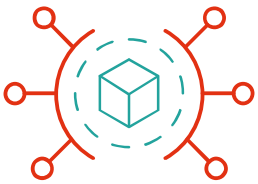


New ICT infrastructure and reference architecture to support Operations in future PI Logistics NETworks

D1.6 Requirements and High Level Specifications for IoT-based Smart PI Containers

Document Summary Information

Grant Agreement No	769119	**Acronym**	ICONET
Full Title	New **IC**T infrastructure and reference architecture to support **O**perations in future PI Logistics **NET**works		
Start Date	01/09/2018	**Duration**	30 months
Project URL	https://www.iconetproject.eu/		
Deliverable	D1.6 Requirements and High Level Specifications for IoT-based Smart PI Containers		
Work Package	WP1		
Contractual due date	M8	**Actual submission date**	18-June-2020
Nature	Report	**Dissemination Level**	Public
Lead Beneficiary	New Generation Sensors (NGS)		
Responsible Author	Claudio Salvadori (NGS)		
Contributions from	Stefano Bocchino (NGS), Phuong Viet Dao (NGS), Ilias Seitanidis (NGS) Francesco Marino (CNIT), Piero Castoldi (CNIT)		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 769119.

Disclaimer

Copyright message

Table of Contents

List of Figures

List of Tables

Glossary of terms and abbreviations used

Abbreviation / Term	Description
"-"	All the words written in quotes, represent DI concepts exploited in the PI scenario
BLE	Bluetooth Low Energy
CRC	Cyclic Redundancy Check
DI	Digital Internet
ETA	Estimated Time of Arrival
GSMA	Global System for Mobile Communications - industry organisation that represents the interests of mobile network operators worldwide
IoT	Internet of Things
IPv6	Internet Protocol version 6 is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.
LL	Living Lab
LP-WAN	Low Power Wide Area Network
OBU	On board unit
OCR	Optical Character Recognition
PI	Physical Internet
PoA	Port of Antwerp
PoR	Port of Rotterdam
SC	Smart Container
SC	Supply chain
SPP	Smart Physical Packet

1 Executive Summary

The main goal of this deliverable is to formalise the requirements and high-level specifications for IoT-based Smart PI Containers, based on in-depth analysis of user requirements and industry needs. This is also supported by an innovative and interoperable IoT architecture built to facilitate end-to-end tracking and monitoring of the goods throughout the logistics chain. The present report also considers and highlights the contribution of versatile IoT components as part of a Physical Internet configuration, designed and developed within the project lifetime.

To reach the objectives described in Section 1.1, thorough analysis of the state-of-the-art of currently available in the market IoT protocols and products has been executed, with special focus on interoperability concerns raised in several flagship Horizon 2020 projects. This analysis allowed us to pinpoint the most promising approaches in terms of interoperability design patterns, integration standardisation and communication protocols.

Thus, following thorough analysis of a wide range of current and future business requirements on logistics and through the PI prism, a set of requirements has been elicited to formalise the architecture of an IoT-enabled PI environment. The proposed architecture envisions a ubiquitous IoT environment, capable to monitor the status of "PI packets" in a geo & time-referenced manner, providing to all the logistics actors (e.g., senders, receivers, hauliers, …) secure, accurate and timely reports on the transported goods thus allowing optimised planning and resource utilisation. In the project context, the central building block of the PI Architecture is the Smart Container, a container enabling continuous monitoring.

In further detail, the deliverable, addresses the following key objectives:

1. Position the needs of PI in the IoT world, analysing how to engage state-of-the-art solutions to resolve the logistics and supply chain concerns,
2. Elicit a generic set of specifications capable to depict the required IoT architecture to support the realisation of the PI,
3. Identify the expected contribution of the IoT components within the PI/ICONET context,
4. Elaborate technological and business innovations generated by the integration of the mentioned IoT components in the PI environment.

Concluding the report lays out the specific IoT technological characteristics and how these can support solutions to the Logistics Industry requirements as identified in today's business environment and thus provide a stepping stone to the overall objective of showcasing the value-adding nature of the Physical Internet concept.

2 Introduction

The Physical Internet (PI) is a boundary spanning field of research, which aims to optimize logistics processes and enable effective and sustainable supply chains by applying the concepts of the Digital Internet (DI) to the physical world. The idea behind the PI is to connect and synchronize all logistics networks to create a collaborative physical network of networks, capable of autonomously optimizing the shipment of encapsulated goods of several types and sizes in compliance with different Quality-of-Service (QoS) requirements by means of routing protocols, tracking mechanisms and interoperability standards.

Though the lessons learned from the DI can guide the development of an efficient global logistic network, the PI is inherently different from the DI because of the nature of the transported items, which are physical objects in the first case and digital information in the second. Nevertheless, the PI will reach a level of pervasiveness and complexity that only a massive exploitation of the Information and Communication Technologies will allow to manage. In particular, the Internet of Things (IoT) paradigm is expected to play a crucial role in filling the gap between the physical and the digital realms, strictly coupling them. In fact, IoT can provide the necessary technological layer to create digital twins of physical logistics flows, which can be operated by resorting to well-known and widespread DI concepts and technologies. In this report, we are going to investigate the role that IoT can play in the design of hyper-connected and interoperable IoT environment, trying to define, in one hand, the issues it can solve, in the other, the technological specifications to tailor it for the PI and logistics world. The report will also address the needs and requirements of Logistics actors of today and how IoT within PI can satisfy these needs in a spectrum of activities and interconnected processes and interests.

The report will address and cover the requirements of Task T1.4 ‘User requirements and system specifications for IoT-based smart container support’ of work package 1 of the project.

2.1 Deliverable Overview and Report Structure

The deliverable will be structured following a “bottom-up” methodology, starting from the analysis of:

1. The *innovative and interoperable IoT interfaces* implemented in the flagship Horizon 2020 projects and standardised by the main entities.
2. The *available IoT protocols*, with a special attention to their power consumption. In fact, the missing of a power supply during the logistics transactions has to be taken into account, to maintain continuously connected the monitored environments.
3. The *market ready IoT solutions* for logistics and supply chain.

It will continue eliciting user and business requirements toward the realisation of a generic IoT-enable PI environment, thus defining an envisioned and ambitious IoT architecture. Finally, the high level technical specifications are detailed. Particularly, this deliverable is organized as followed:

- In **Sec. 3 - Requirements’ elicitation methodology**, the requirements’ elicitation methodology is defined. Moreover, the recipients of this document are identified, to understand the directions to be followed and provide an overall direction of the report
- In **Sec. 4 - Key drivers and Business requirements**, the key drivers coming from the document’s recipients toward the implementation of a hyperconnected PI-environment are listed and described, highlighting the business requirements from the logistics operators, the technology needs from ICT companies interested on exploiting the new business models generated by the PI, and the authorities and policy making imperatives to rule the supply chain and transports world.
- In **Sec. 5 - State of the Art**, the state of the art of the interoperable IoT interfaces and of the market-ready IoT solutions for logistics are described. The analysis is based on conditions prevailing at the time of writing the first version of the report.
- In **Sec. 6 - Technical requirement: user and system requirement**, the technical requirements’ list (i.e., user and the system requirements) is elicited and presented, providing a generic picture of how an IoT-enabled PI environment has to be shaped.

- In **Sec. 7 - System architecture and high-level specifications,** the generic IoT infrastructure capable to resolve the issues arisen on the technical requirements is detailed, and a set of high level technical specifications are elicited for each LL. Finally, the technical details regarding the considered interoperability patterns, the interactions, and data models to communicate with the ICONET remote platform, the used IoT protocols and the available hardware platforms are described.
- In **Sec. 8 - Innovations**, the innovations introduced to realise an IoT-enable PI environment are described, analysing the protocols, architecture and business intelligence point of view. More importantly this section maps precisely how each innovative element will address the identified business requirement and ensure the added value of the PI concepts to stakeholders and users.
- **Conclusions**' section ends the document.

3 Requirements' elicitation methodology

3.1 Introduction

Project requirements are conditions that must be completed to ensure the success or completion of the project. They provide a clear picture of the work that needs to be done. They are meant to align the project's resources with its objectives. The benefits of effectively gathering project requirements include cost reduction, higher project success rates, more effective change management, and improved communication among stakeholders. For these reasons, in this deliverable, we agreed to consider the following definitions of ISO for requirements elicitation:

- "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)
- "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)

Following the guidelines defined by the mentioned ISO Standards, the characteristics of good requirements are the following:

1. **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.
2. **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.
3. **Unambiguous**: The requirement is concisely stated. It expresses objective facts, not subjective opinions. It is subject to one and only one interpretation.
4. **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.
5. **Singular**: The requirement should state a single capability, characteristic, constraint, or quality factor.
6. **Feasible**: The requirement can be realized within entity constraints (e.g., cost, schedule, technical, legal, or regulatory) with acceptable risk.
7. **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.
8. **Correct**: The requirement must be an accurate representation of the entity need.
9. **Consistent**: The requirement does not contradict any other requirement and is fully consistent with all authoritative external documentation.
10. **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.

In this section, a methodology for requirements elicitation is defined to support the design of the IoT environment of the ICONET PI platform.

3.2 Types of requirements

Figure 2 depicts the hierarchy of the main types of requirements to be elicited in a project. In this scenario:

1. **Business requirements** describe why the organization is undertaking the project. They state some benefits that the developing organization or its customers expect to receive from the product. Regarding the ICONET project, the "Business requirements" of the IoT layer derives directly from the general scope of the project, thus they are not considered within this deliverable.

2. **User requirements**, often referred to as user needs, describe what the user does with the system, such as which activities users must be able to perform. User requirements are generally used as the primary input for creating system requirements. For this reason, they must be clearly defined, thus providing enough information to guide the project toward the complete fulfilment of the identified needs. Within the case of ICONET project, the "User requirements" will highlight the issues and the needs of remote monitoring of the goods along the logistics chain.
3. **System requirements** are the building blocks developers use to build the system. These are the traditional "shall" statements that describe what the system "shall do." A functional requirement specifies something that users' needs to perform their work. For example, a system may be required to enter and print cost estimates. For these reasons, the system requirements are expressed in technical language, describing a set of system functions in a measurable manner, thus forming the basis for system realization.

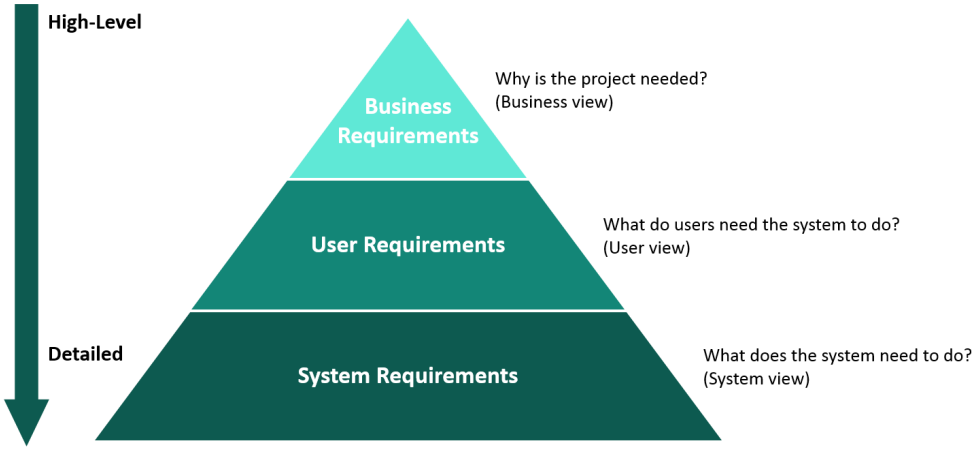


Figure 1 Requirements Hierarchy

To simplify the understanding of the elicitation process, we have divided the requirements in two sections:

1. Sec. 4 - Key drivers and Business requirements where the business requirements are elicited , as well as authorities and policy makers imperatives and high level technology needs are detailed.
2. Sec. 6 - Technical requirement: user and system requirement, where the user and system requirements are elicited, supported by the technical and market information provided in Sec. 5 - State of the Art

3.3 Recipients of this document

To implement an effective requirements' elicitation procedure, we need to identify the recipients of our findings regarding IoT between the stakeholders involved in the realisation of the PI grand-challenge but also the external users. In fact, one of the main objective of this document is to realise a blueprint capable to explain the importance of IoT, seen as a PI enabler, thus to support the digitalisation and to optimisation of the logistics processes, making these sustainable, low cost, efficient and reliable (Montreuil, 2011) , thus realising the Zero Emission Logistic chain (SENSE project , 2020). In this scenario, an in depth analysis of the recipients of this document has to be performed to understand the stakeholders that can contribute to the requirement elicitation, as well as can exploit the results of this document: in the following section the categories of recipients are analysed in detail, highlighting their roles and interests in the realisation of an IoT-enabled PI environment.

3.3.1 Categories of recipients

In this section we thoroughly analyse the recipients of this document, so the stakeholders involved in the realisation of the PI, highlighting their roles and interests on realising it. These stakeholders will support the

definition of the business requirements and the general direction to implement an optimised and efficient supply chain. In the following the detailed list of recipients is described, grouped into three main categories:

1. Logistic operators interested on improving and optimising the logistics' services towards cost reduction or revenues' increase. In the following table, the breakdown of the operators involved in the logistics world is provided.

Table 1 Logistic operators' breakdown

Logistic operators	Description
Shippers	Interested in the end-to-end supply-chain visibility. They usually do not own the containers. However, they can implement circular economy with some assets (e.g., pallets), so interested in monitoring them.
End Customers	Interested to dispatch the goods at the best possible rate and receive the best level of service agreed with the shipper/ LSP. Interested in the end-to-end supply-chain visibility, to understand the correct shipment and storage of the goods (e.g., cold chain), and the status of inventories on the various warehouses.
Freight forwarders	Interested in the digested information derived from the visibility of the supply-chain. They usually do not own the containers or compatible assets.
Retailers	Interested in the result of using the SC transparency data resulting from the analysis of data generated collected. However, they can implement circular economy with some assets (e.g., pallets, baskets), so interested in monitoring them.
Shipping companies	They own containers and they are the actors who receive the most direct value creation from investing in supply chain. Not all containers are directly managed by the shipping companies but could be rented to container leasing companies. Optimized stuffing of containers and minimizing container's dead space maximizes their returns
Container leasing companies	Container leasing companies are, together with the shipping companies, the actors who receive the most direct value creation from investing in supply chain.
Carriers	Interested in the digested information derived from the visibility of the supply-chain. They usually do not own the containers or compatible assets, but they can be interested in fleet monitoring solution capable to integrate their OBUs with standardised interfaces (see for example ISO 19080:2016). Minimizing distances hauled and maximizing load factors is key to their growth.
LSPs	As service providers, they are only interested in the digested information derived from the visibility of the supply-chain to optimize routings.
Hub Operators	At the centre of Logistics activities, interested in full visibility and efficiency of operations, dynamic allocation of resources, cost minimization and optimized asset utilization throughout its range of operations
Warehouses	Interested in having a complete visibility of the warehouses in terms of goods (position, inventory, status monitoring, goods delivered) and assets (pallets, crates, as well as delivery vehicles and machineries). Tracking of incoming consignments (levels, volumes, storage needs etc) supports the scheduling of loadings and optimizing container spaces for cross docking and distribution activities

2. Technologies' and Solutions' Providers, in charge of providing instruments to implement the complete supply chain visibility, as well as providing the automatic intelligence to optimise such processes. In the

following table, the breakdown of the technologies' and solutions' providers involved in the logistics world is provided.

Table 2 Technologies' and Solutions' Providers' breakdown

Technologies' and Solutions' Providers	Description
Value Adding Service Providers	Interested in entering in the PI market providing added value and interoperable service for the logistics operators.
System integrators	Interested in entering in the PI market on supporting the integration of innovative and different services and devices in the PI environment.
IoT Makers	Interested in entering in the PI market on providing IoT devices to provide added value data and information.
H/W Manufacturers	Interested in entering in the PI market producing standard, cost-effective, low power components, and boards.

3. Authorities & Policy Makers with the scope of standardising methodologies and defining regulations to improve the companies' productivity and competitivity, as well as, reducing the traffic and the pollution footprint due to unoptimized logistics. In the following table, the breakdown of the authorities and policy makers involved in the logistics world is provided.

Table 3 Authorities' and policy makers' breakdown

Authorities & Policy Makers	Description
Standardisation entities	Interested in defining a set of harmonised and improved protocols, methodologies, assets, thus realising an open and concurrent scenario.
Governments and local authorities	Interested in exploiting the digested IoT data to optimise the logistics effects (e.g., pollution, traffic), as well as creating a competitive scenario towards a market growth.
Supply Chain and Logistics Associations	Interested in the definition of new approaches toward the operations' optimisation, the costs' reduction and revenues' increase for their associated member-companies.

3.4 Methodology

For the process of requirements elicitation and analysis, we consider a 4-step iterative methodology as depicted in Figure 2 and described in the following:

1. The requirements discovery is the process of interacting with, and gathering the requirements from, the stakeholders about the required system. This process can be implemented using some techniques, like brainstorming, interviews, scenarios, prototypes, etc., which help the stakeholders to understand what the system will be like.
2. The requirements classification is a very important process to organize the overall structure of the system, by putting related requirements together and decomposing the system into subcomponents of related requirements. This step enables the identification of the existing relationships between such components which are to guide the selection of the most suitable architectural design patterns.
3. The requirement prioritisation and negotiation process concern the sorting requirements in importance and finding and resolving requirements conflicts through negotiations with the involved stakeholder. Requirements prioritizing procedure is very useful also for the following steps since it allows to focus with attention on the essentials and core features of the system and effectively meet users' expectations.
4. The requirements specification is the process documenting the definitive version of the requirements, exploiting a tabular approach detailed in the following section.

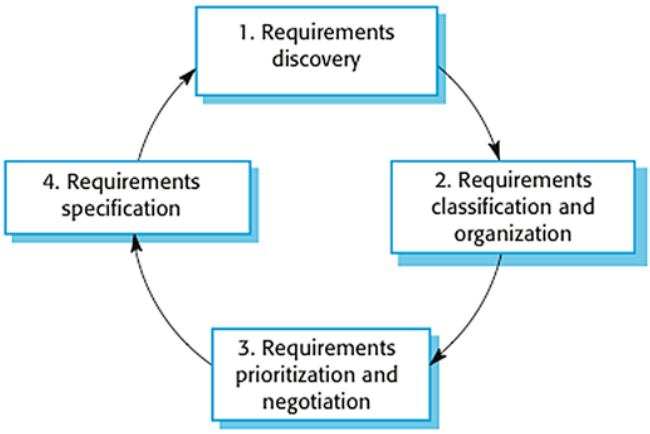


Figure 2 The process of requirements elicitation and analysis

3.4.1 Requirement template

As previously said, each requirement will be mapped in a table line. This section has the objective to define the generalized shape of each requirement. In Table 4 the shape of each line is breakdown, and in the following the meaning of each field detailed.

Table 4 Requirement template

Req. ID	Req. Name	Req. Type	Description	Dependency		Priority
				BR	TR	Category

In this section, some definitions are provided to support the filling of Table 4:

- Req. ID: this field represents the unique ID assigned to each requirement.
- Req. Name: this field represents the requirement name.
- Req. Type: in this document, each requirement is classified following the type defined in Sec. 3.2.
- Description: in this field a short description of the requirement is provided.
- Dependency: defines the dependency of the considered requirements with the other. Particularly, in this field the dependency of the considered requirement from the business requirements (BR, defined in Sec. 4) and from the technical requirements (i.e., user and system requirements, TR, defined in Sec. 6). Of course, BR can depend by other BRs only, while TR can depend by both BR. and TRs.
- Priority: the proposed prioritisation process considers the MoSCoW methodology (Clegg & Barker, 1994), that defines the following five levels:
    - **Must have**: Requirements labelled as “Must” are critical to reach the objective of the project.
    - **Should have**: Requirements labelled as “Should” are important but not necessary for the success of the project.
    - **Could have:** Requirements labelled as “Could” are desirable but not necessary.
    - **Wish have**: Requirements labelled as “Wish” have been agreed by stakeholders as the least-critical, lowest-payback items, or not appropriate at that time.
- Category: we propose to categorise requirements into the following groups:
    - **Functional requirements** (**Funct.**) 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** (**Non-Funct.**) are the behavioural properties that the specified

3.4.2 Requirements' elicitation task forces

In the ICONET project we will consider the brainstorming technique to define the list of the general requirements but also a thorough investigation of the Logistics industry with today's realities and well documented needs and inefficiencies, regarding the envisioned IoT environment for PI. The requirements will be elicited by defining a taskforce of entities with different expertise between the members of the consortium. Particularly:

1. The business and user requirements elicitation operations will be driven mostly by the actual business users in charge of managing the ICONET Living Labs (i.e., PoA, P&G, SB, SON and eBOS), and supported by the logistics associations involved in the project (i.e., ELU, UIRR, ESC). This task is also supported by the analysis of pains and gains in the LLs' scenarios implemented in T4.3 and T4.4 by EGL and CNIT and delivered in D4.6 (Balden, 2020). and D4.8 (Martini, 2020) respectively.
2. The **system requirements** elicitation process will be driven by the Technology/Solution Providers (i.e., ICT expert), involving NGS (as task leader as well as IoT maker and value adding service provider), IBM, eBOS and Inlecom (system integrators), SB (value adding service provider) and CNIT and ITA (research entities).

Particularly, the task force will be composed as depicted in the following table

Table 5 Task force for general specifications' elicitation

Domain experts	ICT company experts	Associations
Philippos Philippou (EBOS, WP3 leader)	Claudio Salvadori (NGS)	Eric Feyen (UIRR)
Koen Cuypers (PoA, LL1)	Stefano Bocchino (NGS)	Andreas Kortenhaus (ESC)
Marc Verelst (P&G, LL2)	Alessandro Vaglini (NGS)	Nathalie Rousseau (ESC)
Angela Cruz (SON, LL3)	Francesco Marino (CNIT)	Steve Rinsler (ELU)
Hamid Badri (SB, LL4)	Piero Castoldi (CNIT)	Brian Bolam (ELU)
Britta Balden (EGL, T4.3 leader)	Barbara Martini (CNIT, T4.4 leader)	
	David Cipres (ITA)	
	Alberto Capella (ITA)	
	Gerasimos Kouloumbis (ILS)	

4 Key drivers and Business requirements

4.1 Introduction

The objective of this section is to elicit a set of business requirements to characterise the realisation of a hyper-connected and interoperable IoT environment for the PI. This process will be in charge of evaluating the high level needs of the actors involved in the realisation and consolidation of the PI, toward the optimisation of the inefficiencies of the logistics sector, as well as the realisation of innovative technology-driven data-models.

The analysis is based on the requirements, needs and imperative of three distinct categories - that represents also the recipient of this document (see Sec. 3.3) – in charge of characterising different perspectives of the IoT-enabled PI environment: business, technology and regulatory. Such type of approach will produce a more comprehensive representation of the complex business spectrum of the industries involved in the realisation of PI, of course with the focus on the realisation of both the architecture and the components of the IoT-enabled PI environment. In fact, the identification of the needs as well as the inefficiencies in the Logistics industry will provide the target spectrum of the IoT elements analysis and design considerations to ensure the value adding element of the PI concept and its appeal to the Logistics users.
In this scenario, the elicitation of the business requirements, produced by the logistics actors, will be enhanced by the definition of a set of high-level technological needs and authorities and policy-makers imperatives.

4.2 Logistics operators' business requirements

The business requirements derive from business issues arisen by logistics actors and operators and they will be represented following the guidelines defined in Sec. 3. They clearly refer to reduce their pains and/or increment their gains. Interviewing the logistic stakeholders involved in the ICONET project, as well as the some analysis performed in ICONET deliverables [(Balden, 2020) (Martini, 2020)] and document [(Montreuil, 2011) (SENSE project , 2020)] coming from internet, we have identified the business requirements described in Table 6, while in Table 7 the effective group of stakeholders that has elicited the considered requirement. The requirements are classified as follow:

1. Requirements related to the **infrastructure costs' minimisation**, that suggest information regarding the cost of the IoT system and its integrability. The "infrastructure costs' minimisation" requirements' ID will be differentiated from the other by considering the prefix "MCR_", thus being shaped as following: MCR_<ID> (where ID is an incremental number).
2. Requirements related to **increase the operational efficiency,** that suggest the actions needed to optimise the inefficiencies in the Logistics industry. The "increase the operational efficiency" requirements' ID will be differentiated from the other by considering the prefix "IER_", thus being shaped as following: IER_<ID> (where ID is an incremental number).
3. Requirements related to **increase the market share,** that suggest the actions needed toward the competitivity improvement of the logistics operators. The "increase the market share" requirements' ID will be differentiated from the other by considering the prefix "MSR_", thus being shaped as following: MSR_<ID> (where ID is an incremental number).
4. Requirements related to **enhance the market offering,** that suggest the actions to improve the service provided to the clients. The "enhance the market offering" requirements' ID will be differentiated from the other by considering the prefix "MOR_", thus being shaped as following: MOR_<ID> (where ID is an incremental number).

