI evaluation task	4	NO	PRO

Table 5. Functional (F) and non-functional (NF) requirements of Pilot 5.

ID	NAME	CATEGORY	TYPE	PRIORITY	RATIONALE	DESCRIPTION	ACCEPTANCE CRITERIA	SATISFACTION	ETHIC	IDENTIFY BY
R-P5-1	Far Edge and Edge storage capacity	NF	System	M	New data will be generated from the sensors continuously. ML models will be trained locally.	1) Distributed On-Site Learning: After deploying a pre-trained ML model from the cloud, each building can then customize it by using local data to engage in further training.	Exhibit that the pipeline is working through the generation of the appropriate ML models.	5	NO	INF
R-P5-2	Cloud storage capacity	NF	System	M	2) Federated Learning: A generic model from the cloud is copied to each building, which then trains it with the local generated data. The updated models (and not the data) from each building are shared with the main model in the cloud. The central model combines the different updates and generates a new model which is then distributed again to the buildings.	Exhibit that the pipeline is working through the generation of the appropriate ML models.	Exhibit that the pipeline is working through the generation of the appropriate ML models.	5	NO	INF
R-P5-3	Support any IoT sensor type and protocol	NF	System	M	New IoT technologies should be incorporated to keep the Pilot5 service being state of the art	The pilot5 platform shall support or be able to support any sensor, any sensor platform and any access technology (WiFi, 2G/3G/4G, NB-IoT, LoRaWAN, sigfox, etc.), so as the sensors can be deployed in any environment (indoors, outdoors, fixed, mobile, wearable).	Demonstrate a multi-sensor IoT network deployments, including various sensors and access technologies.	2	NO	COS

ID	NAME	CATEGORY	TYPE	PRIORITY	RATIONALE	DESCRIPTION	ACCEPTANCE CRITERIA	SATISFACTION	ETHIC	IDENTIFY BY
R-P5-4	Automatic service recovery upon system or network loss	NF	System	M	Service Outage is not acceptable because it can lead to idle labor hours (employees stranded with no placement recommendations)	The pilot5 platform should survive network loss, or system outage and all devices must be automatically restored in the event of failure.	Demonstrate that the sensors and smart building applications automatically reconnect and resume operation upon a network or system failure	5	NO	COS
R-P5-5	IoT Data Collection and processing fully automated, reliably transferred in a configurable manner	NF	User	M	Data completeness and promptness is vital for training the recommendation system and pilot5 intelligence algorithm	The pilot5 data collection should be automated with no human intervention and the user shall be capable of defining the interval between consecutive measurements. Moreover, data must be stored locally in case of communication disruption and be loaded in bulk mode to the backend/cloud.	Demonstrate the automated uploading and storage of measurements at the aerOS cloud infrastructure	4	NO	COS
R-P5-6	IoT system automatic configuration management	NF	User	M	Users do not want to be involved in tedious, time consuming tasks of housekeeping especially since these tasks can be automated	Updates, bug fixes, enhancements associated with sensors' capabilities shall be done without the user's intervention. The user should be notified about the "context" of those changes.	Demonstrate Over-The-Air (OTA) updates.	3	NO	COS
R-P5-7	User-friendly monitoring of system health and remote management	F	User	M	Users need to know at any time if the pilot5 platform is fully operational and offers reliable results/recommendations. Each type of user (employee, maintenance staff, building owner) will have different interest on the level and kind of information to be monitored and this needs to be flexibly supported.	Event Handling/Alarm process, Visualisation dashboards customised per user needs are necessary.	Generate various monitoring dashboards and control buttons based on the pilot5 user profiles.	5	NO	COS
R-P5-8	Scalability to Support Mass Deployments	NF	System	S	The pilot5 system must be easily setup for use in each (new) building	The pilot5 platform shall be capable of integrating mass sensor deployments (in a step-wise approach) without compromising its performance (e.g. delays in measurements storage or delays in data retrieval).	Demonstrate that adding a new smart building is efficient with no unnecessary steps.	2	NO	COS
R-P5-9	Data Analytics & Decision Making at the Edge	F	User	M	Pilot 5 considers self-managed autonomous buildings, and as such intelligence must be demonstrated	By considering the metrics received by a vast range of sensors; the employee's data,		5	YES	COS

ID	NAME	CATEGORY	TYPE	PRIORITY	RATIONALE	DESCRIPTION	ACCEPTANCE CRITERIA	SATISFACTION	ETHIC	IDENTIFY BY
R-P5-10	APIs for 3rd Parties/Stakeholders	F	System	M	historical data on energy consumption, CO2 emissions per office segments, historical data on employees' routine/preferences, the aerOS pilot 5 intelligence system (i) shall select the appropriate room and most suitable seat(s), and instantly direct the employee to pick from the alternative seats proposed through the use of a Mobile App. (ii) Shall exploit the sensors data to actuate appropriately the ventilation, heating and air-condition systems as well as control luminosity. (iii) Exhibit swarm intelligence among the AEROS capable sensors to allow them to co-operate in a decentralized manner and collectively manage each room's condition, so that the office becomes self-organised in terms of health and efficiency.	Exhibit intelligent decisions beyond the automation capabilities of the existing IoT systems		2	NO	COS
R-P5-11	Gateways and Base Stations Heterogeneity	NF	System	M	Integration with other external systems and access to raw data through well-defined APIs is an efficient and transparent process to achieve both flexibility/extensibility and security/privacy	The cloud infrastructure shall offer an API for third parties and/or stakeholders/customers enabling access to their own datasets and/or statistics.	Demonstrate the existence of such an API.	2	NO	FOG
R-P5-12	Web app / Mobile app for end user-system interaction	F	User	M	Gateways and base stations may be different on the set of supported capabilities, their coverage performance, their message aggregation policy, etc.	The gateways shall be able to provide a common set of services to the same type of IoT end devices, regardless of the gateway capabilities. In the same way that various protocols and sensor types will be onboarded in end devices, there will also be different types of gateways to serve either the same set of IoT devices (e.g., gateways that support the same IoT communication protocol but with different capabilities), or a different set of them (e.g., gateways that support different communication protocols). Also, the support of deployments in unlicensed-bands via the functionalities of 3GPP-based networks could be examined (i.e., N3IWF).	Demonstrate a multi-gateway deployment (in the scope of the pilot, two or more gateways should suffice).	4	YES	FOG

ID	NAME	CATEGORY	TYPE	PRIORITY	RATIONALE	DESCRIPTION	ACCEPTANCE CRITERIA	SATISFACTION	ETHIC	IDENTIFY BY
R-P5-13	Occupancy policy	NF	System	M	A policy to determine when a spot is truly free.	The worker may temporarily leave his/her spot, and the sensor may mistakenly indicate that this spot is free. The occupancy policy may be based in simple timer (e.g., absence greater that a threshold) or a more complex set of parameters.		4	YES	FOG
R-P5-14	Message aggregation policy at gateway-level for lower overhead	NF	System	S	An aggregation policy for the uplink messages that arrive to the gateway, to form a packet of multiple IoT end devices' messages and send them under the same header and trailer to the server-side. This requirement will result in lower network overhead for the link between the gateway and the server-side.	The gateways shall implement a message aggregation policy. This suits to pilot 5, since it does not correspond to a time-critical mission use case. For the implementation, it would require a buffering mechanism in the gateway. The advantage is the minimization of the network overhead, since most of the sensors data sizes are of the same order of magnitude of the header/trailer sizes. The policy can be fixed or adjustable to the tradeoff of latency/overhead.	Proven benefits of the policy in terms of network overhead, while the policy does result in a latency that puts QoE below an acceptable level.	1	NO	FOG
R-P5-15	Gateway functionality for harmonizing heterogeneous data	F	System	M	A function either at a gateway-level or after the communication with the server-side but before the server-side storage that can harmonize heterogeneous data.	The function will take as input all the data from all the IoT end devices and output a predefined format for each message. This format will follow the schema of a Data Model based on NGSI-LD, following the context information management standard defined by the	Demo that receives as input heterogeneous data and produces a harmonized output.	2	NO	FOG
R-P5-16	Distributed deployment of workloads/services along the continuum	F	System	M	ETSI. The function can either be integrated in the gateway (gateway-level) or sit between the gateway and the server-side communication. The former approach requires programming of the gateway and maybe remote access in the case of a new data format is defined in the future. The latter approach can be implemented in tools such as NodeRED, and is easily extensible from the administrator PC.	Demo that receives as input heterogeneous data and produces a harmonized output.	Efficient distribution of workloads (e.g., ensure that a great number of services are not deployed on the cloud, edge IEs run only the needed services, …)	5	NO	FOG

C. Legal Framework Surveys

C.1. Pilot 1

C.1.1. INNOVALIA

Appendix C – Legal Framework Survey

1. REGULATORY BODIES & DATA PROTECTION AUTHORITIES

1.1. Which EU-level data protection regulators and data protection authorities are you or could you be connected with?

None.

1.2. Which national and local regulatory bodies are you or could you connect with?

Agencia Española de Protección de Datos (Spanish Data Protection Agency).

1.3. Do you have any conflict of interest with those regulatory bodies?

No

2. EUROPEAN UNION FRAMEWORK

2.1. Have your government or local regulations incorporated the following?

Directive (EU) 2019/1024: open data and the re-use of public sector information.	YES, **Royal Decree-Law 24/2021**, regarding the transposition of directives of the European Union dealing with open data and re-use of public sector information. Link
Directive (EU) 2018/1972: establishing the European Electronic Communications Code.	YES, **Law 11/2022,** General Telecommunications Law Link
EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns "Cybersecurity" issues.	YES, **Royal Decree-Law 12/2018**, regarding network and information systems' security. Link
EU DPR-2012: European Data Protection Regulation	Replaced by EU GDPR
EU Directive-2013/40: this Directive deals with "Cybercrime" (i.e., attacks against information systems).	Yes, **Organic Law 1/2015** of 30 March, concerning the crime of discovery and disclosure of secrets and the crime of computer damages
EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns "Cybersecurity" issues.	Yes, **Royal Decree-Law 12/2018**, September 7th, network and information systems' security
EU Directive 2014/53: this directive is concerned with the standardization issue which is important for the joint and harmonized development of technology in the EU.	Yes, **Ley 11/2022**, 28 de junio, General de Telecomunicaciones, **Law 11/2022**, June 28th, General Telecommunications Law
EU GDPR: European General Data Protection Regulation-2016	Yes, **Organic Law 3/2018** of 5 December, on the Protection of Personal Data & Guarantee of Digital rights.
EU Connected Communities Initiative: This initiative concerns the IoT development infrastructure, and aims to collect information from the market about existing public and private connectivity projects that seek to provide high speed broadband, more than 30 Mbps.	Yes, As of 2015, 10 national projects in Spain were working towards the achievement of the initiative.

3. REGULATIONS

The national legal and ethical framework should cover the following. Please answer YES/NO if your framework does.

Legislation/regulations.	YES
Ethics principles, rules and codes.	YES
Standards/guidelines.	YES
Contractual arrangements.	YES
Regulations for the devices connected.	YES
Regulations for the networks and their security.	YES
Regulations for the data associated with the devices	YES

4. GOVERNMENT REGULATIONS

Governments play a primary role in shaping the future because governments have a dual role, namely

1. User role: governments plan to become major users of IoT, e.g., getting smart cities.
2. Infrastructure provider role: governments should issue regulations for devices not originally intended for connection to the IoT, as well as for devices particularly designed to be connected devices.

4.1. Which of the above is the role of your government?

Both

4.2. Do your government have in force regulations for both roles?

No specific regulation in Spain related to IoT devices or infrastructures.

4.3. What are these regulations?

Regulations as Infrastructure provider role:

No specific regulation for IoT devices or infrastructures in Spain.

Regulations as user role:

No regulation for IoT users in Spain.

4.4. Do your government ensure that IoT products and solutions are used exclusively for their specified goal?

No

4.5. Which sectors of society, industry and the economy are subject to general government legislation?

Generally, to every instance of electronic devices / networks deployed on industries, business and public services, among others:

- Privacy/Data protection institutions
- Telecommunications market
- Standardization organizations

4.6. Does the relevant legislation include the following fields (yes/no and define if possible):

public law	Yes	
business law	Yes	
insurance law	Yes	
tax law	Yes	
private international/human rights law	Yes	
security law	Yes	
criminal law	Yes	
civil liability law	Yes	Art. 40, Law of Consumer Protection
consumer protection law	Yes	
private/data protection law	Yes	
environmental law	Yes	
GDPR law	Yes	

4.7. Do government regulations focus on the system capabilities (e.g., how data can be reused or sold) rather than on implementation (e.g., MySQL vs. Hadoop)?

No specific IoT regulations.

5. CHARACTERISTICS THAT MAY CAUSE ETHICAL PROBLEMS

The main IoT characteristics that may cause ethical problems are the following. Please try to identify the risk of having to deal with some of these (using YES/NO/maybe) in the Use Case you participate in.

