H2020 Work Programme 2016-2017

H202-IoT-02-2016

Duration: 36 months

CROSS FERTILISATION THROUGH ALIGNMENT, SYNCHRONISATION AND EXCHANGES FOR IoT

H2020 – CREATE-IoT Project

Deliverable 06.03

Assessment of convergence and interoperability in LSP platforms

Revision: 1.00
Due date: 30-04-2020 (m40)
Actual submission date: 03-05-2020
Lead partner: ETSI

Dissemination level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Summary					
No and name	**D06.03 Assessment of convergence and interoperability in LSP platforms.**				
Status	Released	**Due**	m40	**Date**	30-04-2020
Author(s)	E. Darmois (ETSI), D. Raggett (ERCIM), O. Vermesan (SINTEF), R. Bahr (SINTEF), M. Serrano (NUIG).				
Editor	E. Darmois (ETSI)				
DoW	The work has been carried out within task T06.01 (IoT Interoperability, standards approaches, validation and gap analysis), and is the final deliverable from this task. T06.01 coordinates the activities with the AIOTI WG on standardisation, SDOs and other various IoT Global Alliances for the validation in usage context of most promising standards and gap analysis identification. It addresses interoperability and integration, through open IoT platforms.				
Comments					

Document history			
Rev.	**Date**	**Author**	**Description**
0.01	02-01-2020	SINTEF	Template/Initial version.
0.02	19-03-2020	ETSI	Initial description of work, and structure.
0.03	21-04-2020	ETSI	Additional content on several clauses
0.04	28-04-2020	ETSI	Restructuring and additional content on several clauses
0.05	30-04-2020	SINTEF	Contribution on the AUTOPILOT Interoperability Framework.
0.06	30-04-2020	ETSI	Restructuring and additional content on several clauses
0.07	30-04-2020	ETSI	Review of section 4 and other small additions
0.08	02-05-2020	ETSI	Final contributions, alignment with D06.03, edits.
0.09	03-05-2020	ETSI	Alignment with D06.03: integration of ERCIM's contribution.
0.10	03-05-2020	SINTEF	Internal review and comments considered.
1.00	03-05-2020	SINTEF	Final version released.

Table of contents

Figures

Tables

1. EXECUTIVE SUMMARY

1.1 Publishable summary

A major challenge for the Internet of Things (IoT) is to enable a large range of innovative services based upon the connection through the Internet of a large set of applications that use the data produced by a variety of sensors and actuators in very different contexts, domains and business models. To reap the expected benefits of the IoT, enable easy deployment of applications, reducing the costs and risks, and providing the confidence and trust, the IoT ecosystem will require that interoperable platforms and technologies be available to the IoT systems designers and developers. These platforms and technologies will be highly relying on common technical elements and solutions that are referred to as an Interoperability Framework.

The purpose of this document is to outline the approaches, the choices and the major results of the LSPs regarding interoperability and platform/technology activities. The accent is put on topics like: the Reference Architecture(s); the main technologies chosen and how they have been dealt with; the new mechanisms that have been developed in support of several scenarios of interoperability; and the supporting IoT platforms and how they are integrated when (which is the case for many of the LSP's use cases) several platforms are participating to the provision of the same service..

This document presents the resulting "LSP Interoperability Framework", and in particular the 3-dimensional Reference Architecture model developed. The 3D model is devised in order to provide a common approach (and a sizeable methodology) to support the various stakeholders involved, across the whole IoT system lifecycle, in the definition, design and deployment of IoT systems.

The expected benefit of the proposed approach is to propose a way to help the many stakeholders involved in the development of IoT systems (across the whole IoT system lifecycle) identify the support they can get from interoperable platforms and technologies, supported by advanced interoperability mechanisms and development methodologies.

More information on the "LSP Interoperability Framework" can be found in the companion deliverable to this document: CREATE-IoT Deliverable D06.06 "Final Report on IoT standardisation activities" [6].

1.2 Non-publishable information

None, the document is classified as public.

2. INTRODUCTION

2.1 How to use this document

2.1.1 Scope and purpose

This document attempts to summarise the achievements of the work done in the EU IoT Large-Scale Pilots Programme projects and assess their relevance and impact within an IoT community which has strongly matured over the more than three years duration of the Large-Scale Pilots projects (LSPs).

The primary purpose of this document is to outline the approaches, the choices and the major results of the LSPs regarding interoperability and platform/technology activities. The accent is put on topics like: the Reference Architecture(s); the main technologies chosen and how they have been dealt with; the new mechanisms that have been developed in support of several scenarios of interoperability; and the supporting IoT platforms and how they are integrated when (which is the case for many of the LSP's use cases) several platforms are participating to the provision of the same service.

In order to maximise the commonalities and the resulting impact of the LSPs, they all have participated to the work within the LSP Activity Group 02 ("Standardisation, Architecture and Interoperability") in coordination with the CREATE-IoT Coordination and Support Action (CSA).

This document presents the resulting "LSP Interoperability Framework", and in particular the 3-dimensional Reference Architecture model developed. The 3D model is devised in order to provide a common approach (and a sizeable methodology) to support the various stakeholders involved, across the whole IoT system lifecycle, in the definition, design and deployment of IoT systems.

2.1.2 Target group

The target group for this document is the community of people that have to address the definition of the LSPs from inception to implementation, in particular regarding the main technical choices that have to be made in order to ensure that the implementations will be effective, interoperable and scalable:

- The identification of the main elements (e.g., reference architectures; technologies and platforms; development methodology, development environments) of the Interoperability Framework that has been used for the implementation of their use cases by the LSPs
- The identification of commonalities and differences regarding IoT platforms interoperability.
- The selection of the reference architecture for the description of the interoperability layers and the main building blocks for the implementation of use cases.