Table 6 Business requirements

Req. ID	Req. Name	Req. Type	Description	Dependency		Priority
				BR	TR	Category
MCR_01	**Affordable system**	**Bus.**	The IoT physical infrastructure has to be affordable for all the users. As a service approach has to be preferred to the device selling.	-	-	**Must** **Funct.**
MCR_02	**Affordable integrability**	**Bus.**	The IoT service must provide interfaces that allows an affordable and secure integration with third parties' software (e.g., Port's RMS, Warehousing, Traffic control, Resources status, TMS etc.), respecting the privacy issues.	-	-	**Must** **Funct.**
MCR_03	**Easy and not invasive installation – Easy maintenance**	**Bus.**	The logistics operators are not expert in technology. The system has to have an easy installation process, in terms of physical deployment, maintenance and configuration.	-	-	**Must** **Non Funct.**
IER_01	**Supply chain visibility at multiple layers**	**Bus.**	The IoT will provide a reliable, low-cost end-to-end and real-time visibility of the whole supply chain (corridors, warehouses, hubs). The visibility has to be implemented with an improved granularity for all the encapsulation layers (e.g. PI container, pallet, packet).	-	-	**Must** **Funct.**
MOR_01	**Supply chain digital twin**	**Bus.**	The IoT system will provide an affordable, reliable, end-to-end shipment visibility at multiple layers In this scenario, each stakeholder involved in the logistics transaction can access to IoT devices deployed at every level of the encapsulation stack (e.g. PI container, pallet, packet).	**IER_01**	-	**Should.** **Funct.**
MOR_02	**Localisation and inventory of goods and products**	**Bus.**	The IoT will provide the position of certain goods at a certain time at multiple layers (e.g. PI container, pallet, packet). In	**IER_01** **MOR_01**	-	**Should.**

			this scenario, an advanced track&trace service can be provided, providing real-time encapsulation information up to the goods layer.			**Funct.**
IER_02	**Localisation and monitoring of assets**	**Bus.**	The IoT will be provide the connectivity for monitoring assets connected to the logistics operations (e.g., shelf, pallets, crates, containers …), thus providing information regarding their position and status.	**IER_01**	**-**	**Could** **Funct.**
EMR_01	**Ensure goods integrity and safety**	**Bus.**	The IoT will monitor the status of the goods in terms of integrity or safety (e.g., cold chain monitoring) at multiple layers (e.g. PI container, pallet, packet).	**IER_01** **MOR_01**	**-**	**Could** **Funct.**
IER_03	**Data-oriented and fact-based decision making and business intelligence**	**Bus.**	Exploiting the data retrieved the IoT environment, Big-data analysis techniques can be implemented to generate knowledge and models to support the decision-making implementing Data-oriented and fact-based business intelligence	**IER_01** **IER_02** **MOR_01** **MOR_02**	**-**	**Should** **Non Funct.**
IER_04	**Assets' management optimisation**	**Bus.**	Exploiting the data gathered by the IoT devices, the improved assets' management will support the optimisation of the operational efficiency implementing of the stakeholders implementing an effective utilisation of the available resources (e.g. for a Hub: cranes, rail network, storage, etc, as well as containers, pallets, boxes, …)	**IER_01** **IER_02** **IER_03**	**-**	**Wish** **Non Funct.**
EMR_02	**Accurate ETA prediction**	**Bus.**	The storage of bigdata generated by the IoT devices, can support the computation of an accurate ETA prediction.	**IER_01** **IER_02** **MOR_01**	**-**	**Must** **Non Funct.**
IER_05		**Bus.**	Improved efficiency improving the capacity of the corridors and of the warehouses, thus reducing the costs and/or	**IER_03** **IER_04**	**-**	**Should**

	Maximise Operational Efficiency and Capacity, Revenue Generation		increasing the profits. Examples: (i) Increasing the transport load factor, thus avoid empty trips; (ii) implementing a reliable and up-to-date warehouse management.			**Non Funct.**
MSR_01	**Increase Customer Satisfaction**	**Bus.**	Implementing a reliable, secure and less expensive logistics services, and offering an advanced information sharing service capable to provide an accurate end-to-end real-time visibility of the goods along the supply chain and accurate predictions.	**EMR_01 IER_03 EMR_02**	-	**Should**
						Non Funct.
MSR_02	**Gain competitive advantage**	**Bus.**	Gain competitive advantage by differentiating against similar supply chain actors (e.g. PoA vs PoR offering a wider range of services and more accurate up-to-date information)	**EMR_02 IER_05**	-	**Should**
						Non Funct.
IER_06	**Scheduling and organisation of the intermodal and the uploading/downloading operations**	**Bus.**	Exploiting the information coming from the IoT, the organisation of PI-hubs will be improved in terms of scheduling and efficiency.	**IER_01 IER_02 MOR_01 MOR_02 IER_03**	-	**Should**
						Non Funct.
EMR_03	**Fault liability**	**Bus.**	Exploiting the information coming from the IoT, the liability of certain event can bring back to the effective party.	**IER_01 MOR_01 EMR_01**	-	**Wish**
						Non Funct.
IER_07	**Circular economy support and optimisation**	**Bus.**	Reusable packaging and assets (e.g., beer kegs) can be re-used properly, thus supporting and optimising the circular economy practices.	**IER_01 IER_02 IER_03 IER_04**	-	**Wish**
						Non Funct.

Table 7 Stakeholders interest on the requirement

Req. ID	Req. Name	Shippers	End costumers	Freight forwarders	Retailers	Shipping companies	Container leasing	Carriers	LSPs	Hub operators	Warehouses
MCR_01	Affordable system	X			X	X	X				X
MCR_02	Affordable integrability	X	X	X	X			X	X	X	X
MCR_03	Easy and not invasive installation – Easy maintenance	X			X	X	X				X
IER_01	Supply chain visibility at multiple layers			X	X				X	X	X
MOR_01	Supply chain digital twin	X	X		X						X
MOR_02	Localisation and inventory of goods and products	X	X		X				X	X	X
IER_02	Localisation and monitoring of assets	X			X	X	X	X			X
EMR_01	Ensure goods integrity and safety	X	X	X	X	X		X			X

IER_03	**Data-oriented and fact-based decision making and business intelligence**	**X**			**X**	**X**					**X**
IER_04	**Assets' management optimisation**	**X**			**X**	**X**	**X**	**X**			**X**
EMR_02	**Accurate ETA prediction**	**X**	**X**		**X**						
IER_05	**Maximise Operational Efficiency and Capacity, Revenue Generation**			**X**		**X**		**X**		**X**	**X**
MSR_01	**Increase Customer Satisfaction**	**X**		**X**		**X**	**X**		**X**	**X**	**X**
MSR_02	**Gain competitive advantage**	**X**		**X**		**X**		**X**	**X**	**X**	**X**
IER_06	**Scheduling and organisation of the intermodal and the uploading/downloading operations**			**X**	**X**			**X**		**X**	
EMR_03	**Fault liability**		**X**	**X**	**X**	**X**	**X**	**X**			**X**
IER_07	**Circular economy support and optimisation**	**X**			**X**		**X**				**X**

The analysis of the proposed tables above shows the different perspectives and areas of interest of each of the actors involved in the supply chain. It is purely based on the business elements, thus it takes care about costs' reduction and revenues generation exploiting the following actions:

1. **Costs' reduction**, reducing the inefficiencies of the logistics ecosystem thus improving the optimisation of operations and services toward the productivity increase.
2. **Revenues' generation**, implementing innovative added value services to increase the customers satisfaction and gaining competitive advantages.

4.3 Technology Needs

In this section the needs required by the technology providers are listed and discussed. Particularly, in the table below the list of technology needs is provided by the different stakeholder involved in the ICONET project or extracted from third parties' documents and whitepapers (Friess, 2016), (Baum). Each technology need will be classified using a unique ID and it will be differentiated from the others by using the prefix "TN_", thus being shaped as following: IT_<ID> (where ID is an incremental number).

Table 8 highlights the different perspectives and areas of interest of each of the technological actors involved in realisation of the IoT components and services though for the PI and the supply chain. This describes a set of general and high-level needs from technical point of view to implement fruitful and innovative business models within the PI and logistics markets.

Table 8 Technology needs

		Value Adding Service Providers	Integrators	IoT Makers	H/W Manufacturers
TN_ID	**Project Actors**	**SB, NGS**	**Inlecom, IBM**	**NGS**	**e.g., TI, STM**
TN_01	**Enhanced (more stable, faster recharge, higher capacity) miniaturised and low-cost batteries**			X	X
TN_02	**Enhanced electronic processors (lower power, lower cost, higher computational power) and various lower power, lower cost sensors (gas, visual, …)**			X	X
TN_03	**Effective and pervasive connectivity everywhere (e.g., 5G and/or IoT access points)**		X	X	X
TN_04	**Consolidation of new open and standardised protocols and interfaces (lower cost, lower power, higher interoperability, higher computational power)**	X	X	X	X
TN_05	**Interoperable, expandable and secure IoT environments**	X	X	X	X
TN_06	**Unified data-structures, Standard/Unified Interfaces**	X	X		
TN_07	**Cost-effective/low-effort integration with backend legacy systems**	X	X		
TN_08	**Cost-effective deployment of new Services**	X			
TN_09	**Cost-effective release of new Services (to be easily "consumed" by a wider customer-base)**	X	X		
TN_10	**Up-selling new services based on existing or new IoT datasets**	X	X		

4.4 Authorities and Policy Making Imperatives

In this section the needs required by the authorities and policy making imperatives are listed and discussed. Particularly, the table below the list of authorities and policy making imperatives is provided by the different stakeholder involved in the ICONET project or extracted from third parties' documents and whitepapers (ISO DIS 19079) (ISO DIS 19080) (SENSE project , 2020). Each authorities and policy making imperative will be classified using a unique ID and it will be differentiated from the others by using the prefix "IM_", thus being shaped as following: IM_<ID> (where ID is an incremental number).

Table 9 highlights the regulatory and supervision point of view of the logistics environment. In fact, these describes a set of imperatives and needs coming from the regulatory and policy making world, thus taking in to account very high-levels problems such as:

1. Implement policy to promote the **concurrency** thus the **productivity**, avoiding monopolies. In this scenario, the realisation of open and standardised environment must be considered.
2. **Reduction the bureaucracy and support to the digitalisation**, toward a procedure simplification and considering a paperless approach, and aiming at the **cost reduction** and a **greener** implementation of the logistics services.
3. **Reduce the traffic, the pollution and improve the transport infrastructures** (roads, rails, …). In fact, having available the data generated by the logistics transaction, higher control and improved scheduling of the traffic can be implemented, as well as the transport infrastructures enhancement can be planned properly exploiting a data-oriented approach.

Table 9 Authorities and policy making imperatives

		Standardisation organisation	Governments and local authorities – other authorities	Supply Chain and Logistics Organisations
IM_ID	**Project Actor**	**e.g., ISO**	**PoA**	**ESC, UIRR**
IM_01	**Facilitate easier and cost-effective collaboration among T&L actors (Data, Communication Protocols, Interfaces Standardisation)**	X		X
IM_02	**Standardisation harmonisation**	X	X	
IM_03	**Awareness regarding cargos' position and status data**		X	X
IM_04	**Improve the productivity through information accuracy and interoperability amongst operators**		X	X
IM_05	**Improve the competitivity of logistics companies vs. non-EU markets – avoid monopolies**		X	X
IM_06	**Reduce bureaucracy - Reduce the time or eliminate unnecessary inspections - Efficient procedures to improve offerings and reduce the costs**		x	X
IM_07	**Environment protection and safety - security improvement**		X	X
IM_08	**Paperless, digitalized business spectrum enhancing shippers' collaborations through transparent and interoperable processes**	X	X	X
IM_09	**Traffic reduction**		X	
IM_10	**Early awareness and full real-time visibility – Data-oriented risk assessment and mitigation - Improved infrastructure maintenance/upgrade planning**		X	
IM_11	**Data security and users' privacy**		X	

5 State of the Art

Internet of Things is a key innovation enabling a massive number of devices to connect to the Internet. The concept of IoT leads to an explosive growth of IoT practical applications that can be found in many fields including smart home, smart health, smart metering, asset tracking, and agriculture (see also Figure 3). It is believed that IoT is revolutionizing human life to be smarter in every life aspect.

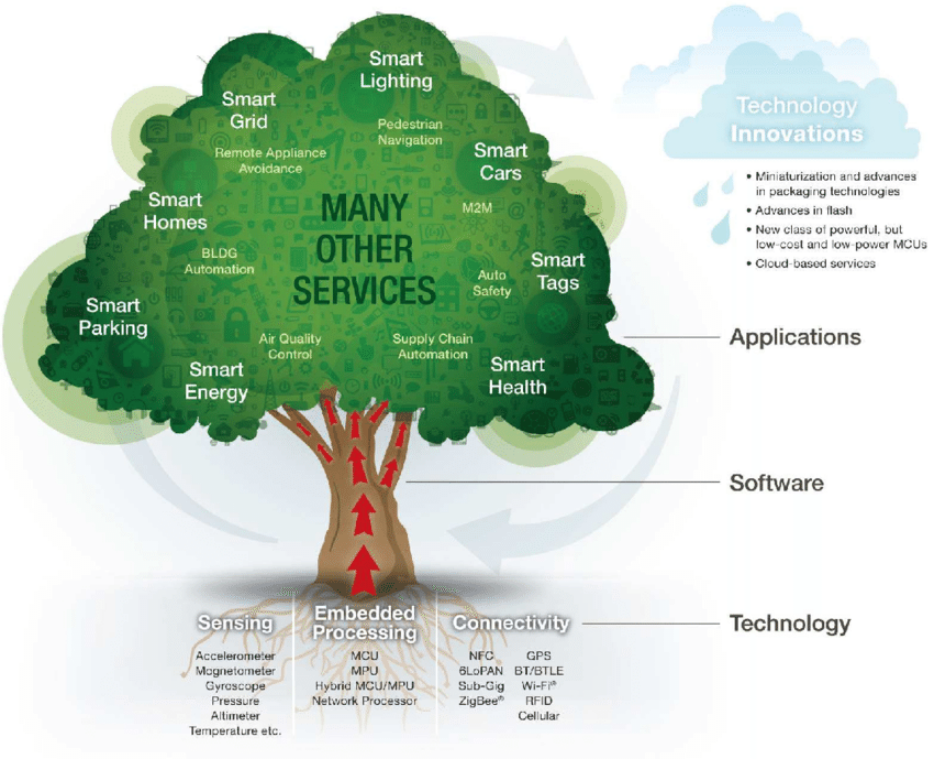


Figure 3: IoT systems in a snapshot

However, the world of IoT is fragmented. The fragmentation of IoT firstly comes from a diverse option of connectivity for end devices provided by different manufacturers. We have seen a dramatic growth of communication technology for IoT in the market. Each technology certainly aims at different application domains. Secondly, there exists a variety of application protocols to connect to the Internet with many data formats that could be exploited. Besides, vendors tend to create their own IoT platform exploited a proprietary protocol that leads to the creation of vertical IoT silos. An IoT silo is similar as a nation using a language that other silos are unable to understand. Those problems are known to be the interoperability issue, and we consider it as a crucial aspect to design our solutions, toward the realisation of a PI common language. Therefore, this section is organised to provide the needed information regarding the interoperability and the state-of-the-art of the IoT protocols to support the definition of an open IoT environment compatible with the PI issues. Finally, an overview about the impact of IoT in logistics with existing solutions in the market is provided at the end of this section.

5.1 Interoperability

The main goal of interoperability is to enable different systems to cooperate in a seamless manner. “Broadly speaking, interoperability can be defined as a measure of the degree to which diverse systems, organizations, and/or individuals are able to work together to achieve a common goal” (Gruber, 1993) . Interoperability allows different systems to understand each other even though they speak in different languages.

There exist many classifications of interoperability in the literature. However, there are two well-known classifications including a classification from LCIM (Levels of Conceptual Interoperability Model, for more details see the following section) (IoT-EPI, 2018) and another one defined by ETSI and AIOTI (H. van der Veer, 2008). Though that the classification from ETSI and AIOTI is more specific to IoT, we are going to review both and provide a comparison.

5.1.1 Classification of Interoperability

5.1.1.1 Levels of Conceptual Interoperability Model

LCIM is abbreviated for Levels of Conceptual Interoperability Models (IoT-EPI, 2018), which is a concept in simulation theory. However, this definition is also applicable for other fields. LCIM specifies seven levels of interoperability (see Figure 4) including the followings:

- **Level 0**: There is no interoperability between systems.
- **Level 1**: The level of Technical Interoperability requires two systems to establish an exchange of data between participating systems. This level of interoperability focuses mainly on building an infrastructure to allow the systems to transfer bits and bytes. Technical Interoperability ensures the common understanding of bits and bytes.
- **Level 2**: On the level of Syntactic Interoperability, there exists a common data structure or format between the participating systems. This level of interoperability requires a clear definition of data structure between the systems. This layer ensures the common understanding of symbols.
- **Level 3**: The level of Semantic Interoperability needs a common information model between the systems. In other words, it is required to have a universal ontology so that the meaning of exchanged data is unambiguously defined between the systems.
- **Level 4**: Pragmatic Interoperability is achieved if the participating systems can understand the context of the exchanged data. That means the meaning of the data can be put into a context without any explicit declaration.
- **Level 5**: The level of Dynamic Interoperability requires an alignment of a state model between the participating systems. That means a system is aware of the state changes of other systems and can take advantage of those changes to understand the exchanged data.
- **Level 6**: The level of Conceptual Model is the highest level of interoperability. At this level of interoperability, a conceptual model is shared between the participating systems. The shared conceptual model is a system with an integration of products, processes. The successful implementation of this conceptual model realises a system capable to dynamically adapt itself to interoperate with components from different manufacturers.

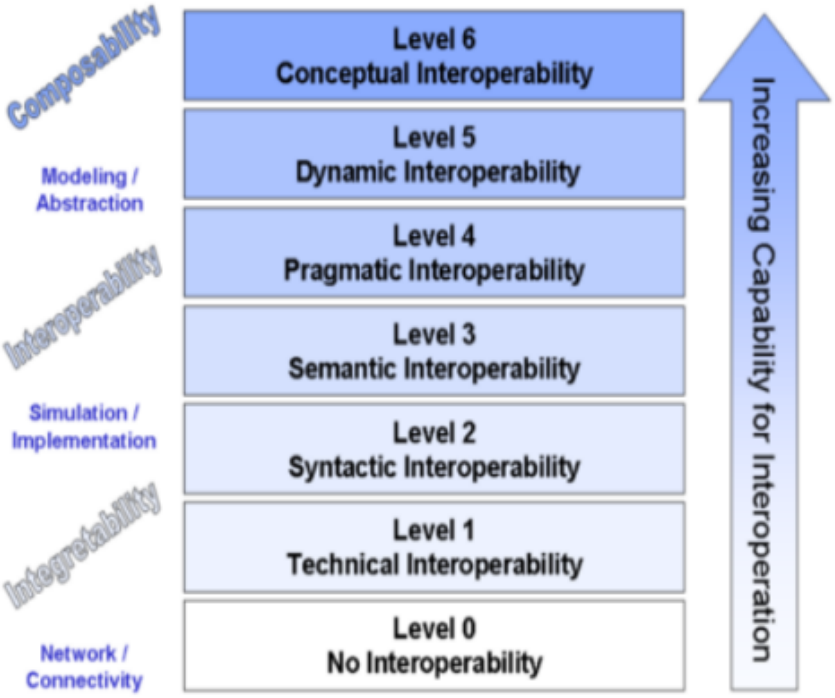


Figure 4: Levels of Conceptual Interoperability Model

5.1.1.2 ETSI and AIOTI Interoperability

Instead of six layers defined in the Levels of Conceptual Interoperability Model, ETSI and AIOTI specifies only four layers, see Figure 5. This categorization is known to be more related to IoT. The layers include the following levels (H. van der Veer, 2008):

- **Technical Interoperability** is usually associated with hardware/software components, systems and platforms that enable machine-to-machine communication to take place. This level of interoperability focuses mainly on the communication protocols and the infrastructures/platforms for those protocols to operate.
- **Syntactic Interoperability** is usually associated with data formats such as RDF, XML, and JSON.
- **Semantic Interoperability** is usually associated with the meaning of content and concerns the human rather than machine interpretation of the content. Thus, interoperability on this level means that there is a common understanding between two systems on the exchanged data.
- **Organizational Interoperability** is the ability to effectively communicate and transfer meaningful data even though they may be using a variety of different information systems over widely different infrastructures, possibly across different geographic regions and cultures. Organizational interoperability depends on successful technical, syntactic and semantic interoperability.

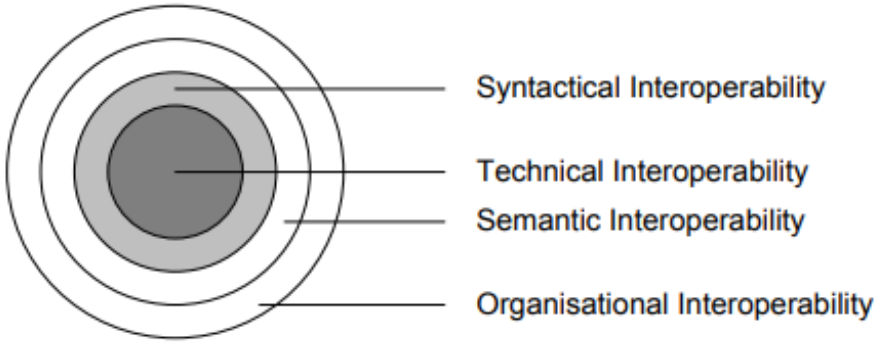


Figure 5: Dimension of Interoperability

5.1.1.3 Comparison and Consideration

As it is described in the previous part, two classifications essentially have the common first three levels, namely technical interoperability, syntactic interoperability, and semantic interoperability. If we look at the levels of interoperability defined in each definition, the LCIM classification specifies more three levels in comparison with the one from ETSI and AIOTI. However, the last level of interoperability according to ETSI is considered to enable **effective** communication **and meaningful data transfer** between different systems regardless of their infrastructures, which can be somehow equal to the last three levels from LCIM in the IoT field (as depicted Figure 6).

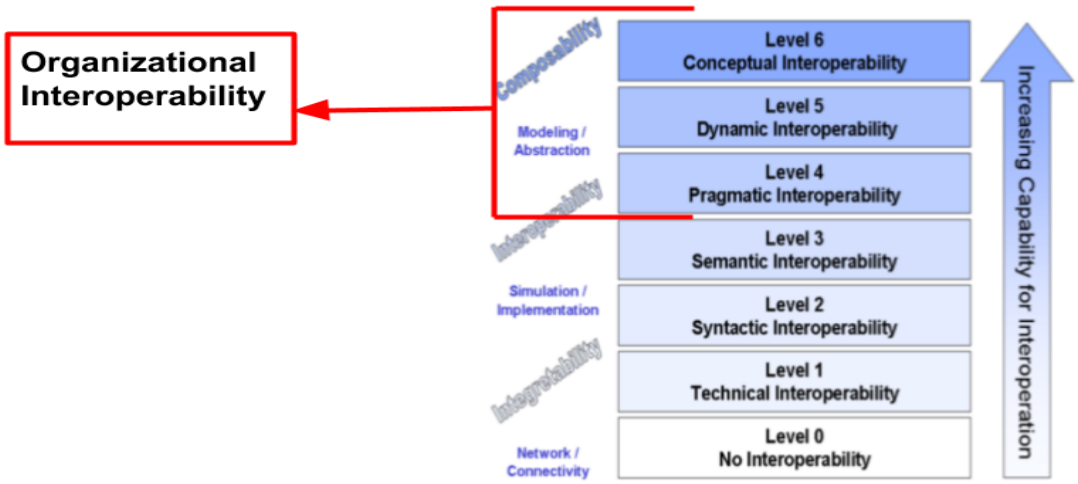


Figure 6: Mapping between Two Classifications of Interoperability

Even though there is an approximate mapping between two classifications, we choose to follow the classification from ETSI and AIOTI since the definition from ETSI and AIOTI is more specific to IoT. In addition, a clear selection of one classification provides consistent information throughout the document.

5.1.2 Interoperability Design Patterns

To enable seamless interoperability between different systems, six generic interoperability design patterns have been specified in the literature. By implementing those six design patterns, a system can be ensured to be easy for re-usage and interoperable. This section describes those design patterns including: Cross-Platform Access, Cross-Application Domain, Platform Independence, Platform-Scale Independence, High-Level Service Facades,

and Platform-to-Platform patterns (IoT-EPI, 2018). For more details regarding the interoperability design pattern see ANNEX I.

5.2 Smart-Interfaces State of the Art

This section provides an overview to seven European projects, which attempt to solve the existing interoperability issues in IoT. Besides, we provide in Table 10 the level of interoperability that each project has achieved for each tier of the general IoT architecture, depicted in Figure 7. For a detailed description regarding the approaches considered by EU flagship projects regarding the interoperability in the IoT domain see ANNEX II.

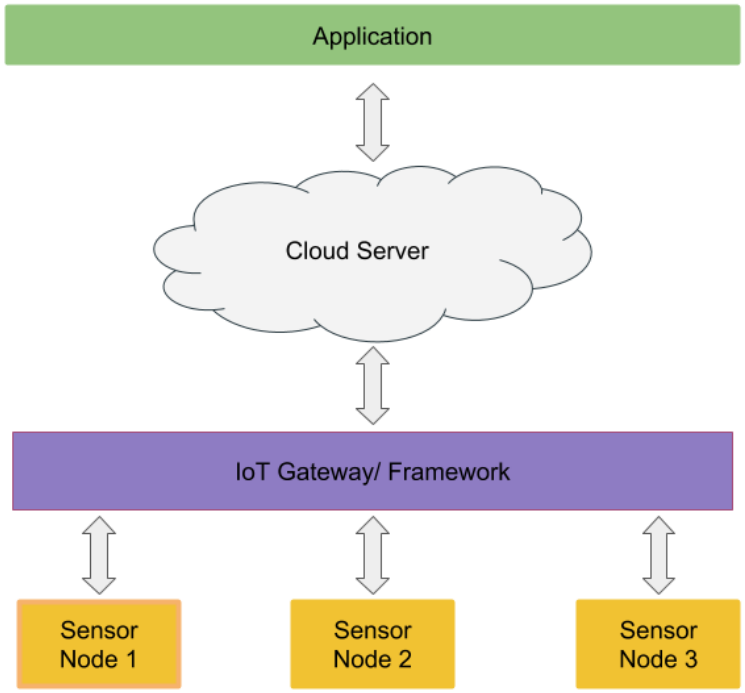


Figure 7: General IoT Architecture

Project	AGILE	BIG IoT	bIoTope	INTER IoT	symbIoTe	TagItSmart	VICINITY
Sensor Nodes	x	x	x	x	x	✓	x
Gateway	✓	x	x	✓	x	x	x
Cloud	x	✓	✓	✓	✓	x	✓
Application	x	✓	x	✓	✓	✓	✓

Table 10: Seven European Projects in a Nutshell

5.3 IoT access protocols' State of the Art

The world of IoT is extremely diverse since devices can connect toward the Internet in many ways. The reason leading to the diversity of IoT protocols is due to domain-dependent requirements. There is currently no unique solution to fit all domains. Each application domain requires a specific need such as cost, power consumption, stringent timeliness, coverage, data rate. Until a dominating technology appears to win the competition in all domains, the variety of connectivity technology still exists, creates, and enables the IoT. The existing IoT protocols in the market has brought up different solutions with trade-offs of cost, power consumption, and coverage. Each protocol has its own features and particularly targets a specific application domain. In this

deliverable the existing **IoT access protocols** for connecting sensor nodes and IoT gateways will be categorised into three groups: short-range, LPWA (Low Power Wide Area), and cellular-based technology.

Table 11, Table 12 and Table 13 summarise the different short-range technologies LPWA (Low Power Wide Area), and cellular-based technology respectively, providing a comprehensive scenario of the available IoT protocols.