Ubiquity/omnipresence: the IoT is everywhere.	YES
Miniaturization/invisibility: computers and devices will be smaller and smaller, and transparent, thus avoiding any inspections, audit, quality control, and accounting procedures.	NO
Ambiguity: the distinction between the natural objects, artifacts, and beings will be more and more difficult to be made, because the transformation from one category to another is easy, based on tags.	NO
Difficult identification: objects/things have an identity in order to be connected to the IoT. The access to these objects and the management of their identities might cause crucial problems of security and control in the IoT ecological world.	YES
Ultra-connectivity: the huge number of connections of objects and people require the transfer of large quantities of data (big data) which could be maliciously used.	YES
Autonomous and unpredictable behaviour: the interconnected objects might interfere autonomously and spontaneously in human activities in unexpected ways for the users or designers. People, artifacts, and devices will belong to the same IoT environment, thus creating hybrid systems with unpredictable behaviour. The incremental development of IoT will lead to emerging behaviours that the users could not fully understand.	MAYBE
Incorporated intelligence: this will make the objects as substitutes of social life. The intelligent objects will be dynamic with an emergent behaviour. Being deprived of these devices will lead to problems (e.g., teenagers without the Google, smart phone or social media, might feel themselves cognitively or socially handicapped).	MAYBE
Decentralized operation: the IoT control and governance cannot be centralized, because of the large number of hubs, switches, and data. The information flows will be eased, and the data transfers will be faster and cheaper, and thus not easily controllable. There will appear emerging properties and phenomena which will require monitoring and governance in an adequate way, and this will further influence the accountancy and control activities.	YES
Property right on data and information: the difficulty in specifying the identification of things and humans is reflected to the difficulty to identify who is the owner of the data retrieved by IoT sensors and devices.	YES
Omnipresence: this makes invisible the boundaries between public and private space. People cannot know where their information ends up.	YES
Accessibility of data: an attack on a PC might cause information loss. A virus or hacker attack in the IoT might have serious effects on human life (e.g., on the life of the driver of a car connected to IoT).	YES
Vulnerability: the list of possible vulnerabilities in IoT is scaring. It ranges from home appliances, to hospitals, traffic lights systems, food distribution networks, transportation systems, and so on.	YES
Digital divide: the digital divide in the IoT is enlarged. IoT operations can be understood only by experts. Communication in IoT devices affects human lives in ways that are difficult to predict or imagine. The digital divide can only be reduced by proper coherent legal and democratic frames to delineate this process.	MAYBE

6. ETHICS QUESTIONS

6.1. Information technology ethics and Internet ethics.

What happens if the Internet connection breaks down?
If the Internet connection fails, the autonomous/remote operation of CMMs will temporarily fail, leading to a disruption of the service, loss of efficiency or, in extreme cases, causing damages to products/parts.
Who is responsible or liable for patching IoT devices, routers, and cloud connections?
Telco technicians and telco engineers.
Is there an assurance that hacking on the cloud side of IoT services will not have access to a home's internal network?
Yes. The infrastructure is secured against external attacks via firewalls.
What happens if an IoT service provider experiences downtime for critical life-supporting devices?
No critical life-supporting devices in our premises
What happens if an IoT device acts without the consent of its owner or acts in unintended ways (e.g., ordering the wrong products, or vacuuming at an unreasonable hour)?
That is not contemplated to happen.
What happens if an IoT product vendor goes out of business and no longer supports the product?
A product vendor going out of business does not instantly disable the function of the IoT product. There is the possibility of finding similar IoT products in the market.
Who owns the data collected by IoT devices?
Our CMM (M3 platform) devices gather data in M3 Server, owned by us.
Are there cases where IoT devices should not be collecting data?
No.
What happens if the user wants to opt out?
The user can do it.
What about those who do not have smart devices or the knowledge to use them? (Digital divide).
All the required devices and its operation is provided by us. Additional training is provided to the user.

6.2. Ethical principles

All activities involving the use of personal data are expected to comply with applicable data protection legislation. Beyond legal compliance, activities must respect ethical principles. Please try to assess whether the use case you lead/participate in complies with the following (definitely/future/probably/not) and comment if necessary):

In IoT activities, individuals should be treated as ends (not as means), and maintain their rights to property, autonomy, private life, and dignity.	Definitely
Individuals should not suffer physical or mental harm from IoT activities.	Definitely
Benefits from the application of IoT should be added to the common good.	Definitely
The necessity and proportionality of an IoT process should be taken into account and capable of being demonstrated.	Definitely
IoT applications should be performed with maximum transparency and accountability via explicit and auditable procedures.	Definitely
There should be equal access to the benefits of IoT accruing to individuals (social justice).	Definitely
IoT activities should have minimum negative impact to all facets of the natural environment.	Definitely
IoT activities should aim to lighten the adverse consequences that data processing may have on personal privacy and other personal and social values.	Definitely
Adverse effects beyond the individual (groups, communities, societies) should be avoided or minimized or mitigated.	Definitely

7. PRIVACY

The European Union General Data Protection Regulations (EU GDPR 2016, etc.) impose the principles that should underlie the processing of personal information. A new principle added to EU GDPR 2016 is the principle of "Privacy by Design".

Does your privacy framework include the following? (yes/no and if yes define)

Privacy regulations	Yes
Data minimization	No
Data portability	Yes
Transparency	Yes
Compliance disclosures	Yes
IoT engagement by default	No
IoT engagement by design	No
Best practice	Yes

The concepts of security and privacy have many complex interrelationships, but they are not identical. Do you have the following relations between security and privacy? (yes/no and comment if necessary)

Reductionism	No
Projectionism	No
Dualism	No
Dialectic	No

8. TRUST

In general, trust can be looked-up from different views and interpretations. Does your trust framework provide the following? (yes/no and explain)

Trustworthiness	**Yes**, considering trustworthiness as the ability of all our systems to preserve confidentiality, integrity and availability of all communications and information exchanged among devices and services.
Dependability	**No**
Sustainability.	**No**

Reliability.	Yes
Availability.	Yes
Resilience.	Yes

8.1. Personal Data Principles

Please answer if the following apply in your legal context (yes/no and explain)

People own the data (or things) they create.	Yes, if someone creates certain information it belongs to them – although it is also shared with the rest of the company.
People own the data someone creates about them.	No data created by externals
People have the right to access data gathered from public space.	No gathered data from public space
People have the right to their data in full resolution in real time.	Yes
People have the right to access their data in a standard format.	Yes
People have the right to delete or backup their data.	Yes
People have the right to use and share their data however they want	No data generated inside the company is restricted to use exclusively inside the platform.

9. ADDITIONAL QUESTIONS (OPTIONAL)

Europe 2020 "Innovation Europe" Initiative, which involves several actions towards achieving the following three goals. What is the state of these goals in your country?

Make Europe one of the world-class science performers.	Here are some of the indicators related to Spain making Europe one of the world-class science performers, according to the European Innovation Scoreboard 2022: - New doctorate graduates: 13th / 27. - International scientific co-publications: 16th / 27. - Scientific publications among the 10% most cited: 12th / 27. - SMEs introducing product innovations: 22nd / 27.
Free the innovation from obstacles such as expensive patenting, market fragmentation, and skills shortages.	According to the European Innovation Scoreboard 2022, Spain is the 17th country among all EU countries in the implementation of attractive research systems.
Revolutionize the way public and private sectors cooperate (e.g., via innovation), and enhance partnerships between European institutions, authorities (national and regional), and business.	According to the European Innovation Scoreboard 2022, Spain is the 19th country among all EU countries in public-private co-publications.

Does the existing framework regarding the protection of users is influenced by the following socio-legal-economic aspects and related issues? (yes/no and if yes define)

The trade-off between the market needs for data and correlation to support innovation, and the business success of the IoT systems and applications (public and private).	Yes
The cost of verifying and implementing privacy enhancing technologies (PET) or other solutions for ensuring appropriate care in collection, storage, and retrieval of data.	Yes
The accountability of IoT applications related to users' privacy.	Yes
Support for the context where the user operates.	Yes

C.1.2. NASERTIC

Appendix C – Legal Framework Survey

1. REGULATORY BODIES & DATA PROTECTION AUTHORITIES

1.1. Which EU-level data protection regulators and data protection authorities are you or could you be connected with?

None.

1.2. Which national and local regulatory bodies are you or could you connect with?

Agencia Española de Protección de Datos (Spanish Data Protection Agency).

1.3. Do you have any conflict of interest with those regulatory bodies?

No

2. EUROPEAN UNION FRAMEWORK

2.1. Have your government or local regulations incorporated the following?

(Answer YES/NO and comment if necessary)

Directive (EU) 2019/1024: open data and the re-use of public sector information.	YES, **Royal Decree-Law 24/2021**, regarding the transposition of directives of the European Union dealing with open data and re-use of public sector information. Link
Directive (EU) 2018/1972: establishing the European Electronic Communications Code.	YES, **Law 11/2022**, General Telecommunications Law Link
EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns "Cybersecurity" issues.	YES, **Royal Decree-Law 12/2018**, regarding network and information systems' security. Link
EU DPR-2012: European Data Protection Regulation	Replaced by EU GDPR
EU Directive-2013/40: this Directive deals with "Cybercrime" (i.e., attacks against information systems).	Yes, **Organic Law 1/2015** of 30 March, concerning the crime of discovery and disclosure of secrets and the crime of computer damages
EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns "Cybersecurity" issues.	Yes, **Royal Decree-Law 12/2018**, September 7th, network and information systems' security
EU Directive 2014/53: this directive is concerned with the standardization issue which is important for the joint and harmonized development of technology in the EU.	Yes, **Ley 11/2022**, 28 de junio, General de Telecomunicaciones, **Law 11/2022**, June 28th, General Telecommunications Law
EU GDPR: European General Data Protection Regulation-2016	Yes, **Organic Law 3/2018** of 5 December, on the Protection of Personal Data & Guarantee of Digital rights.
EU Connected Communities Initiative: This initiative concerns the IoT development infrastructure, and aims to collect information from the market about existing public and private connectivity projects that seek to provide high speed broadband, more than 30 Mbps.	Yes, As of 2015, 10 national projects in Spain were working towards the achievement of the initiative.

3. REGULATIONS

The national legal and ethical framework should cover the following. Please answer YES/NO if your framework does.

Legislation/regulations.	YES
Ethics principles, rules and codes.	YES
Standards/guidelines.	YES
Contractual arrangements.	YES
Regulations for the devices connected.	YES
Regulations for the networks and their security.	YES
Regulations for the data associated with the devices	YES

4. GOVERNMENT REGULATIONS

Governments play a primary role in shaping the future because governments have a dual role, namely

1. User role: governments plan to become major users of IoT, e.g., getting smart cities.
2. Infrastructure provider role: governments should issue regulations for devices not originally intended for connection to the IoT, as well as for devices particularly designed to be connected devices.

4.1. Which of the above is the role of your government?

Both, but the infrastructure provider role is exerted to a bigger extent.

4.2. Do your government have in force regulations for both roles?

To our knowledge, it exists no specific regulation in Spain related **explicitly** to IoT devices / networks neither for provider nor user role. There are some similar regulations that cover all electronic devices in general (which by definition include IoT infrastructures) and will keep covering IoT devices until a more specific regulation applies.

4.3. What are these regulations?

Regulations as Infrastructure provider role:

To our knowledge, there is still no specific regulation for IoT devices / IoT networks in Spain. As of right now, all IoT devices and networks in Spain must follow the regulations that concern all electronic devices in general (the ones related to cybersecurity and data protection stated in the Question 5.1, and other laws related to electromagnetic emissions and electronic commerce). Further laws that do not talk explicitly about IoT but can be related to IoT devices and networks are:

- Royal Decree-Law 7/2022, March 29th, about the technical requirements for the security of 5G networks & 5G electronic communications: not an explicit regulation about IoT, but highly related due to 5G deployment in IoT networks.

Regulations as user role:

To our knowledge, there is still no specific regulation for IoT users roles in Spain.

4.4. Do your government ensure that IoT products and solutions are used exclusively for their specified goal?

No.

4.5. Which sectors of society, industry and the economy are subject to general government legislation?

Despite not having an explicit IoT legislation in Spain, all the related laws apply to absolutely every instance of electronic devices / networks deployed on industries, business and public services (hospitals, public institutions…).

4.6. Does the relevant legislation include the following fields (yes/no and define if possible):

public law	Yes
business law	Yes
insurance law	Yes
tax law	Yes
private international/human rights law	*Don't know*
security law	Yes
criminal law	Yes
civil liability law	Yes
consumer protection law	Yes
private/data protection law	Yes
environmental law	Yes
GDPR law	Yes

4.7. Do government regulations focus on the system capabilities (e.g., how data can be reused or sold) rather than on implementation (e.g., MySQL vs. Hadoop)?

Despite not having yet specific IoT device regulations, the similar regulations that do apply to all electronic devices focus majorly on capabilities (e.g.: maximum power admitted, electromagnetic radiation, material recycling…).

5. CHARACTERISTICS THAT MAY CAUSE ETHICAL PROBLEMS

The main IoT characteristics that may cause ethical problems are the following. Please try to identify the risk of having to deal with some of these (using YES/NO/maybe) in the Use Case you participate in.