2.2 Contributions of partners

This deliverable is the final deliverable of CREATE-IoT Task 06.01 (IoT Interoperability, standards approaches, validation and gap analysis). The list below shows the specific contribution of partners to the current deliverable.

ETSI: As Task Leader and editor of the deliverable, ETSI has contributed to the definition of the overall content and scope of the deliverable, to the definition of the IoT Interoperability Framework, to the synthesis of the main elements of the Framework based on the Activity Group 02 Workshops, and to the review of the deliverable.

ERCIM has contributed to the definition of the overall content and scope of the deliverable, to several sections of the document (based in particular on the work done in Activity Group 02), and to the review of the deliverable.

SINTEF has contributed to the definition of the overall content and scope of the deliverable, provided contributions to various sections of the document based on its involvement in one of the LSPs (e.g. AUTOPILOT), and to the review of the deliverable. SINTEF contributed to the definition of the IoT Interoperability Framework, 3-dimensional IoT Reference Architecture model, the mapping of the IoT platform components to the IoT architectural layers and the definition of crosscutting functions and system properties.

NUIG provided contributions to various sections of the document based on its involvement in one of the LSPs (e.g. ACTIVAGE), and to the review of the deliverable.

2.3 Relations to other activities in the project

The present document has been produced by the CREATE-IoT Work Package 6 " IoT Interoperability and Standardization". WP06 is structured into two complementary tasks:

- Task 06.01 ("IoT Interoperability, standards approaches, validation and gap analysis") focuses on practical topics regarding the implementation of LSP Use Cases.
- Task 06.02 ("Pre-normative and standardisation activities") focuses on the contributions from the LSPs and CREATE-IoT to the IoT standards ecosystem. The present document is a deliverable of this task.

The present document has been developed in Task 06.01 and constitutes its final deliverable. It is one of the two deliverables (D06.03 and D06.06) that present and assess the results of the CREATE-IoT Work Package 6.

A very important part of the work for the present deliverable has been done in the context of the IoT LSPs Activity Group 02 (AG02 - "IoT standardisation, architecture and interoperability") that coordinates the activities of the LSPs and of the two associated Coordination and Support Actions (CSA), CREATE-IoT and U4IoT, on interoperability and standardisation. The information has been gathered and discussed in several workshops held in 2018 and 2019 ([8], [9], [10] and [11]). Whose main objective was to establish a common basis across the different IoT Large-Scale Pilots (LSPs) regarding topics such as: reference architecture models; interoperability framework and reference implementations based on use cases; analysis of components and standards, existing IoT platforms, etc.

The present deliverable is complementary to deliverable D06.06 " Final report on IoT standardisation activities " (produced in Work Package 6 Task 06.02). Whereas the present deliverable focuses on interoperability aspects, in particular the Interoperability Framework, D06.06 focuses on standardisation aspects.

The work on standardisation outlined in the current deliverable is making use of the work of CREATE-IoT Work Package 2 ("IoT Large-Scale Pilots Ecosystems Arena for Sharing Common Approaches "), in particular when it comes to Use Cases, open APIs or common methodologies (as was done in D02.02 “Reference Architecture for Federation and Cooperation Between IoT Deployments”[12]).

This deliverable is addressing some of the issues that are in the scope of WP05 ("IoT Policy Framework - Trusted, Safe and Legal Environment for IoT"). The requirements in terms of security as well as in terms of privacy – whose coverage will ensure trust and user acceptance - are key to the success of LSPs.

3. IoT INTEROPERABILITY FRAMEWORK AND CONVERGENCE

3.1 The need for IoT interoperability

The Internet of Things has matured during the course of the development of the Large-Scale Pilots. It has become a business and technology ecosystem that supports the definition of innovative and complex services, spanning across variety of business sectors (e.g., food, health, industry, transportation, etc.).

In the early developments of IoT systems, many of the available solutions in the market have been developed in the form of application silos, often supporting large numbers of devices and users, but where interoperability was limited by the scope of the specific solutions selected that could not operate in other systems or domains. The spectacular maturation of IoT and the possibility to define more complex and interconnected services has required solutions that are less and less confined in silos. Examples of such use cases are services in Smart Cities that aggregate existing services in different city silos, or Industrial IoT applications that require the integration of IoT solutions with other solutions (often legacy ones) in complex value chains.

As a consequence, interoperability has become a major challenge for those who want to define, develop and deploy IoT systems. In addition, in many of the new IoT systems, the number of IoT devices is potentially (very) large as can also be the number of end-users: for such systems, interoperability needs to support scalability. In order to limit the trade-off between interoperability and scalability, it is important to identify the best practices to design, develop and implement large-scale interoperable IoT systems using as many standardised generic solutions as possible, even if they are used in different sectors.

As a result of the early days of developing point solutions, the huge potential for IoT can be limited by fragmentation into incompatible platforms, standards and technologies. A key objective for IoT systems designers and developers is to make sure that interoperability is supported wherever it is needed within or across IoT systems. The rationale for building a common Interoperability Framework is to reduce duplication and fragmentation, and to address interoperability through various angles: operational behaviour, information exchange, technology integration, etc.

3.2 Interoperability Levels and Objectives

The complex IoT systems that are now deployed in fully operating settings are, in most cases, an aggregation of heterogeneous elements such as large variety of devices, communication protocols, data models, software components from various sources, etc. A key objective for the designers and developers of such IoT systems is to make sure that interoperability is supported wherever it is needed within IoT sub-systems as well as or across IoT systems.