Table 11 Short-range Technologies Summary

Technology	Frequency Band	Maximum Range	Maximum Data Rate	Channel Bandwidth	Topology
IEEE 802.15.4	868 MHz, 915 MHz, and 2.4 GHz	100 m	250 kbps	2 MHz	Peer-to-peer, Star
BLE	ISM 2.4 GHz	1 km	2 Mbps	2 MHz	Star, Mesh
IEEE 802.11 ah (Wi-Fi Halow)	sub 1-Ghz ISM	1 km	78 Mbps	2 MHz, 4 MHz, 8 MHz, 16 MHz	Star
RFID	Multiple Frequency band ranging from low to high frequency band: Low frequency: 125 kHz – 134 kHz, High Frequency: 13.56 MHz, Ultra-high Frequency: 860 MHz – 960 MHz	Less than 10m for passive tags, Less than 100 m for active tags	less than 1 kbps, High Frequency:25 kbps, Ultra-high Frequency: 30 kbps	Region-specific	Point-to-Point

Table 12 LPWA Technologies Summary

Technology	Frequency Band	Maximum Range	Maximum Data Rate	Channel Bandwidth	Topology
LoRa	Sub 1-GHz	15 km	37.5 kbps	125 kHz, 250 kHz, 500 kHz	Star
SigFox	Sub 1-GHz	50 km	100 bps for uplink, 600 bps for downlink	100 Hz	Star
Ingénue	ISM 2.4 GHz	15 km	78 kbps for uplink, 19.5 kbps for downlink	1 MHz	Star, Tree

Table 13 Cellular Technologies Summary

Technology	Frequency Band	Maximum Range	Maximum Data Rate	Channel Bandwidth	Topology
LTE-M (eMTC)	Supports licensed LTE Bands In-band	Less than 15 km	1 Mbps	1.08 MHz (1.4 MHz carrier bandwidth)	Star
EC-GSM	Supports licensed LTE	Less than 15 km	74 kbps (GMSK) and 240 kbps (8PSK) for both uplink and downlink	200 kHz	Star
NB-IoT	Supports licensed LTE in-band,	Less than 15 km	170 kbps for downlink	180 kHz (200 kHz carrier bandwidth)	Star

	guard-band, standalone		250 kbps for uplink		

5.4 Application/messaging Protocols' State of the Art

The selection of a standard communication technology is an inevitable step for the development of IoT applications, toward the interconnection of sensors/gateways with the remote Cloud/server applications, or to dispatch the data from a Cloud/server platform to another. However, the selection of a standard and effective messaging protocol is a challenging task for any organisation because it depends on the nature of the IoT system and its messaging requirements. For this reason, it is important to understand the pros and cons of the widely accepted and emerging messaging protocols for IoT systems to determine their best-fit scenarios. In the following, the most common messaging protocols (i.e., MQTT, CoAP, AMQP and HTTP) are analysed to support the selection of the most suitable for the IoT systems. In the following table (Naik, 2017) , the considered protocols' features are summarised.

Table 14 Messaging protocols comparison

Criteria	MQTT	CoAP	AMQP	HTTP
1. Year	1999	2010	2003	1997
2. Architecture	Client/Broker	Client/Server or Client/Broker	Client/Broker or Client/Server	Client/Server
3. Abstraction	Publish/Subscribe	Request/Response or Publish/Subscribe	Publish/Subscribe or Request/Response	Request/Response
4. Header Size	2 Byte	4 Byte	8 Byte	Undefined
5. Message Size	Small and Undefined (up to 256 MB maximum size)	Small and Undefined (normally small to fit in single IP datagram)	Negotiable and Undefined	Large and Undefined (depends on the web server or the programming technology)
6. Semantics/ Methods	Connect, Disconnect, Publish, Subscribe, Unsubscribe, Close	Get, Post, Put, Delete	Consume, Deliver, Publish, Get, Select, Ack, Delete, Nack, Recover, Reject, Open, Close	Get, Post, Head, Put, Patch, Options, Connect, Delete
7. Cache and Proxy Support	Partial	Yes	Yes	Yes
8. Quality of Service (QoS)/ Reliability	QoS 0 - At most once (Fire-and-Forget), QoS 1 - At least once, QoS 2 - Exactly once	Confirmable Message (similar to At most once) or Non-confirmable Message (similar to At least once)	Settle Format (similar to At most once) or Unsettle Format (similar to At least once)	Limited (via Transport Protocol - TCP)
9. Standards	OASIS, Eclipse Foundations	IETF, Eclipse Foundation	OASIS, ISO/IEC	IETF and W3C
10. Transport Protocol	TCP (MQTT-SN can use UDP)	UDP, SCTP	TCP, SCTP	TCP
11. Security	TLS/SSL	DTLS, IPSec	TLS/SSL, IPSec, SASL	TLS/SSL
12. Default Port	1883/ 8883 (TLS/SSL)	5683 (UDP Port)/ 5684 (DLTS)	5671 (TLS/SSL), 5672	80/ 443 (TLS/SSL)
13. Encoding Format	Binary	Binary	Binary	Text
14. Licensing Model	Open Source	Open Source	Open Source	Free
15. Organisational Support	IBM, Facebook, Eurotech, Cisco, Red Hat, Software AG, Tibco, ITSO, M2Mi, Amazon Web Services (AWS), InduSoft, Fiorano	Large Web Community Support, Cisco, Contiki, Erika, IoTivity	Microsoft , JP Morgan, Bank of America, Barclays, Goldman Sachs, Credit Suisse	Global Web Protocol Standard

5.5 A Short Review of Data Formats

As we mentioned in the definition and classification interoperability in IoT, syntactic interoperability requires a common data structure/format between two systems. Therefore, we go through state-of-the-art data

structures/formats in this section that are exploited in the IoT to achieve the level of syntactic interoperability. In Table 15, the summary of the main characteristics of the considered data formats is shown.

Table 15 Data format state of the art

XML	JSON	EXI	CBOR
XML is a mark-up language, not a programming language	JSON is a format written in JavaScript.	EXI is a compressed format of XML	CBOR is a compressed format of XML
XML data is stored as a tree structure.	Data is stored like a map with key value pairs.	Like XML	Like JSON
Bulky and slow in parsing	Very fast and the size of file is considerably small.	Slower in parsing than XML (encoding and decoding phases are added), it has a very small size footprint	Slower in parsing than JSON (encoding and decoding phases are added), it has an extremely small size footprint
Standardisation: W3C recommendation	Standardisation: IETF RFC 8259	Standardisation: W3C recommendation	Standardisation: IETF RFC 7049

5.6 IoT products for logistics available in the market

The Internet of Things is promising to revolutionize traditional logistics across the entire logistics value chain including warehousing operations, transportation management, and last-mile delivery. The IoT revolution is believed to enhance operational efficiency, safety, and customer experience. With the exploitation of IoT into logistics, managers can monitor assets status in real time, make decision and plan to avoid time-consuming repairing procedures in critical situations beforehand based on IoT value-added services such as predictive maintenance, error rooting, hence improve quality and predictability, and lower cost. In addition, IoT will enable effective cooperation between workers, systems, and their activities, which leads to an optimized and safe working environment. These enhancements bring tremendous profit to transportation and logistics companies, and in fact, attract them to integrate IoT technologies into their legacy solutions.

In this section, we will explore some products which are segmented according to the supply chain containing warehousing operations, intermodal logistics, and last-mile delivery. However, all the proposed solutions consider vertical solutions not organised in a common and interoperable environment, where different application can cooperate. This issue becomes critical in the scenario of intermodal logistics and PI, where the granularity of tracking and monitoring can be more detailed than a container-wise vision (e.g., PI Smart Pallets, PI Smart Packets). In this scenario, as for the DI grand-challenge, a set of standard IoT protocols must be defined to provide them the connectivity to exchange information with the PI remote manager, in charge of organising the effectiveness of the transaction.

The analysis provided in the following refers to IoT devices available in the market at the end of 2018.

5.6.1 Warehousing Operations

Warehouses are vital hubs in the flow of goods within the supply chains, and nowadays they store several kinds of products. Therefore, the organization of warehouses is essential to provide a seamless exchange of goods. A warehouse can be considered as a resource that must be optimally utilized in every square meter. The integration of IoT into warehousing operation helps to ease the life of warehouse operators and managers and creates the so-called Smart Warehouse.

One big advantage that IoT brings to warehousing operations is smart inventory management system. Such system is promising to maintain seasonal production, seasonal demand, quick supply, continuous production, and price stabilization. It usually exploits the widespread adopted RFID technology with small low-cost identification tags. One example solution is provided by RFID4U Warehouse Management & Inventory Control System (https://rfid4u.com/), which can perform full inventory management by exploiting a combination of technologies including RFID tags, RFID readers, barcodes, sensors, Wi-Fi networks and the Internet. Besides, the company also provides a system software to categorize each inventory item, which is easily and quickly set up to meet the individual company requirements.
Other solutions offered by Strategic Systems (https://www.sstid.com/) and RampRFID (https://www.ramprfid.com/), to name a few, have these functionalities. In addition, smart inventory management in a warehouse is also the capability to predict future orders to avoid surplus inventory and emergency orders, hence improve customer service and customer satisfaction.
Besides smart inventory management, IoT also enables predictive maintenance avoiding unexpected accidents in a warehouse by exploiting a variety of sensors. The data can be processed on the sensor devices or collected at a central processing controller, which can analyse it to determine if there is any necessity to schedule a maintenance appointment. For instance, RackEye (https://www.asafe.com) devices provided by A-SAFE monitor vibration and impact to racking structures and alert warehouse operators when a possible damage is detected (see Figure 8 and Figure 9).

Figure 8 RackEye Device

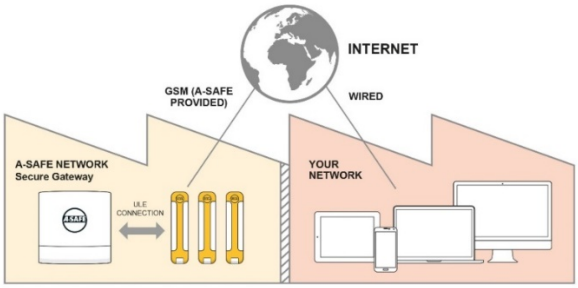


Figure 9 A-SAFE Network Architecture with RackEye Devices

IoT can optimize asset utilization by enabling machine to machine and vehicle-to-vehicle communication through a central system. A system that implements these functionalities can provide real-time visualization for warehouse managers to monitor all assets status. Additionally, a notification is sent to warehouse managers in case there is an asset is not optimally deployed. In order to provide these services, a sensor network should be integrated into different machineries to collect data about their working capacity and status. The data is then analysed to assign the optimal workload for each asset.
In this direction we can mention the Swisslog's "SmartLIFT" system (www.swisslog.com) which deploys forklifts sensors and directional barcodes placed on the ceiling of the warehouse, then fuse the collected data with the warehouse management system data to produce an accurate GPS data. The GPS data is exploited to support the forklift drivers to identify the location and direction of pallets. In addition, a warehouse manager can also observe the real-time speed, location, and productivity of all forklift drivers and visibility on inventory accuracy.
IoT can be fruitfully used in logistics to enable a connected workforce in warehouses, introducing a new way to monitor health and fatigue of workers and the walkways in a warehouse. This application helps warehouse managers to provide solutions to ensure the workers' health and working condition. One solution is provided by Locoslab (https://www.locoslab.com/), which utilizes beacons, active and passive RFID for indoor localization and movement monitoring. The application analyses collected data and guarantees optimal navigation of humans and objects in indoor environments, therefore improving workers' safety.
Finally, IoT sensor networks can be leveraged to optimize energy consumption in a warehouse. A smart warehouse energy management system can consist of many sensors integrated into the warehouse infrastructure, which can control HVAC and utilities networks according to activity in the warehouse, thus reducing energy waste. Transwestern exploited 95,000 embedded sensors in an office in Houston, Texas

connecting fire alarms, video surveillance cameras, temperature sensors, HVAC, and other utilities to optimize the energy consumption (https://www.cisco.com).

5.6.2 Intermodal logistics

Millions of shipments are made every day and the IoT represents a great opportunity for them. One of the most common application of IoT in logistics is track and trace. The Internet of Things is nowadays capable of bringing clear end-to-end visibility to customers about goods condition and location. Customers can monitor their goods status at any desired time and place. This tracking feature ensures that goods arrive at the right place and in time without any damage, hence improving customer satisfaction. One solution is the SmartSensor created by DHL (http://www.dhl.com), which can provide information about temperature, humidity, shock, light, and location data to customers. This information can also help logistics companies to change the process and transportation route in case any of the conditions laid down by customers for their goods are not satisfied.

Another available solution enabling smart containers is offered by TRAXENS (http://www.traxens.com). TRAXENS brings a complete solution to logistic companies from sensors to clouds. It provides TRAXENS-BOX S+, which is permanently attached to containers and collects data such as GPS position, temperature, impacts, movement, and vibration. The sensors are connected via a wireless network, namely TRAXENS-NET, and then transmitted to the TRAXENS-HUB cloud. For the detailed architecture, see Figure 10.

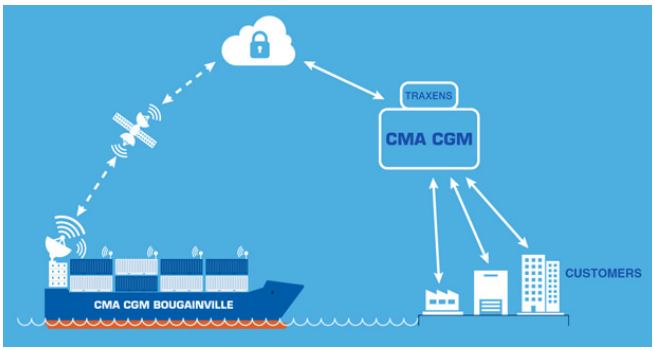


Figure 10 TRAXENS solution architecture

Besides, we report also the IoT Tracker product created by Accent Systems. It is a Plug and Play solution ready for production and with industrial-grade hardware. Ineo-sense has devised a smart container logistics security seal (https://www.ineo-sense.com) employing Clover-Net, LoRa, and NFC for communication and sophisticated sensors for monitoring. These promise to deliver a secure solution to logistic customers.

5.6.3 Last-Mile Delivery

The last step in the supply chain is last-mile delivery, which is probably the most challenging and sophisticated since customer demands change, and the number of delivery points continues to multiply. It is complex for logistics companies to optimize cost and meet customer's requirements. The integration of IoT in such last step enables new solutions to solve this problem.

In this direction the current trend involves connected mailboxes, providing not only a cost-effective solution for the logistics player, but also satisfaction for the customers. One relevant example is DHL Parcelbox. DHL Parcelbox is a delivery box with a smart locker. Only couriers can unlock the Parcelbox. DHL Parcelbox also integrates sensors inside to detect whether it is empty and, if so, transmits a signal that is then processed in real time to optimize the collection routes. Smart delivery boxes can notify customers when their packages arrive. Similar smart delivery boxes are also produced by Cottner (http://www.cottnertechnologies.com). Besides the smart mailbox, Panasonic Corporation of North American and Hussmann have recently introduced the LastMile Hub (https://na.panasonic.com/us/iot-solutions) which aims at the last-mile delivery of groceries. The hub solution offers on-demand convenience and flexibility for customers. Customers can choose the place they want to retrieve their food and the purchasing method they prefer. The hub can be considered as a secure locker with customizable storage unit modules and temperature setting capability, which can ensure the quality of customer's food.

Another common IoT-based trend in the consumer world can be named as the connected fridge. The fridge can track the expiration dates of products being stored, detects when supplies are insufficient, and orders online automatically. This solution can be considered as automatic replenishment and anticipatory shipping, which brings huge advantages to logistics providers since they can prepare beforehand required goods to avoid stock-outs, thus reducing lead time for delivery. In this respect, Amazon has patented an algorithm which can predict

customers' purchases which can be used to move products closer to the customers in advance in order to reduce delivery time. Moreover, this solution certainly increases product selling chance to the customer. In the end we report the Amazon Dash button a small device that can be programmed to order a consumer good in a manual or automatic way, which can be considered a special connected fridge that offers a convenient shopping way to customers.

IoT can also play a role in optimizing last-mile shippers delivering trips. For instance, the collected data from urban traffic can be analysed to estimate the delivery time to customers' desired-pickup points. Further, the IoT sensors attached to the packages enable transparency to customers. Besides, IoT can bring together shipping orders with driving by shippers, especially independent drivers, which may help to monetize their return trip. We can mention two logistics company that focuses on last-mile delivery, namely Dipper (http://www.usedipper.com) and Shippify (https://www.shippify.co/). Both companies provide an end-to-end visibility platform that connects verified independent drivers.

5.6.4 Intermodal logistics analysis (April 2020)

The analysis provided in the following refers to IoT devices available in the market in April 2020 and it is done to integrate the previous analysis.

- **Globe Tracker** (https://www.globetracker.com/) is addressing end to end cold chain visibility for logistics companies, installing a power supplied device (GT sense device) on top of reefers and capable to manage different BLE devices. GT sense device behave only a tracker (only GPS, not other added-value sensors installed) and added value measurements are guaranteed only by the integration of proprietary sensor nodes (capable to implement edge computing functionalities). Remote communication: 2G (it is not clear whether it is 5G-ready). Sampling period: 5min. Data-logging in case of lacking connectivity. No information regarding its openness for the exploitation of third parties' devices.
- **Sensolus** (https://www.sensolus.com/) has developed a battery-powered tracker based on the Sigfox technology (private and closed protocol, no 5G-ready). Added-value sensors on board and possibility to manage BLE nodes, only GPS. No information regarding sampling period.
- **Most** (https://most.tech/) has realised a battery-powered tracker capable to collect information regarding the position from the 2G cell (no GPS, un-precise measurement). It has to be installed within the container, and it is capable to collect data from calibrated sensors and implement some simple edge computing capabilities. It behaves essentially as data-logger, transmitting only when the 2G signal is available (i.e., when the container doors are open).
- **Keeptrucking** (https://keeptruckin.com/) implements a battery-powered tracker enhanced with a solar power capable to collect GPS data and dispatch this remotely through NB-IoT network (5G-ready). Equipped with BLE antenna, no local data collection functionality is mentioned. No information regarding added-value sensors installed. Sampling period: 5min.
- **Nexxiot** (https://www.nexxiot.com/) has developed a battery-powered tracker enhanced with a solar power capable to collect GPS data and temperature data. It allows the integration of third parties hardware and to behave as gateways for external sensors. Sampling period: 5min.
- **Traxens** (https://www.traxens.com/) has developed a 5G-ready battery-powered tracker enhanced with a solar power capable to collect GPS data and added-value measurements. It integrates interoperable wireless interface capable to collect added value data from external IoT sensor nodes, as well as to collaborate with other compliant devices (deployed in the containers).
- **Ambrosus** (https://ambrosus.com/) has developed a set of devices capable to cooperate with each other and capable to define the granularity of the monitoring along the whole supply-chain. Though they use a well-known protocol (BLE), they have developed a proprietary middleware and its interoperability with third parties' devices is not certain. The smart pallet is implemented using a complex router that maybe

can be too expensive compared with the cost of the pallet (less than 50€). Platform based on a proprietary and open-source Blockchain technology.

In summary, these solutions implement a container-wise monitoring and tracking and consider a minimal interaction between the IoT-nodes, thus not representing the goods encapsulation. In some of these solutions, the tracker can establish a sensor network, but only inside or outside the container. Only Traxense improvements envision an interoperation with third parties' solutions, implementing a cooperative and open IoT environment, however they cannot provide an effective monitoring inside the containers.

6 Technical requirement: user and system requirement

6.1 Introduction

The objective of this section is to define the technical requirements to characterise the realisation of a hyper-connected and interoperable IoT environment for the PI. In fact, following the parallelism with DI, the "PI packets" can be seen as the physical duals of the "DI packets". Just like "DI packets", they can be encapsulated (e.g., in a boat), arranged in flows or stored in a warehouse (proxy in DI). Unlike DI packets their retransmission because of loss or corruption implies costs and delays which are much less tolerated. For this reason, they must be avoided or at least timely detected. Moreover, being aware of the status of goods along the logistics chain allows to take proactive actions to improve the goods safety and to avoid products deterioration. On the other hand, in case unrecoverable damages are detected, such type of reporting will support decision making processes to arrange proper countermeasures without waiting for the unserviceable goods to reach their destination, or to identify the damage liability.

In this scenario and following the key drivers and the business requirements discussed in Sec. 4, a set of technical requirements will be elicited to drive the realisation of a IoT-enabled PI environment. The mapping of the key drivers and the business requirements on the technical will support the recipients on defining the right methodology to digitalise the supply chain and the logistics transactions.

6.2 Technical requirement

In this section the list of general requirements will be elicited. The elicitation process for this requirement will be based, as mentioned in Sec. 3 - Requirements' elicitation methodology, exploiting brainstorming methodology. The requirements will be classified as described in the following:

1. **Architectural requirements**. These requirements must provide details how to shape the IoT architecture for the PI environment. The architectural requirements' ID will be differentiated from the other by considering the prefix "AR_", thus being shaped as following: AR_<ID> (where ID is an incremental number).
2. **Interoperability requirements**. These requirements provide the guidelines to define how IoT components have to interoperate, following the theory described in Sec. 5.1. The interoperability requirements' ID will be differentiated from the others by using the prefix "IT_", thus being shaped as following: IT_<ID> (where ID is an incremental number).
3. **Integration requirements**. These requirements describe integration and installation details to be followed within the logistics environment. The integration requirements' ID will be differentiated from the others by using the prefix "IG_", thus being shaped as following: IG_<ID> (where ID is an incremental number).

All the technical requirements of Table 16 are elicited by the technical team (i.e., ICT company expert in Table 5) and will derive directly from the key drivers descried in Sec. 4 (i.e., logistics operator business requirements, technology needs, and authorities and policy making imperatives). For this reason, the technical requirements will be uniquely tagged with the respective set of business requirements directly on the table.

The technical requirements of Table 16 highlight several suggestions of how to implement the system in terms of:

1. **Architecture**, proposing a pervasive open and interoperable vision, capable to satisfy the digital encapsulation issues. In this scenario, modular and composable devices will be capable to ubiquitously monitoring the goods (presence and status) and cooperate with third parties' devices and on data collection and sharing, considering standardised protocols and representations.
2. **Device implementation,** that must be easy to install (wireless and battery powered, with internal battery), maintain (long duration internal battery) and integrate (interoperable with the proposed architecture).
3. **Integration**, suggesting the realisation of a remote Cloud platform to implement the brokerage of a scalable set of IoT transaction, the data persistence and its sharing with third parties in a secure manner respectful of the privacy (ad-hoc transactions).

The realisation of the technical requirements will be discussed in Sec. 7 - System architecture and high-level specifications.

Table 16 Technical requirements table

Req. ID	Req. Name	Req. Type	Description	Related to		Priority
				BR	TR	Category
AR_01	**Goods and asset real-time tracking and localisation**	**User**	Each PI "packet" must be tracked/localised, making its position available to all the stakeholders interested on the shipped goods (shippers, senders, receivers, etc.). IoT will support PI routing issues answering to the question Where? and When?	**Logistics operators' business requirements: IER_01, MOR_01, MOR_02, IER_02, IER_04, EMR_02, IER_05, MSR_01, MSR_02, IER_06, EMR_03, IER_07** **Technology needs: -** **Authorities and policy making imperatives: IM_03, IM_04, IM_06, IM_10**	**-**	**Must** **Funct.**
AR_02	**Goods real-time continuous monitoring**	**User**	Each PI "packet" has to be continuously monitored, making its status/quantity known at any time and answering to the questions "How?". To enable the implementation of the same service done by "CRC" in the DI, the goods has to be monitored to understand whether a packet is "corrupted" or not. The monitoring has to be implemented all along the supply chain (along the corridors, in the hubs, in the warehouses).	**Logistics operators' business requirements: IER_01, MOR_01, EMR_01, IER_05, MSR_01, EMR_03** **Technology needs: TN_02** **Authorities and policy making imperatives: IM_03, IM_04, IM_06**	**-**	**Should** **Funct.**
AR_03	**IoT enablement**	**Syst.**	To provide information about the PI packet an IoT communication infrastructure has to be set-up, enabling the communication from the field toward the IoT Cloud platform. No other cost of setting-up and maintaining the network infrastructure.	**Logistics operators' business requirements: MCR_02, IER_01, MOR_01, MOR_02, IER_02, EMR_01, MSR_02** **Technology needs: TN_03, TN_04, TN_05** **Authorities and policy making imperatives: IM_02, IM_05**	**AR_01** **AR_02**	**Must** **Funct.**
AR_04	**Modularity**	**Syst.**	Since the need of monitoring modular each PI "packets" (packets, container, group of containers), also the IoT environment must be modular, enabling the continuous monitoring and the tracking/localisation of the goods.	**Logistics operators' business requirements: IER_01, MOR_01, MOR_02, IER_02, EMR_01, IER_05, EMR_03, IER_07** **Technology needs: TN_05** **Authorities and policy making imperatives: IM_04**	**AR_01** **AR_02** **AR_03**	**Funct.** **Wish**

AR_05	**Composability**	**Syst.**	"PI packets" can be composed with other in a hierarchy of packets (physical encapsulation). This behaviour must be considered also in the design of the IoT environment (digital encapsulation). A relation between contained and container packets must be implemented.	**Logistics operators' business requirements: IER_01, MOR_01, MOR_02, IER_02, EMR_01, IER_05, MSR_01, EMR_03, IER_07** **Technology needs: TN_05** **Authorities and policy making imperatives: IM_04**	**AR_01** **AR_02** **AR_03** **AR_04**	**Funct.** **Wish**
AR_06	**IoT networks pervasivity**	**Syst.**	Since each PI packed must be continuously monitored, all the supply chain must be completely covered by the IoT connectivity. An IoT enabled PI environment must be enabled to provide a pervasive network solution, thus ubiquitously connecting the PI "packets" to the PI platform.	**Logistics operators' business requirements: MCR_02, MCR_03, IER_01, MOR_01, MOR_02, IER_02, EMR_01, IER_05, MSR_02** **Technology needs: TN_03, TN_05** **Authorities and policy making imperatives: IM_02**	**AR_01** **AR_02** **AR_03**	**Funct.** **Wish**
AR_07	**Edge computing enablement**	**Syst.**	The exploitation of edge computing devices will enable the distribution of intelligence along the network. Edge computers can enable the local data processing, e.g., detection of an alarm, thus allowing the provision of added value information (e.g., bump) at every level of the encapsulation granularity	**Logistics operators' business requirements: MOR_01, EMR_01, EMR_03** **Technology needs: TN_02** **Authorities and policy making imperatives: IM_04**	**AR_02** **AR_04**	**Non Funct.** **Should**
AR_08	**Resilience on data loss**	**Syst.**	The PI IoT environment must consider devices with local storage functionalities to maintain data whether the communication with the remote platform is not available (e.g., inside a tunnel or in the middle of the sea).	**Logistics operators' business requirements: MOR_01, EMR_01, EMR_03** **Technology needs: TN_02** **Authorities and policy making imperatives: IM_04**	**AR_02** **AR_04**	**Non Funct.** **Should**
IT_01	**Level 1 interoperability**	**Syst.**	Satisfaction of Level 1 (technical) Interoperability requirements (ETSI/AIOT classification) both at the data collection side (devices to gateways) and at the data sharing side (gateways to Cloud platforms and Cloud Platform to Cloud Platform)	**Logistics operators' business requirements: MCR_01** **Technology needs: TN_04, TN_05, TN_07,** **Authorities and policy making imperatives: IM_01, IM_02, IM_04, IM_05, IM_08, IM_10**	**-**	**Must** **Funct.**

