IoT enabling PI:

towards hyperconnected and interoperable smart containers

Francesco Marino[2] and Ilias Seitanidis[3] and Phuong Viet Dao[3] and Stefano Bocchino[3] and Piero Castoldi[1,2] and Claudio Salvadori[3]

1. Consorzio Nazionale Interuniversitario per le Telecomunicazioni, Pisa, Italy
2. Scuola Superiore Sant'Anna, Pisa, Italy
3. New Generation Sensors, Pisa, Italy

Corresponding author: fr.marino@santannapisa.it

Abstract: *The Physical Internet (PI) concept is going to bring a disruptive change in the world of logistics, enabling effective and efficient supply-chain operation management. A key building block of the PI is the smart container, the physical dual of the Digital Internet packet which will provide unprecedented real-time visibility over the goods flowing in the supply-chain. Internet of Things (IoT) systems are expected to play a crucial role in the implementation of smart containers, providing the needed pervasive and hyperconnected sensing infrastructure. While IoT sensor networks have always been used as an effective means to collect and transmit information in a wide range of operational systems, the modularity and dynamicity of the PI scenario introduce a number of new challenges to be addressed in terms of system architecture and interoperability. The paper discusses the solutions that are being developed in the context of the EU H2020 ICONET project to tackle those challenges, paving the way to future developments of the PI.*

Keywords: *Physical Internet, Internet of Things, IoT system architecture for PI, smart containers, modularity, interoperability.*

1 Introduction

The Physical Internet (PI) is a boundary spanning field of research launched by Montreuil B. et al. (2012), 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 supply chain and logistics stakeholders 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

This project has received funding from the European Union's Horizon 2020 research and innovation programme
under grant agreement No 769119
The views expressed by the ICONET Consortium do not necessarily represent the views of the EU Commission/INEA.
The Consortium and the EU Commission/INEA is not responsible for any use that may be made of the information it contains

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 paper we build on the outcomes of the EU H2020 ICONET project, whose main goal is to extend the state-of-the-art research and development around the PI concept by designing a new networked architecture for interconnected logistics hubs and by developing a cloud-based PI framework and platform. In this paper we investigate the role that IoT can play in the design of hyperconnected and interoperable “smart containers” as building blocks of the PI architecture. We report the requirements highlighted in this respect by the ICONET industrial partners and we propose possible solutions which will be tested in the ICONET Living Labs.

2 State of the art

The first relevant initiative towards the development of interconnected logistics at the European level was the EU FP7 Modulushca project, which focused on the design of modular and composable PI-containers able to establishing digital interconnectivity with each other. To achieve this goal the project stated that each PI-container must have a unique worldwide identifier in the PI networks (by using, for example, Electronic Product Code with Global Returnable Asset Identifier), and that PI-containers must always be trackable, monitorable and interoperable with each other and with other PI actors (by featuring long and short range communication technologies).

Montreuil et al. (2016) envisaged three modular categories of PI-containers, respectively the transport, handling and packaging levels, which allow containers to efficiently complement each other through encapsulation and composition, achieving this way a better use of the means of transportation.

Krommenacker et al. (2016) proposed the use of wireless sensors networks to facilitate the composition and decomposition of PI containers. In their setting wireless nodes are attached to each container and store information about the container. According to their transmission range the nodes create a spontaneous multi-hop network and expose themselves a single virtual container.

An holonic framework formalizing the encapsulation and composition mechanisms is presented by Sallez et al. (2016). Here containers provided with different level of activeness, namely the capability to acquire proprioceptive and exteroceptive information and take decisions, are made able to autonomously combine with each other to increase efficiency.

All the mentioned works envisage a massive use of sensing and communication technologies on containers to make them packets flowing in the PI. In this direction, several IoT products enabling the smart containers concept are today available on the market.

Just to mention a few, we cite the DHL SmartSensor, providing through GSM information about temperature, humidity, shock, light, and location data to customers which can be used by 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: TRAXENS-BOX S+ are permanently attached to containers and collect data such as GPS position, temperature, impacts, movement, and vibration. The sensors are connected via a wireless TRAXENS-NET network, through which data is transmitted to the TRAXENS-HUB cloud.

Finally, we report the smart container logistics security seal by Ineo-sense, employing Clover-Net, LoRa, and NFC for communication and sophisticated sensors for monitoring.