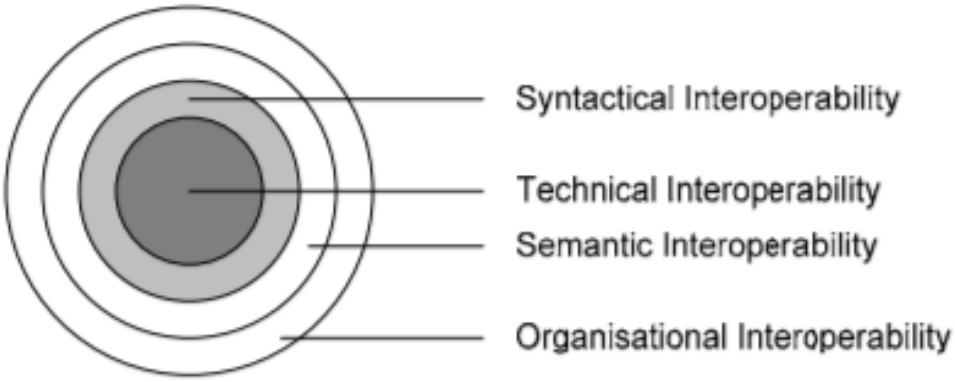


Figure 1: Layers of Interoperability

Interoperability can be seen through various angles: operational behaviour, information exchange, etc. By far, interoperability cannot be reduced to a means for two systems to exchange information at the network layer. In particular, a layered approach to interoperability has become the accepted paradigm for the description of systems (and this is also true for IoT systems) with a specific focus on four layers. More precisely:

- *Technical Interoperability* is associated with communication protocols and the infrastructure needed for those protocols to operate.
- *Syntactic Interoperability* is associated with data formats and encodings along with techniques for compressing them.
- *Semantic Interoperability* is associated with shared understanding of the meaning of the exchanged content (information).
- *Organisational Interoperability* is associated with the ability of organisations to effectively communicate and transfer information even across different information systems, infrastructures or geographic regions and cultures.

3.3 IoT interoperability frameworks

3.3.1 Requirements

Interoperability requires agreements between elements of a system that may be of very different nature, not only technology but also other systems and elements in the ecosystem.

On top of the interoperability requirements addressed in generic manner by IT systems, some more IoT specific ones have to be taken into account. Table 1 outlines the major requirements that need to be supported by an IoT Interoperability Framework.

Table 1: Interoperability objectives and associated layers

Interoperability Objective	Rationale	Interoperability Layer
Support of common IoT communication protocols	Due to the fact that different types of devices can be used in different locations of the ecosystem, there should be no limitation on the supported communication protocols.	Technical
Support for M2M communications	The interaction between IoT nodes can follow the concept of Machine-to-Machine (M2M) communication with machines communicating with back-end information systems and/or directly with other machines, in order to provide real-time data and run processes.	Technical
Standard protocols for device communications	Devices need a standard protocol to exchange data with any platform and providing at least ID, security, authentication, position, etc. The protocols are technology dependent but should be compliant with European and International standards.	Technical
Support of the main IoT middleware platforms	Given the diversity of IoT middleware platforms available, support to the most adopted one is needed. The system under design needs to be connected to the different IoT platforms to access their services in order to enable the software wrappers that will support interoperability.	Technical

Interoperability Objective	Rationale	Interoperability Layer
Unique Device ID / Naming	An identifier system must be developed/selected in order to be able to identify each device in a unique way. In addition, there should be no limitation on the number of devices that can be connected, and the number of identifier codes must be large enough to accompany all current and future devices.	Technical Syntactic
Gateway Capabilities and Protocol Conversion	The system must have gateway capabilities and support multiple interfaces to work with different protocols and operation modes with a gateway running at the device layer or at the network layer.	Technical Syntactic
Extensibility for different sensor types	The system architecture must be able to receive data from multiple sensor types and foster extensibility. It should be able to easily support extensions, upgrades and inclusion of new modules as they are being integrated	Syntactic
User Device Detection Capability	The system architecture must provide tools and services for checking the capacity of user's devices. With device-detection techniques and exchange of communication protocols, this information must be verified upfront.	Syntactic
Syntactic interoperability	Syntactic interoperability can be achieved through a simple mapping- translation mechanism, by using dedicated wrappers (connecting producers and consumers of data) to interpret a model and get the necessary information to be passed to another component.	Syntactic
Semantic interoperability	Semantic interoperability must be supported in order to exchange not only data, but information and features related to the source of the information i.e. location, status, technology associated, etc. facilitating the reduction of the vertical information silos of the different heterogeneous platforms that the current IoT data lakes represents.	Semantic

3.3.2 Main elements

The IoT community has addressed the question of interoperability in many initiatives during the 2010s. The objective was to rationalise the approach to interoperability by relating it to several elements around which the main design and technology decisions could be taken in the development of an IoT system.

The following elements have been gradually emerging as key elements for building coherent and complete frameworks:

- *Reference Architectures*. In order to achieve interoperability, a lot of elements such as models, definitions or well-defined set of vocabularies need to be agreed upon by the IoT stakeholders in order to ensure a common understanding about the concepts, this is also a preamble to standardisation.
- *Platforms and technologies*. There are hundreds of IoT platforms available for the development of IoT systems. The question of a choice of platform(s) by IoT system

designers is complex. Some dimensions have to be considered such as their scope and breadth, the maturity and ownership of their components, and the level of support by standards (and more and more by Open Source).