Ubiquity/omnipresence: the IoT is everywhere.	YES
Miniaturization/invisibility: computers and devices will be smaller and smaller, and transparent, thus avoiding any inspections, audit, quality control, and accounting procedures.	NO
Ambiguity: the distinction between the natural objects, artifacts, and beings will be more and more difficult to be made, because the transformation from one category to another is easy, based on tags.	NO
Difficult identification: objects/things have an identity in order to be connected to the IoT. The access to these objects and the management of their identities might cause crucial problems of security and control in the IoT ecological world.	YES
Ultra-connectivity: the huge number of connections of objects and people require the transfer of large quantities of data (big data) which could be maliciously used.	YES
Autonomous and unpredictable behaviour: the interconnected objects might interfere autonomously and spontaneously in human activities in unexpected ways for the users or designers. People, artifacts, and devices will belong to the same IoT environment, thus creating hybrid systems with unpredictable behaviour. The incremental development of IoT will lead to emerging behaviours that the users could not fully understand.	NO
Incorporated intelligence: this will make the objects as substitutes of social life. The intelligent objects will be dynamic with an emergent behaviour. Being deprived of these devices will lead to problems (e.g., teenagers without the Google, smart phone or social media, might feel themselves cognitively or socially handicapped).	MAYBE
Decentralized operation: the IoT control and governance cannot be centralized, because of the large number of hubs, switches, and data. The information flows will be eased, and the data transfers will be faster and cheaper, and thus not easily controllable. There will appear emerging properties and phenomena which will require monitoring and governance in an adequate way, and this will further influence the accountancy and control activities.	YES
Property right on data and information: the difficulty in specifying the identification of things and humans is reflected to the difficulty to identify who is the owner of the data retrieved by IoT sensors and devices.	YES
Omnipresence: this makes invisible the boundaries between public and private space. People cannot know where their information ends up.	YES
Accessibility of data: an attack on a PC might cause information loss. A virus or hacker attack in the IoT might have serious effects on human life (e.g., on the life of the driver of a car connected to IoT).	YES
Vulnerability: the list of possible vulnerabilities in IoT is scaring. It ranges from home appliances, to hospitals, traffic lights systems, food distribution networks, transportation systems, and so on.	YES
Digital divide: the digital divide in the IoT is enlarged. IoT operations can be understood only by experts. Communication in IoT devices affects human lives in ways that are difficult to predict or imagine. The digital divide can only be reduced by proper coherent legal and democratic frames to delineate this process.	NO

6. ETHICS QUESTIONS

6.1. Information technology ethics and Internet ethics.

What happens if the Internet connection breaks down?
If the Internet connection fails at any point in the Governments' infrastructure (provided and controlled by us), the users affected must contact the Governments' Troubleshooting Callcenter, which will then redirect the issue to us. Once we get to know the issue, we solve it as soon as possible.
Who is responsible or liable for patching IoT devices, routers, and cloud connections?
Telco technicians and telco engineers.
Is there an assurance that hacking on the cloud side of IoT services will not have access to a home's internal network?
Yes, our government's infrastructure is secured. To begin with, the Government's network is made up entirely by our own infrastructure, physically isolated from other networks. The entire Government's network has a unique access point to the Internet, and it is thoroughly secured via a firewall, which prevents the access from anyone coming from the Internet external to the organization. Furthermore, every subnetwork is logically isolated from one another via the firewall as well. Accessing the servers where services are hosted does not enable access to end users' network.
What happens if an IoT service provider experiences downtime for critical life-supporting devices?
We do not have critical life-supporting devices in our network. Despite that, most of our network is redundant so that if a certain part of the network goes down, a parallel path is able to replace it.
What happens if an IoT device acts without the consent of its owner or acts in unintended ways (e.g., ordering the wrong products, or vacuuming at an unreasonable hour)?
That is not contemplated to happen.
What happens if an IoT product vendor goes out of business and no longer supports the product?
We do not work with IoT product vendors – we do work with telecommunication electronics (switches, routers) from different vendors. A product vendor going out of business does not disable our ability to reach similar products. However, all the deployed electronic which no longer has support from its vendor will eventually get replaced.
Who owns the data collected by IoT devices?
We do not work with IoT devices, but we do work with telecommunication electronics which also produce information which we analyse and monitor to obtain meaningful information. All that information is gathered and stored in servers, owned and managed by few individuals.
Are there cases where IoT devices should not be collecting data?
No.
What happens if the user wants to opt out?
It can do it with no problem.
What about those who do not have smart devices or the knowledge to use them? (Digital divide).
The relation of the end user with our infrastructure only takes place at 2 points: - When they try to connect to the WiFi Access Points that we provide all throughout the network. - When they try to connect to the wired Internet connection via Internet. Both procedures are very straight forward, but even if someone had connectivity issues, a Government Troubleshooting Callcenter is available to provide guidance.

6.2. Ethical principles

All activities involving the use of personal data are expected to comply with applicable data protection legislation. Beyond legal compliance, activities must respect ethical principles. Please try to assess whether the use case you lead/participate in complies with the following (definitely/future/probably/not) and comment if necessary:

In IoT activities, individuals should be treated as ends (not as means), and maintain their rights to property, autonomy, private life, and dignity.	Definitely
Individuals should not suffer physical or mental harm from IoT activities.	Definitely
Benefits from the application of IoT should be added to the common good.	Definitely
The necessity and proportionality of an IoT process should be taken into account and capable of being demonstrated.	Definitely
IoT applications should be performed with maximum transparency and accountability via explicit and auditable procedures.	Definitely
There should be equal access to the benefits of IoT accruing to individuals (social justice).	Definitely
IoT activities should have minimum negative impact to all facets of the natural environment.	Definitely
IoT activities should aim to lighten the adverse consequences that data processing may have on personal privacy and other personal and social values.	Definitely
Adverse effects beyond the individual (groups, communities, societies) should be avoided or minimized or mitigated.	Definitely

7. PRIVACY

The European Union General Data Protection Regulations (EU GDPR 2016, etc.) impose the principles that should underlie the processing of personal information. A new principle added to EU GDPR 2016 is the principle of "Privacy by Design". Does your privacy framework include the following? (yes/no and if yes define)

Privacy regulations	Yes
Data minimization	Yes
Data portability	Yes
Transparency	Yes
Compliance disclosures	Yes
IoT engagement by default	No
IoT engagement by design	No
Best practice	Yes: integrated system for the protection of personal data & Compliance within the organization

The concepts of security and privacy have many complex interrelationships, but they are not identical. Do you have the following relations between security and privacy? (yes/no and comment if necessary)

Reductionism	?
Projectionism	?
Dualism	?
Dialectic	?

8. TRUST

In general, trust can be looked-up from different views and interpretations. Does your trust framework provide the following? (yes/no and explain)

Trustworthiness	**Yes**, considering trustworthiness as the ability of all our systems to preserve confidentiality, integrity and availability of all communications and information exchanged among devices and services.
Dependability	**Yes**, the Government of Navarra (and thus the whole Navarra's society as a whole) depend entirely on us to deliver telecommunication services and infrastructure to all the region.
Sustainability.	-
Reliability.	**Yes**, as we consider reliability granted by the availability and resilience.
Availability.	**Yes**, a telco infrastructure (network) works continuously. The resilience also contributes to the permanent availability.
Resilience.	**Yes**, we are providers of telco infrastructure, and we deploy redundant devices and redundancy protocols to ensure that our network is resilient.

8.1. Personal Data Principles

People own the data (or things) they create.	Yes, if someone creates certain information it belongs to them – although it is also shared with the rest of the company.
People own the data someone creates about them.	As long as the data is created within the organization, the affected person must be put into knowledge of the existence of such information.
People have the right to access data gathered from public space.	We do not have access to sensible end user information – we only have access to network information (connectivity throughputs, etc…)
People have the right to their data in full resolution in real time.	Yes
People have the right to access their data in a standard format.	Yes
People have the right to delete or backup their data.	Yes, our organization provides a set of backup services and tools to ensure everyone's information is safely backed up.
People have the right to use and share their data however they want	No, data generated inside the company is restricted to use exclusively inside the company.

9. ADDITIONAL QUESTIONS (OPTIONAL)

Europe 2020 "Innovation Europe" Initiative, which involves several actions towards achieving the following three goals. What is the state of these goals in your country?

Make Europe one of the world-class science performers.	Here are some of the indicators related to Spain making Europe one of the world-class science performers, according to the European Innovation Scoreboard 2022: - New doctorate graduates: 13th / 27. - International scientific co-publications: 16th / 27. - Scientific publications among the 10% most cited: 12th / 27. - SMEs introducing product innovations: 22nd / 27.
Free the innovation from obstacles such as expensive patenting, market fragmentation, and skills shortages.	According to the European Innovation Scoreboard 2022, Spain is the 17th country among all EU countries in the implementation of attractive research systems.
Revolutionize the way public and private sectors cooperate (e.g., via innovation), and enhance partnerships between European institutions, authorities (national and regional), and business.	According to the European Innovation Scoreboard 2022, Spain is the 19th country among all EU countries in public-private co-publications.

Does the existing framework regarding the protection of users is influenced by the following socio-legal-economic aspects and related issues? (yes/no and if yes define)

The trade-off between the market needs for data and correlation to support innovation, and the business success of the IoT systems and applications (public and private).	Yes
The cost of verifying and implementing privacy enhancing technologies (PET) or other solutions for ensuring appropriate care in collection, storage, and retrieval of data.	Yes
The accountability of IoT applications related to users' privacy.	Yes, all the creation, deletion and retrieval of data is accounted / logged.
Support for the context where the user operates.	Yes, we know the particularities that each user requires, and we provide our services based on that.

C.1.3. MADE and POLIMI

Appendix C – Legal Framework Survey

1. REGULATORY BODIES & DATA PROTECTION AUTHORITIES

1.1. Which EU-level data protection regulators and data protection authorities are you or could you be connected with?

CEN-CENELEC-ETSI Coordination Group on Smart Manufacturing

1.2. 1.2. Which national and local regulatory bodies are you or could you connect with?

Italian Ministry of Economic Development
Lombardy Region (Ministry of Economic Development, Councilor of Productive Activities)

1.3. 1.3. Do you have any conflict of interest with those regulatory bodies?

No (both for POLIMI and MADE).

2. EUROPEAN UNION FRAMEWORK

2.1. 2.1. Have your government or local regulations incorporated the following?

Directive (EU) 2019/1024: open data and the re-use of public sector information.	
Directive (EU) 2018/1972: establishing the European Electronic Communications Code.	
EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns “Cybersecurity” issues.	
EU DPR-2012: European Data Protection Regulation	Y
EU Directive-2013/40: this Directive deals with “Cybercrime” (i.e., attacks against information systems).	Y
EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns “Cybersecurity” issues.	Y
EU Directive 2014/53: this directive is concerned with the standardization issue which is important for the joint and harmonized development of technology in the EU.	Y
EU GDPR: European General Data Protection Regulation-2016	Y
EU Connected Communities Initiative: This initiative concerns the IoT development infrastructure, and aims to collect information from the market about existing public and private connectivity projects that seek to provide high speed broadband, more than 30 Mbps.	N

3. REGULATIONS

The national legal and ethical framework should cover the following. Please answer YES/NO if your framework does.

Legislation/regulations.	Y
Ethics principles, rules and codes.	Y
Standards/guidelines.	N
Contractual arrangements.	Y
Regulations for the devices connected.	Y
Regulations for the networks and their security.	Y
Regulations for the data associated with the devices	Y

4. GOVERNMENT REGULATIONS

Governments play a primary role in shaping the future because governments have a dual role, namely

1. User role: governments plan to become major users of IoT, e.g., getting smart cities.
2. Infrastructure provider role: governments should issue regulations for devices not originally intended for connection to the IoT, as well as for devices particularly designed to be connected devices.

4.1. Which of the above is the role of your government?

2: national government issues regulations for devices and ICT infrastructures, which are embodied by private (or public/private) providers.

4.2. Do your government have in force regulations for both roles?

Only for providers.

4.3. What are these regulations?

A specific public authority (namely AGCOM) provides and updates requirements and guarantees for the commercialization of Communication devices and networks.

4.4. Do your government ensure that IoT products and solutions are used exclusively for their specified goal?

No.

4.5. Which sectors of society, industry and the economy are subject to general government legislation?

Manufacturing, Healthcare, Food Telecommunication.

4.6. Does the relevant legislation include the following fields (yes/no and define if possible):

public law	Y
business law	Y
insurance law	N
tax law	Y
private international/human rights law	N
security law	Y
criminal law	Y
civil liability law	Y
consumer protection law	Y
private/data protection law	Y
environmental law	Y
GDPR law	Y

4.7. Do government regulations focus on the system capabilities (e.g., how data can be reused or sold) rather than on implementation (e.g., MySQL vs. Hadoop)?

At the time being, nothing executive has been released, but is a (pretended) topic in the government agenda.

5. CHARACTERISTICS THAT MAY CAUSE ETHICAL PROBLEMS

The main IoT characteristics that may cause ethical problems are the following. Please try to identify the risk of having to deal with some of these (using YES/NO/maybe) in the Use Case you participate in.