3 PI Smart containers: architectural requirements

Smart containers are the physical duals of DI packets. Just like DI packets, they can be encapsulated (e.g., in a boat) and arranged in flows. Unlike DI packets, however, their retransmission as a result 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. In other words, Supply Chain Visibility (SCV) for parts, components and products must be ensured throughout all the network, from producers to consumers. Being consistently aware of the status of goods inside containers allows in fact to take proactive actions to avoid products deterioration or, in case unrecoverable damages are detected, to arrange proper countermeasures without waiting for the unserviceable goods to reach their destination or to identify who is liable for the damage.

To achieve this goal, smart containers must provide functionalities related to:

- **goods routing and tracking**: each PI "packet" has to be tracked, making its position available to all the stakeholders interested on the shipped goods (shippers, senders, receivers, customs, port authorities, canal authorities, etc). To enable the implementation of the goods' routing services (as in the DI), the PI platform has to know the correct position of the goods. In this scenario, IoT will support PI routing issues answering to the question Where? and When? (i.e., providing geo&time-referenced information).
- **goods continuous monitoring**: each PI "packet" has to be continuously monitored, making its status 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.

These user level requirements result in the following system architecture requirements:

- **IoT enablement**: to provide information about the PI packet an IoT communication infrastructure has to be set-up, enabling the communication from the field toward the PI platform. An IoT enabled PI environment requires the deployment (or the exploitation of already deployed) of an IoT network to communicate to the PI platform the data collected from the field.
- **Interoperability**: in fact the IoT environment must be able to communicate with the PI open platform and with the stakeholders involved along the supply-chain.
- **Modularity**: since the need of monitoring modular PI "packets" (packets, container, group of containers), also the IoT environment has to be modular, enabling the continuous monitoring and the tracking of the goods. Each PI module ("packet") has to be IoT connected, thus continuously providing information about itself.
- **Composability**: given the modularity of the "PI packets", they can be encapsulated into other packets, according to a hierarchy. This behaviour has to be considered also in the design of the IoT environment. All the IoT elements must be composable in networks to allow the monitoring of encapsulated goods.
- **IoT networks pervasivity**: since each PI packed has to be continuously monitored, it has to be connected with the PI platform all along the logistics chain (from the sender to be receiver). An IoT enabled PI environment has to provide a pervasive network solution, thus ubiquitously connecting the PI "packets" to the PI platform.
- **Edge computing enablement**: the exploitation of edge computing devices will enable the distribution of intelligence along the network. Edge computers are IoT devices

equipped with computational capability and extended memory, positioned at the edge of the IoT data collection chain. Edge computers can enable the local data processing (e.g., detection of an alarm), the cooperation of the PI IoT environment with different operators (also on the field, e.g., truck drivers can understand what is happening within the transported containers) and external devices/infrastructure (e.g., Intelligent Transport Systems, communicating for example the transport infrastructure).

- **Resilience on data loss**: the PI IoT environment has to consider devices with local storage functionalities to maintain data when the communication with the remote platform is not available (e.g., in the middle of the sea or inside a tunnel). Alongside there will be a need to extend global access to PI data nodes with increased satellite power, coverage and bandwidth.

While IoT sensor networks have always been used as an effective means to collect and transmit information in a wide range of operational systems, the modularity and dynamicity of the PI scenario, as shaped in the discussed requirements, introduce a number of new challenges to be addressed in terms of system architecture and interoperability. In the following subsections we extensively discuss such challenges and we propose possible solutions.

3.1 IoT system architecture for PI smart containers

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 (***Figure 1***).

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.