- *Support of design and development*. For several IoT projects, in particular those who span large domains (e.g., Smart Cities), cross-domain interoperability is a key requirement for achieving large scale deployment of IoT-enabled services. On top of a reference architecture model, other elements are required such as cross-application interoperability points (describing where interoperability is supported) and some supporting mechanisms (describing how the support is provided). On top of ad-hoc approaches, project by project, some specifications and standards are emerging to this purpose.
- *Standards and pre-normative activities.* Standards are a key element in the IoT Interoperability Framework. A first requirement is to clearly outline the support offered by the current state-of-the-art in standardisation. Beyond this, it is also important to outline the gaps and overlaps (in particular the standard's gaps and overlaps): the missing elements of the IoT landscape, mostly due to its complexity, that need to be identified before they may be resolved in the near future. Pre-normative activities explore promising directions, and just as importantly, attempt to present these in ways that are easy to explain to other communities, thereby helping to build a shared understanding on what new standards are needed. As already pointed out, these aspects are addressed in the companion deliverable D06.05 (Initial report on IoT standardisation activities) [5].
- *Alignment with other IoT architectures.* A key requirement for the system architecture is the alignment with the reference models of other IoT projects, especially The Alliance for Internet of Things Innovation (AIOTI) for example. The AIOTI HLA architecture model is suitable for guiding the development of any LSP architecture. The use of the AIOTI vision of the Internet Architecture of Things will be useful to use its results and other projects to avoid reinventing a new architectural model from scratch and align and be compatible with those projects.

3.3.3 Reference Architecture Models

3.3.3.1 A coherent view of IoT systems across the interoperability levels

The four levels of interoperability (defined in 3.2) are outlining a series of interoperability challenges related to the complex nature of the elements addressed at each of the levels: protocols at the technical interoperability layer, data models at the syntactic interoperability level, meaning of information at the semantic interoperability layer or organisation workflows at the operational interoperability level.

Interoperability may be required between different elements that are defined within a given level, with the example of technical interoperability where a high number of available protocols may have to be handled concurrently within an IoT system, for instance because different devices have to cooperate in the provision of a given service).

Interoperability can be required as well as across adjacent levels with the issues related to making interoperable elements that are defined for syntactic interoperability (e.g., static data models for information exchange) with elements defined for semantic interoperability (e.g., ontologies), for instance for ensuring that greenfield IoT systems are able to work with legacy systems (such as frequently required in Industrial IoT).

In order to achieve intra-level interoperability, a lot of elements such as models, definitions or well-defined set of vocabularies need to be agreed upon by the IoT stakeholders in order to ensure a common understanding of the concepts.

But this may not enough to provide a global and coherent view of the IoT system under consideration (e.g., under definition, design, deployment).

This requirement for offering a coherent view of a system to the stakeholders involved (system contractors, designers, developers, security specialists, etc) has induced the creation of reference architectures potentially able to deal with a very large variety of IoT systems architectures.

The adoption and utilization of reference architectures is meant to provide a blueprint for the design and development of future systems and components and can be used for various purposes such as:

- To communicate on a common view and language about a system, within a sector, across industry, customers, regulators, etc.
- To support the analysis and evaluation of variant implementations of an architecture.
- To integrate various existing state-of-the-art approaches into one model.
- To support the transition from an existing legacy architecture to a new architecture.
- To help assessing conformance to identified standards or interoperability requirements.
- To document decisions taken during the development process of a system.

3.3.3.2 Examples of IoT Reference Architectures

Some examples of relevant reference architectures are listed in Table 2. They have been developed in within projects (e.g., EU projects), Standardisation organisations or Alliances.

Table 2: Examples of IoT Reference Architectures

Organisation	Description
AIOTI	The HLA primarily introduces a domain model, which describes entities in the IoT domain and the relationships between them, and a functional model, which describes functions and interfaces (interactions) within the IoT domain. The AIOTI functional model describes functions and interfaces between functions of the IoT system. Functions do not mandate any specific implementation or deployment.
ETSI CIM NGSI-LD	ETSI NGSI-LD is the specification of a standard Application Programming Interface (API) to manage Context Information Management at large scale. The adoption of this API in order to get access to context data allows breaking silos and vendor-locks and abstracts the complexity and low-level details of the multiple IoT protocols that may be part of the same system. An open-source reference implementation of NGSI-LD standard is provided with FIWARE Context Broker component.
IEEE P2413	IEEE P2413 defines an architectural framework for the IoT that provides a reference model which defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements. It also provides a blueprint for data abstraction and the four elements for trust that include protection, security, privacy, and safety."
IIC	The Industrial Internet Consortium (IIC) has developed the Industrial Internet Reference Architecture (IIRA) in order to address the need for a common architecture framework to develop interoperable IIoT systems for diverse applications across a broad spectrum of industrial verticals in the public and private sectors.
Industrie 4.0 RAMI	Industrie 4.0 aims at connecting all stakeholders involved in the business processes of the manufacturing and process industry so that all participants involved share a common perspective and develop a common understanding. The Reference Architectural Model Industrie 4.0 (RAMI 4.0) is a three-dimensional map in support of the most important aspects of Industrie 4.0 which aims at connecting all stakeholders involved in the business processes of the manufacturing and process industry.
IoT-A	The IoT-A (Internet of Things - Architecture) project has proposed an IoT-A Architectural Reference Model (ARM) together with the definition of an initial set of key building blocks. The IoT-A ARM is a set of best practices, guidelines, and a starting point to generate specific IoT architectures