Ubiquity/omnipresence: the IoT is everywhere.	Y
Miniaturization/invisibility: computers and devices will be smaller and smaller, and transparent, thus avoiding any inspections, audit, quality control, and accounting procedures.	N
Ambiguity: the distinction between the natural objects, artifacts, and beings will be more and more difficult to be made, because the transformation from one category to another is easy, based on tags.	Y
Difficult identification: objects/things have an identity in order to be connected to the IoT. The access to these objects and the management of their identities might cause crucial problems of security and control in the IoT ecological world.	N
Ultra-connectivity: the huge number of connections of objects and people require the transfer of large quantities of data (big data) which could be maliciously used.	Y
Autonomous and unpredictable behaviour: the interconnected objects might interfere autonomously and spontaneously in human activities in unexpected ways for the users or designers. People, artifacts, and devices will belong to the same IoT environment, thus creating hybrid systems with unpredictable behaviour. The incremental development of IoT will lead to emerging behaviours that the users could not fully understand.	Y
Incorporated intelligence: this will make the objects as substitutes of social life. The intelligent objects will be dynamic with an emergent behaviour. Being deprived of these devices will lead to problems (e.g., teenagers without the Google, smart phone or social media, might feel themselves cognitively or socially handicapped).	Y
Decentralized operation: the IoT control and governance cannot be centralized, because of the large number of hubs, switches, and data. The information flows will be eased, and the data transfers will be faster and cheaper, and thus not easily controllable. There will appear emerging properties and phenomena which will require monitoring and governance in an adequate way, and this will further influence the accountancy and control activities.	Y
Property right on data and information: the difficulty in specifying the identification of things and humans is reflected to the difficulty to identify who is the owner of the data retrieved by IoT sensors and devices.	Y
Omnipresence: this makes invisible the boundaries between public and private space. People cannot know where their information ends up.	Y
Accessibility of data: an attack on a PC might cause information loss. A virus or hacker attack in the IoT might have serious effects on human life (e.g., on the life of the driver of a car connected to IoT).	Y
Vulnerability: the list of possible vulnerabilities in IoT is scaring. It ranges from home appliances, to hospitals, traffic lights systems, food distribution networks, transportation systems, and so on.	Y
Digital divide: the digital divide in the IoT is enlarged. IoT operations can be understood only by experts. Communication in IoT devices affects human lives in ways that are difficult to predict or imagine. The digital divide can only be reduced by proper coherent legal and democratic frames to delineate this process.	Y

6. ETHICS QUESTIONS

6.1. Information technology ethics and Internet ethics.

What happens if the Internet connection breaks down?
Depending on the duration of disconnection, data losses and degradation of data reliability could happen. Online services (e.g., predictive maintenance) could be lost.
Who is responsible or liable for patching IoT devices, routers, and cloud connections?
Both internal technical staff and external service suppliers.
Is there an assurance that hacking on the cloud side of IoT services will not have access to a home’s internal network?
Only if guaranteed by the cloud provider (apart from “normal” countermeasures such as hardware and software firewalls).
What happens if an IoT service provider experiences downtime for critical life-supporting devices?
No such device is embodied in the use case
What happens if an IoT device acts without the consent of its owner or acts in unintended ways (e.g., ordering the wrong products, or vacuuming at an unreasonable hour)?
Nothing, apart need of reconfiguration on the next working shift.
What happens if an IoT product vendor goes out of business and no longer supports the product?
Depending on the specific device: - Support interruption - Change of service supplier - Acquiring of a new device from a different vendor
Who owns the data collected by IoT devices?
Data are owned by the suppliers who provides the devices (according to the standard conract signed by MADE and its suppliers)
Are there cases where IoT devices should not be collecting data?
N/A
What happens if the user wants to opt out?
N/A
What about those who do not have smart devices or the knowledge to use them? (Digital divide).
Both MADE and POLIMI provide courses (free or paid) to upskill personnel and fill the gap.

6.2. Ethical principles

All activities involving the use of personal data are expected to comply with applicable data protection legislation. Beyond legal compliance, activities must respect ethical principles. Please try to assess whether the use case you lead/participate in complies with the following (definitely/future/probably/not) and comment if necessary:

In IoT activities, individuals should be treated as ends (not as means), and maintain their rights to property, autonomy, private life, and dignity.	Definitely
Individuals should not suffer physical or mental harm from IoT activities.	Definitely
Benefits from the application of IoT should be added to the common good.	Probably not (it is supposed to generate business, not charity)
The necessity and proportionality of an IoT process should be taken into account and capable of being demonstrated.	Definitely
IoT applications should be performed with maximum transparency and accountability via explicit and auditable procedures.	Definitely
There should be equal access to the benefits of IoT accruing to individuals (social justice).	Probably not
IoT activities should have minimum negative impact to all facets of the natural environment.	Definitely
IoT activities should aim to lighten the adverse consequences that data processing may have on personal privacy and other personal and social values.	Definitely
Adverse effects beyond the individual (groups, communities, societies) should be avoided or minimized or mitigated.	Definitely

7. PRIVACY

The EU General Data Protection Regulations (EU GDPR 2016 etc.) impose the principles that must underlie the processing of personal information. A new principle added to the 2016 EU GDPR is the principle of "Privacy by Design". Does your privacy framework include the following? (yes/no and if so specify)

Privacy regulations	Y
Data minimization	N
Data portability	N
Transparency	Y
Compliance disclosures	Y
IoT engagement by default	N
IoT engagement by design	Y
Best practice	Y

The concepts of security and privacy have many complex interrelationships, but they are not identical. Do you have the following relations between security and privacy? (yes/no and comment if necessary)

Reductionism	N
Projectionism	N
Dualism	Y
Dialectic	Y

8. TRUST

In general, trust can be looked-up from different views and interpretations. Does your trust framework provide the following? (yes/no and explain)

Trustworthiness	Y (partners and customers provide/are provided internally verified data)
Dependability	N (data are not maintained)
Sustainability.	N
Reliability.	Y (partners and customers provide/are provided reliable data)
Availability.	N (devices are not continuously online)
Resilience.	N

8.1. Personal Data Principles

People own the data (or things) they create.	Y

People own the data someone creates about them.	Depends from the application
People have the right to access data gathered from public space.	N
People have the right to their data in full resolution in real time.	Y (theoretically)
People have the right to access their data in a standard format.	Y
People have the right to delete or backup their data.	Y
People have the right to use and share their data however they want	N (it depends on the specific signed agreement)

Please answer if the following apply in your legal context (yes/no and explain)

9. ADDITIONAL QUESTIONS (OPTIONAL)

Europe 2020 "Innovation Europe" Initiative, which involves several actions towards achieving the following three goals. What is the state of these goals in your country?

Make Europe one of the world-class science performers.	Implementation of "Piano Industria 4.0" including financial benefits for manufacturing companies implementing R&D projects and renewal of productive infrastructure to the latest ICT standards.
Free the innovation from obstacles such as expensive patenting, market fragmentation, and skills shortages.	Development of regulatory sandboxes to enhance technology transfer. Development of ad hoc tax incentives for training and upskilling initiatives.
Revolutionize the way public and private sectors cooperate (e.g., via innovation), and enhance partnerships between European institutions, authorities (national and regional), and business.	Creation of competence centres

Does the existing framework regarding the protection of users is influenced by the following socio-legal-economic aspects and related issues? (yes/no and if yes define)

The trade-off between the market needs for data and correlation to support innovation, and the business success of the IoT systems and applications (public and private).	Embodiment of European directives in terms of creation and maintenance of Digital Innovation Hubs and European Digital Innovation Hubs in creating a one-stop-shop to allow manufacturing firms to adapt their technological skills and business strategies to bridge among the capability of production/management and analysis of data and the market needs.
The cost of verifying and implementing privacy enhancing technologies (PET) or other solutions for ensuring appropriate care in collection, storage, and retrieval of data.	N/A
The accountability of IoT applications related to users' privacy.	N/A
Support for the context where the user operates.	GDPR embodiment

C.1.4. SIPBB

Appendix C – Legal Framework Survey

1. REGULATORY BODIES & DATA PROTECTION AUTHORITIES

1.1. Which EU-level data protection regulators and data protection authorities are you or could you be connected with?

None

1.2. Which national and local regulatory bodies are you or could you connect with?

- Swiss Federal Data Protection and Information Commissioner (EDÖB)

The Federal Data Protection and Information Commissioner (EDÖB) is an independent authority in Switzerland responsible for protecting privacy and monitoring data protection. The FDPIC promotes compliance with data protection laws and makes recommendations on their implementation. It also promotes the disclosure of information in the public interest and monitors compliance with public disclosure laws. https://www.edoeb.admin.ch/edoeb/de/home.html

- The Federal Office if Communications (BAKOM)

The Federal Office of Communications (OFCOM) is a Swiss federal authority responsible for regulating and supervising the telecommunications and postal markets. OFCOM promotes access to fast Internet and mobile communications in Switzerland, monitors compliance with quality and security standards, and allocates frequencies for mobile communications and other applications. In addition, OFCOM works to promote media diversity and freedom of expression and is responsible for implementing laws and international agreements in the telecommunications and postal sectors. https://www.bakom.admin.ch/bakom/en/homepage.html

1.3. Do you have any conflict of interest with those regulatory bodies?

No

2. EUROPEAN UNION FRAMEWORK

2.1. Have your government or local regulations incorporated the following?

(Answer YES/NO and comment if necessary)

Directive (EU) 2019/1024: open data and the re-use of public sector information.	YES
Directive (EU) 2018/1972: establishing the European Electronic Communications Code.	YES
EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns "Cybersecurity" issues.	YES
EU DPR-2012: European Data Protection Regulation	Y
EU Directive-2013/40: this Directive deals with "Cybercrime" (i.e., attacks against information systems).	Y
EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns "Cybersecurity" issues.	Y
EU Directive 2014/53: this directive is concerned with the standardization issue which is important for the joint and harmonized development of technology in the EU.	Y
EU GDPR: European General Data Protection Regulation-2016	Y
EU Connected Communities Initiative: This initiative concerns the IoT development infrastructure, and aims to collect information from the market about existing public and private connectivity projects that seek to provide high speed broadband, more than 30 Mbps.	N

3. REGULATIONS

The national legal and ethical framework should cover the following. Please answer YES/NO if your framework does.

Legislation/regulations.	Y
Ethics principles, rules, and codes.	Y
Standards/guidelines.	Y
Contractual arrangements.	Y
Regulations for the devices connected.	Y
Regulations for the networks and their security.	Y
Regulations for the data associated with the devices	Y

4. GOVERNMENT REGULATIONS

Governments play a primary role in shaping the future because governments have a dual role, namely

1. User role: governments plan to become major users of IoT, e.g., getting smart cities.
2. Infrastructure provider role: governments should issue regulations for devices not originally intended for connection to the IoT, as well as for devices particularly designed to be connected devices.

4.1. Which of the above is the role of your government?

Both. Switzerland is pushing Innovations like smart cities and other IoT related Innovation topics. Switzerland has also regulations for devices which are upgrade with connectivity and also for new IoT devices.
https://www.smartcityhub.ch/home.4en.html

4.2. Do your government have in force regulations for both roles?

Yes

4.3. What are these regulations?

The Federal Office of Communications is dedicated governmental authority (namely BAKOM) provides regulations for digitalization and internet. Within the BAKOM there is a dedicated sector about IoT.
https://www.bakom.admin.ch/bakom/en/homepage/digital-switzerland-and-internet/internet/internet-of-things.html

4.4. Do your government ensure that IoT products and solutions are used exclusively for their specified goal?

Yes
https://www.bakom.admin.ch/bakom/en/homepage/digital-switzerland-and-internet/internet/internet-of-things.html

4.5. Which sectors of society, industry and the economy are subject to general government legislation?

In Switzerland general government legislation is called the "Federal Constitution" and includes every sector of society, industry and the economy. More information can be found here:
https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/1999/404/20160101/de/pdf-a/fedlex-data-admin-ch-eli-cc-1999-404-20160101-de-pdf-a.pdf

4.6. Does the relevant legislation include the following fields (yes/no and define if possible):

public law	Y
business law	Y
insurance law	Y
tax law	Y
private international/human rights law	Y
security law	Y
criminal law	Y
civil liability law	Y
consumer protection law	Y
private/data protection law	Y
environmental law	Y
GDPR law	Y

4.7. Do government regulations focus on the system capabilities (e.g., how data can be reused or sold) rather than on implementation (e.g., MySQL vs. Hadoop)?

Yes

5. CHARACTERISTICS THAT MAY CAUSE ETHICAL PROBLEMS

The main IoT characteristics that may cause ethical problems are the following. Please try to identify the risk of having to deal with some of these (using YES/NO/maybe) in the Use Case you participate in.