IT_02	**Level 2 interoperability**	**Syst.**	Satisfaction of Level 2 (syntactical) Interoperability requirements (ETSI/AIOT classification) both at the data collection side (devices to gateways) and at the data sharing side (gateways to Cloud platforms and Cloud Platform to Cloud Platform)	**Logistics operators' business requirements: MCR_01 Technology needs: TN_04, TN_05, TN_06, TN_07 Authorities and policy making imperatives: IM_01, IM_02, IM_04, IM_05, IM_08, IM_10**	**IT_01**	**Must** **Funct.**
IT_03	**Exploitation of standard protocols**	**Syst.**	The exploitation of standard protocols can guarantee and support both Level 1 and Level 2 interoperability. Also, standard de-facto protocols can be considered (e.g., LoRaWAN)	**Logistics operators' business requirements: MCR_01 Technology needs: TN_04, TN_05, TN_07 Authorities and policy making imperatives: IM_01, IM_02, IM_04, IM_05, IM_08, IM_10**	**IT_01 IT_02**	**Must** **Funct.**
IT_04	**IoT connectivity as a service**	**Syst.**	Providing an interoperable and pervasive IoT infrastructure in the PI environment will allow the exploitation of connectivity as a service. In this scenario, all the actors involved in the PI can connect the Smart PI packet with the PI platforms thus enabling their tracking/localisation and monitoring.	**Logistics operators' business requirements: MCR_01, MCR_02, MOR_02, IER_02, IER_04, MSR_02 Technology needs: TN_06, TN_07 Authorities and policy making imperatives: IM_01, IM_02, IM_04, IM_05, IM_08, IM_10**	**AR_01 AR_02 AR_03 AR_04 AR_05 IT_01 IT_02 IT_03**	**Could** **Non Funct.**
IT_05	**Open IoT environment**	**Syst.**	The IoT environment has to be open, thus supporting the integration with/to third parties' interoperable components.	**Logistics operators' business requirements: MCR_02, IER_01, IER_02, MOR_02, EMR_01 Technology needs: TN_04, TN_05, TN_06, TN_07 Authorities and policy making imperatives: IM_01, IM_02, IM_04, IM_05, IM_08, IM_10**	**IT_01 IT_02**	**Must** **Non Funct.**
IG_01	**Seamless and affordable integration**	**User**	Seamless and affordable integration with third parties back-end systems (such as TMS).	**Logistics operators' business requirements: MCR_02, MSR_01 Technology needs: TN_05, TN_06, TN_07 Authorities and policy making imperatives: IM_01, IM_02, IM_04, IM_08, IM_10**	**AR_01 AR_02 IT_01 IT_02 IT_03 IT_04**	**Must** **Non Funct.**
IG_02	**Easy installation and maintenance**	**User**	The devices must be designed to be easy to install and to maintain (in general, these must be wireless, and battery powered). The add-up of new IoT devices must be Plug&Play.	**Logistics operators' business requirements: MCR_02, MCR_03 Technology needs: TN_01, TN_02 Authorities and policy making imperatives: IM_01**	**AR_06 IT_01 IT_02 IT_04**	**Must** **Non Funct.**

IG_03	**Secure and ad-hoc access**	**User**	Secure transaction (encryption). Data access allowed only to authorised operators.	**Logistics operators' business requirements: MCR_02** **Technology needs: TN_05** **Authorities and policy making imperatives: IM_11**	**-**	**Must** **Non Funct.**
IG_04	**Horizontal integration and scalability**	**User**	The system must be capable to manage several components, that can behave and compose themself in different manner, depending on the goods or the assets to be monitored and the monitoring granularity requirements. Cooperation with third parties' devices has to be considered.	**Logistics operators' business requirements: MCR_01, MCR_02, IER_01** **Technology needs: TN_04, TN_05** **Authorities and policy making imperatives:IM_01, IM_02, IM-04, IM-05, IM_06**	**.**	**Must** **Funct.**
IG_05	**IoT broker and Data persistence**	**User**	A platform capable to store the data is required. This platform will oversee managing a scalable set of transactions from the IoT devices (IoT broker) and storing the data collected in a database	**Logistics operators' business requirements: IER_01, IER_03, IER_04, EMR_02, IER_05, MSR_01, EMR_03, IER_07** **Technology needs: TN_08, TN_09, TN_10** **Authorities and policy making imperatives: IM_09, IM_10**	**IT_01** **IT_02** **IT_03** **IG_04**	**Must** **Funct.**
IG_06	**Interoperable interfaces, real-time reporting, and Big-data analysis enablement**	**User**	The platform must share the data collected considering interoperable interfaces, allowing real-time reporting. Big-data engines, PI components and logistics operators involved in the transactions can access to the data considering a secure and ad-hoc approach.	**Logistics operators' business requirements: MCR_02, IER_01, MOR_01, IER_03, IER_04, IER_05, MSR_01, IER_06, EMR_03, IER_07** **Technology needs: TN_05, TN_06, TN_07, TN_08, TN_09, TN_10** **Authorities and policy making imperatives: IM_01, IM_02, IM_04, IM_06, IM_08, IM_09, IM_10, IM_11**	**IT_01** **IT_02** **IT_03** **IG_01** **IG_03** **IG_04** **IG_05**	**Must** **Funct.**

7 System architecture and high-level specifications

7.1 Introduction and state-of-the-art IoT architecture

At this stage it is crucial to identify a reference architecture able to support the development of an IoT system meeting the peculiar requirements of the PI scenario elicited in Sec. 6. Indeed, a reference architecture provides consistent definitions, a standard vocabulary and, in short, a common framework which can be leveraged to further elaborate and discuss on the considered system. Moreover, by avoiding unnecessary specifics, a reference architecture provides the level of abstraction required to have a comprehensive and organic view of the system to identify the most relevant issues and to enable subsequent refinements and different patterns.
The most general architecture for Industrial IoT systems is the so-called three-tier architecture pattern. This pattern includes the edge, platform and enterprise tiers, which play specific roles in processing the data and control flows and which are connected by three networks, namely the proximity, access and service networks (see Figure 11).

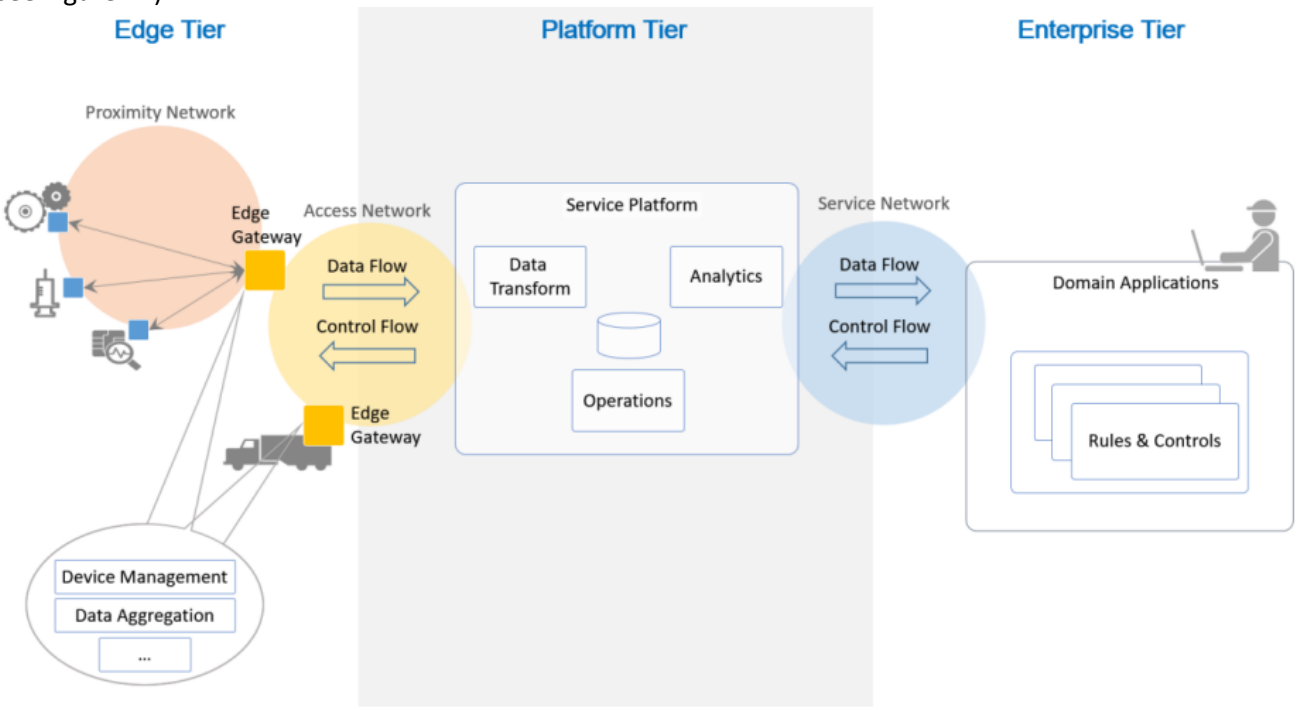


Figure 11 Three-Tier System Architecture

The *edge tier* collects data from a wide range of sensors, actuators, devices, control systems and assets using the proximity network. The architectural characteristics of this tier, including the edge nodes' types and their breadth of distribution and location, vary depending on the specific applications.
The *platform tier* consolidates and analyses data flows from the edge tier and provides management functions for devices and assets which can be leveraged by the enterprise tier. It also offers non-domain specific services such as data query and analytics.
The *enterprise tier* implements domain-specific applications and decision-making support systems and provides interfaces to end-users including operation specialists. The enterprise tier receives data flows from the edge and platform tiers and issues control commands to them.
The tiers are interconnected by different networks:

- The *proximity network* connects with each other the edge nodes, typically organized as one or more clusters, and each cluster with a gateway which acts as a bridge toward other networks. The nature of the proximity network is application dependent.
- The *access network* provides the connectivity for the data and control flows between the edge and the platform tiers. It may be a corporate or a virtual private network, or a 4G/5G network.

- The *service network* enables connectivity between the platform tier services and the enterprise tier. It may be a virtual private network or the Internet itself.

This section aims at the definition of the architecture of the IoT systems' edge segment. Usually, the reference IoT architecture adopts a gateway-mediated edge connectivity and management pattern (Figure 12). This pattern basically comprises a local area network of edge nodes connected to a wide area network through an edge gateway. The gateway isolates the edge nodes and behaves as single entry point toward the access network, breaking down this way the complexity of the IoT system by localizing operations and controls, so that it can easily scale up both in numbers of managed assets and networking. The gateway can also play the role of management and data aggregation point for devices and assets, hosting locally deployed control logic and data analytics processes.

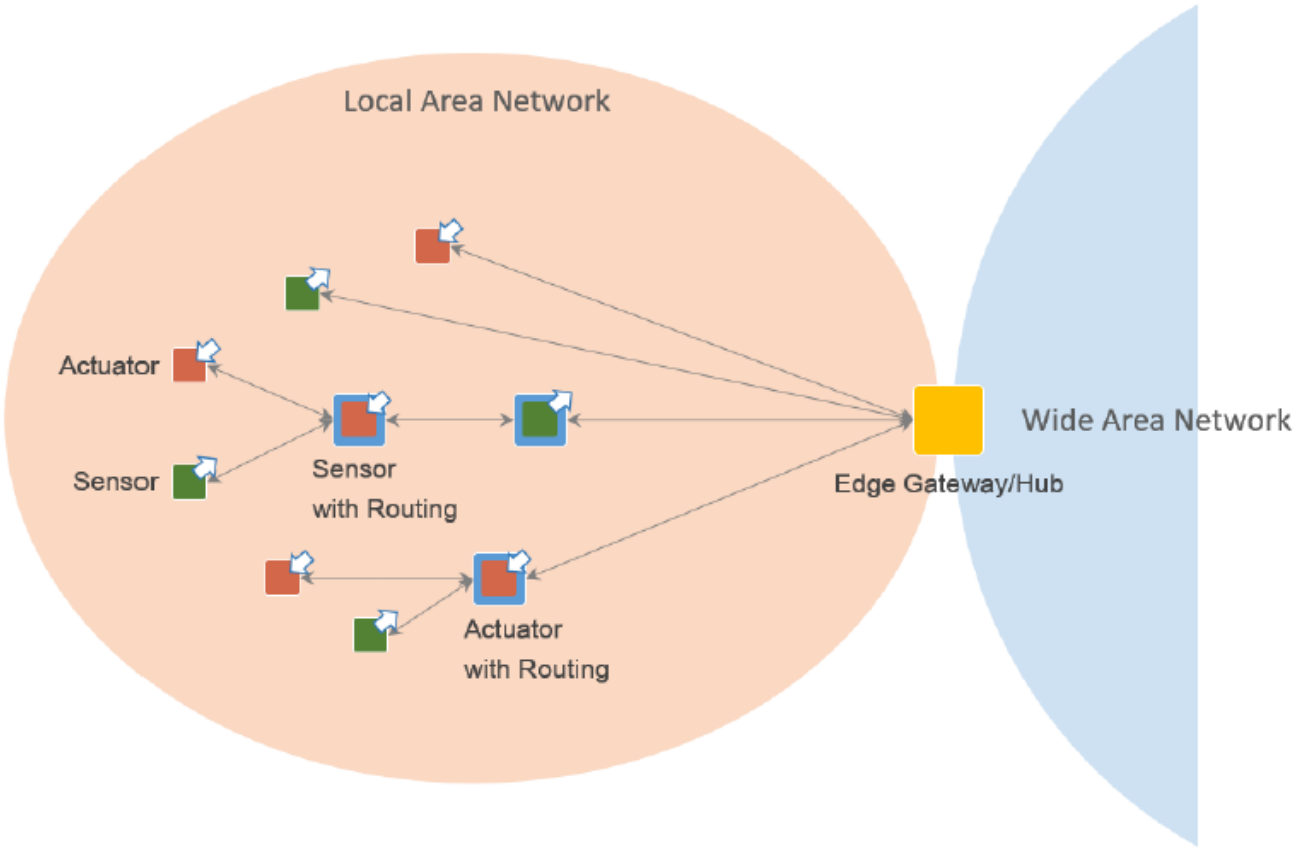


Figure 12 Gateway-Mediated Edge Connectivity and Management Pattern

The local network can be arranged according to different topologies:

- the *hub-and-spoke* topology: in this case the edge nodes are connected to each other through the gateway, which has a direct connection with the managed edge nodes, and the capability to interact with the platform tier conveying in-flow data and out-flow control;
- The *mesh network* topology: in this case some of the edge nodes have routing capabilities, and therefore the routing paths between edge and to the gateway may change dynamically. This topology is best suited to provide broad area coverage for low-power and low-data rate applications on resource-constrained devices that are geographically distributed.

In both topologies the edge nodes are not directly accessible from the wide area network, but they can be reached through the gateway, acting as an endpoint for the wide area network by providing, for example routing and address translation. In this scenario, the gateway provides:

- *Local IoT connectivity* through wired serial buses and short-range wireless protocols. New communication technologies are continuously emerging in new deployments.
- *Network and protocol bridging* supporting various data transfer modes between the edge nodes and the wide area network: asynchronous, streaming, event-based and store-and-forward.
- *Local data processing* including aggregation, transformation, filtering, consolidation and analytics.
- *Device and asset control and management functionalities* to manage the edge nodes locally and via the wide area network.
- *Site-specific decision and application logic* relevant within the local scope.

The described patterns, conveniently developed and adapted, can certainly provide a solid framework to guide the definition of an IoT architecture for the ICONET PI infrastructure, which takes into account the specific features and challenges of the PI scenario. In this respect, the specifications that mostly impact the design of a PI-tailored IoT architecture are the modularity (AR_04) and the IoT network pervasivity (AR_06). Indeed, following the PI approach, goods are expected to be encapsulated in modular "physical packets", ranging from cargo containers to parcels (following what elicited in the technical requirements AR_04 and AR_05). Since PI aims at the tracking/routing and the monitoring of each packet, it has to be equipped by modular IoT devices, that has to interoperate (IT01 and IT02) with several and/or different open (IT05) and pervasive IoT networks.
Moreover,"physical packets" can therefore be "encapsulated" into bigger "physical packets" (e.g., a set of parcels can be encapsulated into containers) and composed with other "physical packets" (e.g., containers in a train, a boat, …). Thus, the physical packets' modularity allows them to better complement each other, enabling this way a more efficient use of the transport means and in general a standardized and streamlined management. In this scenario, the cornerstone of an IoT-enabled PI infrastructure is the "Smart Physical Packet" (SPP). An SPP is a connected "physical packet" equipped with sensors. In fact, each SPP is expected to gather information about its own state, and communicate that to the remote management PI platform, exploiting pervasive IoT network, shaped with the architecture described in Sec. 7.2.
Finally, the system has to provide the complete and real-time visibility of the supply chain (AR_01 and AR_02), thus exploiting a set of available and pervasive (AR_06) networks to interoperate with the remote IoT Cloud platform (IT01 and IT02). In this scenario, the following actions must be required:

1. Multiple network connectors to exploit as better as possible the available connectivity. As far as possible, each SSP must have the possibility to communicate with local IoT network environment (as suggested by DSCA[1]), as well as exploits the mobile connectivity (i.e., GPRS, NB-IoT, LTE CAT-M[2]), when the former is missing. In this scenario, an **opportunistic routing** approach is required enabling the selection of the most convenient network to reach the Cloud platform. In this manner, to maintain the real-time dispatchment requirement is satisfied as well as the cost reduction in terms of mobile traffic and maintenance minimisation (i.e. select the protocol that guarantee the minimum battery consumption – IG_02).
2. A **pervasive, open, scalable, and interoperable infrastructure** capable to implement a horizontal and vertical cooperation between devices by different producers (IG_04).
3. In case of no connectivity (e.g., in the middle of the sea), **a buffer must be available** to store the collected data thus allowing the dispatchment, when the communication is possible (AR_08).

7.2 The IoT architecture for PI

To provide connectivity to each SPP, the IoT architecture previously proposed is inadequate. As discussed previously, the pervasive, open, scalable, and interoperable infrastructure IoT ecosystem must be able to:

1. Automatically monitor the presence of the "encapsulated" SPP.

[1] DSCA envision to define a common framework to implement digitalization in logistics "*focusing on defining the properties of IoT devices mounted on the container and gateways in terminals, warehouses and vessels*" (DSCA - Digital Container Shipping Association, s.d.).
[2] Though the LTE CAT-M and the NB-IoT are designed to satisfy the low consumption issues of the IoT, their consumption is much more expensive with respect to the 2.4GHz protocols as (IEEE802.15.4 and IEEE802.15.1 – BLE).

2. Automatically monitor status of the "encapsulated" SPP. As matter of example, considering the groupage of wine pallet, a distributed bump analysis could be required to monitor the possibility of breakages, thus understanding the liability.
3. Automatically monitor the position and status of the container itself (e.g., predictive maintenance for reefers, the status of its seal, …).
4. Dynamically and automatically adapt its behaviour according to the evolving surrounding environments. In fact, the SSP may be "encapsulated" in a connected mean, and it may interact with other third parties and interoperable SCs' gateways.
5. Identify the most optimised path to follow, to send data toward the PI platform. In more details, the SC gateway can be able to reach the remote platform directly, but also route its data cooperating in a hierarchical ecosystem of IoT devices.

Generally, considering a hierarchy of SPP (as depicted in Figure 13), opportunistic networks must be considered to enable optimised information dispatchment toward the remote IoT platform, or eventually locally toward local operators (e.g., using mobile apps).

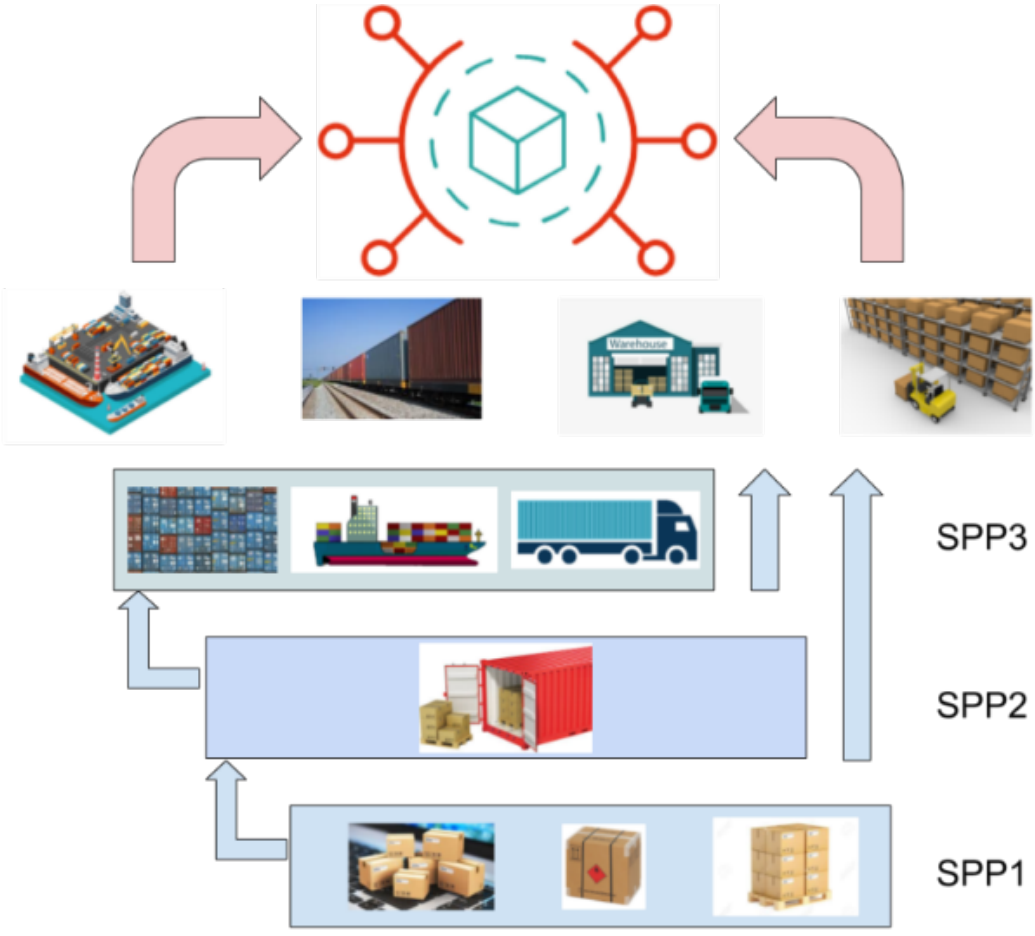


Figure 13 Hierarchy of SPPs

To simplify the reasoning toward the definition of the final and proposed IoT architecture for PI environments, we start from a specific type of SPP, that we consider as the main brick of an intermodal approach as PI: the "Smart Container" (SC). The SC is a container capable to communicate remotely information about itself (position at certain time) but also information about the "encapsulated" SPPs. In this scenario, it will be equipped by a

battery powered device (called smart router), capable to collect by itself several measurements (gathered by on-board sensors, as GPS, temperature, bump), as well as it must provide:

1. The connectivity to the encapsulated SSPs (encapsulated goods cannot communicate outside the container made by metal, that does not allow the propagation of wireless signals - Faraday cage).
2. The in-container connectivity to internal IoT sensors node capable to measure added value data (e.g., gas concentration).
3. The connectivity to external IoT sensors node capable to measure added value data (e.g., predictive maintenance solutions for reefers or the smart-seal status).

Finally, smart router must be able to dynamically set-up optimised communications toward the remote Cloud platform. In fact, the smart router will be able to set-up reliable opportunistic networks to deliver remotely the collected information, thus optimising a set of cost functions. As matter of example, it can select the interoperable low-power communication path (see ANNEX III) made available by gateways installed in terminals, warehouses, vessels, trains and trucks (DSCA - Digital Container Shipping Association, s.d.), going in the direction of reducing the maintenance costs (in line with the business requirement MCR_03, see Sec. 4).

In the meantime, the encapsulated SSP, when downloaded by the SC, must set-up reliable opportunistic networks communications toward the remote Cloud platform, for example exploiting the interoperable network of the new higher-level encapsulation SSP (e.g., a warehouse where it is stored).

In this direction, it is necessary to consider a *recursive version of the gateway-mediated edge connectivity and management pattern* (see Figure 14). In such kind of architecture every single local area network, can contain and be contained by an arbitrary number of local area networks, resulting in IoT systems shaped as network of networks, as depicted in Figure 15). To support this architecture, the hierarchy of devices, depicted in Figure 16, has to be in charge of monitoring the hierarchy of SPPs of Figure 13. These devices must self-organize themself in properly arranged networks by providing all the interoperability and security functionalities required by such heterogeneous and challenging scenario (Francesco Marino, 2019).