Organisation	Description
ISO/IEC CD 30141	ISO/IEC CD 30141 (developed by ISO/IEC JTC 1) is a standardized IoT Reference Architecture using a common vocabulary, reusable designs and industry best practices. It uses a top down approach, provides a generic IoT conceptual model, a high-level system-based reference model and five architecture views: functional view, system view, user view, information view and communication view.
ITU-T SG13 Y.2060	ITU-T Y.2060 provides an overview of the IoT; clarifies the concept and scope of the IoT, identifies the fundamental characteristics and high-level requirements of the IoT and describes the IoT reference model: four layers (application, service & application support, network and device), complemented with two verticals (management and security).
OASC	OASC addresses a technical plane and focuses on off-the-shelf and open data platforms and solutions that have been extensively assessed before. A clear objective is to guarantee interoperability among cities with a "driven-by-implementation" approach relying on three domains: Common APIs, Data Models and Open Data Platform.
oneM2M	oneM2M is developing specifications for the service layer for machine-to-machine communication and the IoT. oneM2M aims to provide common services layer to IoT applications and devices of different service domain/verticals. The oneM2M Common Services Layer provides common service functions to applications and devices in the form of APIs: by providing the common services layer, different vendors and service domains can use the same APIs
W3C	The W3C WoT architecture, an abstract architecture for the Web of Things (WoT), which seeks to enable interoperability across IoT platforms and application domains, is designed to describe what exists rather than to prescribe what to implement, i.e. to preserve and complement existing IoT standards and solutions. The approach is illustrated in respect to a variety of different deployments and accompanied with security and privacy considerations.

3.3.4 Supporting Mechanisms

Research and pre-standardisation activities have addressed the issue of providing higher-level constructs in support of interoperability.

One of the objectives is to offer a way to improve the effectiveness of Application Programming Interfaces (APIs) by offering a more dynamic support to their application to different syntactic and semantic contexts (by providing possible mapping) or by finding ways to organise the identification of and subscription to APIs in structured exchange places (and provide a path in the "jungle of APIs"). Another objective is to push those mechanisms towards standardisation.

Several approaches, under consideration and development in the LSP community and beyond, are analysed below.

In these developments, the IoT European Platforms Initiative (IoT-EPI) has been instrumental in providing a coordinated view (available in [31] and [32]) of several EU H2020 research projects involved in the development of advanced IoT platforms.

3.3.4.1 Semantic Interoperability

Beyond Technical Interoperability, syntactic and semantic interoperability have been expanded over time to provide effective support mechanisms that may help the IoT application developers and ensure that they can effectively use supporting standards proposed by the industry.

The main expectation of semantic interoperability is to provide a shared unambiguous meaning of what the "things" that two (or more) platforms may agree upon, thus bridging the potential

semantic gap coming from different descriptions and implementations of the "thing" under concern.

The challenge of semantic interoperability is in general a cross-platform issue, though it can be also met with two components on the same platform.

The IoT-EPI has proposed a classification of the possible approaches to semantic interoperability with a model that is depicted in Figure 2. There are two dimensions in their analysis:

- The possible technical approaches that range from a single Core Information Model (CIM) that every platform must comply to (irrespective of the domain or sector) up to the definition of the models that a platform can support with the objective that these models can be aligned by using a semantic mapping that can be shared across platforms;
- The type of interoperability that can be expected: "by chance" (where a platform will interoperate with another one only if their models happen to be the same), "by standardisation" (where platforms agree on whole or part of a common standardised model) or "by mapping" (where some translation "logic" is applied between different models).