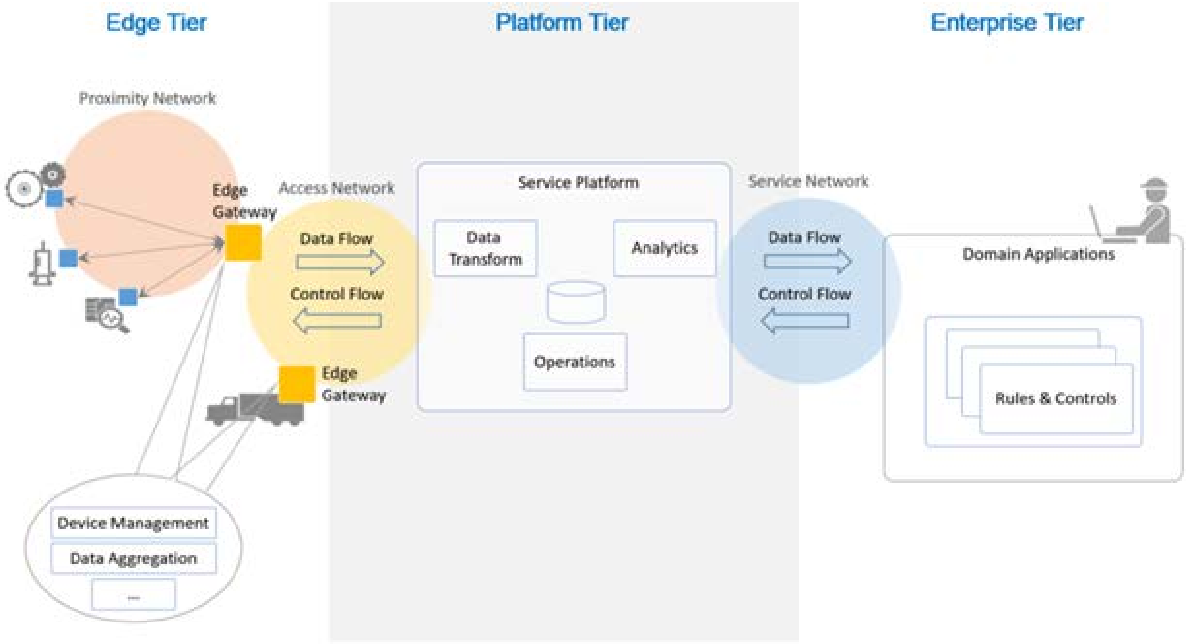

Figure 1: Three-tier system architecture

Usually, the reference IoT architecture adopts a gateway-mediated edge connectivity and management pattern (Figure 2). 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.

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 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.

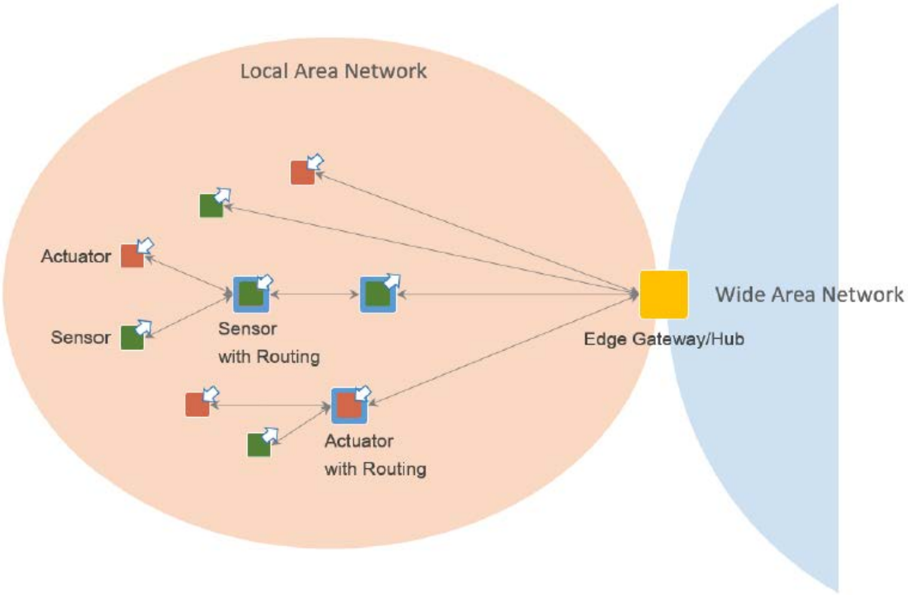

Figure 2: Gateway-Mediated Edge Connectivity and Management Pattern

Although widely tried and tested in several scenarios, the described patterns fall short in the PI context. Indeed, since smart containers are expected to be encapsulated in an unpredictable manner depending on wide range of ever-changing parameters, and since their physical characteristics may interfere with the communication technologies adopted in this context (e.g. containers are often Faraday cages preventing the use of a unique pervasive wireless technology), the PI gateways may not be able to reach a remote destination directly, but they can/must pass through a (not known in advance) hierarchy of gateways. In other words, PI gateways must be able to dynamically set up opportunistic networks to deliver their services.