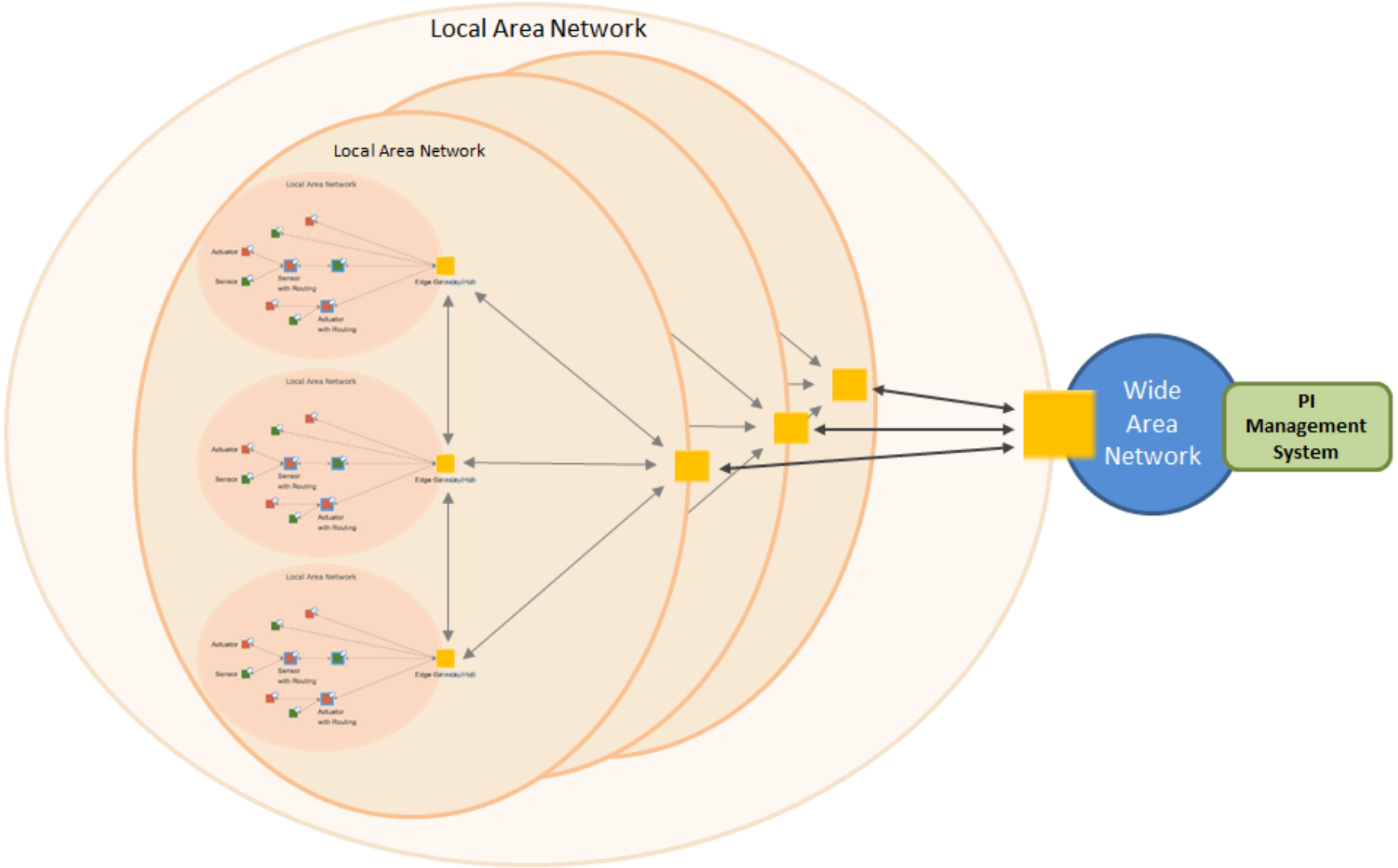


Figure 14 Recursive Gateway-Mediated Edge Connectivity and Management Pattern

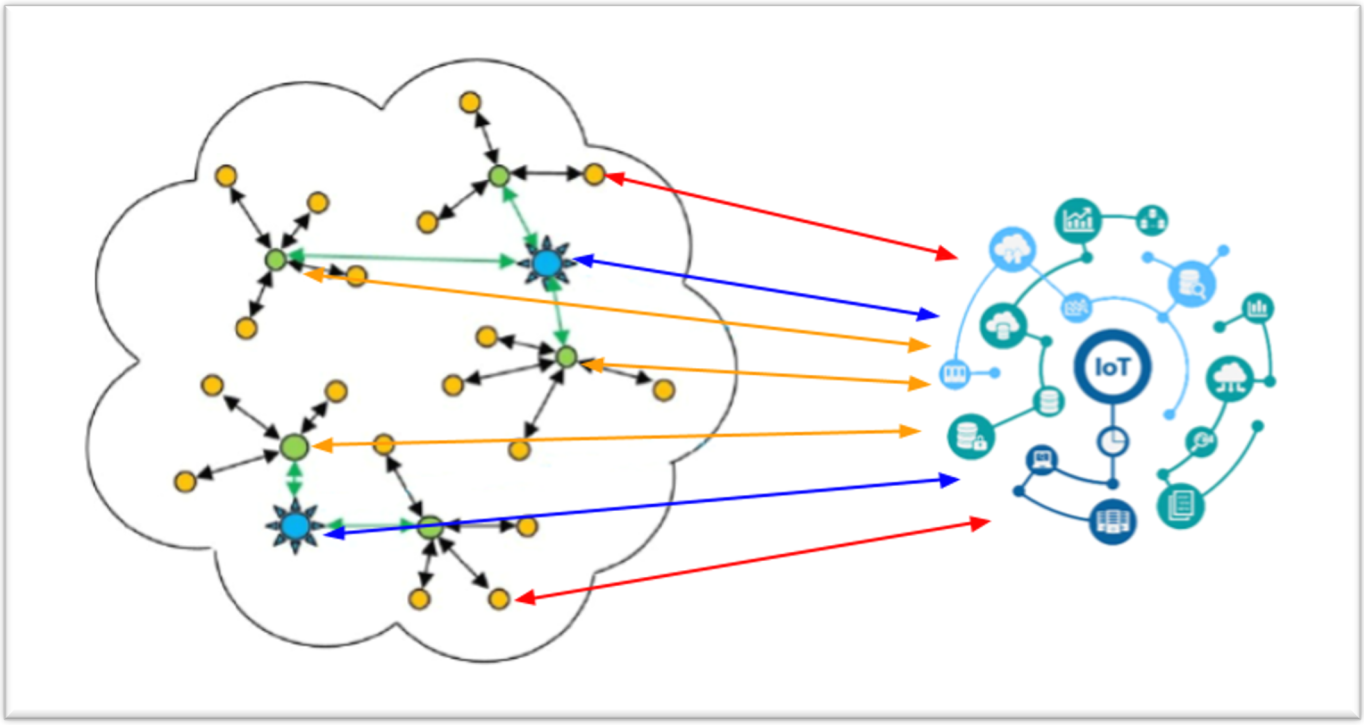


Figure 15 The IoT network of network architecture

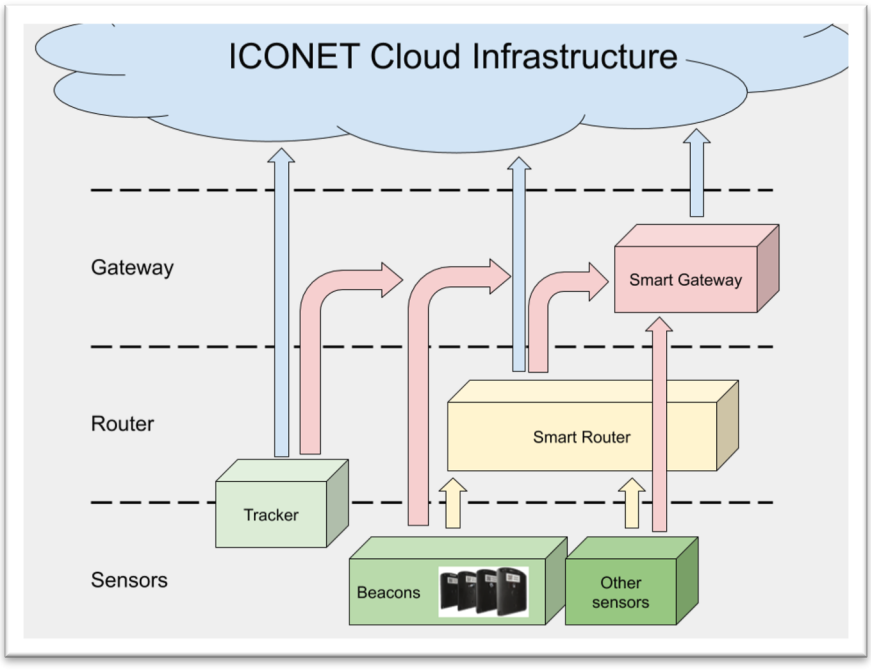


Figure 16 A hierarchy of devices

7.3 The ICONET LLs high level technical specifications

In the ICONET project 4 different LLs will be realised and deployed to demonstrate the first attempts on implementing the PI. In this section the contributions provided by IoT to support the PI realisation are analysed in detail for each LL by describing possible applicative scenarios and eliciting high level technical specifications for each of these.

To define the technical specification, we consider a simplified template with respect the one for the requirements, as depicted in the following table.

Table 17 High level technical specifications template

Spec. ID	Spec. Name	Spec. description	Priority	Dependency

In the following, all the definitions of the fields of Table 17 are provided:

1. Spec. ID: this field represents the unique ID assigned to each requirement. The technical specifications' ID will be differentiated from the other by considering the prefix "LLx" (where "x" is the identified of the LL), thus being shaped as following: LLx_<ID> (where ID is an incremental number).
2. Spec. Name: this field represents the specification name.
3. Spec. description: in this field a short description of the requirement is provided.
4. Priority: the proposed prioritisation process considers the MoSCoW methodology (Clegg & Barker, 1994), that defines the following five levels:
    a. **Must have**: Requirements labelled as "Must" are critical to reach the objective of the project.
    b. **Should have**: Requirements labelled as "Should" are important but not necessary for the success of the project.
    c. **Could have**: Requirements labelled as "Could" are desirable but not necessary.
    d. **Wish have**: Requirements labelled as "Wish" have been agreed by stakeholders as the least-critical, lowest-payback items, or not appropriate at that time.
5. Dependency: defines the dependency of the from the technical requirements.

7.3.1 IoT within LL1 – PI Hub-centric Network

ICONET's PI Hub-centric UC, is designed based on the requirements of the Port of ANTWERP (PoA), with primary target to validate PI concepts in the versatile and complex transport network composed by a considerable number of terminals and links. The central goal is better coordination of this network with the underlying connectivity infrastructures, providing near real-time visibility to the logistics and transportation operations for all involved stakeholders. In fact, in most cases, Port Authorities (managing this kinds of PI Hubs) have no control on the logistics vehicles/PI means/SPP (e.g., trains, trucks, ships) moving within its land-side, despite the fact that they also need to identify and track those PI means in order to improve the efficiency of the overall port infrastructure (both in the ground side and the sea side). Table 9 addresses the high-level technical specifications for the realisation of PI Hub-centric Networks. In Table 18 the high level technical specifications' list for the realisation of the IoT environment within LL1 are summarized.

Table 18 LL1 high level technical specifications

Spec. ID	Spec. Name	Spec. description	Priority	Dependency
LL1_S01	**Logistics vehicles and asset monitoring**	The system has to be able to monitor the vehicle entering/exiting and moving within the hub (i.e., seaport landside). The integration of such a system has to be easy as well as its maintenance.	**Must**	**AR_01, AR_02, AR_05, AR_06, IT_01, IT_02, IT_04, IT_05, IG_02, IG_04**

LL1_S02	**Geo&time-reference and remote communication**	The collected information by the system has to be completed with information regarding the position and the time, thus allowing the logistics vehicles' tracking service. The information gathered must be dispatched remotely toward a data persistence platform exploiting an open pervasive and plug&play IoT network installed as a service.	**Must**	**AR_01, AR_03, AR_06, IT_04, IT_05**
LL1_S03	**Remote data persistence platform with secure and ad-hoc access**	The data gathered by the IoT devices in the field must be stored in a platform located in a remote server/Cloud. The access to these data as to be allowed only to the proper users in a secure manner.	**Must**	**IG_01, IG_03, IG_05, IG_06**
LL1_S04	**Interoperable data sharing**	An interoperable (technical and syntactical) interoperability) data sharing service has to be provided to establish a connection with the final users	**Must**	**IT_01, IT_02, IT_03, IG_01, IG_04, IG_05**

In this scenario, two approaches can be followed:

1. **Exteroceptive approach**: vehicle identification using a Smart Camera device that embeds a dedicated OCR algorithm capable to recognize the IDs on the PI means (e.g., locomotives, wagons, trucks, containers, etc.). This solution is less invasive (it has not to be installed in the stakeholder vehicles), but it needs to be installed properly and the line-of-sight must be guaranteed. Since the devices has to be installed only in the infrastructure, these can be considered as supplied from the fixed power network. The exteroceptive approach architecture is depicted in Figure 17.
2. **Proprioceptive approach**: each vehicle has to be equipped with a (affordable) devices (i.e., RFID tag or battery powered BLE beacon) deployed on the PI means (e.g., locomotives, wagons, trucks, containers, etc.). This approach is more invasive (i.e., the device has to be installed on the PI means, thus requiring the authorisation of the involved stakeholder), but it required less installation constraints. In this scenario, while devices must be energy autonomous (passive or battery powered), the gateway has to be supplied from the fixed power network. The proprioceptive approach architecture is depicted in Figure 18.

Both the approaches will communicate toward the remote Cloud IoT platform, in charge of implementing data persistence services and to manage secure and ad-hoc accesses to the users.

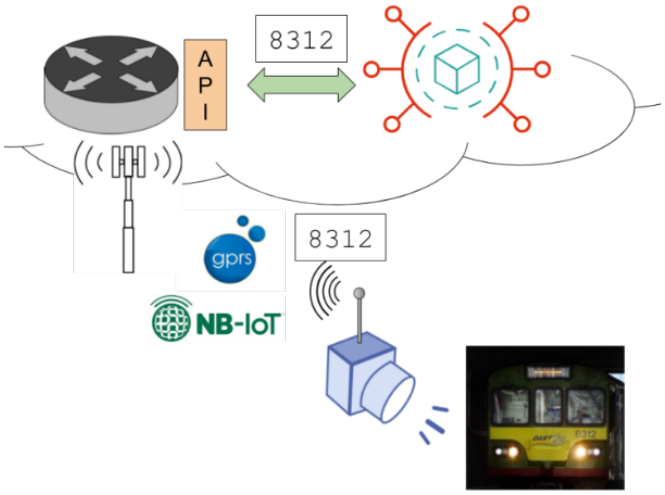


Figure 17 Exteroceptive approach

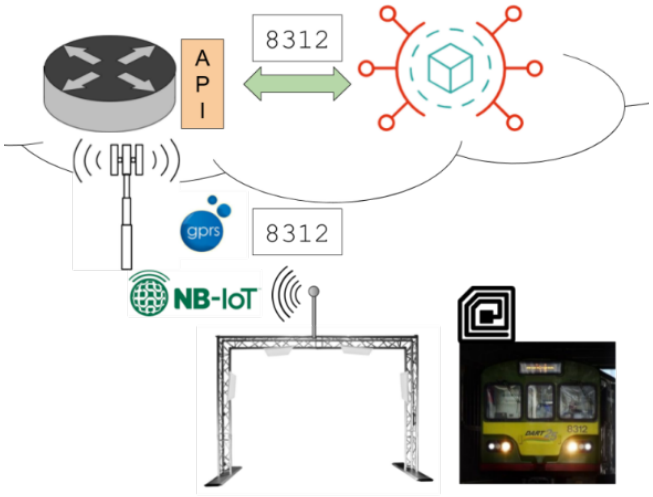


Figure 18 Proprioceptive approach

7.3.2 IoT within LL2 – Corridor-centric PI Network

LL2 aims at the implementation of IoT solutions for transforming typical transport corridors into PI corridors, enhancing the reliability of intermodal connections, thus implementing the so called "synchromodality". The implementation of synchromodal logistics transaction will allow decision-making regarding delays, pulling forward loads and modal shift. LL2 will implement a fully interoperable IoT-enabled synchromodal corridor and it will be tested along the two corridors depicted in Figure 19 and Figure 20.

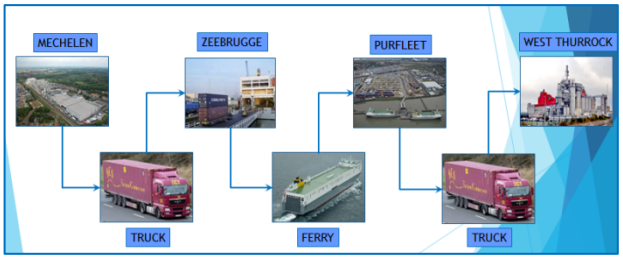


Figure 19 Corridor Mechelen (B) – West Thurrock (UK)

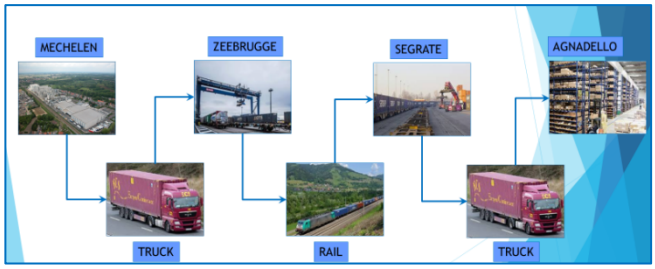


Figure 20 Corridor Mechelen (B) – Agnadello (I)

In Table 19 the high level technical specifications' list to implement an IoT-enabled synchromodal corridor within LL2 are summarized.

Table 19 LL2 high level technical specifications

Spec. ID	Spec. Name	Spec. description	Priority	Dependency
LL2_S01	**Geo&time-reference and remote communication**	Implementing synchromodality means firstly having continuously the knowledge where the goods are and when. The SC has to enable an interoperable communication toward the remote IoT platform.	**Must**	**AR_01, AR_03, AR_06, IT_04, IT_05**
LL2_S02	**Internal and external IoT connectivity**	The SC must enable internal and external connectivity to implement added value and distributed monitoring functionalities.	**Should**	**AR_03, AR_04, AR_05, AR_06**
LL2_S03	**Non-invasive goods monitoring**	The monitoring of the goods has to be done using non-invasive devices, deployed together with the goods. Thus, these have to communicate wireless toward a remote IoT	**Should**	**AR_01, AR_02, AR_03, AR_04, AR_05, AR_06,**

		platform exploiting the interoperable connectivity provided by the IoT enabled SC.		**IT_01, IT_02, IT_04, IT_05, IG_01, IG_02, IG_04**
LL2_S04	**Edge computation and storage**	The IoT devices must implement edge computing operations, as, for example, to understand asynchronous events (e.g., bump), or to store data in case of lacking remote communication.	**Must**	**AR_07, AR_08**
LL2_S05	**Battery powered**	Usually in the container world, the direct power supply is not available. Thus, the device to enable LL2 are installed in the containers must be energy autonomous. The battery duration has to be maximised, thus reducing the human intervention in the battery management (i.e., substitution or recharge).	**Must**	**IG_02**
LL2_S06	**Anti-tampering**	Implementing solution capable to notify the status of the containers' locks (i.e., not used, closed, broken). This solution must be integrated with the container IoT connectivity.	**Wish**	**IG_02**
LL2_S07	**Remote data persistence platform with secure and ad-hoc access**	The data gathered by the IoT devices in the field must be stored in a platform located in a remote server/Cloud. The access to these data as to be allowed only to the proper users in a secure manner.	**Must**	**IG_01, IG_03, IG_05, IG_06**
LL2_S08	**Interoperable data sharing**	An interoperable (technical and syntactical) interoperability) data sharing service must be provided to establish a connection with the final users.	**Must**	**IT_01, IT_02, IT_03, IG_01, IG_04, IG_05**

In this LL, one of the main bricks of the intermodal IoT-enabled PI environment will be implemented: the Smart Container (SC). A SC is the SPP that can be mapped physically on a connected (physical) container, as depicted in Figure 21. Particularly, a SC has enabled:

1. An internal (and, sometimes, external, e.g., anti-tampering seal sensor) IoT network for implementing data collection from the sensors deployed within the (physical) container and on the goods.
2. An interoperable remote communication, to dispatch the data remotely toward the remote Cloud IoT platform, in charge of implementing data persistence services and to manage secure and ad-hoc accesses to the users.

The main functionalities of the SC are the following:

1. Acquire information about position and time (answering to the questions: where? and when?), supporting the PI reliability issues.
2. Inspect the status of the goods they encapsulate (answering to the question: how?).
3. Exchange information with other containers (e.g., encapsulated in the same transport mean), and establish opportunistic networks to reach the remote Cloud IoT platform (e.g., for reducing the power consumption).
4. Send the gathered data, tagged with a geo&time-reference, to the remote PI management Cloud platform.

Finally, the architecture of the SC is depicted in Figure 22.

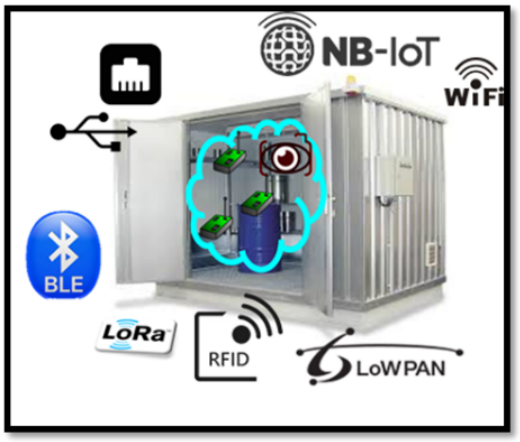


Figure 21 The smart container

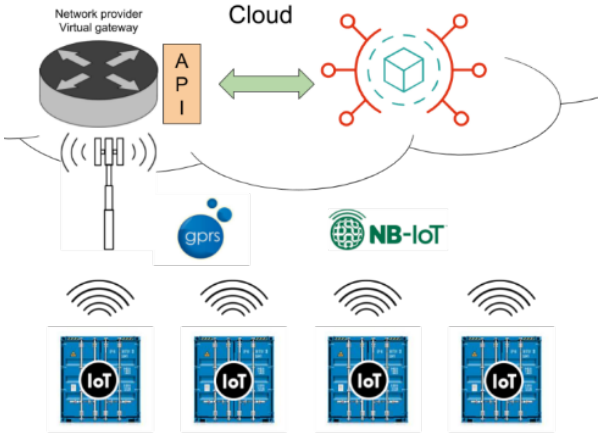


Figure 22 Smart Container IoT Architecture

7.3.3 IoT within LL4 - Warehousing as a service

LL4 is designed to investigate the potential of e-Warehousing as a key enabler of the PI concept, envisioning a warehouse in a multi-client perspective, where its plots are shared and organized to satisfy the needs of different stakeholders. The high-level technical specifications for LL4 are listed in Table 20.

Table 20 LL4 high level technical specifications

Spec. ID	Spec. Name	Spec. description	Priority	Dependency
LL4_S01	**Goods' and assets' monitoring and real-time inventory services**	Monitoring the goods status (e.g. temperature in case of perishable goods), implementing a real-time inventory service, maybe interoperable with the same approaches defined in LL2.	**Must**	**AR_02, IT_05, IG_01, IG_04**
LL4_S02	**Position and time reference**	To tag the collected information area within the hubs are located the goods at certain time, or when and where and event has happened.	**Could**	**AR_01**
LL4_S03	**Pervasive IoT connectivity**	A pervasive IoT environment must be deployed to enable the distributed data collection.	**Must**	**AR_03, AR_04, AR_05, AR_06**
LL4_S04	**Improved technical and syntactical interoperability at the IoT network layer**	Multi-MAC gateways have to be integrated ease the integration of different IoT nodes with different measuring purposes. This selection can simplify the selection of IoT devices available in the market.	**Must**	**IT_01, IT_02, IT_03, IT_04, IT_05**
LL4_S05	**Non-invasive sensor nodes**	All the sensor nodes must be wireless and power independent (battery supplied or passive), thus simplify their installation and relocation.	**Must**	**IG_02**
LL4_S06	**Interoperable remote communication**	An interoperable (technical and syntactical interoperability) remote communication has to be provided to establish a connection with remote Cloud platform	**Must**	**IT_01, IT_02, IT_03, IG_01**
LL4_S07	**Remote data persistence platform with secure and ad-hoc access**	The data gathered by the IoT devices in the field must be stored in a platform located in a remote server/Cloud. The access to these data as to be allowed only to the proper users in a secure manner.	**Must**	**IG_01, IG_03, IG_05, IG_06**

LL4_S08	**Interoperable data sharing**	An interoperable (technical and syntactical) interoperability) data sharing service has to be provided to establish a connection with the final users	**Must**	**IT_01, IT_02, IT_03, IG_01, IG_04, IG_05**

The main task in this LL is to deploy a pervasive and multi-protocol IoT network capable to collect information regarding the inventory, the conditions of certain goods (e.g., perishable goods as food), as well as integrating devices in charge of monitoring the status of assets (e.g., shelfs). In this scenario, we propose to implement a scenario as depicted in Figure 23, thus capable to take care regarding the following services:

Figure 23 LL4 architecture

1. To monitor the presence (real-time inventories), the quantities and the position of the goods. In this manner, the status of the stocks can be made available to all the actors involved, thus providing real-time adding value information regarding the stock's levels, and the warehouse occupation level.
2. To enable interoperable services with other LLs, exploiting interoperable protocols. In this scenario, the container arrived in a certain warehouse can communicate exploiting the available IoT connectivity, thus notifying its encapsulation in the considered hub. The same for the lower level SSPs, that can seamlessly associate themselves with the interoperable warehouse IoT connectivity in a seamless manner.
3. To monitor the status of sensitive goods (e.g., perishable food) with added value sensor, capable to provide ubiquitous monitoring of the warehouses. Special area can install special sensors to monitor measurements for certain goods (e.g., ethylene monitoring where fruit is stored).

7.3.4 IoT within LL3 - e-Commerce centric PI Network

LL3 aims at implementing the PI principles in Fulfilment of e-Commerce Purchase Orders optimisation, realising a consumer driven approach. In this scenario, the IoT environment to be deployed within the considered hubs (either central warehouses, desk-stores, or convenient-stores) to implement the same functionalities described for the LL4, as well as in the transport means when the goods are moved from a warehouse to another or toward the final client.

The table in the following shares the subset of requirements related to the warehouses' monitoring with LL4 (until LL3_08) but introduce a set of specifications related to the goods movement and dispatchment (from LL3_09). Particularly, the monitoring of the assets used for the e-commerce (e.g., reusable baskets) and of the status of perishable goods is highlighted.

Table 21 LL3 high level technical specifications

Spec. ID	Spec. Name	Spec. description	Priority	Dependency
LL3_S1	**Goods' and assets' monitoring and real-time**	Monitoring the goods status (e.g. temperature in case of perishable goods), implementing a real-time inventory service, maybe interoperable with the same approaches defined in LL2.	**Must**	**AR_02, IT_05, IG_01, IG_04**

	inventory services			
LL3_S2	**Position and time reference**	To tag the collected information area within the hubs are located the goods at certain time, or when and where and event has happened.	**Could**	**AR_01**
LL3_S3	**Pervasive IoT connectivity**	A pervasive IoT environment must be deployed to enable the distributed data collection.	**Must**	**AR_03, AR_04, AR_05, AR_06**
LL3_S4	**Improved technical and syntactical interoperability at the IoT network layer**	Multi-MAC gateways must be integrated ease the integration of different IoT nodes with different measuring purposes. This selection can simplify the selection of IoT devices available in the market.	**Must**	**IT_01, IT_02, IT_03, IT_04, IT_05**
LL3_S5	**Non-invasive sensor nodes**	All the sensor nodes have to be wireless and power independent (battery supplied or passive), thus simplify their installation and relocation.	**Must**	**IG_02**
LL3_S6	**Interoperable remote communication**	An interoperable (technical and syntactical interoperability) remote communication has to be provided to establish a connection with remote Cloud platform	**Must**	**IT_01, IT_02, IT_03, IG_01**
LL3_S7	**Remote data persistence platform with secure and ad-hoc access**	The data gathered by the IoT devices in the field must be stored in a platform located in a remote server/Cloud. The access to these data as to be allowed only to the proper users in a secure manner.	**Must**	**IG_01, IG_03, IG_05, IG_06**
LL3_S8	**Interoperable data sharing**	An interoperable (technical and syntactical) interoperability) data sharing service has to be provided to establish a connection with the final users	**Must**	**IT_01, IT_02, IT_03, IG_01, IG_04, IG_05**
LL3_09	**Logistics vehicles and asset monitoring**	The vehicles involved in the goods' supply chain must be monitored (i.e., wheels pressure), as well as the assets encapsulated (e.g., pallets, baskets). This means that each vehicle must enable an interoperable IoT network.	**Must**	**AR_01, AR_02, AR_05, AR_06, IT_01, IT_02, IT_04, IT_05, IG_02, IG_04**
LL3_10	**Geo&time-reference and remote communication**	Implementing synchromodality means firstly having continuously the knowledge where the goods are and when. In this scenario, a track&trace service for the vehicles and the connected goods/assets.	**Must**	**AR_01, AR_03, AR_06, IT_04, IT_05**
LL3_11	**Non-invasive goods monitoring**	The monitoring of the goods has to be done using non-invasive devices, deployed together with the goods. Thus, these have to communicate wireless toward a remote IoT platform exploiting the interoperable connectivity provided by the IoT enabled vehicles.	**Should**	**AR_01, AR_02, AR_03, AR_04, AR_05, AR_06, IT_01, IT_02, IT_04, IT_05, IG_01, IG_02, IG_04**
LL3_12	**Edge computation and storage**	The IoT devices must implement edge computing operations, as, for example, to understand asynchronous events (e.g., bump or goods loading/unloading), or to store data in case of lacking remote communication.	**Must**	**AR_07, AR_08**

LL3_13	**Cold chain monitoring**	Monitoring of the temperature of preserving the food all along the e-commerce dispatchment chain.		**AR_07, AR_08**

The main task in this LL is to deploy a pervasive and multi-protocol IoT network capable to collect information regarding the presence and the status of the goods, as well as the assets and the vehicles all along the e-commerce chain (i.e., between hubs or toward the final customer). The considerations regarding the warehouses can be assimilated to the one of LL4 (see Sec. 7.3.3).
In this scenario, we propose to improve the LL4 considerations introducing:

1. Added value sensors to monitor the condition of perishable goods, for example implementing the complete visibility of the cold chain.
2. Added value service to monitoring the evolution of the dispatchment process: for example, understanding when the track door is open or closed (in the vision of the cold chain monitoring), or when the goods are uploaded/downloaded.
3. Added value service for assets' monitoring and tracking&tracing, especially regarding the reusable smart shopping baskets suggested in D4.6 (Balden, 2020).