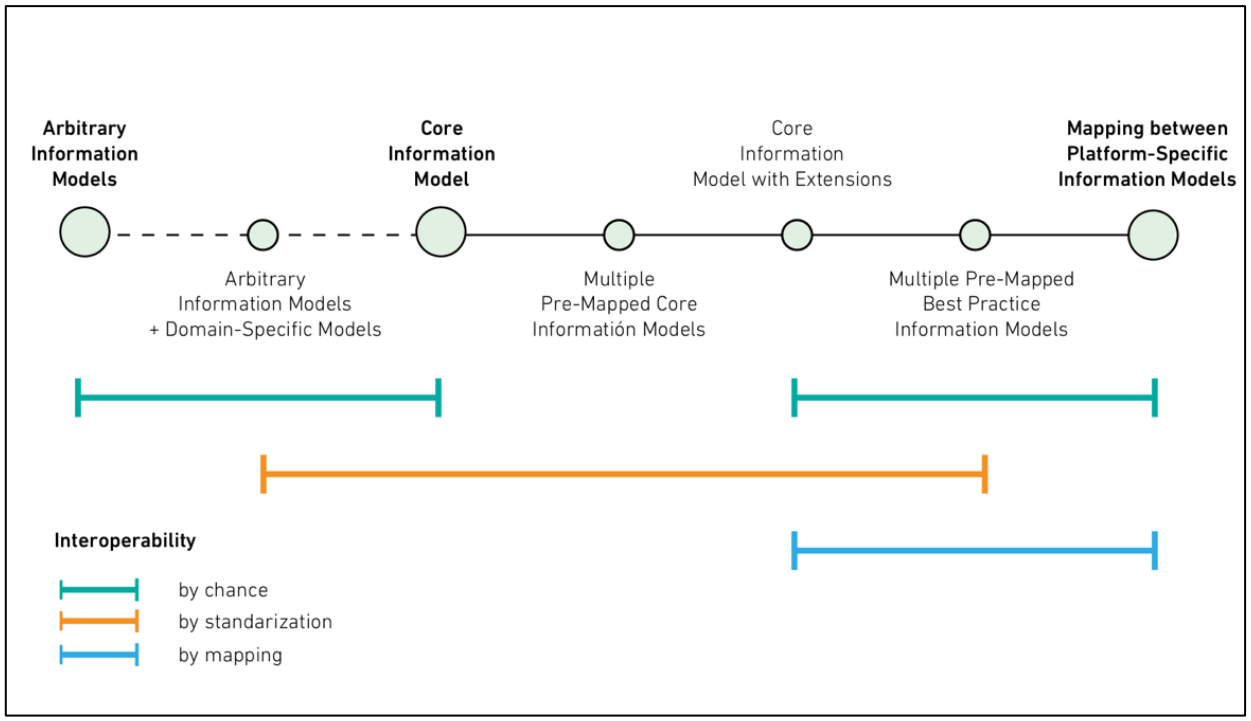


Figure 2: Possible approaches to semantic interoperability

The concrete applicability of semantic interoperability in an industrial setting has been addressed by ETSI under the form of "Guidelines for Semantic Interoperability in the Industry" [33].

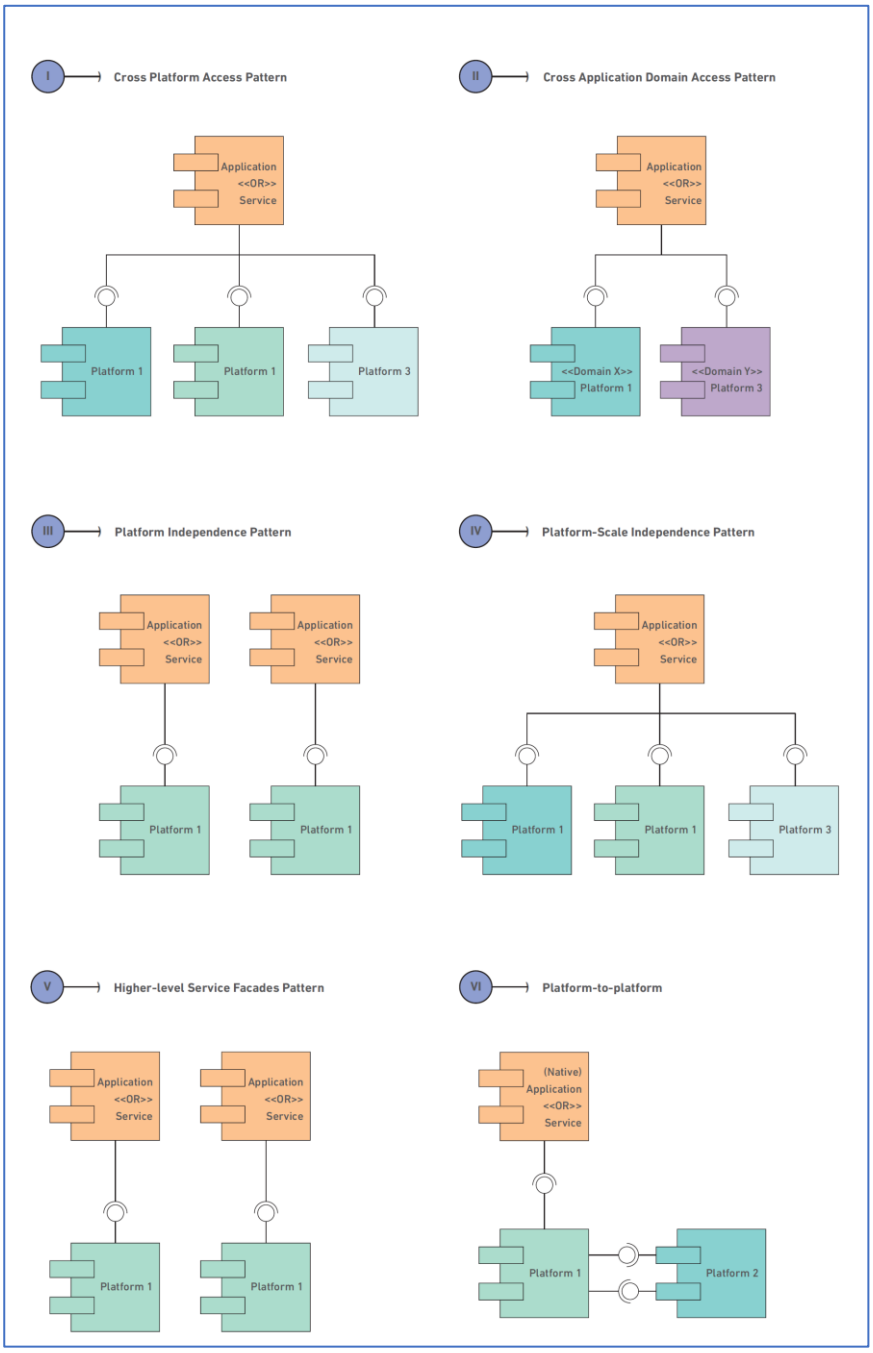
On top of an analysis of the mechanisms in support of semantic interoperability (from glossaries to ontologies), and a presentation of significant existing solutions from academia, standards and industry, the Technical Report provides a set of guidelines to foster a wider adoption of semantic interoperability beyond academics towards industry as a whole.

3.3.4.2 Interoperability Patterns

The IoT-EPI has identified (see [32]) six generic interoperability patterns that apply to systems in general.

The development of efficient IoT platforms is in particular linked to the support they can provide to one or more of these patterns.

The six patterns are described in Figure 3.



I. Cross-Platform Access. The basic pattern where an application can interoperate with several platforms.

II. Cross-Application Domain Access. This pattern expands the previous with the ability to interoperate with platforms in different domains.