In this direction, in this paper we propose a recursive version of the gateway-mediated edge connectivity and management pattern, as depicted in Figure 3. In this architecture every single local area network, which can be mapped in the PI context to a smart container, has to interoperate with an arbitrary number of local area networks, resulting in IoT systems shaped as network of networks. To support this architecture PI gateways must be able to self-organize themselves in properly arranged networks by providing all the interoperability and security functionalities required by such a heterogeneous and challenging scenario.

Moreover, since containers cannot know in advance which other containers they will have to interact with, interoperability mechanisms between the corresponding IoT networks must be put in place.

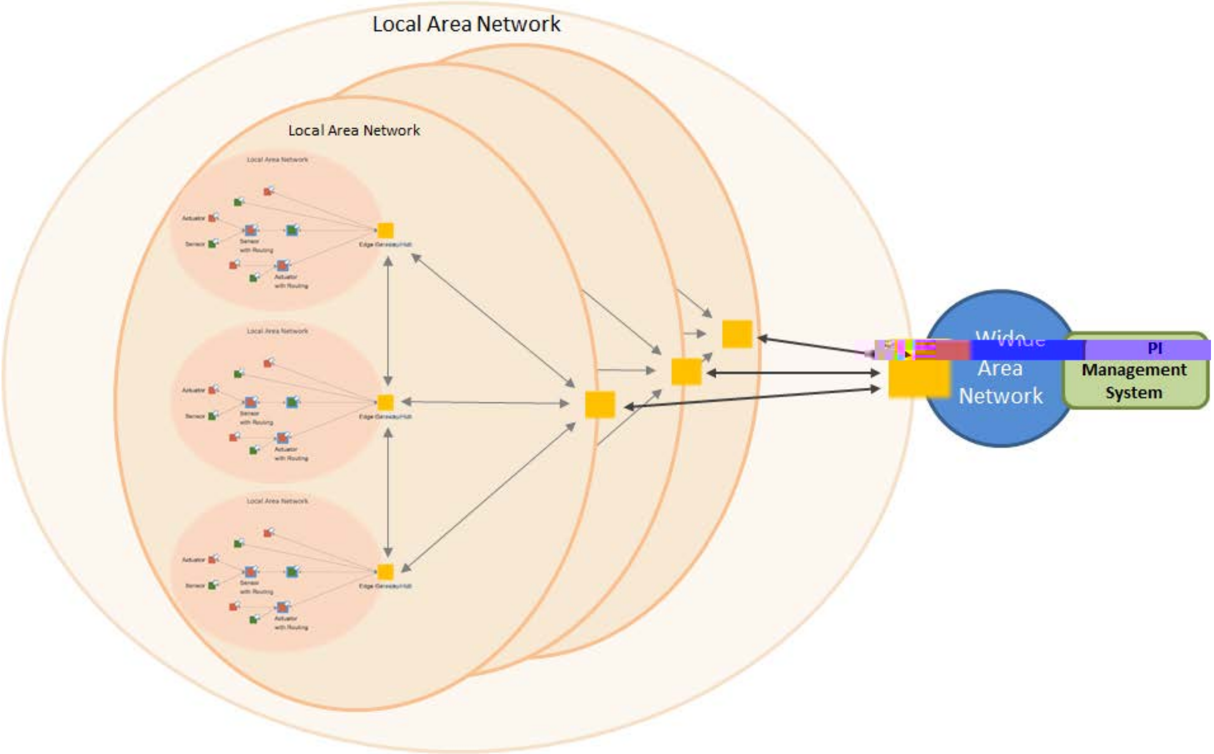

Figure 3: Recursive Gateway-mediated Edge Connectivity and Management pattern

4 PI Smart Containers: interoperability requirements

The IoT world is fragmented. This fragmentation is mainly due to the diverse options of connectivity for end devices provided by manufacturers. We have seen a dramatic growth of communication technology for IoT in the market, targeting different domains. Moreover, there is 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 exploiting proprietary protocol that lead to the creation of vertical IoT silos.

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. In essence, interoperability allows different systems to understand each other even though they speak in different languages.

Interoperability classification for the IoT domain is provided by ETSI (2008), which identify the following interoperability layers (***Figure 4***):

- **Technical Interoperability**: 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**: usually associated with data formats such as RDF, XML, JSON.
- **Semantic Interoperability**: 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**: 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.