Ubiquity/omnipresence: the IoT is everywhere.	Y
Miniaturization/invisibility: computers and devices will be smaller and smaller, and transparent, thus avoiding any inspections, audit, quality control, and accounting procedures.	N
Ambiguity: the distinction between the natural objects, artifacts, and beings will be more and more difficult to be made, because the transformation from one category to another is easy, based on tags.	Y
Difficult identification: objects/things have an identity in order to be connected to the IoT. The access to these objects and the management of their identities might cause crucial problems of security and control in the IoT ecological world.	N
Ultra-connectivity: the huge number of connections of objects and people require the transfer of large quantities of data (big data) which could be maliciously used.	Y
Autonomous and unpredictable behaviour: the interconnected objects might interfere autonomously and spontaneously in human activities in unexpected ways for the users or designers. People, artifacts, and devices will belong to the same IoT environment, thus creating hybrid systems with unpredictable behaviour. The incremental development of IoT will lead to emerging behaviours that the users could not fully understand.	maybe
Incorporated intelligence: this will make the objects as substitutes of social life. The intelligent objects will be dynamic with an emergent behaviour. Being deprived of these devices will lead to problems (e.g., teenagers without the Google, smart phone or social media, might feel themselves cognitively or socially handicapped).	Y
Decentralized operation: the IoT control and governance cannot be centralized, because of the large number of hubs, switches, and data. The information flows will be eased, and the data transfers will be faster and cheaper, and thus not easily controllable. There will appear emerging properties and phenomena which will require monitoring and governance in an adequate way, and this will further influence the accountancy and control activities.	Y
Property right on data and information: the difficulty in specifying the identification of things and humans is reflected to the difficulty to identify who is the owner of the data retrieved by IoT sensors and devices.	Y
Omnipresence: this makes invisible the boundaries between public and private space. People cannot know where their information ends up.	Y
Accessibility of data: an attack on a PC might cause information loss. A virus or hacker attack in the IoT might have serious effects on human life (e.g., on the life of the driver of a car connected to IoT).	Y
Vulnerability: the list of possible vulnerabilities in IoT is scaring. It ranges from home appliances, to hospitals, traffic lights systems, food distribution networks, transportation systems, and so on.	Y
Digital divide: the digital divide in the IoT is enlarged. IoT operations can be understood only by experts. Communication in IoT devices affects human lives in ways that are difficult to predict or imagine. The digital divide can only be reduced by proper coherent legal and democratic frames to delineate this process.	Y

6. ETHICS QUESTIONS

6.1. Information technology ethics and Internet ethics.

What happens if the Internet connection breaks down?
Data losses, Factory break downs and production stops if a production system relies on the connection. General Services on the platform would out (OEE, Dashboarding, predictive Maintenance, Optimized Producion etc.)
Who is responsible or liable for patching IoT devices, routers, and cloud connections?
The internal staff of the company and the suppliers of machines and production systems.
Is there an assurance that hacking on the cloud side of IoT services will not have access to a home's internal network?
No, it must be ensured that no hacking occurs on the cloud side of IoT services.
What happens if an IoT service provider experiences downtime for critical life-supporting devices?
There are no life-supporting devices included in the use-case
What happens if an IoT device acts without the consent of its owner or acts in unintended ways (e.g., ordering the wrong products, or vacuuming at an unreasonable hour)?
Nothing serious, the production of the demo-case could be interrupted.
What happens if an IoT product vendor goes out of business and no longer supports the product?
There must be searched for an alternative product vendor or a new kind of device must be procured.
Who owns the data collected by IoT devices?
The entity that owns the IoT device also owns the data collected by the IoT device.
Are there cases where IoT devices should not be collecting data?
Yes, if the data is useless
What happens if the user wants to opt out?
If the data is user-based data, the device will not be able to collect data anymore.
What about those who do not have smart devices or the knowledge to use them? (Digital divide).
The technical staff in the SSF is very well educated and all have the knowledge to use them

6.2. Ethical principles

All activities involving the use of personal data are expected to comply with applicable data protection legislation. Beyond legal compliance, activities must respect ethical principles. Please try to assess whether the use case you lead/participate in complies with the following (definitely/future/probably/not) and comment if necessary):

In IoT activities, individuals should be treated as ends (not as means), and maintain their rights to property, autonomy, private life, and dignity.	Definitely
Individuals should not suffer physical or mental harm from IoT activities.	Definitely
Benefits from the application of IoT should be added to the common good.	Definitely
The necessity and proportionality of an IoT process should be taken into account and capable of being demonstrated.	Definitely
IoT applications should be performed with maximum transparency and accountability via explicit and auditable procedures.	Definitely
There should be equal access to the benefits of IoT accruing to individuals (social justice).	Definitely
IoT activities should have minimum negative impact to all facets of the natural environment.	Definitely
IoT activities should aim to lighten the adverse consequences that data processing may have on personal privacy and other personal and social values.	Definitely
Adverse effects beyond the individual (groups, communities, societies) should be avoided or minimized or mitigated.	Definitely

7. PRIVACY

The European Union General Data Protection Regulations (EU GDPR 2016, etc.) impose the principles that should underlie the processing of personal information. A new principle added to EU GDPR 2016 is the principle of "Privacy by Design".

Do your privacy framework include the following? (yes/no and if yes define)

In our demo production-line, we do not have any personal data. All personal related data is based on random fictional persons. Therefore, most of the following points are not relevant.

Privacy regulations	Y
Data minimization	N
Data portability	N
Transparency	Y
Compliance disclosures	Y
IoT engagement by default	N
IoT engagement by design	N
Best practice	Y

The concepts of security and privacy have many complex interrelationships, but they are not identical. Do you have the following relations between security and privacy? (yes/no and comment if necessary)

Reductionism	N
Projectionism	N
Dualism	N
Dialectic	N

8. TRUST

In general, trust can be looked-up from different views and interpretations. Does your trust framework provide the following? (yes/no and explain)

Trustworthiness	Y
Dependability	Y
Sustainability.	Y
Reliability.	Y
Availability.	Y
Resilience.	Y

8.1. Personal Data Principles

In our demo production-line, we do not have any personal data. All personal related data is based on random fictional persons. Therefore, the following points are not relevant.

Please answer if the following apply in your legal context (yes/no and explain

People own the data (or things) they create.	Y
People own the data someone creates about them.	Y
People have the right to access data gathered from public space.	Y
People have the right to their data in full resolution in real time.	Y
People have the right to access their data in a standard format.	Y
People have the right to delete or backup their data.	Y
People have the right to use and share their data however they want	Y

9. ADDITIONAL QUESTIONS (OPTIONAL)

Europe 2020 "Innovation Europe" Initiative, which involves several actions towards achieving the following three goals. What is the state of these goals in your country?

Make Europe one of the world-class science performers.	
Free the innovation from obstacles such as expensive patenting, market fragmentation, and skills shortages.	
Revolutionize the way public and private sectors cooperate (e.g., via innovation), and enhance partnerships between European institutions, authorities (national and regional), and business.	*Switzerland is absolutely pushing the cooperation between research (Innovation Parks, Universities) and private companies national and Europewide. More info:* *https://www.innosuisse.ch/inno/de/home.html* *https://www.innosuisse.ch/inno/de/home/forderung-fur-internationale-projekte/eurostars.html*

C.2. Pilot 2

C.2.1. ELECTRUM

Appendix C – Legal Framework Survey

1.REGULATORY BODIES & DATA PROTECTION AUTHORITIES

1.1.Which EU-level data protection regulators and data protection authorities are you or could you be connected with?

None, see also #2.

1.2.Which national and local regulatory bodies do you have or could you connect with?

URE - Urząd Regulacji Energetyki (eng: Office for Energy Regulations)

1.3.Do you have any conflict of interest with those regulatory bodies?

No, we design systems that work with or without the government operated and regulated energy grid infrastructure.

2.EUROPEAN UNION FRAMEWORK

2.1.Have your government or local regulations incorporated the following?

Directive (EU) 2019/1024: open data and the re-use of public sector information.	YES, L 172 (EU 2019/1024): https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ:L:2019:172:TOC
Directive (EU) 2018/1972: establishing the European Electronic Communications Code.	YES, L321 (EU 2018/1972): https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ:L:2018:321:TOC
EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns "Cybersecurity" issues.	YES
EU DPR-2012: European Data Protection Regulation	YES
EU Directive-2013/40: this Directive deals with "Cybercrime" (i.e., attacks against information systems).	YES
EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns "Cybersecurity" issues.	YES
EU Directive 2014/53: this directive is concerned with the standardization issue which is important for the joint and harmonized development of technology in the EU.	YES
EU GDPR: European General Data Protection Regulation-2016	YES
EU Connected Communities Initiative: This initiative concerns the IoT development infrastructure, and aims to collect information from the market about existing public and private connectivity projects that seek to provide high speed broadband, more than 30 Mbps.	YES, Poland had the highest representation of projects (https://digital-strategy.ec.europa.eu/en/news/connected-communities-initiative)

3.REGULATIONS

The national legal and ethical framework should cover the following. Please answer YES/NO if your framework does.

Legislation/regulations.	YES
Ethics principles, rules and codes.	YES
Standards/guidelines.	YES
Contractual arrangements.	YES
Regulations for the devices connected.	YES
Regulations for the networks and their security.	YES
Regulations for the data associated with the devices	YES

4.GOVERNMENT REGULATIONS

Governments play a primary role in shaping the future because governments have a dual role, namely

1. User role: governments plan to become major users of IoT, e.g.: smart cities.
2. Infrastructure provider role: governments should issue regulations for devices not originally intended for connection to the IoT, as well as for devices particularly designed to be connected devices.

4.1.Which of the above is the role of your government?

Both.

Ad. 1 – Polish government promotes IoT. Polish Ministry of Foreign Affairs prepares a new project to promote Polish companies offering technologies that improve management and quality of life in cities (https://www.gov.pl/web/govtech/dolacz-do-wspolnej-oferty-polish-smart-city-i-zdobywaj-nowe-zagraniczne-rynki). Polish Development Fund Group prepared "PFR for Cities" program whose main purpose is to support the development of Polish smart cities of the future (https://pfr.pl/en/pfr-for-cities.html).

Ad. 2 – Polish regulations on IoT can be divided into four basic groups: a) cybersecurity, b) protection of personal data and privacy c) civil law and liability for damage d) intellectual property rights.

4.2.Do your government have in force regulations for both roles?

Yes.

4.3.What are these regulations?

The most important regulations are as follows:

- Law on the national cybersecurity system (*pl. Ustawa o krajowym systemie cyberbezpieczeństwa*),
- Telecommunications law (*pl. Ustawa prawo telekomunikacyjne*),
- Law on provision of electronic services (*pl. Ustawa o świadczeniu usług drogą elektroniczną*)
- Law on personal data protection and the GDPR,
- Civil Code,
- Law on copyright and related rights,
- Consumer rights law (*pl. Ustawa o prawach konsumenta*).

4.4.Do your government ensure that IoT products and solutions are used exclusively for their specified goal?

Polish legal regulations concern, among others:

1. the responsibilities of product producers and solution providers,
2. civil liability for damage,
3. protection of personal data and privacy,
4. cybersecurity,
5. copyright.

Taking into consideration the above, in our opinion Polish government ensures that IoT products and solutions are used exclusively for their specified goal.

4.5.Which sectors of society, industry and the economy are subject to general government legislation?

Society: e.g. home appliances, health&fitness (regulations on privacy, responsibility for the product and consumer protection).

Industry and economy: a.o. smart manufacturing and agriculture (e.g. regulations on environmental protection), energy sector (smart grids etc.), telecommunication, e-commerce, transportation and logistics.

4.6.Does the relevant legislation include the following fields (yes/no and define if possible):

public law	YES	Public Procurement Law (*pl. Ustawa prawo zamówień publicznych*)
business law	YES	Commercial Companies Code and Civil Code
insurance law	YES	Insurance and Reinsurance Business Act (*pl. Ustawa o działalności ubezpieczeniowej i reasekuracyjnej*) and Civil Code
tax law	YES	Acts on PIT, CIT, VAT and Tax ordinance
private international/human rights law	YES	Private international law (*pl. Ustawa prawo prywatne międzynarodowe*), Convention for the Protection of Human Rights and Fundamental Freedoms
security law	YES	Law on the national cybersecurity system
criminal law	YES	Criminal Code
civil liability law	YES	Civil Code
consumer protection law	YES	Consumer rights law and law on provision of electronic services
private/data protection law	YES	Law on personal data protection, the GDPR, Law on provision of electronic services and Telecommunications law
environmental law	YES	Environmental protection law (*pl. Ustawa prawo ochrony środowiska*)
GDPR law	YES	Law on personal data protection and the GDPR

4.7.Do government regulations focus on the system capabilities (e.g., how data can be reused or sold) rather than on implementation (e.g., MySQL vs. Hadoop)?

Yes. Polish government regulations focus on the system capabilities rather than on implementation.

5.CHARACTERISTICS THAT MAY CAUSE ETHICAL PROBLEMS

The main IoT characteristics that may cause ethical problems are the following. Please try to identify the risk of having to deal with some of these (using YES/NO/maybe) in the Use Case you participate in.