7.3.5 Technical details

7.3.5.1 IoT environment interoperability

In general, an IoT architecture can consist of sensor nodes, IoT gateway, cloud server, and application. In order to achieve semantic interoperability, there must exist preferably a common ontology/dictionary required to be synchronized between different systems. Therefore, the ontology/dictionary should be enabled at higher levels than the IoT interfaces. In this scenario, NGS aims at addressing realisation of level 2 interoperability patterns, as defined in the requirements and as depicted in Figure 24.

The main actors to reach those objectives are the smart gateway and smart router side**,** that are in charge of implementing both the technical and the syntactic level interoperability for the connections between sensor nodes and the IoT gateway, and between the IoT gateway and the cloud server. To reach the mentioned objective, NGS will provide the smart gateway and the smart router capable of communicating with a variety of technologies in the market, capable to implement the technical interoperability with the sensors and toward the Cloud (see Sec. 7.3.5.2). In addition, the devices will implement their communication with the remote Cloud/server platforms exploiting standard data structures, implementing a syntactic interoperability pattern (see Sec. 7.3.5.3).

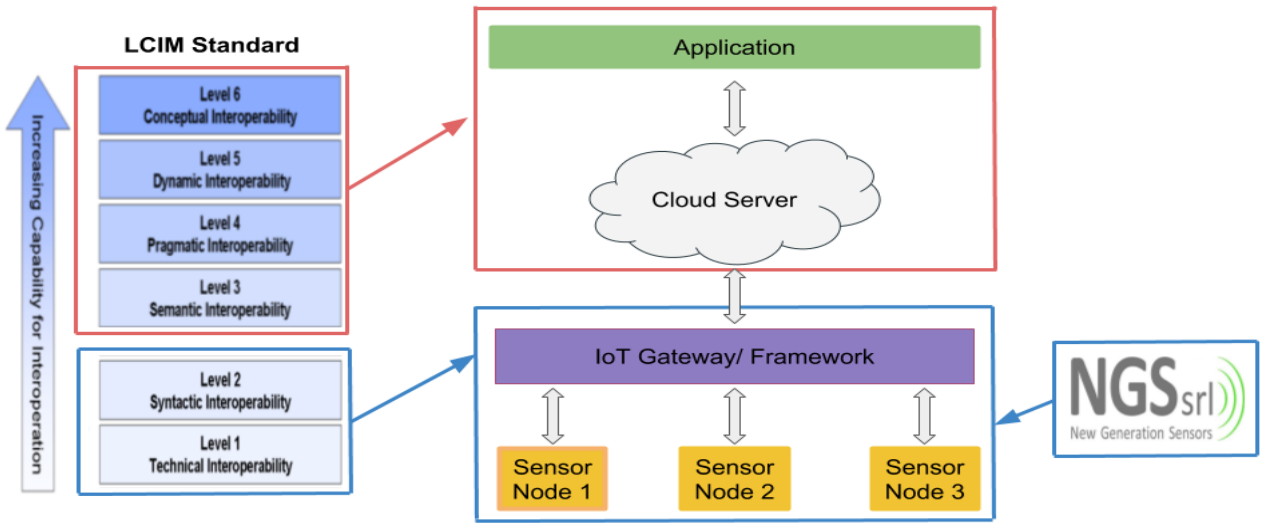


Figure 24: Reaching the Interoperability Level 2

7.3.5.2 Interoperability at the IoT network side

Technical (level 1) and syntactic (level 2) interoperability is guaranteed by the exploitation of several protocols in both the smart router and the smart gateway: in Table 22 the list of protocols managed by them. As it is possible to see in the following list, we have preferred to select standard protocols, while in the smart router we have integrated also a LoRaWAN concentrator to cover large environments as logistics hubs.
Since the popularity of these protocols several sensor nodes' solutions are already available on the market, thus simplifying the exploitation of the IoT technology in the logistics domain.

Table 22 interoperability level 1 and level 2 at the IoT network side

Device name	Level 1 Interoperability	Level 2 Interoperability
Smart router	Bluetooth 5 (IEEE 802.15.1)	Eddystone and iBeacon
	6LoWPAN+CoAP over IEEE 802.15.4	JSON
Smart gateway	Bluetooth 5 (IEEE 802.15.1)	Eddystone and iBeacon
	6LoWPAN+CoAP over IEEE 802.15.4)	JSON
	LoRaWAN	JSON

The cross-platform design pattern is considered for implementing both the technical and syntactic interoperability at the IoT network side following the guidelines of the flagship EU project called AGILE (an

Adaptive & Modular Gateway for the IoT)[3], that we consider as reference for the smart gateway software platform implementation.

7.3.5.3 Interoperability with the remote platform

Both technical (level 1) and syntactic (level 2) interoperability is guaranteed by the exploitation of the envisioned smart gateway and smart router, since their capability of managing the most common protocols and representation formats for the internet connection. As in Sec. 7.3.5.2, the selection of standardised protocols is promoted Table 22 shows the list of protocols managed by these devices.

Gateway name	L1 Interoperability	Standardisation	L2 Interoperability	Standardisation
Smart Router	HTTP over NB-IoT/GPRS	IETF – 3GPP	JSON or XML	W3C - IETF
Smart Gateway	HTTP over NB-IoT/GPRS	IETF – 3GPP	JSON or XML	W3C - IETF
	HTTP over Wi-Fi	IETF – IEEE	JSON or XML	W3C - IETF
	HTTP over Ethernet	IETF – IEEE	JSON or XML	W3C - IETF

The cross-platform design pattern is considered for implementing both the technical and syntactic interoperability when Wi-Fi or Ethernet protocols. In fact, in this case the remote Cloud platform can manage different connections based on these protocols and representation formats.

In the case of NB-IoT/GPRS, the technical interoperability is implemented using a Platform-to-Platform pattern. In fact, as depicted in Figure 25, the messages sent exploiting the NB-IoT protocol are managed by the intermediate (virtual gateway) platform owned by the telecom provider. This platform has in charge the dispatchment of the mentioned messages toward the IoT Cloud platform, exploiting the selected protocols. On the other side, the syntactic interoperability is implemented using the cross-platform pattern, since remote Cloud platform can manage different gateways based on the mentioned representation formats.

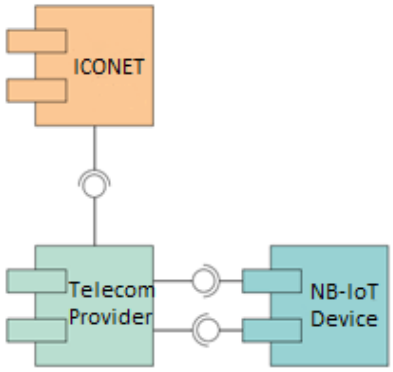


Figure 25 NB-IoT interoperability pattern

7.3.5.4 Considered IoT communication protocols

All the solution proposed by NGS within the ICONET project will be based on the protocols listed in Table 23. These protocols will guarantee the technical interoperability with the sensor nodes deployed in the LLs. This selection is based on the following considerations:

- **Battery consumption**, of the gateway and of the sensors. Since the NB-IoT is part of the 5G network, the gateways for this protocol are not considered.
- **Plug&Play**. This functionality allows the seamless and automatic authentication within an existing IoT network of new compatible components.
- **Scalability**. A scalable system allows to instantiate many IoT components.
- **Standard protocols**. The selection is done considering essentially standard protocols.
- **Coverage**, considering long range protocols (e.g., LoRaWAN), to implement large area network to implement IoT services in large hubs.

[3] http://agile-iot.eu/

Table 23 Considered IoT protocols

Protocol name	Battery consumption		Scalability	Plug&Play	Standard protocol	Coverage
	Sensors	Gateway				
IEEE 802.15.4 and 6LoWPAN+CoAP	Low	Low	High	Yes	Yes (IEEE)	Up to 200m
IEEE 802.15.1	Very low	Low	High	Yes	Yes (IEEE)	Up to 1km
LoRaWAN	Low	Very High	Medium	Yes	No	Up to 16km (LOS)
NB-IoT	Low	-	High	Yes	Yes (3GPP)	-

7.3.5.5 Interaction and data model

One of the considerations when designing the interaction between two endpoints is the way of communication that must be designed to guarantee a seamless and scalable exchange of data. The solution for this is the use of a RESTful API (see ANNEX IV) that specifies how the two endpoints will interact. In this scenario, we will introduce a set of RESTful APIs (http or https) to interoperate with the IoT Cloud platform and with third parties involved in the project, thus exchanging JSON files shaped following certain data-models. Particularly, for the communication of data from the gateways toward the IoT Cloud platform a dynamically structured JSON format message is exchanged implementing an HTTP POST request (see Figure 26).

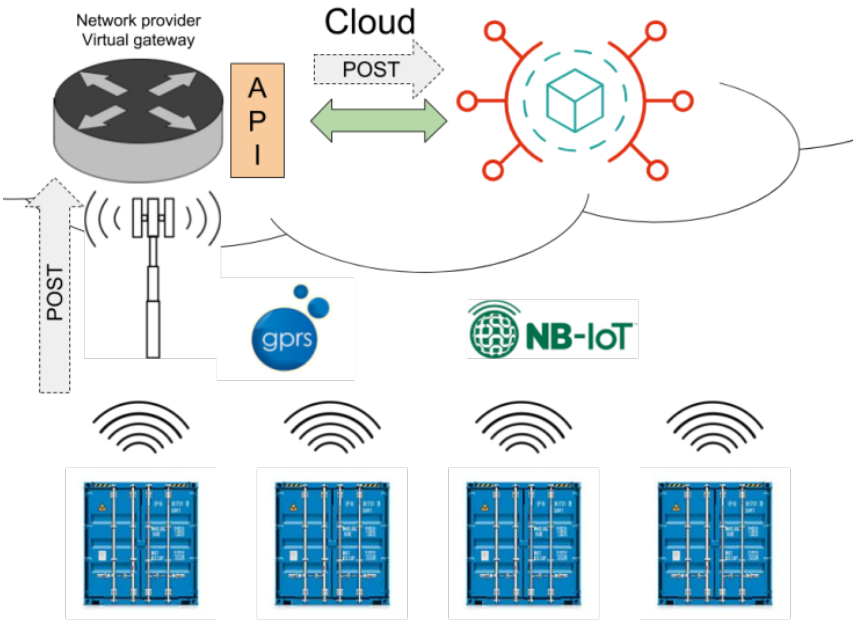


Figure 26 The POST request within the LL2

The JSON data-model will be dynamically built based on the sensor data that it carries (e.g. Temperature, Humidity, Latitude and Longitude, etc.). A preliminary example for structuring the message is shown Figure 27. In this case, the message is separated in two parts:

1. The **mandatory data** (highlighted in yellow in Figure 27) like the id of the sensor device, the timestamp and the position coordinates (where needed, retrieved by the GPS/GLONASS sensor).

2. The **optional part**, which changes based on the installed sensors. On the Cloud side, the endpoint has to appropriately store the data by parsing the JSON array and mapping the key-value pairs.

```
var str = "{"
str+= "device_id": "f8:27:16:90:19:a7:c0:8b",
str+= "timestamp": "2019-03-07 16:20:30",
str+= "lat": "47.644548",
str+= "lon": "-122.326897",
str+= "Content:["
If temperature not empty
        str+= "temperature":"27.08"
str+= "]}"
```

Figure 27 JSON pseudo-code (example for temperature)

7.3.6 The remote IoT platform

The remote IoT platform aims at the management of the data and information dispatched from the different connected IoT devices (i.e., trackers, smart routers, smart gateways), in terms of brokerage (IG_05), storage, visualisation and dispatchment with third parties' platforms (IG_06). It enables a seamless and affordable integration of new devices (IG_01) and allows the exploitation of the tracking and monitoring services (IG_02) by the users, considering a secure and ad-hoc access (IG_03). Figure 28 shows its simplified architecture.

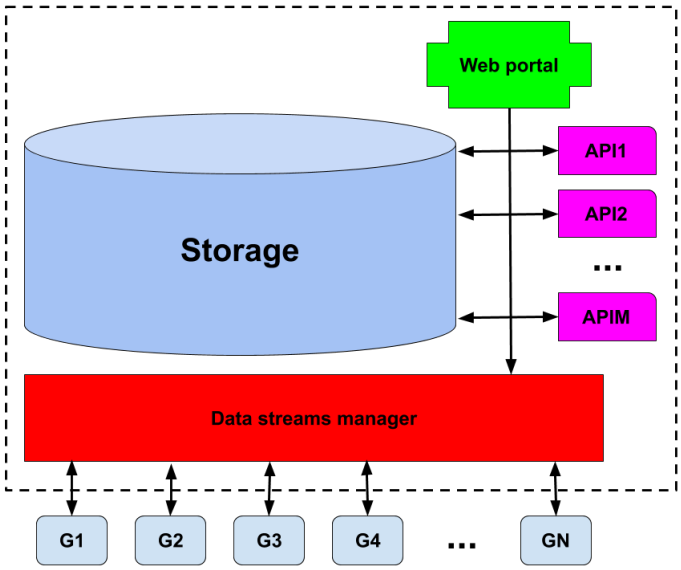


Figure 28 The remote IoT Platform

7.3.7 The considered hardware platforms

To implement the proposed architecture, we consider the exploitation of three types of devices as depicted in Figure 29 and described in the following:

1. **The IoT sensor nodes** Installed inside or outside the container to monitor the goods' presence and conditions, as well as the asset (e.g., predictive maintenance monitoring in the reefers' containers). These nodes must be non-invasive (i.e., wireless and battery-powered) and interoperable with the smart router (described in the following), as well as affordable. Regarding the possibility of implementing real-time inventory within the container, we prefer to consider BLE beacons instead RFID, since the latter has to install on the smart router's high consumption readers, not suitable for battery powered devices.
2. **The tracker.** Battery powered device capable of providing information about the goods position at certain time and added value information gathered by on-board sensors (e.g., about bumps, acceleration, temperature, light, humidity). This solution can be connected toward the remote platform implementing the innovative protocol NB-IoT (or GPRS) based on the 5G network, exploiting standard/interoperable interaction representation protocols (JSON over HTTP). However, it can communicate exploiting other IoT protocols (i.e., BLE and IEEE802.15.4) with higher level gateway.
3. **The smart router**. Battery powered device with the same characteristics of the FLEXX tracker, but it can also manage IoT sensors networks (based on Bluetooth 5 and IEEE802.15.4). It communicates remotely using NB-IoT. This solution is thought to track containers in terms of position and time, but also monitoring internal (e.g., temperature and humidity, bump) and external parameters (e.g., predictive maintenance monitoring in the reefers' containers). Compared with what is written in the original ICONET proposal (FIWARE based device on top of LINUX OS, directly power supplied), the proposed solution must be battery powered. In this scenario the hardware architecture requires modifications, considering low power microcontrollers and extremely low protocols (RFID cannot be considered).
4. **The Smart Gateway**. It is power supplied gateway capable to manage several protocols (LoRaWAN concentrator, Bluetooth, IEEE802.15), and to communicate remotely exploiting Wi-Fi, NB-IoT/GPRS and Ethernet. This solution is thought for the installation within the PI hubs, to provide a heterogeneous connectivity, thus enabling the functionalities of the above described architecture.

Together with the gateways, we propose to base the monitoring exploiting un-expensive commercial sensors node based on BLE beacon technology (example of beacons node are depicted in Figure 29). These solutions can be easily deployed, since their small size and their power autonomy (coin cell battery powered, up to 6-12 months).

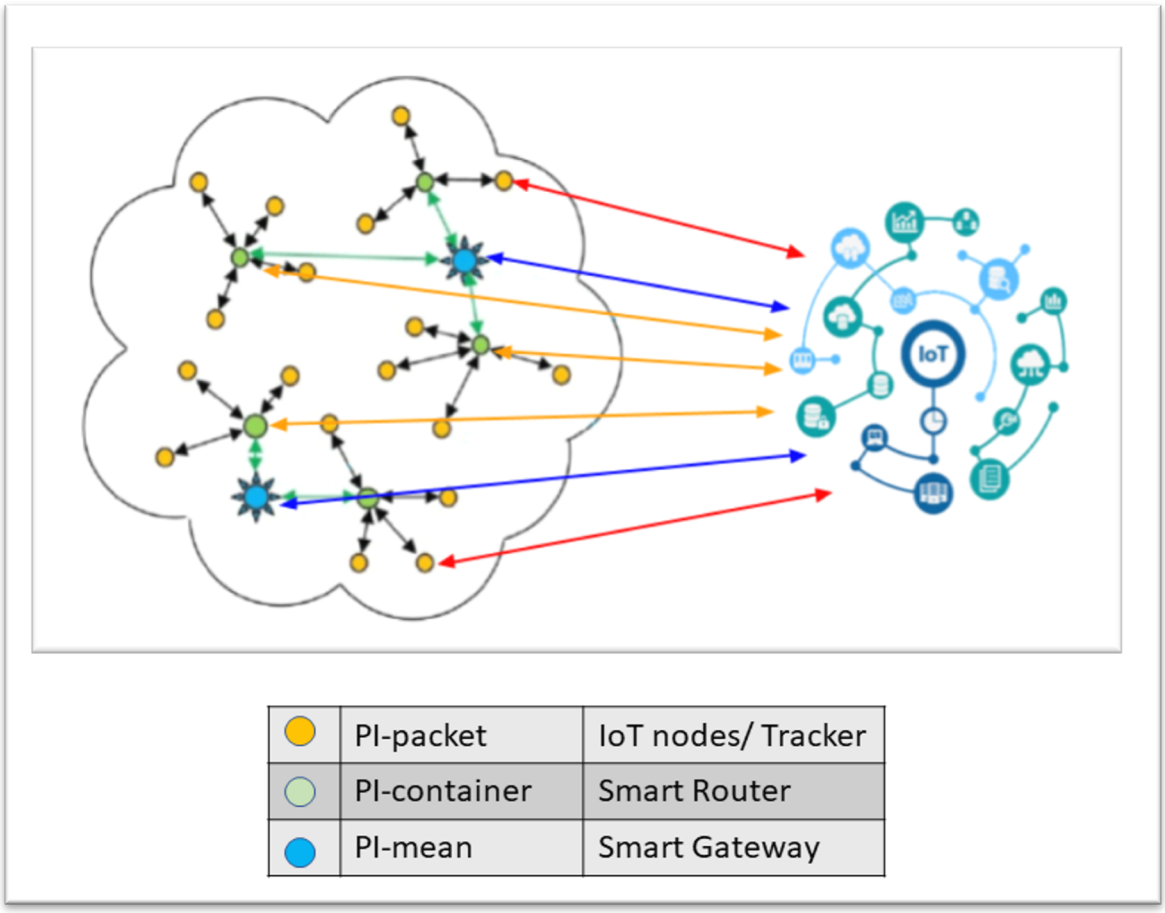


Figure 29 Mapping of the devices on the proposed architecture

8 Innovations

Previous Section (3, 4, and 6) have provided a very detailed review on who is the recipient of the findings of this report, what are those entities' needs and how exactly these needs are mapped to the technical elements of the IoT offering.

The growing demand and complexity of the supply chain processes today in a world characterized by the globalization of trade, prompt to digitization of information by using technology solutions and very much relying on research work like ICONET endeavours. The aim is to improve speed, dynamics, and resiliency of the supply chain operations and this will most probably result in a new way of doing business with customers and a re-engineering of existing processes.

The IoT holds a dominant place in above effort as a solution able to transform the Logistics playfield. It has been shown that, amongst others, key components of the supply chain like the inventory management, fleet routing, resource allocation and capacity design will vastly improve gaining flexibility and through real time visibility of the assets involved in the whole network, substantial tangible benefits will emerge. The innovations discussed above provide the very tool to improve service levels, minimize costs, enhance security and overall control.

This section depicts the technological and business innovation elements introduced by IoT within PI-driven environments. Particularly, it highlights the innovations in the following three domains:

- **IoT Protocols innovation,** exploiting new protocols, standardised in the last years, capable to improve the scalability and the communication range, thus reducing the battery consumption.
- **Architectural innovation**, defining an open and interoperable architecture capable to enable the complete visibility of the supply chain.
- **Business intelligence innovation**, exploiting the edge computing paradigm and interoperable interfaces, thus providing information both remotely (within the control rooms) but also locally (e.g., operators on the field), toward the optimisation of the logistics processes

It also discusses the ways these innovations will satisfy the needs and requirements of the various stakeholders and users involved in the Supply Chain Industry of the future as how these were analysed and documented in earlier parts of this report. Table 24 shows the mapping of the proposed innovations to the requirements, providing the big picture of our reasonings, while a detailed explanation will be provided in the following sections, where these innovations are detailed. Moreover, through the satisfaction of these needs how the IoT can support the realisation of the PI, through the testing work of the Living Labs, adding a real value to the project context.

Table 24 Mapping the innovation to the business requirements

Req. ID	Req. Name	IoT protocols innovation	Architectural innovation	Business intelligence innovation
MCR_01	**Affordable system**	**X**	**X**	

MCR_02	**Affordable integrability**	**X**	**X**	
MCR_03	**Easy and not invasive installation – Easy maintenance**	**X**	**X**	
IER_01	**Supply chain visibility at multiple layers**		**X**	
MOR_01	**Supply chain digital twin**			**X**
MOR_02	**Localisation and inventory of goods and products**		**X**	
IER_02	**Localisation and monitoring of assets**		**X**	
EMR_01	**Ensure goods integrity and safety**		**X**	
IER_03	**Data-oriented and fact-based decision making and business intelligence**		**X**	**X**
IER_04	**Assets' management optimisation**		**X**	**X**
EMR_02	**Accurate ETA prediction**			**X**
IER_05	**Maximise Operational Efficiency and Capacity, Revenue Generation**			**X**
MSR_01	**Increase Customer Satisfaction**			**X**
MSR_02	**Gain competitive advantage**			**X**

IER_06	**Scheduling and organisation of the intermodal and the uploading/downloading operations**		**X**	**X**
EMR_03	**Fault liability**		**X**	**X**
IER_07	**Circular economy support and optimisation**		**X**	**X**

8.1 IoT Protocols Innovations

In this section, the innovation we elaborate is based upon the exploitation of recently standardised IoT protocols. In particular, we propose ICONET as an early user of the following protocols:

1. **NarrowBand-IoT**: its specification was frozen in in June 2016, while its commercial services have started at the end of 2018. Some open issues are not already solved (e.g., international roaming).
2. **BLE 5.0**, released in July 2016 by the Bluetooth SIG, and integrated for the first time in a mobile in March 2017. This BLE 5.0 maintains the low power characteristics of the previous releases, but improving the communication range (capable to reach 1km of distance in line-of-sight configuration, 400m otherwise) and the data rate (enabling, for example, the streaming of more structured data type, as images, maintaining a very low power profile).

Referring to the hardware components described in Sec. 7.3.7, the NGS objectives regarding the exploitation of the innovative afore mentioned protocols are the following:

1. To develop solution **5G ready** (i.e., 3GPP standardised protocols), capable to implement standalone functionalities for the good tracking and monitoring. In this manner, the system is ready for the new challenge for the forthcoming technology.
2. To **support the operativity** also enabling e-GPRS services and allowing the deployment of a working system though the 5G services are not already available. In this scenario, chipset that allow the interchangeability 5G (i.e., NB-IoT) and e-GPRS protocols must be selected.
3. To enable **multi-protocol (standardised) IoT networks to enable cooperation with gateways[4] or with other devices**. This feature can enable, for example, the reduction of the power consumption of the battery powered devices, thus reducing their maintenance. In fact, as described in ANNEX III, though NB-IoT implements an improved battery saving policy compared with other mobile protocols (e.g., GPRS), its power consumption is the higher compared with the other IoT protocols (e.g., BLE and IEEE802.15.4).
4. To **enable multi-protocol (standardised) local data-collection IoT networks**, thus enhancing the technical interoperability with different type of IoT sensor nodes available in the market.
5. To allow an **IPv6 enablement** for short range IoT protocols in points 3 and 4, considering compatible MAC and PHY layers (i.e., IEEE802.15.4 and BLE). This improvement allows the implementation of the following functionalities:
    a. **Service orientation**, allowing asynchronous real-time reporting functionalities, as well as on-line system configuration.
    b. **Routing operations**, thus improving the network coverage, and allowing to reach far gateways considering multi-hop routes.

[4] Installed within terminals, warehouses and vessels (DSCA - Digital Container Shipping Association, s.d.)

8.1.1 5G and NarrowBand-IoT

5G is the fifth-generation technology standard for cellular networks, thus the planned successor to the 4G networks which is the current connectivity exploited by most of the mobile-phones. Its main improvements compared with the previous protocols are (see also Figure 30):

1. **Mobile IoT/Massive IoT/LPWAN**. In fact, it aims at providing improved network coverage, long device operational lifetime (implementing improved power saving functionalities) and a high density of connections (improve the scalability managing a huge amount of IoT devices).
2. **Critical communications**, implementing high performance, ultra-reliable, low latency industrial IoT and mission critical applications.
3. **Enhanced Mobile Broadband**, implementing improved performance and a more seamless user experience accessing multimedia content for human-centric communications.

Figure 30 5G 3 directions (GSMA, 2018)

NarrowBand-Internet of Things (NB-IoT) is a standards-based low power wide area (LPWA) technology developed to enable a wide range of new IoT devices and services. Its specification was frozen in 3GPP Release 13 (LTE Advanced Pro), in June 2016 (3GPP, 2016) . NB-IoT significantly improves the power consumption of user devices, system capacity and spectrum efficiency, especially in deep coverage. Particularly, the energy saving functionalities are improved with respect to the standard mobile protocols, introducing Power Saving and Extended Discontinuous Reception Mode (see ANNEX III) (GSMA , 2018) . The first NB-IoT commercial launches have been completed and Figure 31[5] depicts the updated NB-IoT coverage at the end of 2018. These coverages are implemented as a fragmented patchwork and the international roaming in not realised, as described in Sec. 8.1.1.1.