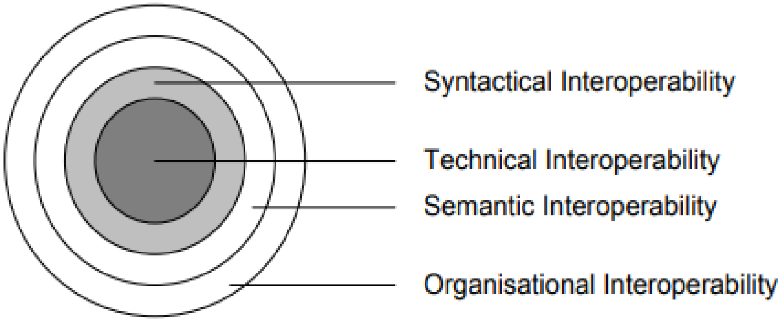
Syntactical Interoperability
Technical Interoperability
Semantic Interoperability
Organisational Interoperability

Figure 4: Dimensions of interoperability

Six generic interoperability design patterns (***Figure 5***) have been identified by IoT-EPI (2018) fostering the implementation of interoperable and easily reusable systems:

- **cross platform access pattern**, envisaging 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**, which extends the previous one by allowing services/applications to access information and functions not only from different platforms, but also from different domains contained in one platform.
- **platform-independence pattern**, which aims at allowing a single application or service to be used on top of different IoT platforms.
- **platform-scale independence pattern**, which 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 spatial-temporal scope, and device-level platforms which allows direct access to sensors and actuators, and host a small amount of data.
- **higher-level service facades patterns**, extending 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**, enabling 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/infrastructure defined by the organizational interoperability.