Ubiquity/omnipresence: the IoT is everywhere.	MAYBE
Miniaturization/invisibility: computers and devices will be smaller and smaller, and transparent, thus avoiding any inspections, audit, quality control, and accounting procedures.	MAYBE
Ambiguity: the distinction between the natural objects, artifacts, and beings will be more and more difficult to be made, because the transformation from one category to another is easy, based on tags.	MAYBE
Difficult identification: objects/things have an identity in order to be connected to the IoT. The access to these objects and the management of their identities might cause crucial problems of security and control in the IoT ecological world.	MAYBE
Ultra-connectivity: the huge number of connections of objects and people require the transfer of large quantities of data (big data) which could be maliciously used.	MAYBE
Autonomous and unpredictable behaviour: the interconnected objects might interfere autonomously and spontaneously in human activities in unexpected ways for the users or designers. People, artifacts, and devices will belong to the same IoT environment, thus creating hybrid systems with unpredictable behaviour. The incremental development of IoT will lead to emerging behaviours that the users could not fully understand.	MAYBE
Incorporated intelligence: this will make the objects as substitutes of social life. The intelligent objects will be dynamic with an emergent behaviour. Being deprived of these devices will lead to problems (e.g., teenagers without the Google, smart phone or social media, might feel themselves cognitively or socially handicapped).	MAYBE
Decentralized operation: the IoT control and governance cannot be centralized, because of the large number of hubs, switches, and data. The information flows will be eased, and the data transfers will be faster and cheaper, and thus not easily controllable. There will appear emerging properties and phenomena which will require monitoring and governance in an adequate way, and this will further influence the accountancy and control activities.	MAYBE
Property right on data and information: the difficulty in specifying the identification of things and humans is reflected to the difficulty to identify who is the owner of the data retrieved by IoT sensors and devices.	MAYBE
Omnipresence: this makes invisible the boundaries between public and private space. People cannot know where their information ends up.	MAYBE

Accessibility of data: an attack on a PC might cause information loss. A virus or hacker attack in the IoT might have serious effects on human life (e.g., on the life of the driver of a car connected to IoT).	MAYBE
Vulnerability: the list of possible vulnerabilities in IoT is scaring. It ranges from home appliances, to hospitals, traffic lights systems, food distribution networks, transportation systems, and so on.	MAYBE
Digital divide: the digital divide in the IoT is enlarged. IoT operations can be understood only by experts. Communication in IoT devices affects human lives in ways that are difficult to predict or imagine. The digital divide can only be reduced by proper coherent legal and democratic frames to delineate this process.	MAYBE

6.ETHICS QUESTIONS

6.1.Information technology ethics and Internet ethics.

What happens if the Internet connection breaks down?
Critical data must be buffered and synchronized later, when the connection is established.
Who is responsible or liable for patching IoT devices, routers, and cloud connections?
System provider / operator.
Is there an assurance that hacking on the cloud side of IoT services will not have access to a home's internal network?
There will be such assurance with implementation of Trusted Execution Environment.
What happens if an IoT service provider experiences downtime for critical life-supporting devices?
People may die. However, they might be already dead if no life-supporting devices were used.
What happens if an IoT device acts without the consent of its owner or acts in unintended ways (e.g., ordering the wrong products, or vacuuming at an unreasonable hour)?
Disaster / operational chaos would happen in such case.
What happens if an IoT product vendor goes out of business and no longer supports the product?
Most likely replacement of IoT device(s) by new vendor or systems provider.
Who owns the data collected by IoT devices?
It depends on the system. In some cases the data ownership can be public.
Are there cases where IoT devices should not be collecting data?
Yes, for instance our face recognition system (find missing person or terrorists) is not collecting data, only sends alerts when the missing or wanted person was detected.
What happens if the user wants to opt out?
No technical issue. User can opt out at any time.
What about those who do not have smart devices or the knowledge to use them? (Digital divide).
Those people simply won't benefit from digital world features.

6.2.Ethical principles

All activities involving the use of personal data are expected to comply with applicable data protection legislation. Beyond legal compliance, activities must respect ethical principles. Please try to assess whether the use case you lead/participate in complies with the following (definitely/future/probably/not) and comment if necessary:

In IoT activities, individuals should be treated as ends (not as means), and maintain their rights to property, autonomy, private life, and dignity.	Y
Individuals should not suffer physical or mental harm from IoT activities.	Y
Benefits from the application of IoT should be added to the common good.	Y
The necessity and proportionality of an IoT process should be taken into account and capable of being demonstrated.	Y
IoT applications should be performed with maximum transparency and accountability via explicit and auditable procedures.	Y
There should be equal access to the benefits of IoT accruing to individuals (social justice).	Y
IoT activities should have minimum negative impact to all facets of the natural environment.	Y
IoT activities should aim to lighten the adverse consequences that data processing may have on personal privacy and other personal and social values.	Y
Adverse effects beyond the individual (groups, communities, societies) should be avoided or minimized or mitigated.	Y

7.PRIVACY

The European Union General Data Protection Regulations (EU GDPR 2016, etc.) impose the principles that should underlie the processing of personal information. A new principle added to EU GDPR 2016 is the principle of "Privacy by Design".

Does your privacy framework include the following? (yes/no and if so specify)

Privacy regulations	YES
Data minimization	YES
Data portability	YES
Transparency	YES
Compliance disclosures	YES
IoT engagement by default	YES
IoT engagement by design	YES
Best practice	YES

The concepts of security and privacy have many complex interrelationships, but they are not identical. Do you have the following relations between security and privacy? (yes/no and comment if necessary)

Reductionism	
Projectionism	
Dualism	

6.2.Ethical principles

All activities involving the use of personal data are expected to comply with applicable data protection legislation. Beyond legal compliance, activities must respect ethical principles. Please try to assess whether the use case you lead/participate in complies with the following (definitely/future/probably/not) and comment if necessary:

In IoT activities, individuals should be treated as ends (not as means), and maintain their rights to property, autonomy, private life, and dignity.	Y

Dialectic	

8.TRUST

In general, trust can be looked-up from different views and interpretations. Does your trust framework provide the following? (yes/no and explain)

Trustworthiness	YES
Dependability	YES
Sustainability.	YES
Reliability.	YES
Availability.	YES
Resilience.	YES

8.2.Personal Data Principles

People own the data (or things) they create.	YES
People own the data someone creates about them.	YES
People have the right to access data gathered from public space.	YES
People have the right to their data in full resolution in real time.	YES, for basic data. More complex data may not be available in real time.
People have the right to access their data in a standard format.	YES
People have the right to delete or backup their data.	YES, unless critical data is correlated with others (e.g., payment history)
People have the right to use and share their data however they want	NO, only in specific ways

Please answer if the following apply in your legal context (yes/no and explain)

C.3. Pilot 3

During the course of task T2.3 (Legal and regulatory analysis and governance specification), several actions have been performed in order to identify the legal framework surrounding activities in Pilot 3. Germany, where the use case will take place, is aligned with all relevant European directives.

The content of this analysis, as it includes information protected by companies' policies, is not delivered in this document. Further analysis will take place later, where it will be evaluated a proper summary of data to be potentially provided in deliverable D2.3.

C.4. Pilot 4

C.4.1. EGCTL

Appendix C – Legal Framework Survey

1. REGULATORY BODIES & DATA PROTECTION AUTHORITIES

1.1. Which EU-level data protection regulators and data protection authorities are you or could you be connected with?

We do not connect directly to EU-wide regulatory bodies or data protection authorities.

1.2. Which national and local regulatory bodies are you or could you connect with?

- Deputy Ministry of Shipping https://www.dms.gov.cy/

  DMS is the regulatory authority for Port Security issues.

- Ministry of Energy, Commerce and Industry Ministry of Energy, Commerce and Industry (meci.gov.cy)

  MECI is the competent authority for all departments / entities that regulate Port operations. It is also the Grantor of the private terminal concession agreements, which is the agreement Eurogate operates under.

- Cyprus Ports Authority Home - CPA

  CPA is the competent authority that regulates the way ports and port terminals operate in Cyprus. It has a regulatory role in the implementation of all legislation in Cyprus ports. It is also the Security authority for all Ports.

- Digital Security Authority Digital Security Authority - Αρχική (dsa.cy)

  According to Law 89(I)/2020 on Network and Information Systems Security, DSA has the following responsibilities (Article 17):

  - advise the Minister on issues relating to the security of networks and information systems, digital security and cybersecurity in the Republic;
  - implement, in matters of security of networks and information systems, the general policy framework to be followed in accordance with the provisions of subsection (2) of Article 16;
  - be a national single point of contact for the security of networks and information systems (hereinafter referred to as the 'single point of contact');
  - exercise, as a single point of contact, liaison functions to ensure cross-border cooperation with the competent authorities of the other Member States, the competent authorities of the Republic, the Cooperation Group and the CSIRTs network, as provided for in the provisions of Article 33; [...more here]

- Office of the Commissioner for Personal Data Protection / Ministry of Internal Affairs Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (dataprotection.gov.cy)

  - The Commissioner for personal data protection is an independent public authority responsible for monitoring the implementation of Regulation (EU) 2016/679 (GDPR) and other laws aiming at the protection of individuals with regards to the processing of their personal data.
  - The Commissioner performs the duties and exercises the powers assigned by the GDPR or any other relevant law in complete independence.
  - The Commissioner represents the Republic of Cyprus in the relevant bodies and committees of the European Union, the Council of Europe, and other International Organisations. Among other things, the Commissioner participates in the European Data Protection Board, which is composed of all Supervisory Authorities of EU Member States and the European Data Protection Supervisor, as well as by the European Commission.

- Office of the Commissioner of Electronic Communications & Postal Regulation ΓΕΡΗΕΤ|OCECPR (ee.cy)

  OCECPR is responsible for the application of the harmonised framework for the regulation of electronic communications networks, electronic communications services, associated facilities and associated services, and certain aspects of terminal equipment, which was transposed through the National Law N. 24(I)/2022. The applicability of the current regulatory framework depends on whether the respective service in the IoT value chain is qualified as an Electronic Communication Service. Electronic communications service' means a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services:

  - internet access service' as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;
  - interpersonal communications service; and
  - services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting

- Department of Customs and Excise CUSTOMS & EXCISE - Welcome to our Website (mof.gov.cy)

  "In general terms our department is responsible mainly for the imposition and collection of duties and taxes on goods, the safeguarding of the supply chain of goods, the enforcement of restrictions and prohibitions on goods imported, exported or in transit the facilitation of legitimate trade and support of business activities' development and the protection of the consumers health and safety."

- Deputy Ministry of Research, Innovation and Digital Policy Deputy Ministry of Research, Innovation and Digital Policy | Deputy Ministry of Research, Innovation and Digital Policy (dmrid.gov.cy)

  Functions

  - To develop and implement a national digital policy and strategy and to participate in forming a suitable regulatory framework, at European and international level, for the development of digital policy
  - To develop, coordinate and implement the national strategy for research and innovation and to supervise the operation of the National Governance System for Research and Innovation
  - To specialise and implement policies in Information and Communication Technologies and e-government in the public service
  - To design and coordinate the implementation of a national broadband plan
  - Political guidance and supervision of the Research and Innovation Foundation To develop and implement a national digital policy and strategy and to participate in forming a suitable regulatory framework, at European and international level, for the development of digital policy
  - To develop, coordinate and implement the national strategy for research and innovation and to supervise the operation of the National Governance System for Research and Innovation
  - To specialise and implement policies in Information and Communication Technologies and e-government in the public service
  - To design and coordinate the implementation of a national broadband plan
  - Political guidance and supervision of the Research and Innovation Foundation

- Research and Innovation Foundation HORIZON 2020 – ΙδΕΚ (research.org.cy)

  The coordination of the activities for the participation of Cyprus in the Horizon 2020 has been assigned to RIF.

1.3. Do you have any conflict of interest with those regulatory bodies?

Many of these are regulatory authorities that regulate our operations. However, there should be no conflict.

2. EUROPEAN UNION FRAMEWORK

2.1. Have your government or local regulations incorporated the following?

(Answer YES/NO and comment if necessary)

Directive (EU) 2019/1024: open data and the re-use of public sector information.	Law 143(I)/2021
Directive (EU) 2018/1972: establishing the European Electronic Communications Code.	Law N 22(I)/2022
EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns "Cybersecurity" issues.	Law N 89(I)/2020 (latest amendment)
EU DPR-2012: European Data Protection Regulation	Replaced by EU GDPR
EU Directive-2013/40: this Directive deals with "Cybercrime" (i.e., attacks against information systems).	Yes
EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns "Cybersecurity" issues.	Yes
EU Directive 2014/53: this directive is concerned with the standardization issue which is important for the joint and harmonized development of technology in the EU.	Yes
EU GDPR: European General Data Protection Regulation-2016	Yes
EU Connected Communities Initiative: This initiative concerns the IoT development infrastructure, and aims to collect information from the market about existing public and private connectivity projects that seek to provide high speed broadband, more than 30 Mbps.	No

3. REGULATIONS

The national legal and ethical framework should cover the following. Please answer YES/NO if your framework does.

Legislation/regulations.	Yes
Ethics principles, rules and codes.	When it comes to ethics principles, rules and codes relating to IoT, the answer is NO.
Standards/guidelines.	Yes
Contractual arrangements.	Yes
Regulations for the devices connected.	No
Regulations for the networks and their security.	Yes
Regulations for the data associated with the devices	Yes

4. GOVERNMENT REGULATIONS

Governments play a primary role in shaping the future because governments have a dual role, namely

1. User role: governments plan to become major users of IoT, e.g., getting smart cities.
2. Infrastructure provider role: governments should issue regulations for devices not originally intended for connection to the IoT, as well as for devices particularly designed to be connected devices.