[5] CREDITS: GSMA

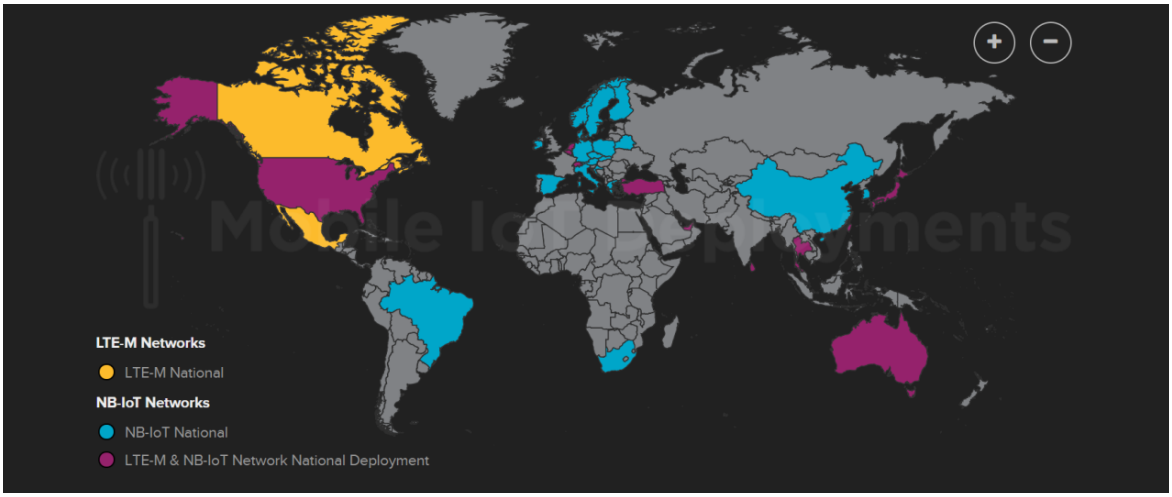


Figure 31 NB-IoT worldwide coverage (end 2018)

In this scenario, considering the guidelines coming from the GSMA white paper of April 2018 (GSMA, 2018), NB-IoT can be considered as forerunner protocol toward 5G. In fact, Figure 32 shows the various 5G network components that are built up and deployed over time. It highlights that NB-IoT, already (partially) operational, is considered (together with LTE-M) as the 5G technology capable to enable the **Mobile IoT/Massive IoT/LPWAN**, and it will coexist with the other 5G components (i.e., enhanced mobile broadband and critical communications) when these will be deployed.

NGS will use this innovative and 5G ready components as enabling technology to implement the connection between the container and remote IoT platform, described in Sec. 7.3.6. In fact, the tracker, the smart router and the smart gateway will be equipped with NB-IoT enabled transceivers, thus becoming 5G ready.

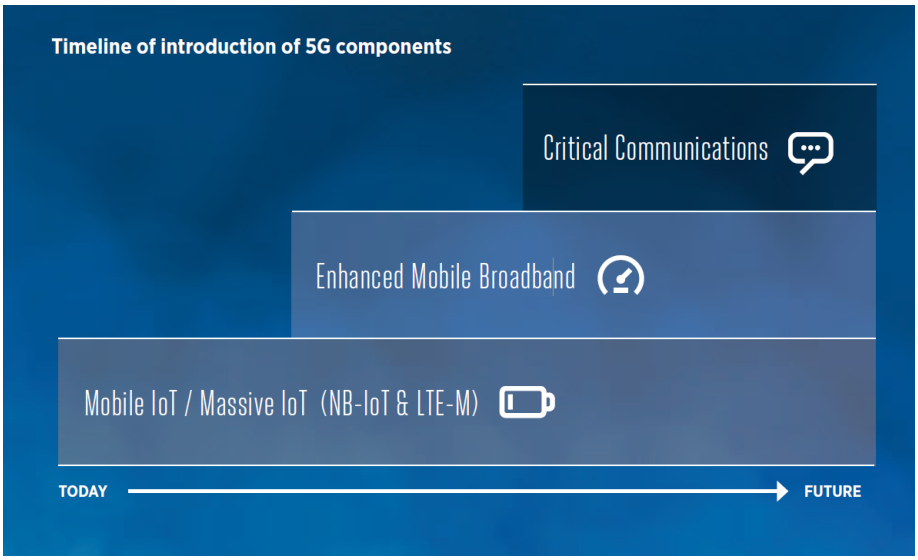


Figure 32 Timeline of introduction of 5G components (GSMA, 2018)

8.1.1.1 NB-IoT open issues

Nowadays, the main issues to exploit NB-IoT in logistic corridors around Europe are that there are no commercial roaming agreements or even protocols for arranging Narrowband-IoT technology internationally. This means that if the same IoT device is "travelling" along multiple countries, the NB-IoT services and functionalities (as for example PSM and eDRX) can be exploited only in the nation where the SIM is emitted. The European roadmap of enabling the NB-IoT international roaming is not clear, though Deutsche Telekom and Vodafone completed the first successful NB-IoT Roaming trial in June 2018 (GSMA, 2018).
Moreover, the NB-IoT deployment is currently a fragmented patchwork, thus a continuative remote communication cannot be guaranteed also at national level. Particularly, the coverage is limited to only the towns.
To provide an effective device for implementing the LLs purposes, we need to consider specific transceivers capable to enable 5G (i.e., NB-IoT), as well as to maintain the operativity using eGPRS. For these reasons, the proposed devices will be based on the Quectel transceiver BG96[6], characterised by the following features:

1. It is capable to manage the 5G forerunners protocols as LTE Cat.M1 and Cat.NB1 (NB-IoT), as well as the EGPRS connectivity (to enable the operativity.
2. Ultra-low power consumption optimised for the IoT communications.
3. Pin-to-Pin compatible with single protocol (lower cost) transceivers BC95[7] (NB-IoT, 5G ready) and M95[8] (eGPRS)

8.1.2 BLE 5.0

Bluetooth 5.0, released in July 2016 by the Bluetooth SIG (Special Interest Group), is the latest version of the short-range wireless standard. With respect with the previous releases, Bluetooth 5 increases both the wireless range and the throughput and enable broadcasting (it is possible to send data to two wireless devices at once). A comparison between different Bluetooth releases is shown in **Error! Reference source not found.**.
BLE 5 support the integration of 6LoWPAN protocol on top of it, thus enabling an IPv6 compatible networking (J. Nieminen & - et al., 2015).

Table 25 Bluetooth 5.0 compared with previous releases

	BLUETOOTH 2.1	BLE 4.0	BLE 5
Range	Up to 100 m	Up to 100 m	Up to 400 m
Max range (free field)	Around 100 m (class 2 outdoors)	Around 100 m (outdoors)	Around 1,000m (outdoors)
Frequency	2.402 – 2.481 GHz	2.402 – 2.481 GHz	2.402 - 2.481 GHz
Max data rate	1- 3 Mbit/s	1 Mbit/s	2 Mbit/s

[6] https://www.quectel.com/product/bg96.htm
[7] https://www.quectel.com/product/bg95.htm
[8] https://www.quectel.com/product/m95.htm

Application Throughput	0.7-2.1 Mbit/s	Up to 305 Kbit/s	Up to 1,360 Kbit/s
Topologies	Point-to-point, scatternet	Point-to-point, mesh network	Point-to-point, mesh network
Network Standard	IEEE 802.15.1	IEEE 802.15.1	IEEE 802.15.1

8.1.3 Mapping the IoT protocols' innovations into the business requirements

In Table 26 a reasoned and detailed mapping of the innovations proposed in the ICONET approach to the requirements is provided. Particularly, it will demonstrate how the consideration of such protocols will affect the complex business environment of the logistics and of the PI.

Table 26 Mapping the IoT protocols' innovations to the business requirements

Req. ID	Req. Name	Requirements
MCR_01	**Affordable system**	The exploitation of innovative protocols for IoT allow the reduction of the cost of the devices, since the related optimised components allow the realisation of affordable devices. Therefore, no significant investment will be required to materialize the benefits
MCR_02	**Affordable integrability**	The proposed protocols allow a scalable and plug&play integration. This provides needed flexibility
MCR_03	**Easy and not invasive installation – Easy maintenance**	The proposed protocols are wireless and optimised for reducing the battery consumption[9], thus reducing the maintenance of the derived devices. Again, cost considerations are always important.

8.2 IoT Architectural innovations

ICONET's proposed **IoT architecture** allows to whom to implement a pervasive and ubiquitous environment, thus providing the visibility to all the supply chain. We propose a **recursive architecture** capable to represent the encapsulation of the PI packets. The deployment of such architecture foresees the IoT coverage of all the supply-chain exploiting the most convenient communication between the mobile network (5G ready, as discussed in the previous section) or other IoT connectivity. For instance, the proposed system can cooperate with OBUs on trucks based on the CALM protocol suite (ISO, 2016), that integrates 6LoWPAN and CoAP protocols.

The architecture proposed in this report (depicted in Figure 33) envisions to realise an innovative support to enable the supply chain complete visibility. In fact, the architecture proposed in this document is capable to enable the following features:

[9] The communication is the most energy expensive operation in the IoT devices.

1. **Interoperable, Standardised and Plug&Play.** An improvement technical interoperability is required to manage different IoT protocols, preferably standardised and plug&play (i.e., to ease the installation and the maintenance).
2. **Open, comprehensive, and pervasive architecture,** that allow to accommodate components from different parties, since based on standardised protocols (belonging to the IPv6 suite). A standardisation path must be implemented toward the PI common language and the definition of a shared data-model, following also the suggestion by DSCA (DSCA - Digital Container Shipping Association, s.d.). In this scenario, each component of the supply chain can communicate remotely in a seamless manner, as depicted in Figure 34.
3. **Ad-hoc connection and opportunistic routing,** thus allowing to each connected good to communicate toward the Cloud (and the destination set of users) selecting the most convenient route, as well as highlighting the encapsulation details.
4. **Optimised dispatchment.** The selection of the most convenient route allows the optimisation of the IoT network, thus reducing the power consumption (i.e., reducing the system maintenance) and the transaction costs (i.e., selecting a local IoT connection instead a mobile IoT service).
5. **Standardisation harmonisation,** allowing the seamless integration with IPv6-based solutions as well as with the CALM architecture for Intelligent Transport Systems (ISO, 2016) (ISO, 2016).

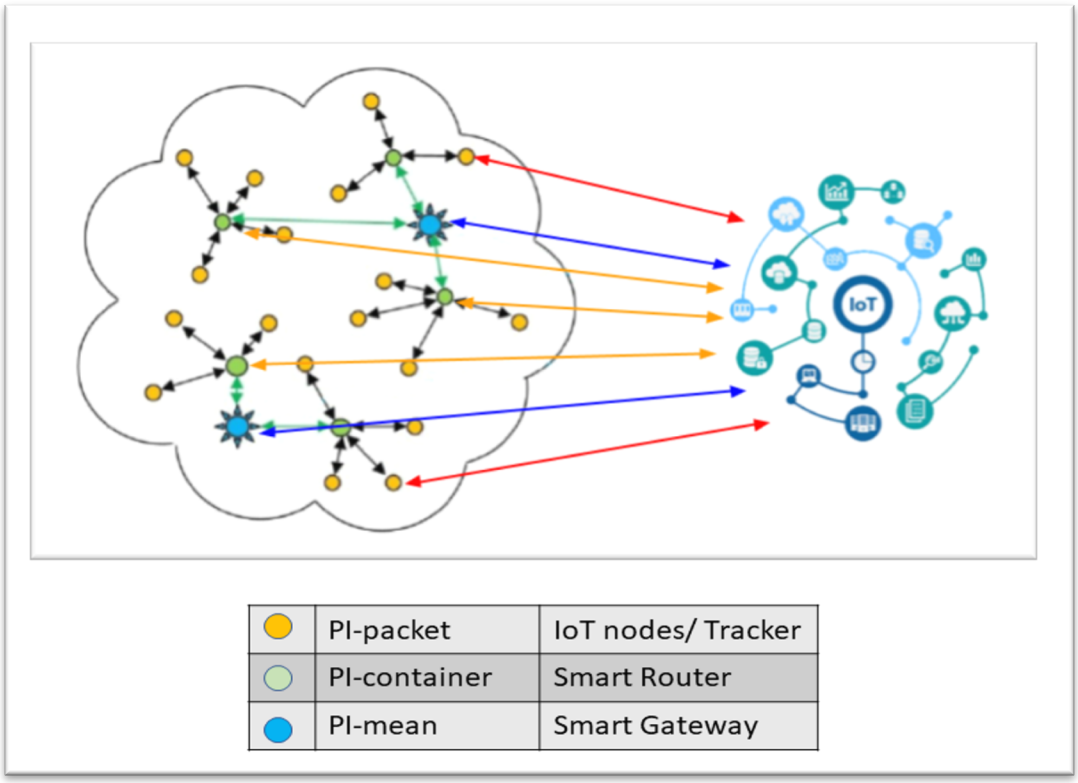


Figure 33 The IoT-enabled PI environment architecture

Regarding the realisation of the Smart PI container (the main topic of this report), the objective of the proposed architecture is to provide:

1. An **interoperable, cooperative, and open IoT environment**, capable to interoperate with components by different providers, thus monitoring different aspects of the goods (internal connectivity) and of the container itself.
2. A **goods-centric monitoring** and not only on a container-level as current state-of-the-art products, allowing to define ex-ante the granularity of the monitoring (at container, pallet, or packet level).
3. **Smart PI-pallets and smart PI-packets**[10] can be enabled in parallel and cooperation with the smart PI-containers. For instance, a smart PI-pallet paired with a certain smart PI-container, can communicate toward the Cloud IoT platform exploiting its internal IoT connectivity.
4. **A hierarchy of PI-objects**, mapping the goods' encapsulation providing a continuous real-time information of the position and of the location of the goods (e.g., at a certain time a certain pallet is encapsulated in a certain container transported in certain mean).

The key component to realise it is the **smart router**. The smart router represents the key components in charge of:

1. Integrating **on-board sensors** (i.e., temperature-humidity, acceleration, light) capable to generate asynchronous events such as bump detection, movement detection, temperature thresholds exceeding and door open/close detection.
2. Implementing an inter**nal and external container connectivity,** thus allowing the management of the encapsulation of the connected goods as well as their (distributed) monitoring, and the monitoring of the container itself (e.g., connected seals status).
3. Tagging the data and information gathered from both the IoT devices and the on-board sensors with their **geo&time-reference**, allowing to understand the place and the time where certain events have happened.
4. Implementing an **improved interoperable connectivity**, integrating 5 different protocols in the same board (i.e., GPRS, NB-IoT, LTE Cat-M1, BLE, IEEE802.15.4). This approach will allow a simplified selection of commercial sensors, as well as an improved integration with the existing communication infrastructures toward the Cloud.
5. Implement **opportunistic routing** of the information collected, allowing both the stand-alone connectivity toward the Cloud (i.e., using **5G** network) or cooperating with low-power and low-cost communications, exploiting **IPv6**-based solutions. In this manner, the most convenient route can be selected toward the reduction of the costs (i.e., cost of maintenance or cost of network access).
6. **Battery powered and energy harvesting,** thus improving its integrability and reducing its maintenance.

[10] *Smart PI pallet and Smart PI packet:* connected PI objects capable to notify their presence and a distributed set of information (e.g., temperature, humidity, bump) regarding itself..

Figure 34 A pervasive IoT-enabled PI environment

8.2.1 Mapping the architectural innovations in the business requirements

In Table 27 a reasoned and detailed mapping of the innovations proposed in the ICONET approach is provided. Particularly, it will demonstrate how the proposed IoT architecture will affect the complex business environment of the logistics and of the PI.

Table 27 Mapping the architectural innovations to the business requirements

Req. ID	Req. Name	Requirements
MCR_01	**Affordable system**	The design of each component of the proposed architecture can be based on affordable and costs' scalable components. The possibility of using energy harvesting solutions allows the reduction of the batteries' size and cost. The possibility of implementing optimised opportunistic routing support the cost reduction selecting the lowest cost path.
MCR_02	**Affordable integrability**	The provision of ubiquitous connectivity with an improved interoperability eases the integration of added value IoT devices to improve the goods monitoring. The opportunistic routing and the standardisation effort can guarantee a seamless integration of the devices.

MCR_03	**Easy and not invasive installation – Easy maintenance**	The opportunistic routing allows the selection of the lower power path to reach the Cloud, thus reducing the battery consumption and the system maintenance.
IER_01	**Supply chain visibility at multiple layers**	The recursive approach allows the authentication of lower hierarchy devices, thus implementing the visibility of all the goods and representing the encapsulation rules.
MOR_02	**Localisation and inventory of goods and products**	The functionalities derived from the recursive approach allows the geo&time-reference tagging, as well as the realisation of real time inventories of the encapsulated goods.
IER_02	**Localisation and monitoring of assets**	The functionalities derived from the recursive approach allows the geo&time-reference tagging, as well as the realisation of real time inventories of the encapsulated assets (container, pallets, …).
EMR_01	**Ensure goods integrity and safety**	The functionalities derived from the recursive approach allows the monitoring of the goods, thus understanding and notifying problems regarding their integrity and safety.
IER_03	**Data-oriented and fact-based decision making and business intelligence**	The pervasive data-collection service enabled by the proposed architecture deeply support the decision making and provides precise data to develop business intelligence techniques appropriate to the real needs with maximum effect.
IER_04	**Assets' management optimisation**	A pervasive data-collection service enabled by the proposed architecture provide information toward an optimised asset management.
IER_06	**Scheduling and organisation of the intermodal and the uploading/downloading operations**	Having available information regarding the position and the presence of the goods, the destination hub/warehouse can schedule and organise the personnel to manage the uploading/downloading operations along the supply chain
EMR_03	**Fault liability**	Having available detailed information collected in a pervasive manner referenced with geo&time tags, the liability of certain faults (e.g., breaks due to bumps) can be evaluated and mitigated.
IER_07	**Circular economy support and optimisation**	A pervasive data-collection service enabled by the proposed architecture provide information toward an optimised circular economy (e.g., beer kegs tracking and optimisation)

8.2.2 Consideration regarding the actuality of the architecture (May 2020)

The proposed architecture was defined at the end of 2018/beginning of 2019 (D1.6 due date is Feb. 2019, M6) where the architectures proposed by the main IoT companies consist in closed environments, where each components communicates remotely in a stand-alone manner (considering 2G) or cooperation in private environments (e.g., Traxens). It is interesting to highlight that the efforts of some more advanced companies in the realization of IoT environments for the logistics (e.g., Traxens and Ambrosus) are in line with what we have envisioned with the one proposed within the ICONET project, though most of the solutions currently available in the market are offering only stand-alone solutions that exploit mobile communications only (usually 2G and

sometimes NB-IoT). However, ICONET's proposed architecture represents a deeper integration on the design of the IoT environments, that is differentiating itself in terms of:

1. **Improved cooperation** between the IoT devices derived from an interoperable and open IoT environment, where a scalable set of devices by different stakeholders can be seamlessly integrated.
2. **Real-time data and information generation at different granularity levels**, toward the implementation of a good-centric monitoring.

8.3 Business intelligence innovations

In a scenario where goods, assets, means/transport networks and hubs are connected, a continuous and distributed tracking and reporting services (on-demand and/or periodic) can be implemented following to map the goods encapsulation. In fact, the proposed findings enable the realisation of a goods-oriented, service-oriented and users-oriented solution of the PI issues, able to provide tracking, monitoring, and reporting services at different granularity. The privacy of the data is guaranteed by considering **secure transactions** at all the levels of the data collection chain, as well as an **ad-hoc access** to the gathered information, thus providing the authorisation to a certain user to monitor the contents related to the transactions related to its activities.
Considering the findings of the report, we can implement the following functionalities:

1. **Internet of Hubs**, where all the users and the stakeholders involved in a certain logistics transaction can monitor the presence (i.e., when? and where?) and the condition of certain goods/assets/means (i.e., how?) in a certain hub. In this manner it will be possible to evaluate the quality of certain services making available some metadata (e.g., how long a certain container stays queued waiting for cross-docking operations) or extract statistics to suggest the selection of certain service with respect to others (e.g., the duration average of certain operations, as custom, etc.). On the other side, it can provide the big picture of the localisation of un-used assets, toward their most efficient management.
2. **Internet of Warehouses,** where all the users and the stakeholders involved in the logistics transactions can monitor the presence (i.e., when? and where?) and the condition of certain goods/assets/means (i.e., how?) in a certain hub. Enabling a pervasive IoT network in warehouses, an effective monitoring of the goods (e.g., monitoring the storage temperature of perishable food or medicines) as well as of assets (e.g., status of the shelves or pallets, baskets, kegs) can be implemented. Assets' inventory, maintenance, and management operations can be enabled, warehouses' status can be monitored thus allowing the implementation of services to improve their exploitation and optimisation, for example implementing "PULL"-oriented strategies.
3. **Internet of Means**, where all the users and the stakeholders involved in the logistics transactions can monitor the presence (i.e., when? and where?) and the condition of certain goods (i.e., how?) in a certain transport mean. This allows the improvement of the transport optimisation (e.g., improving the load factor) reducing the carbon footprint of the logistics, assets' monitoring - management, as well as the optimisation and the deterministic scheduling of the intermodal and uploading/downloading operations.
4. **Internet of Containers**, where all the users and the stakeholders involved in the logistics chain can monitor the presence (i.e., when? and where?) and the condition of certain goods (i.e., how?) in a certain container. Internet of container is the enabler od the realisation of a good-centric monitoring along the corridors, it is considered as one of the most important enablers in the ICONET project. It allows in one side to identify and track&trace a certain container all along the supply chain (supporting the assets' monitoring and management), as well as providing the connectivity for the pervasive tracking and monitoring of both itself (e.g., door open/closed) and the encapsulated goods. In this manner, data-oriented and fact-based decision-making procedures can be enabled to support the logistics regulation and business intelligence operations.

5. **Internet of Goods**, providing the geo&time-reference and the condition of a certain good. Particularly, in ICONET we propose an improved and goods-oriented supply chain visibility enabling a pervasive IoT networking, capable to allow the tracking&traceing and the monitoring of each encapsulated elements, toward the realisation of the smart PI pallets and the smart PI packet.

8.3.1 Mapping the business intelligence innovations in the business requirements

In Table 28 a reasoned and detailed mapping of the innovations proposed in the ICONET approach is provided. Particularly, it will demonstrate how the proposed solution will affect the complex business environment of the logistics and of the PI in terms of data-oriented and fact-based decision-making.

Table 28 Mapping the business intelligence innovations into the business requirements

Req. ID	Req. Name	Requirements
MOR_01	**Supply chain digital twin**	The proposed solution can provide to users a complete picture of what is happening in the PI physical world, implementing the, so-called, digital-twin or PI-twin. To maintain the privacy of the collected data, this can be visualised only by the authorised stakeholders in a **secure and ad-hoc manner**.
IER_03	**Data-oriented and fact-based decision making and business intelligence**	The supply chain digital twin allows the information generation (through analytics) and their visualisation thus supporting a proactive decision-making process.
IER_04	**Assets' management optimisation**	Having available assets data and information, an effective and proactive asset management can be implemented, thus improving the connected logistics services.
EMR_02	**Accurate ETA prediction**	The generation of big-data databases supports the improvement of estimation, allowing a more precise and punctual computation of ETA, thus providing effective information regarding the quality of service to the clients enabling proper resource allocation of assets involved
IER_05	**Maximise Operational Efficiency and Capacity, Revenue Generation**	The exploitation of standardised packaging and the goods-oriented monitoring can support the improvement of the logistics operational efficiency and capacity, thus reducing the cost and increasing the revenues.
MSR_01	**Increase Customer Satisfaction**	The optimisation of the whole supply chain generated by its complete visibility improves its reliability and its quality thus increasing the Customers' satisfaction.
MSR_02	**Gain competitive advantage**	Optimisation of the supply chain means reduction of costs, thus the possibility to reduce the customers' prices and gaining competitive advantages.
IER_06	**Scheduling and organisation of the intermodal and the uploading/downloading operations**	Most optimised operations can be implemented within logistics hubs, allowing the operation scheduling thus reducing the processes' latencies.

EMR_03	**Fault liability**	Having available detailed data and information regarding the whole logistics transaction can support the detection and the liability of the faults.
IER_07	**Circular economy support and optimisation**	Having available assets data and information, an effective and proactive asset management can be implemented, thus improving the circular economy.

9 Conclusions

The ICONET project aims to materialize an early PI prototype purposed to realise significant efficiencies in the logistics industry, through end-to-end visibility, increase load factors and reduced operational costs and environmental footprint. This report has elaborated how IoT can be considered as a key enabling technology for realising this prototype, by providing a set of data that would enable synchro-modal functionalities. In fact, exploiting the data collected from the IoT sensors, the PI environment and the integrated platforms are enabled to retrieve the position and the status of the goods in a time referenced manner, answering questions such as: "*When?",* "*Where?"* and "*How?".*

In this context, this report has taken a thorough look on the Supply Chain industry and looking closely on the business needs of all interested parties through the lens of a technological offering built for tracking and monitoring of consignments. The various components of today's Logistics networks comprise of interrelated systems, service-providing hubs and information technology elements which although they serve a common goal - delivering cargo from origin to destination - they do so in a massively fragmented and disconnected manner. This significantly hinders the operational efficiency and sustainability of today's Supply Chain industry.

The benefits of bringing together all these components are multiple and have been at the core of the PI concept and the ICONET vision. The developed IoT Architecture and components within the PI context ensures the T&L industry complete visibility across the network. In this way, it assists a fact-based decision-making process of involved actors, and in parallel provides a clear view on how key components can be largely improved and interconnection of diversified areas can be enhanced. In fact, the proposed architecture foresees an opportunistic and pervasive IoT network designed to provide connectivity to all the actors involved in the logistics chain, thus providing them improved supply chain visibility and value-adding information in regards with goods, containers, means and hubs, representing both modularity needs as well as encapsulation relations.