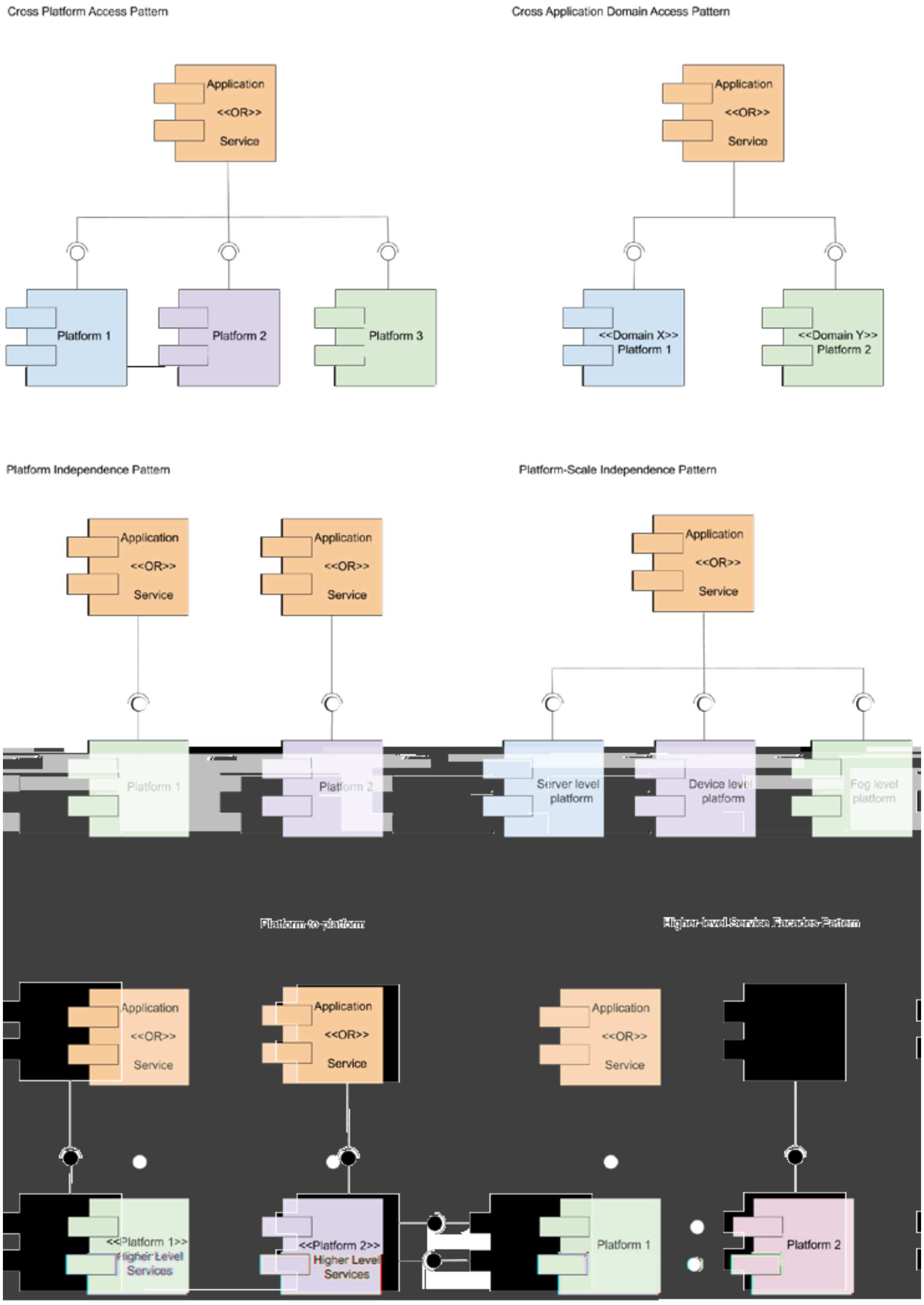

Figure 5: Interoperability design patterns

4.1 Considerations regarding interoperability within PI environments

One of the biggest issues within PI regards the cooperation of the different platforms owned by the different stakeholders involved in the logistics transactions, to realise an open PI environment. For this reason a common language has to be defined between the different platforms, implementing both the semantic and organisational interoperability (following the ETSI interoperability layers mapping, as depicted in ***Figure 6***).

Regarding the IoT components, they are usually connected with the Cloud platform owned by the mentioned stakeholders. For example, the tracking information will be collected by the shipper platform and, afterwards, shared with the common PI platform. In this scenario, the IoT components have to satisfy the technical and syntactical interoperability, thus focusing on the connection between sensor nodes and the IoT gateway, and the connection between the IoT gateway and the cloud server.

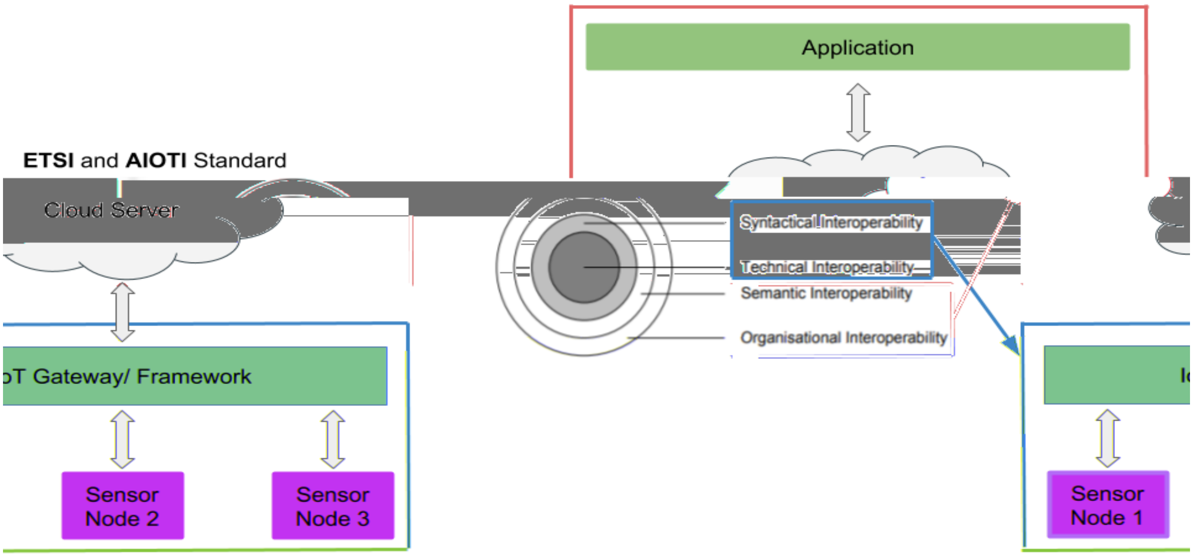
Application
ETSI and AIOTI Standard
Cloud Server
Syntactical Interoperability
Technical Interoperability
Semantic Interoperability
Organisational Interoperability
oT Gateway/ Framework
Sensor Node 2
Sensor Node 3
Sensor Node 1

Figure 6 ETSI interoperability layers mapping

5 Validation activities

The validation activities of the work proposed in this paper will be realised within the Living Lab 2 (LL2) of the ICONET project, called Corridor-centric PI Network. This LL 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 7*** and ***Figure 8***.