4.1. Which of the above is the role of your government?

No available data

4.2. Do your government have in force regulations for both roles?

No

4.3. What are these regulations (regarding IoT)?

There are no implemented regulations but there is a proposal for implementing them.

Cyber Resilience Act

The proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, bolsters cybersecurity rules to ensure more secure hardware and software products.

Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of €5.5 trillion by 2021.

Such products suffer from two major problems adding costs for users and the society:

1. a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and

2. an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

While existing internal market legislation applies to certain products with digital elements, most of the hardware and software products are currently not covered by any EU legislation tackling their cybersecurity. In particular, the current EU legal framework does not address the cybersecurity of non-embedded software, even if cybersecurity attacks increasingly target vulnerabilities in these products, causing significant societal and economic costs.

Two main objectives were identified aiming to ensure the proper functioning of the internal market:

1. create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle; and

2. create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

Four specific objectives were set out:

1. ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle;
2. ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers;
3. enhance the transparency of security properties of products with digital elements, and
4. enable businesses and consumers to use products with digital elements securely.

4.4. Do your government ensure that IoT products and solutions are used exclusively for their specified goal?

Not applicable for the private sector yet, hence the lack of legislation.

4.5. Which sectors of society, industry and the economy are subject to general government legislation?

Almost all sectors of society, industry and the economy are subject to general government legislation. The list is too long to be set out here and would not be exhaustive.

4.6. Does the relevant legislation include the following fields (yes/no and define if possible):

public law	YES
business law	YES
insurance law	YES
tax law	YES
private international/human rights law	YES
security law	YES
criminal law	YES
civil liability law	YES
consumer protection law	YES

IoT activities should have minimum negative impact to all facets of the natural environment.	maybe
IoT activities should aim to lighten the adverse consequences that data processing may have on personal privacy and other personal and social values.	maybe
Adverse effects beyond the individual (groups, communities, societies) should be avoided or minimized or mitigated.	definitely

7. PRIVACY

The European Union General Data Protection Regulations (EU GDPR 2016, etc.) impose the principles that should underlie the processing of personal information. A new principle added to EU GDPR 2016 is the principle of "Privacy by Design".

Do your privacy framework include the following? (yes/no and if yes define)

Privacy regulations	
Data minimization	
Data portability	
Transparency	
Compliance disclosures	
IoT engagement by default	
IoT engagement by design	
Best practice	

The concepts of security and privacy have many complex interrelationships, but they are not identical. Do you have the following relations between security and privacy? (yes/no and comment if necessary)

Reductionism	
Projectionism	
Dualism	
Dialectic	

8. TRUST

In general, trust can be looked-up from different views and interpretations. Does your trust framework provide the following? (yes/no and explain)

Trustworthiness	
Dependability	
Sustainability.	
Reliability.	
Availability.	
Resilience.	

8.1. Personal Data Principles

People own the data (or things) they create.	No. There is no provision in the applicable legislative framework concerning personal data protection that refers to personal data as being "created" or indeed being the subject of "ownership". Recital 7 of the General Data Protection Regulation 768/2016 (**"GDPR"**) merely refers to natural persons having the right to control their personal data.
People own the data someone creates about them.	No. There is no provision in the applicable legislative framework concerning personal data protection that refers to personal data as being created or being

private/data protection law	YES
environmental law	YES
GDPR law	YES

4.7. Do government regulations focus on the system capabilities (e.g., how data can be reused or sold) rather than on implementation (e.g., MySQL vs. Hadoop)?

No available data.

5. Characteristics that May Cause Ethical Problems

The main IoT characteristics that may cause ethical problems are the following. Please try to identify the risk of having to deal with some of these (using YES/NO/maybe) in the Use Case you participate in.

Ubiquity/omnipresence: the IoT is everywhere.	Yes
Miniaturization/invisibility: computers and devices will be smaller and smaller, and transparent, thus avoiding any inspections, audit, quality control, and accounting procedures.	Yes
Ambiguity: the distinction between the natural objects, artifacts, and beings will be more and more difficult to be made, because the transformation from one category to another is easy, based on tags.	No
Difficult identification: objects/things have an identity in order to be connected to the IoT. The access to these objects and the management of their identities might cause crucial problems of security and control in the IoT ecological world.	Yes
Ultra-connectivity: the huge number of connections of objects and people require the transfer of large quantities of data (big data) which could be maliciously used.	Yes
Autonomous and unpredictable behaviour: the interconnected objects might interfere autonomously and spontaneously in human activities in unexpected ways for the users or designers. People, artifacts, and devices will belong to the same IoT environment, thus creating hybrid systems with unpredictable behaviour. The incremental development of IoT will lead to emerging behaviours that the users could not fully understand.	Yes
Incorporated intelligence: this will make the objects as substitutes of social life. The intelligent objects will be dynamic with an emergent behaviour. Being deprived of these devices will lead to problems (e.g., teenagers without the Google, smart phone or social media, might feel themselves cognitively or socially handicapped).	No
Decentralized operation: the IoT control and governance cannot be centralized, because of the large number of hubs, switches, and data. The information flows will be eased, and the data transfers will be faster and cheaper, and thus not easily controllable. There will appear emerging properties and phenomena which will require monitoring and governance in an adequate way, and this will further influence the accountancy and control activities.	Yes
Property right on data and information: the difficulty in specifying the identification of things and humans is reflected to the difficulty to identify who is the owner of the data retrieved by IoT sensors and devices.	No
Omnipresence: this makes invisible the boundaries between public and private space. People cannot know where their information ends up.	No
Accessibility of data: an attack on a PC might cause information loss. A virus or hacker attack in the IoT might have serious effects on human life (e.g., on the life of the driver of a car connected to IoT).	Yes
Vulnerability: the list of possible vulnerabilities in IoT is scaring. It ranges from home appliances, to hospitals, traffic lights systems, food distribution networks, transportation systems, and so on.	Yes
Digital divide: the digital divide in the IoT is enlarged. IoT operations can be understood only by experts. Communication in IoT devices affects human lives in ways that are difficult to predict or imagine. The digital divide can only be reduced by proper coherent legal and democratic frames to delineate this process.	Maybe

6. ETHICS QUESTIONS

6.1. Information technology ethics and Internet ethics.

What happens if the Internet connection breaks down?
Local Network: Operations will be heavily affected as all terminal operations are dependent on the internal network. Cloud: Some operations will be affected or slowed down as connectivity to edge devices relies on the 4G network. Operations will switch to manual / verbal mode which will cause a significant delay.
Who is responsible or liable for patching IoT devices, routers, and cloud connections?
Internal network is maintained by Eurogate staff and 3rd party contractors. Cloud services are maintained by 3rd party contractors (i.e. service providers and communication providers).
Is there an assurance that hacking on the cloud side of IoT services will not have access to a home's internal network?
Yes. Our internal network is behind a firewall.
What happens if an IoT service provider experiences downtime for critical life-supporting devices?
We do not utilize IoT services providers (only communication providers), and they do not service life-supporting devices.
What happens if an IoT device acts without the consent of its owner or acts in unintended ways (e.g., ordering the wrong products, or vacuuming at an unreasonable hour)?
An accident could occur.
What happens if an IoT product vendor goes out of business and no longer supports the product?
Service/replacement could be made difficult and in the end a replacement would be required.
Who owns the data collected by IoT devices?
Eurogate does. If there are personal data involved, then the user is also the owner.
Are there cases where IoT devices should not be collecting data?
No
What happens if the user wants to opt out?
He can contact the companies' DPO to request so, only in the cases this is applicable. From our experience, there is no procedure in Eurogate where opting-out in the collection of personal data would be practicable.
What about those who do not have smart devices or the knowledge to use them? (Digital divide).
No data is collected through personal devices although some non-critical services to employees are provided through their smart devices. The company has not designed a plan to address this issue yet.

6.2. Ethical principles

All activities involving the use of personal data are expected to comply with applicable data protection legislation. Beyond legal compliance, activities must respect the ethical principles. Please try to assess whether the use case you lead/participate in complies with the following (definitely/future/probably/not) and comment if necessary:

In IoT activities, individuals should be treated as ends (not as means), and maintain their rights to property, autonomy, private life, and dignity.	definitely
Individuals should not suffer physical or mental harm from IoT activities.	definitely
Benefits from the application of IoT should be added to the common good.	definitely
The necessity and proportionality of an IoT process should be taken into account and capable of being demonstrated.	
IoT applications should be performed with maximum transparency and accountability via explicit and auditable procedures.	definitely
There should be equal access to the benefits of IoT accruing to individuals (social justice).	probably not

	the subject of "ownership". Recital 7 of the GDPR merely refers to natural persons having the right to control their personal data.
People have the right to access data gathered from public space.	In certain cases yes, however, this right, is not absolute. S.30 of the Protection of Natural Persons Against the Processing of Personal Data and the Free Transmission of Such Data 125(I)/2018 stipulates that personal data appearing in official documents which are held by a public authority or agency for the performance of a duty in the public interest must be revealed, save for certain categories of information which are expressly exempt pursuant to the provisions of the Right to Access Information in the Public Sector Law (184(I)/2017.
People have the right to their data in full resolution in real time.	Data subjects have the right to access their data subject to restrictions provided pursuant to the provisions of the GDPR – however other than the obligation to provide data in an accessible, concise and intelligible format, the GDPR does not expressly refer to the timing and manner in which personal data shall be made available.
People have the right to access their data in a standard format.	Yes, subject to any restrictions provided pursuant to the provisions of the GDPR. Data subjects have the right to access and receive a copy of their personal data, and other supplementary information. The information must be provided in an accessible, concise and intelligible format.
People have the right to delete or backup their data.	Right to Delete Data – Yes, data subject may make a request to have their personal data erased, but again this right is not absolute and is subject to certain restrictions provided pursuant to the provisions of the GDPR. Right to backup data – the GDPR contains no express provision which relates to the right to backup data. However, a data subject may request the removal of data from backups.
People have the right to use and share their data however they want	There is no reference in the GDPR to the right of data subjects to "use" and "share" data. However, one of the core objectives of the GDPR is to afford data subjects a great degree of control over the use of their data.

Please answer if the following apply in your legal context (yes/no and explain)

C.5. Pilot 5

C.5.1. Cosmote

Appendix C – Legal Framework Survey

1. REGULATORY BODIES & DATA PROTECTION AUTHORITIES

1.1. Which EU-level data protection regulators and data protection authorities are you or could you be connected with?

None

1.2. Which national and local regulatory bodies are you or could you connect with?

- The HDPA(**Hellenic Data Protection Authority**), a constitutionally consolidated independent authority, serves as the watchdog of the personal data and privacy of individuals in accordance with the provisions of Law 4624/2019 and Law 3471/2006. An additional mission of the HDPA is the support and guidance to Controllers in their compliance with the obligations set by the law.
- The EETT (Hellenic Telecommunications and Post Commission), an independent authority granted with specific rights under the Hellenic Constitution, acts as the national regulator of the telecommunications and postal market. It was established in 1992 by virtue of Law 2075/1992; however, several new laws and amendments have expanded its competence. The Laws in force are 4070/2012 (for electronic communications), 4053/2012 (for postal services market and electronic communication matters) and 4727/2020 (for Digital Governance).
- The **ADAE (Hellenic Authority for Communication Security and Privacy)** has been established under Law 3115/2003 and Art. 19 par. 2 of the Hellenic Constitution, having, inter alia, the competence to: issue regulations regarding the assurance of the confidentiality of communications; perform audits on communications network/service providers, public entities as well the Hellenic National Intelligence Service; and hold hearings of the aforementioned entities, to investigate relevant complaints from members of the public and to collect relevant information using special investigative powers.
- The National Cyber Security Authority – Ministry of Digital Governance (NCSA) , as designated by Law 4577/2018 implementing the NIS Directive, consists of the **Directorate of Cyber Security** of the **General Secretariat of the Ministry of Digital Policy, Telecommunications and Media** (as established by Art. 15 of Decree 82/2017 and amended by Art. 50 of Law 4635/2019 and Ministerial Decision No. 1027/2019). The HCA monitors, inter alia, the implementation of the NIS Directive, cooperates with the Hellenic CSIRT and is designated as the single point of contact to ensure cross-border cooperation with competent authorities of other EU Member States. Moreover, Art. 36 of the Law 4961/2022 about "Emerging information and communication technologies, strengthening digital governance and other provisions" as published in 27/07/2022 states that the HCA, in cooperation with the relevant response team: (a) verifies the compliance of manufacturers, importers, distributors and IoT operators with the obligations under Arts 32-35, as applicable, par. 3 and 4 of Art. 34, and par. 3 and 4 of Art. 34, except in the cases referred to in par. 3 and 4 of Art. 34, and par. 4 of Art. 35, and may request any other necessary information from the persons and bodies referred to in the first subparagraph; (b) assesses the conformity of the IoT technology devices used by IoT operators with the technical specifications of the ministerial decision referred to in para. (a), 12a of Art. 113; (c) assesses the compliance with the adequacy of the measures taken by IoT operators to prevent and mitigate the impact of incidents affecting the security of the devices; and (d) receives notifications from IoT operators concerning the occurrence of incidents or vulnerabilities. If, following the audit or assessment referred to in par.1, the HCA finds non-compliance, it shall require the manufacturer, importer or distributor of the apparatus to take all necessary corrective actions to achieve compliance and shall inform the operator to whom the apparatus has been made available. The body shall, upon receipt of the information, take all necessary corrective measures, which may include suspension of the use of the apparatus.