Starting from this envisioned architecture, a set of high-level specifications has been elicited from each Living Lab of the project, to describe a set of IoT applications capable to solve some of the issues arisen by these. The following IoT applications have been considered:

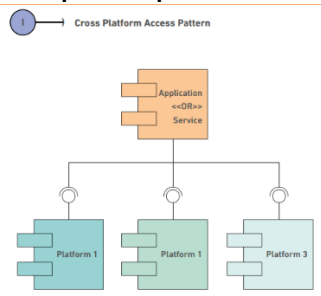
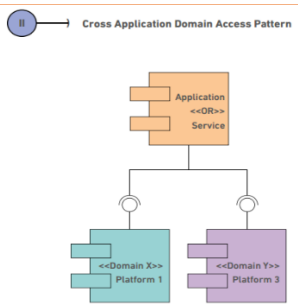
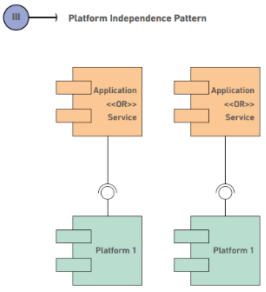
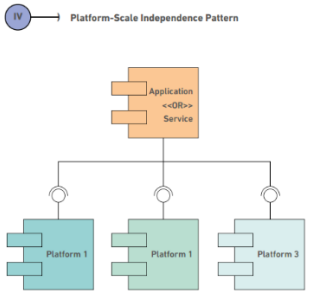
1. IoT-based PI means tracking all along the Antwerp seaport landside is proposed, considering two approaches: the exteroceptive, i.e. based on the smart camera technology, and the proprioceptive, i.e. based on sensors deployed within vehicles.
2. IoT-based synchro-modal monitoring of PI containers utilising a system capable to collect and dispatch remotely different type of data in a geo&time-referenced manner.
3. IoT-based tracking and monitoring of warehouses goods and assets (incl. dispatchment process control through smart camera technology).

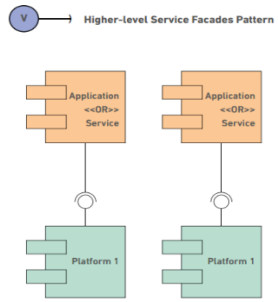
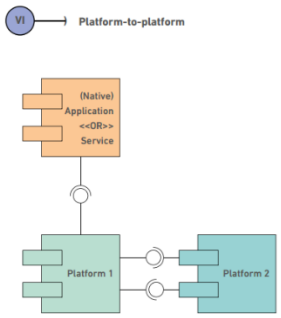
Finally, the report highlights the innovations that the ICONET IoT proposition introduces in both the TLC and PI, in the areas of:

1. **IoT Architecture:** envisioning a Recursive Gateway-Mediated Edge Connectivity and Management Pattern, capable to enable the complete and goods-centric visibility of the supply chain.
2. **IoT Protocols:** proposing standard protocols capable to improve system scalability as well as reduced device maintenance. Particularly focus is given in the exploitation of NB-IoT protocol, that would allow the project to exploit the new frontiers enabled by 5G.
3. **Business Intelligence:** enabling periodic and/or on-demand reporting towards all the actors involved in the supply chain, thus supporting data-centric, fact-based decision making, leading to measurable operational improvements and sustainability.

ANNEX I - Interoperability patterns

Table 29 Interoperability pattern table

Interoperability patter	Description	Graphical representation
Cross-Platform Access Pattern	The purpose of Cross Platform Access pattern is to create a unique interface specification for applications or services to access different platforms. This pattern allows different platforms from different providers to interoperate through a common interface.	
Cross Application Domain Access Pattern	Cross-Application Domain Access pattern is an extension of the Cross-Platform Access pattern. The pattern permits services/applications to access information and functions not only from different platforms, but also from different domains contained in one platform.	
Platform-Independence Pattern	Platform-Independence Pattern aims at providing a single application or service to be used on top of different IoT platforms. The application or service is supposed to interact with different platforms in a uniform manner.	
Platform-Scale Independence Pattern	Platform-Scale Independence Pattern hides different platform scales towards the connecting services and applications. The IoT platforms can be categorized according to their scale as server-level platforms which can manage a large number of devices and a huge amount of data, fog-level platforms which can handle data with limited spatio-temporal scope, and device-level platforms which allows direct access to sensors, actuators, etc. and hosts a small amount of data.	

Higher-level Service Facades Pattern	Higher-level Service Facades Pattern extends the interoperability requirements from platforms to higher-level services. The purpose of this pattern is to enable the management of platforms, services, and functions through a common API. Thus, a service acts as a facade towards an IoT platform and use or process the IoT resources provided from different IoT platforms to offer value-added functionalities	
Platform-to-Platform Pattern	Platform-to-Platform enables existing applications to use resources managed and operated by other federated platforms as if they were offered by a single platform. This pattern facilitates the communication between two platforms in technical, syntactic, and even semantic manner. By implementing this feature, the pattern also supports the idea of effective communication between organizations defined by the organizational interoperability.	

ANNEX II – EU flagship projects

AGILE

AGILE[11] is abbreviated for Adaptive Gateways for dIverse muLtiple Environment), which builds a modular hardware and software gateway to enable the technical and syntactic interoperability. AGILE creates a hardware supporting state-of-the-art IoT protocols with many other features such as device and data management, data visualization, security, and external cloud communication. On the hardware side, AGILE extends the capabilities of the popular and low-cost Raspberry Pi platform with a modular extension cape. The technical interoperability is enhanced via the new modular hardware design. On the software side, the syntactic interoperability is achieved via two modules, namely the Device Management UI and IoT Data Management UI. AGILE design employs the cross-platform design pattern, hence offers an ability to connect with many cloud platforms. In addition, the AGILE project provides open-source code for the community through the Eclipse Foundation. Besides, the software is designed with minimization of dependencies, therefore supports also other hardware platforms available in the market.

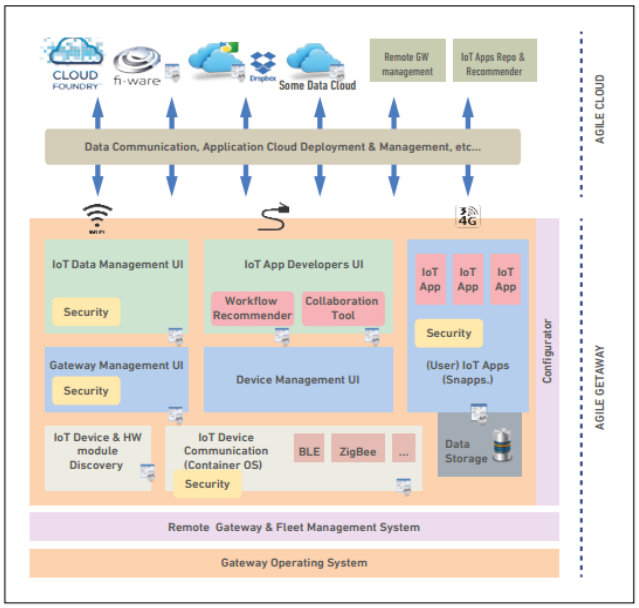


Figure 35: AGILE Detailed Architecture

The AGILE architecture (see Figure 35) consists of five components, namely, Data Management UI, Developer UI, PaaS Deployer, Cloud Recommender, and IDM.

- **Data Management UI:** an interface is built to retrieve or represent the stored data, and to manage what data will be stored. This UI also has a capability of permitting users to push sensor data to the cloud.
- **Developer UI:** an interface based on NodeRed.
- **Paas Deployer:** provides application deployment capability to the AGILE platform.
- **Cloud Recommender:** gives a cloud recommendation to AGILE users.
- **IDM:** or Identity Management supports user authentication and the definition of entities and attributes in order to allow the definition of access policies for said entities.

[11] http://agile-iot.eu/

BIG IoT

The main goal of BIG-IoT[12] project is not to create another platform but provide a common Web API platform enabling a seamless integration of other IoT platforms, therefore, establishing syntactic and semantic interoperability. The BIG IoT architecture contains two components (see also Figure 36), namely an open BIG IoT API and BIG IoT Marketplace. The BIG IoT API is created from a set of defined functionalities including Identity Management, Discovery, Access, Tasking, Vocabulary Management, Security Management, and Charging. The IoT platforms are integrated via this unified API enabling the syntactic interoperability. It is worth noticing that BIG IoT divides IoT platforms into five main types according to the IoT platform base and connectivity type. The categorized platforms include:

- **Type 1: Server Infrastructure or Cloud based IoT Platform** assumed to be "always online" and anytime accessible by applications or services via the Internet.
- **Type 2: Device-level IoT Platform, hosted on devices that are unconstrained with respect to communication, compute and memory resources** assumed to be "always online" whereby connectivity and communication resources is assumed to be charged on a "flat-rate" plan.
- **Type 3: Device-level IoT Platform, hosted on devices that are unconstrained with respect to communication, compute and memory resources, but are "not always online".**
- **Type 4: Device-level IoT Platform hosted on devices that are unconstrained with respect to communication, compute and memory resources, but are connected to the Internet via a "pay-per-use" plan.** Type 4 devices are often also of Type 3.
- **Type 5: Device-level IoT Platform hosted on devices that are constrained with respect to communication, compute and/or memory resources.**

Besides, the marketplace employs the schema.org ontology, which is known to be a cross-domain vocabulary, to meet the requirement of the semantic interoperability. BIG IoT design deploys the cross-platform access, cross-domain access, platform scale independence design pattern. Therefore, the architecture supports cross-standard, cross-platform, and cross-domain IoT services and applications.

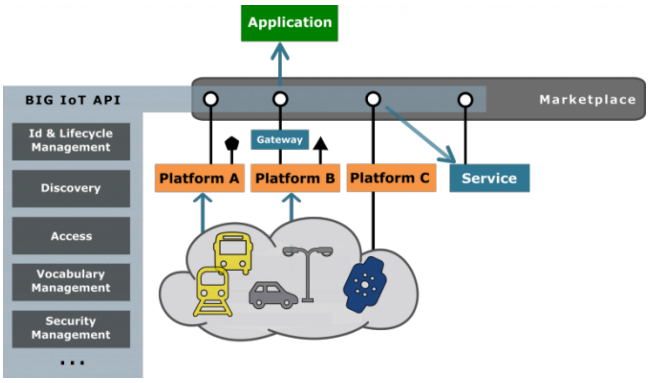


Figure 36: BIG IoT Architecture

[12] http://big-iot.eu/

bIoTope

The objective of bIoTope[13] are to build a platform that can enable companies to easily create new IoT systems and rapidly harness available information using advanced Systems-of-Systems (SoS) capabilities for Connected Smart Objects. The architecture of bIoTope, depicted in Figure 37, can be considered as a bridge to semantic interoperability and somehow organizational interoperability.

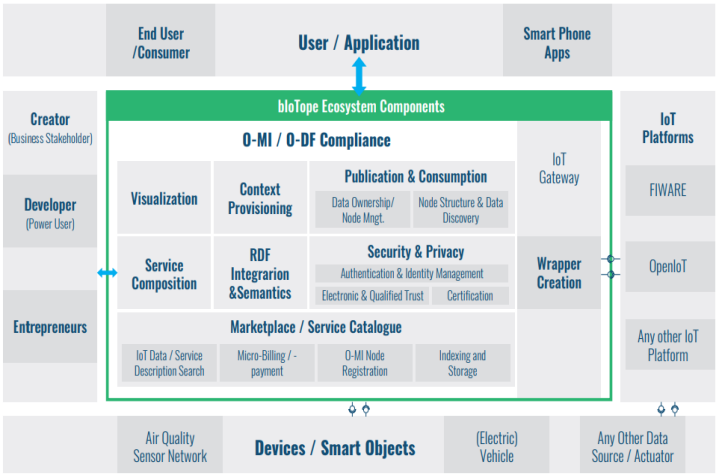


Figure 37: bIoTope Reference Architecture

[13] https://biotope-project.eu/

INTER IoT

INTER IoT[14] aims at providing a layer-oriented solution for enabling seamless IoT platforms' interoperability. That means different IoT platforms can interconnect and transparently interoperate among them at any specific layer or level (Device, Network, Middleware, Application, Data and Semantics). The project develops an interoperability solution at any layer and across layers among different IoT systems and platforms, as depicted in Figure 38. The solution presented by INTER IoT offers a tight bidirectional integration, higher performance, complete modularity, high adaptability and flexibility, and increased reliability.

Device Layer (D2D): a modular gateway supporting a vast range of protocols as well as raw forwarding is created.

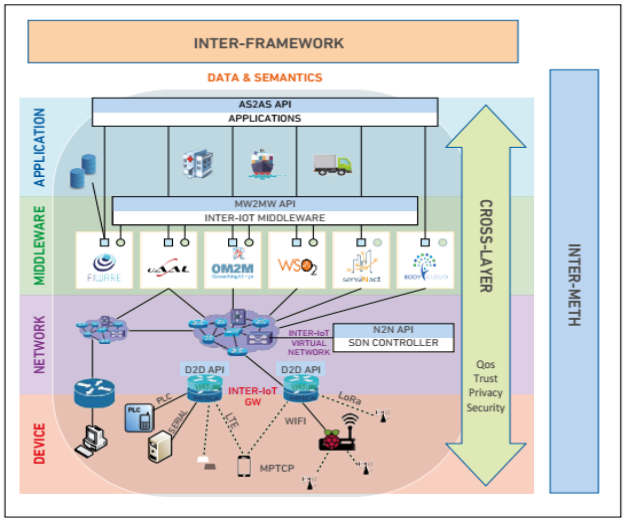


Figure 38: INTER-IoT layered architecture

Network layer (N2N): The network-to-network interoperability is enabled through this layer.
Middleware layer (MW2MW): The interoperability at the middleware layer is reached by the creation of an abstraction layer and the attachment of IoT platforms to it.
Application and Services layer (AS2AS): AS2AS solution is implemented to allow the exploitation of unified services among different IoT platforms through a set of common APIs

Semantics and Data layer (DS2DS): This layer enhances common understanding between exchanged data and information across different IoT platforms and diverse data sources.

Cross-Layer: This level is generated to ensure non-functional aspects at all layers: trust, security, privacy, and quality of service.

[14] https://iot-epi.eu/project/inter-iot/

symbIoTe

The main goal of symbIoTe[15] is not to create another IoT platforms but a flexible and secure interoperability middleware across IoT platforms to enhance rapid development of IoT applications among platforms, collaboration between platforms, and create dynamic and adaptive smart spaces. symbIoTe middleware allows the cooperating systems to share their resources. In symbIoTe, resources mean sensors, actuators that a platform wants to offer to other platforms or different applications. They also mean composite services that a platform is able to produce. In order to reach the mentioned goal, symbIoTe defines four domains (see also Figure 39) including Application Domain, Cloud Domain, Smart Space Domain, and Smart Device Domain. Each domain has its own features that empower the interworking between IoT devices and platforms.

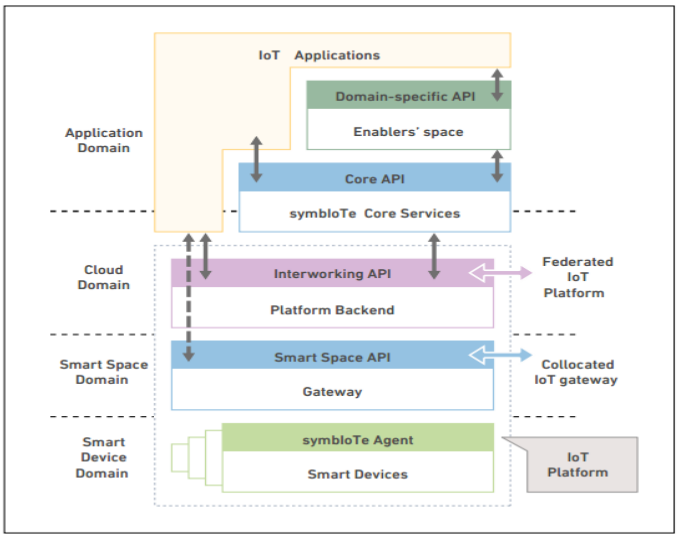


Figure 39: The symbIoTe high-level architecture

The Application Domain allows the registration of virtualized IoT devices and resources for IoT platforms to advertise.
The Cloud Domain implements an access method to the registered virtualized IoT devices and resources.
The underlying domain is Smart Space Domain, which enables the cooperation of IoT devices and gateways registered in the same space.
Finally, the Smart Device Domain offers the roaming capability of smart devices through the IoT platforms registered in the IoT federation while keeping their identities.

[15] https://www.symbiote-h2020.eu/

TagItSmart

TagItSmart[16] aims at integrating mass-market objects as a part of an IoT ecosystem. In order to reach this objective, TagItSmart devises a smart markers, namely Functional Codes (FunCodes/FCs)/ Smart Tags to support secure and reliable acquisition and consumption of such contextual data, while preserving user privacy, to the provision of generic functionalities and a service composition platform. The tags are essentially context sensitive, printable QR codes that can be attached to products to provide necessary information along the products' lifecycle to customers.

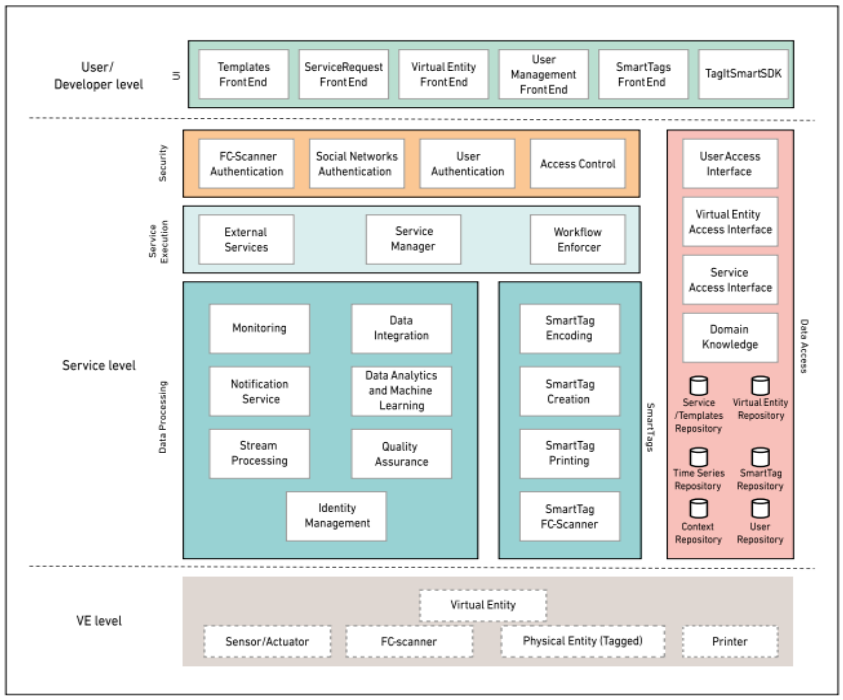


Figure 40: TagItSmart Detailed Architecture

The TagItSmart architecture consists of three levels (see also Figure 40): User/Developer Level, Service Level, and Virtual Entity Level. The User/Developer level essentially provides front-end functionalities to access other TagItSmart components. The Service level offers security, capability of executing services registered in the platform, processing data obtained from the platform. Besides this level also supports integration, creation, and scanning of the SmartTags. In addition, it provides corresponding registries, semantic models, and repositories on which SmartTag operates. Finally, the virtual entity level allows the access to data and functionalities.
TagItSmart is designed as a set of loosely coupled components which can ease the integration process in and across different environments (IoT platforms).

[16] https://www.tagitsmart.eu/

VICINITY

The VICINITY[17] project defines a way to connect different IoT ecosystems through the VICINITY platform, which enables the interaction between IoT objects across the diverse IoT platforms. VICINITY aims at building a platform and ecosystem that provides interoperability as a service for infrastructures on the Internet of Things. The interoperability services offer an environment where value-added services can be deployed, processed, and exchanged across different domains.

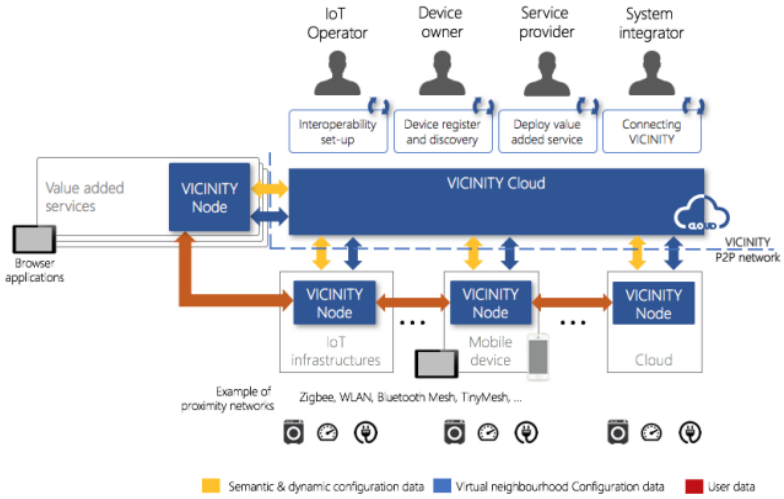


Figure 41: VICINITY Overall Architecture

VICINITY contains two main parts, namely VICINITY node and VICINITY Cloud, as depicted in Figure 41.
VICINITY Cloud is responsible to establish peer-to-peer interaction between IoT environments.
VICINITY Node is in charge of associating IoT infrastructures and value-added services to the VICINITY Cloud
To achieve a cross-domain semantic interoperability, VICINITY uses its own dictionary, namely VICINITY ontology, which is considered to be the common and abstract information model. Besides, the W3C Web of Things Thing Description (TD) is chosen as the framework to describe IoT objects connected to VICINITY. In addition, the Gateway Adapter APIs are capable of providing service discovery in semantic-based criteria.

[17] https://vicinity2020.eu/vicinity/

ANNEX III – Power consumption consideration

NB-IoT power saving functionalities

In the following some details regarding the modes implemented by NB-IoT to save energy. Particularly, it allows to enter in sleep mode without losing the connection with the mobile network (an energy intensive operation, since it can require up to 2A currents) implementing the PSM and the eDRX modes described in the following.

Power Saving Mode (PSM)

IoT transceivers are usually designed to be optimised in power consumption thus implementing low power communications and enabling deep sleep (or power off) functionalities. A power off functionality is also available for mobile transceivers, but the device would subsequently have to reattach to the network when the radio module was turned back on. The reattach procedure consumes a small amount of energy, but the cumulative energy consumption of reattaches can become significant over the lifetime of a device, especially when the sampling operations are frequent: power consumption can be optimised whether this procedure could be avoided. Power Saving Mode (PSM) is a mechanism to reduce the energy used by the transceiver and it was introduced in 3GPP Release 12 and is available for all LTE device categories. When a device initiates PSM with the network, it provides two timers: PSM time is the difference between these timers. The network may accept these values or set different ones. In this scenario, the network retains the status information of the device, thus it remains registered with the network: if a device awakes and sends data before the expiration of this time interval, a reattach procedure is not required. The maximum time a device may sleep is approximately 413 days. The maximum time a device may be reachable is 186 minutes.

Extended Discontinuous Reception (eDRX)

Extended Discontinuous Reception (eDRX) is an extension of an existing LTE feature, which can be used by IoT devices to reduce power consumption. eDRX can be used without PSM or in conjunction with PSM to obtain additional power savings. It is an extension of the already existing discontinuous reception (DRX) mode, already in use in many smartphones to extend battery life between recharges. It is based in a momentarily switching off the receive section of the radio module for a fraction of a second: in this period the smartphones cannot be contacted by the network, but, considering short intervals, the quality of service will not have a noticeable degradation. eDRX allows the time interval extension during which a device is not listening the network. In fact, for an IoT application, it might be quite acceptable for the device to not be reachable for few seconds or longer.

Power saving comparison

In the following table the comparison of the main some IoT protocols are compared with the cellular based one.

Table 30 Power consumption comparison

Protocol (transceiver)	Sleep	Transmission	Reception
IEEE802.15.4 (nRF52840[18])	0,4uA	6,40mA	6,53mA
BLE (nRF52840[61])	0,4uA	3,83 - 16 mA[19]	10,10mA
LoRa (RN2483[20])	1,6uA	40mA	14mA
NB-IoT (BG-96[21])	10uA[22]	78mA	40mA
GPRS[23]	1,5mA	250mA	40mA

[18] https://infocenter.nordicsemi.com/pdf/nRF52840_PS_v1.1.pdf
[19] This range depends on the used configuration (BLE mode or high speed mode – 1Mbps)
[20] https://www.microchip.com/wwwproducts/en/RN2483
[21] https://www.quectel.com/UploadFile/Product/Quectel_BG96_LTE_Specification_V1.5.pdf
[22] Power saving mode (PSM)
[23] GPRS is not thought for IoT, thus it does not implement PSM. In this scenario, to reconnect with the network it can require current up to 2A.

Bibliography

GSMA . (2018, April). NB-IoT Deployment Guide to Basic Feature set Requirements.

3GPP. (2016, August 19). "Standardization of NB-IOT completed".

Balden, B. (2020). *D4.6 ICONET Business Plan and Exploitation.*

Baum, A. (n.d.). *A link to the Internet of Things.* Retrieved from http://www.ti.com/technologies/internet-of-things/overview.html

Clegg, D., & Barker, R. (1994). Case Method Fast-Track: A RAD Approach. Addison-Wesley.

DSCA - Digital Container Shipping Association. (n.d.). *Digital Container Shipping Association*. Retrieved from https://dcsa.org/

Francesco Marino, I. S. (2019). IoT enabling PI: towards hyperconnected and interoperable smart containers. *Proceedings of 6th International Physical Internet Conference .* London.

Friess, O. V. (2016). Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds. River Publishers, Gistrup.

Gruber, T. (1993). A translation approach to portable ontology specifications. *Knowledge acquisition*.

GSMA. (2018, June 4). *GSMA Announces Completion of First European NB-IoT Roaming Trial*. Retrieved from gsma.com: https://www.gsma.com/newsroom/press-release/gsma-announces-completion-of-first-european-nb-iot-roaming-trial/

GSMA. (2018). *Mobile ioT in the 5G future - NB-IoT and LTE-M in the context of 5G.*

H. van der Veer, A. W. (2008, April). *Achiveing Technical Interoperability – the ETSI Approach.* ETSI White Paper.

INCOSE. (2010). *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. Version 3.2.1.* San Diego, CA, USA.

IoT-EPI. (2018). *Advancing IoT platform interoperability.* Gistrup (DK): River Publishers.

IoT-EPI. (2018). Advancing IoT Platforms Interoperability. *River Publishers Series in Information Science and Technology,*. Retrieved from 2018, https://iot-epi.eu/wp-content/uploads/2018/07/Advancing-IoT-Platform-Interoperability-2018-IoT-EPI.pdf

ISO. (2016). *ISO 19079:2016 - Intelligent transport systems — Communications access for land mobiles (CALM) — 6LoWPAN networking.*

ISO. (2016). *ISO 19080:2016 - Intelligent transport systems — Communications access for land mobiles (CALM) — CoAP facility.*

ISO DIS 19079. (n.d.).

ISO DIS 19080. (n.d.).

ISO/IEC. (2007). *Systems and Software Engineering -- Recommended Practice for Architectural Description of Software-Intensive Systems.* Geneva.

J. Nieminen, & - et al. (2015). *rfc7668 - IPv6 over BLUETOOTH(R) Low Energy.* IETF.

Martini, B. (2020). *D4.8 Transferability Framework – Capacity Building Programme v1.*

Montreuil, B. (2011). Toward a Physical Internet: meeting the global logistics sustainability grand challenge. *Logist. Res.*

Naik, N. (2017). Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. *IEEE International Systems Engineering Symposium (ISSE).* Vienna.

SENSE project . (2020). *D2.1 Roadmap to the Physical Internet.*

Wikipedia. (n.d.). *https://en.wikipedia.org/wiki/Conceptual_interoperability.*