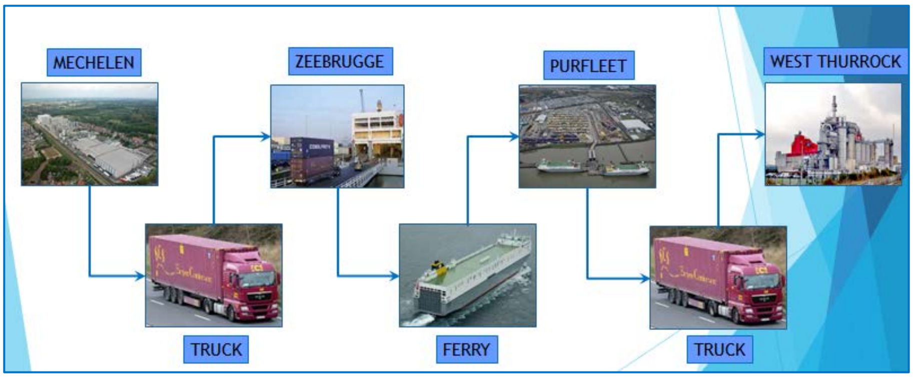

Figure 7: Corridor Mechelen (B) - West Thurrock (UK)

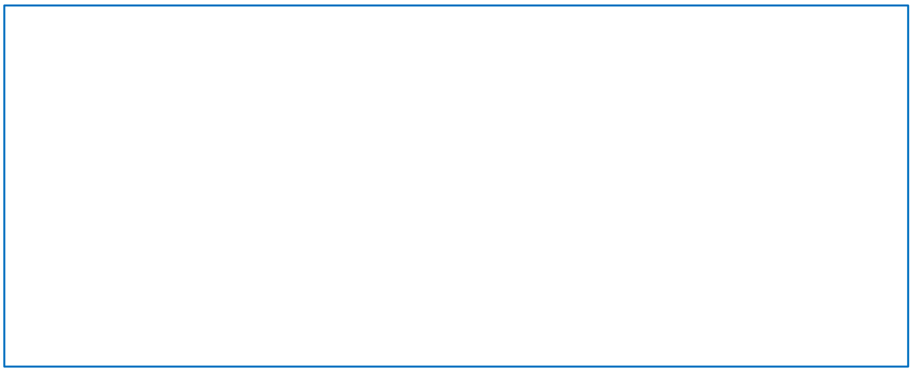

Figure 8: Corridor Mechelen (B) - Agnadello (I)

Particularly, in this LL the physical container will be upgraded to become a PI Smart Container, thus equipped with both IoT sensors, and an interoperable remote communication, to dispatch the data remotely toward the PI remote platform.
As discussed in Sec. 3, the PI Smart Containers will be evaluated in terms of the improvements they will be able to introduce with regard to the KPI depicted in ***Table 1***.

KPI ID	KPI Name	KPI Description
	Goods monitoring	
	Product safety	
	Support decision making processes	
	Real time reporting	

Table 1: Smart Containers KPIs

The instance of the generic architecture of ***Figure 3*** to implement the PI Smart Container is depicted in ***Figure 9***, where each container will be equipped with an optimised and battery powered gateway capable to:

1. Collect data from sensors nodes deployed within the container (e.g., the presence of certain goods, the environmental temperature and the humidity, …).
2. Dispatch these data, remotely in a geo&time-referenced manner.

Figure 9: PI Smart Container network architecture

5.1 The considered devices

The considered hardware devices for the implementation of container tracking and monitoring services (and developed by New Generation Sensors within the ICONET project) are:

- The *FLEXX tracker*, that represents the first step toward the realisation of the "Smart PI-container". In fact, it will be in charge of collecting position and time information of the considered PI-containers and dispatch those toward the Cloud platform, thus answering to the questions "Where?" and "When?". Moreover, on-board sensors will allow the container internal monitoring, thus answering to the question "How?".
- The *Micro-FLEXX gateway* will aim of implementing an advanced release of the Smart Container. This release will allow to track the container along the corridors, but also to: (i) monitor the presence of connected PI-packets encapsulated within it (e.g., monitoring pallets within the container, in a "groupage[1]" configuration); (ii) collect added value environmental data inside/outside the container, exploiting short range IoT protocols.