III. Platform Independence. The same application or service can be used on top of two different IoT platforms (e.g. in different regions) without changes.

IV. Platform-Scale. With this pattern, the focus is on integrating platforms of different scale.

V. High-Level Service Facades. This pattern extends the interoperability requirements from platforms to higher-level services where not only platforms but also services offer information and functions via the common API.

VI. Platform-to-Platform. This pattern extends the interoperability requirements across platforms.

Figure 3: Six Patterns of Interoperability [32]

3.3.4.3 Interoperability Points and Mechanisms

There is a potentially very large number of ways to architecture an IoT system and no specific guaranty that its different sub-systems will be able to interwork properly.

In order to reduce the difficulty of providing interoperability on this context, a fruitful approach is to reduce the number of contact points between the elements of the IoT system and provide standardised way to manage the necessary interactions.

The two essential elements in support of this approach are the following:

- *Interoperability Points* which are the main interfaces that allow applications to interact with the supporting platform. These interfaces must be independent from the specific software components that realize them and offer various potential implementation variants. Examples

of such interfaces in the context of the LSPs are northbound interfaces, southbound interfaces or shared data models.
- *Interoperability Mechanisms* represent the actual interface specifications at the Interoperability Point. Examples of such mechanisms are standard API (e.g., for security, data storage) and guidelines.

The LSPs have developed such points and mechanisms with, in particular, the solutions developed by SynchroniCity and IoF2020 that are addressed below in section 4.

3.3.4.4 Market Places and APIs

The new paradigm for IoT systems that are subject to large-scale deployments is to use layered, potentially cloud-based or edge-enabled architectures.

Such architectures come with strong requirements on the connectivity between actors (e.g. sensors, gateways, platforms, data processing and analytics functions, etc.) and their support requires complex interoperability schemes.

IoT systems and application developers are expecting that the very large number of devices to be deployed and connected to the network are able to interoperate seamlessly with the largest range possible of platform services (e.g. data analytics, monitoring, visualization, etc.) and very diverse end-user/end-customers applications.

A new approach is to consider the stakeholders of the IoT systems can be seen as consumers and providers within an "application marketplace" which can be seen as a new platform to extends the "traditional" IoT platforms with forms of brokerage that support automated discovery, trading and even pricing.

Within such an IoT marketplace, the IoT device owners have the possibility to selectively grant access and trade their data with many potential vendors.

The support of a multi-vendor and multi-owner environment is creating an environment where monetization and efficiently development of innovative solutions can be effectively fostered.

Marketplace architectures are in general supported by:

- The publication of several Application Programming Interfaces (APIs) that hide the actual underlying provision of the service from the consumer of the service. The implementation of the service can change without impacting the rest of the system and the evolution of the APIs can be mastered via the publication mechanism.
- An approach based on Microservices where any service (whichever its size and scope) can be published and consumed. This approach provides system flexibility; supports lean software principles; and allows fast adaptation to support emerging standards without impacting the whole system architecture. It is in general supported by many Open Source communities.

Data marketplaces

This kind of architecture (and associate solutions) is especially important in the context of the emergence of data marketplaces.

Data marketplaces are enabling the exchange of data sets and data streams and are analogous to the digital marketplaces that have emerged in the last decade.

These marketplaces are still under deployment and are subject to questioning, in particular regarding their commercial viability, discussed in an AIOTI contribution [34] that propose a high-level architecture for an IoT data market place.

Several stakeholders are involved in the provision of the marketplace:
- *Data Sellers* are entities that deploy an IoT infrastructure and are interested in selling the collected data or subsets of that data.

- *Data Aggregators* offer the aggregation of mostly 'dumb' data streams from different sources, merging these data streams to create more valuable sources of information.
- *Managed Data Lakes* would typically store a massive amount of (non-commercial) data and metadata to enable data discovery.
- *Data Enrichers* are buying commercial data or consuming open data with the intention of applying algorithms to enrich data and resell new data sets as a value-added service.
- *Data Buyers* consuming data streams or downloading data sets are interested in the additional value that external data can bring to their internal data.