1.3. Do you have any conflict of interest with those regulatory bodies?

No

2. EUROPEAN UNION FRAMEWORK

2.1. Have your government or local regulations incorporated the following?

Directive (EU) 2019/1024: open data and the re-use of public sector information.	Yes, Law 4727/2020 regarding Digital Governance-Electronic Communications.
Directive (EU) 2018/1972: establishing the European Electronic Communications Code.	
EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns "Cybersecurity" issues.	
EU DPR-2012: European Data Protection Regulation	Yes, replaced by GDPR.
EU Directive-2013/40: this Directive deals with "Cybercrime" (i.e., attacks against information systems).	Yes-Greek Law 4411/2016
EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns "Cybersecurity" issues.	Yes – Greek Law 4577/2018 HCA (Hellenic Cyber Security Authority) of the Ministry of Digital Governance
EU Directive 2014/53: this directive is concerned with the standardization issue which is important for the joint and harmonized development of technology in the EU.	YES According to Law 4070/2012*, article 12, as amended by the Law 4313/2014* article 60: radio equipment issues are regulated by the **Presidential Decree 98/2017*** (Official Gazette 139/A/20-09-2017) "Harmonisation of the Greek legislation to the DIRECTIVE 2014/53/EC of the European Parliament and the Council of April 16th, 2014 (EE L 153/22.05.2014), regarding to the making radio equipment available on the market and the repealing of DIRECTIVE 99/5/EC*.
EU GDPR: European General Data Protection Regulation-2016	YES – Greek Law 4624/2019
EU Connected Communities Initiative: This initiative concerns the IoT development infrastructure, and aims to collect information from the market about existing public and private connectivity projects that seek to provide high speed broadband, more than 30 Mbps.	

3. REGULATIONS

The national legal and ethical framework should cover the following. Please answer YES/NO if your framework does.

Legislation/regulations.	Yes
Ethics principles, rules and codes.	Yes
Standards/guidelines.	Yes
Contractual arrangements.	Yes
Regulations for the devices connected.	Yes
Regulations for the networks and their security.	Yes
Regulations for the data associated with the devices	Yes

4. GOVERNMENT REGULATIONS

Governments play a primary role in shaping the future because governments have a dual role, namely

1. User role: governments plan to become major users of IoT, e.g., getting smart cities.
2. Infrastructure provider role: governments need to issue regulations for devices that were not originally intended to be connected to IoT, as well as for devices that are specifically designed to be connected devices.

4.1. Which of the above is the role of your government?

Both

4.2. Do your government have in force regulations for both roles?

Law 4961/2022

4.3. What are these regulations?

The Law 4961/2022 is the Greek legal framework and constitutes a primary, but high level endeavor in view of the forthcoming and more detailed EU legislation on new technologies, including artificial intelligence ('AI'), the Internet of Things ('IoT'), Blockchain and Distributed Ledger Technology ('DLT'), smart contracts, as well as 3D printing.

The new Law defines IoT as 'any technology which: (a) allows devices or a group of interconnected or interrelated devices to perform, through their connection to the Internet, based on a software, automatic processing of digital data, including the technology relating to the interconnection of physical objects, in particular devices, vehicles and buildings, with electronic components, software, sensors, actuators, radio links and network connections; and (b) allows the collection and exchange of digital data to provide a variety of services to users, with or without human intervention'.

4.4. Do your government ensure that IoT products and solutions are used exclusively for their specified goal?

No

4.5. Which sectors of society, industry and the economy are subject to general government legislation?

The new law focuses on IoT and cybersecurity. In order to ensure an increased level of cybersecurity during the life cycle of devices using IoT technology, all actors involved, including manufacturers, importers and distributors, as well as operators of IoT devices, need to comply with a series of security safeguards and monitoring obligations preventing unauthorized third parties from tampering with the use of or their performance. IoT devices must be accompanied with a compliance declaration issued by the manufacturer and instructions regarding the safe installation, configuration and operation according to the intended use of IoT device together with a list of potential risks. Further technical specifications will be introduced by virtue of Ministerial Decisions to be issued on these matters.

4.6. Does the relevant legislation include the following fields (yes/no and define if possible):

public law	Yes	Law 4961/2022
business law	No	No explicit reference is found
insurance law	No	No explicit reference is found
tax law	No	No explicit reference is found
private international/human rights law	Yes	GDPR regulations
security law	Yes	Law 4961/2022
criminal law	No	No explicit reference is found
civil liability law	No	No explicit reference is found
consumer protection law	No	No explicit reference is found
private/data protection law	Yes	as part of the GDPR regulations
environmental law	No	No explicit reference is found
GDPR law	Yes	GDPR regulations

4.7. Do government regulations focus on the system capabilities (e.g., how data can be reused or sold) rather than on implementation (e.g., MySQL vs. Hadoop)?

No reference to this.

5. CHARACTERISTICS THAT MAY CAUSE ETHICAL PROBLEMS

The main IoT characteristics that may cause ethical problems are the following. Please try to identify the risk of having to deal with some of these (using YES/NO/maybe) in the Use Case you participate in.

Ubiquity/omnipresence: the IoT is everywhere.	Yes
Miniaturization/invisibility: computers and devices will be smaller and smaller, and transparent, thus avoiding any inspections, audit, quality control, and accounting procedures.	No
Ambiguity: the distinction between the natural objects, artifacts, and beings will be more and more difficult to be made, because the transformation from one category to another is easy, based on tags.	No
Difficult identification: objects/things have an identity in order to be connected to the IoT. The access to these objects and the management of their identities might cause crucial problems of security and control in the IoT ecological world.	Yes
Ultra-connectivity: the huge number of connections of objects and people require the transfer of large quantities of data (big data) which could be maliciously used.	No
Autonomous and unpredictable behaviour: the interconnected objects might interfere autonomously and spontaneously in human activities in unexpected ways for the users or designers. People, artifacts, and devices will belong to the same IoT environment, thus creating hybrid systems with unpredictable behaviour. The incremental development of IoT will lead to emerging behaviours that the users could not fully understand.	No
Incorporated intelligence: this will make the objects as substitutes of social life. The intelligent objects will be dynamic with an emergent behaviour. Being deprived of these devices will lead to problems (e.g., teenagers without the Google, smart phone or social media, might feel themselves cognitively or socially handicapped).	No
Decentralized operation: the IoT control and governance cannot be centralized, because of the large number of hubs, switches, and data. The information flows will be eased, and the data transfers will be faster and cheaper, and thus not easily controllable. There will appear emerging properties and phenomena which will require monitoring and governance in an adequate way, and this will further influence the accountancy and control activities.	Yes
Property right on data and information: the difficulty in specifying the identification of things and humans is reflected to the difficulty to identify who is the owner of the data retrieved by IoT sensors and devices.	Yes
Omnipresence: this makes invisible the boundaries between public and private space. People cannot know where their information ends up.	No
Accessibility of data: an attack on a PC might cause information loss. A virus or hacker attack in the IoT might have serious effects on human life (e.g., on the life of the driver of a car connected to IoT).	No
Vulnerability: the list of possible vulnerabilities in IoT is scaring. It ranges from home appliances, to hospitals, traffic lights systems, food distribution networks, transportation systems, and so on.	No
Digital divide: the digital divide in the IoT is enlarged. IoT operations can be understood only by experts. Communication in IoT devices affects human lives in ways that are difficult to predict or	Yes

imagine. The digital divide can only be reduced by proper coherent legal and democratic frames to delineate this process.	

6. ETHICS QUESTIONS

6.1. Information technology ethics and Internet ethics.

What happens if the Internet connection breaks down?
The UC is supposed to operate in a decentralised manner, internet connection is necessary for the federation alignment purposes and user's notification if outside the short-range reach. The appropriate monitoring and error control mechanisms will take upon the definition of the error control procedure.
Who is responsible or liable for patching IoT devices, routers, and cloud connections?
The IoT system operator
Is there an assurance that hacking on the cloud side of IoT services will not have access to a home's internal network?
The pilot builds secure communication through VPNs in all interactions of the IOT front-end and back-end communication.
What happens if an IoT service provider experiences downtime for critical life-supporting devices?
There is no critical life-supporting device in our UC
What happens if an IoT device acts without the consent of its owner or acts in unintended ways (e.g., ordering the wrong products, or vacuuming at an unreasonable hour)?
Not Allowed in our UC
What happens if an IoT product vendor goes out of business and no longer supports the product?
Will be replaced with other devices with similar capabilities – this is inherent part of the aerOS meta-os capabilities to integrate various devices
Who owns the data collected by IoT devices?
the customer where the UC is deployed - COSMOTE
Are there cases where IoT devices should not be collecting data?
No
What happens if the user wants to opt out?
User's collaboration will be ensured as part of the consent forms. In all cases, data is collected cumulatively and id anonymised.
What about those who do not have smart devices or the knowledge to use them? (Digital divide).
The UC will consider alternative options for all cases as need be

6.2. Ethical principles

All activities involving the use of personal data are expected to comply with applicable data protection legislation. Beyond legal compliance, activities must respect ethical principles. Please try to assess whether the use case you lead/participate in complies with the following (definitely/future/probably/not) and comment if necessary:

In IoT activities, individuals should be treated as ends (not as means), and maintain their rights to property, autonomy, private life, and dignity.	Yes
Individuals should not suffer physical or mental harm from IoT activities.	Yes
Benefits from the application of IoT should be added to the common good.	Yes
The necessity and proportionality of an IoT process should be taken into account and capable of being demonstrated.	Yes
IoT applications should be performed with maximum transparency and accountability via explicit and auditable procedures.	Yes
There should be equal access to the benefits of IoT accruing to individuals (social justice).	Yes
IoT activities should have minimum negative impact to all facets of the natural environment.	Yes
IoT activities should aim to lighten the adverse consequences that data processing may have on personal privacy and other personal and social values.	Yes
Adverse effects beyond the individual (groups, communities, societies) should be avoided or minimized or mitigated.	Yes

7. PRIVACY

The EU General Data Protection Regulations (EU GDPR 2016 etc.) impose the principles that must underlie the processing of personal information. A new principle added to the 2016 EU GDPR is the principle of "Privacy by Design".

Does your privacy framework include the following? (yes/no and if so specify)

Privacy regulations	Yes
Data minimization	Yes
Data portability	Yes
Transparency	Yes
Compliance disclosures	Yes
IoT engagement by default	Yes
IoT engagement by design	Yes
Best practice	Yes

The concepts of security and privacy have many complex interrelationships, but they are not identical. Do you have the following relations between security and privacy? (yes/no and comment if necessary)

Reductionism	??
Projectionism	??
Dualism	??
Dialectic	??

8. TRUST

In general, trust can be looked-up from different views and interpretations. Does your trust framework provide the following? (yes/no and explain)

Trustworthiness	Yes
Dependability	Yes
Sustainability.	Yes
Reliability.	Yes
Availability.	Yes
Resilience.	Yes

8.1. Personal Data Principles

People own the data (or things) they create.	Depends on the data – for example aggregated or anonymized data are not owned by users. Raw data that can be directly related to a user belong to the user.
People own the data someone creates about them.	Depends on the data.
People have the right to access data gathered from public space.	Yes
People have the right to their data in full resolution in real time.	Yes
People have the right to access their data in a standard format.	Yes
People have the right to delete or backup their data.	Yes
People have the right to use and share their data however they want	Yes

Please answer if the following apply in your national legal context (yes/no and explain)

9. ADDITIONAL QUESTIONS (OPTIONAL)

Europe 2020 "Innovation Europe" Initiative, which involves several actions towards achieving the following three goals. What is the state of these goals in your country?

Make Europe one of the world-class science performers.	Greece 2.0 2022-2024 RRF Programme
Free the innovation from obstacles such as expensive patenting, market fragmentation, and skills shortages.	
Revolutionize the way public and private sectors cooperate (e.g., via innovation), and enhance partnerships between European institutions, authorities (national and regional), and business.	Greece 2.0 2022-2024 RRF Programme

Does the existing framework regarding the protection of users is influenced by the following socio-legal-economic aspects and related issues? (yes/no and if yes define)

The trade-off between the market needs for data and correlation to support innovation, and the business success of the IoT systems and applications (public and private).	Yes
The cost of verifying and implementing privacy enhancing technologies (PET) or other solutions for ensuring appropriate care in collection, storage, and retrieval of data.	Yes
The accountability of IoT applications related to users' privacy.	Yes
Support for the context where the user operates.	Yes