5.1.1 Implemented interoperability patterns

As defined in Sec. 4.1, the interoperability level considered to connect the IoT environment with the remote Cloud platform are the first two in the ETSI mapping (see ***Figure 4***, i.e., technical and the syntactic level).

On the other hand, the interoperability patterns applied to connect the remote cloud platforms together with the IoT environment depends directly the considered protocol. In the scenario of FLEXX tracker and Micro-FLEXX gateway, the exploitation of a mobile IoT protocol (e.g., GPRS, NB-IoT, LTE Cat-M, …) allows the application of the Platform-to-

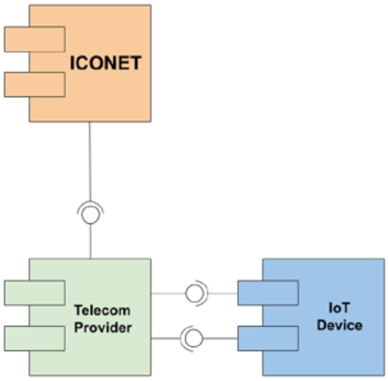

Figure 10 Platform-to-Platform pattern

6 Conclusion

The end PI goal is to realize efficient logistics transactions, in order to reduce their cost and their impact on the environment. In this paper we highlighted that IoT is a keystone technology of the PI framework, since it provides the continuous flow of information needed to implement the so-called synchro-modal functionalities. In fact, exploiting the data collected from the IoT sensors, the PI environment and the platforms on which it is based can retrieve the position and the status of the goods in a time referenced manner, answering to the questions: “When?”, “Where?” and “How?”.

To define an innovative and generalized IoT architecture capable of enabling synchro-modal functionalities in the PI environment we analysed the requirements highlighted by domain and TLC experts in the context of the ICONET project. The architecture we propose in this paper answers on the one hand to the inherent modularity of logistics, and on the other hand to the hierarchy derived by the encapsulation capabilities of packets, pallets and containers. For these reasons, an innovative, opportunistic and pervasive IoT network architecture is designed to provide connectivity to all the actors involved in the logistics transactions.

This report describes the need to implement both technical and syntactic interoperability functionalities for the IoT and the remote communication networks, thus simplifying the integration of commercial-of-the-shelf sensors nodes and the integration with the PI platforms respectively. From these considerations, a set of different protocols (standardized and not) and interoperability patterns are evaluated and selected.

The architectural and interoperability solutions presented in this paper are planned to be extensively assessed in the ICONET Living Labs, providing a sound ground for future PI development.

7 Acknowledgements

The work described in this paper was funded by Horizon 2020 Research and Innovation Programme under Project ‘ICONET’ (grant agreement No 769119).

References

- ETSI (2008) : Achieving Technical Interoperability – the ETSI Approach. White Paper No.3, 3rd edition.
- ICONET project, https://www.iconetproject.eu/
- Ineo-sense, https://www.ineo-sense.com/smart-container-logistics-security-seal/
- IoT-EPI (2018): *Advancing IoT Platforms Interoperability*. River Publishers Series in Information Science and Technology.
- Krommenacker N., Charpentier P., Berger T., Sallez Y. (2016) : *On the Usage of Wireless Sensor Networks to Facilitate Composition/Decomposition of Physical Internet Containers*. Service Orientation in Holonic and Multi-Agent Manufacturing, Springer, v640, 81-90.
- Modulushca Project. http://www.modulushca.eu/.
- Montreuil B., Ballot E., Tremblay W. (2016) : *Modular design of Physical Internet containers*. Progress in Material Handling Research, vol. 13, MHI.
- Montreuil B., Meller R. D., Ballot E. (2012): *Physical Internet Foundations*. IFAC Proceedings Volumes, v45, no6, 26-30.
- Sallez Y., Pan S., Montreuil B., Berger T., Ballot E. (2016) : *On the activeness of Intelligent Physical Internet containers*. Computers in Industry, v81, 96-104.
- SmartSensor, http://www.dhl.com/en/about_us/logistics_insights/dhl_trend_research/smartsensor.html
- Traxens, http://www.traxens.com