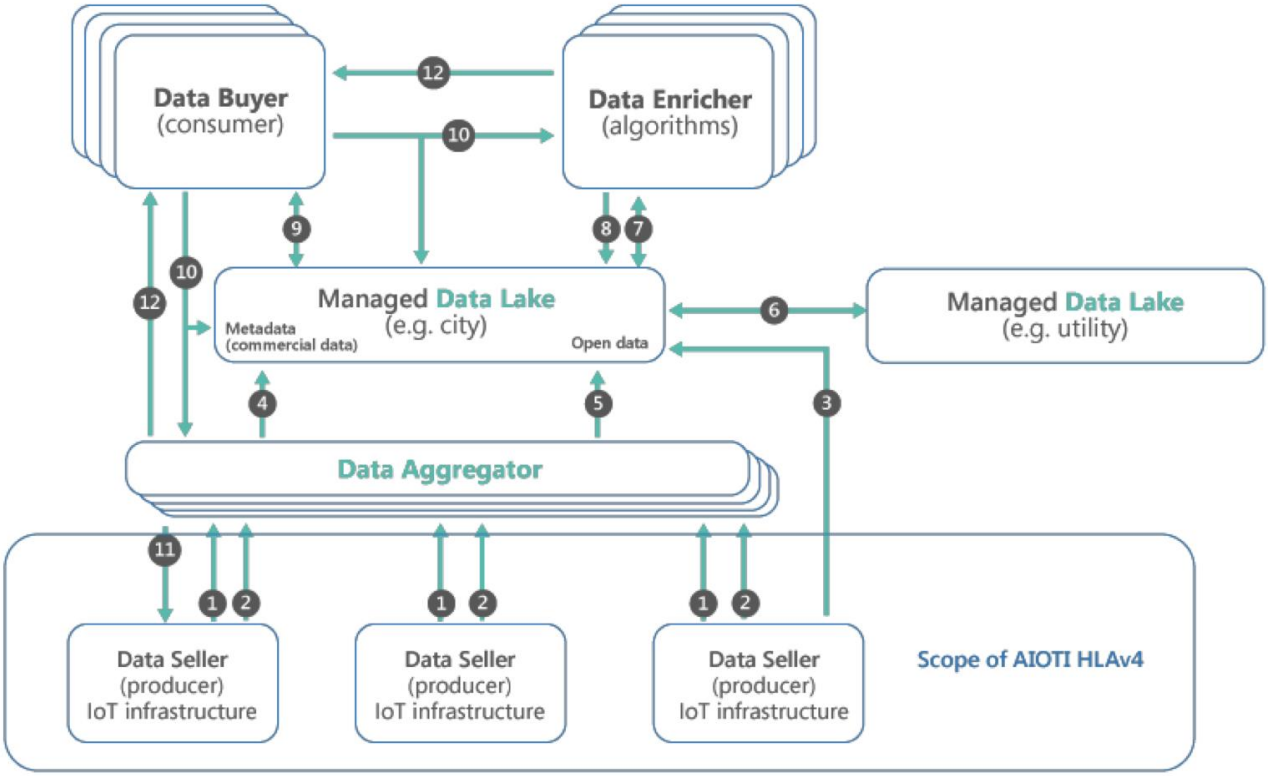


Figure 4: A possible high-level architecture for an IoT Data Marketplace

(source: AIOTI)

3.3.5 Interoperability Framework: Technologies, Platforms and Supporting Environments

This section addresses the requirements related to the IoT platforms, some of which have been used within the LSPs for their use cases implementations.

Those platforms will be potentially very different in span and scope (even within a single LSP).

The purpose of this section is to identify the major platform requirements, how some of these platforms may be chosen and used and how these platforms can interoperate when necessary.

3.3.5.1 The IoT Platform landscape

There are hundreds of IoT platforms available for the development of IoT systems. Several landscape have been undertaken, for example by the UNIFY-IoT Coordination and Support Action (in [35], [36] and [37]) and by the IoT-EPI (in [31]).

The analysis done in 2017 undertaken in Deliverable D03.01 [35] has led to the identification of 24 platforms that are shown in Figure 5.

Though the panorama is largely outdated (with some of the platforms listed terminated in the meantime), their classification is still relevant as to the way the landscape can be analyzed.

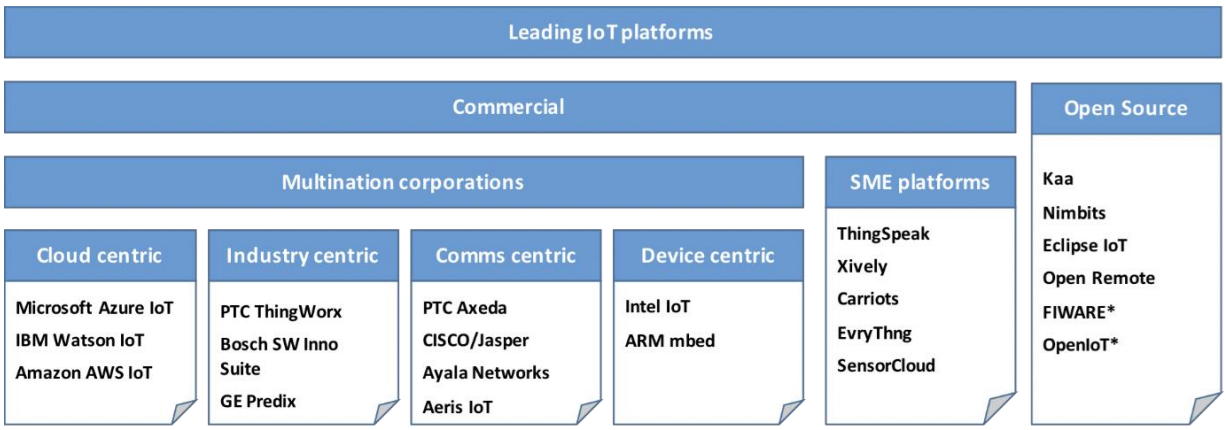


Figure 5: UNIFY-IoT: Leading IoT Platforms selected for in-depth analysis (2017)

The 8 IoT-EPI projects (AGILE, bIoTope, BIG IoT, Inter-IoT, symbIoTe, TagItSmart! and VICINITY) have developed various interoperability solutions addressing different layers in the IoT architecture; and offering mechanisms for providing interoperability between different IoT platforms. The IoT-EPI projects are in general embedding several platforms with a selection of platforms that is a good illustration of the actual situation of many IoT systems which, most of the time, have to deal with legacy platforms that must interoperate with newly developed ones. The Table 3 is listing the platforms used by the projects (those used across several IoT-EPI projects are highlighted in bold). In total, 34 different platforms are used by the 8 IoT-EPI projects referenced.

Table 3: Platforms used by the IoT EPI Projects

Project	IoT Platforms
AGILE	Eclipse IoT, **NodeRED**, Resin.io.
bIoTope	DIALOG, eAir web, **FIWARE**, Mist, **NodeRED**, O-MI/O-DF Reference Implementation, **Open IoT**, Warp 10
BIG IoT	BEZIRK, Bitcarrier/Sensefield/FastPrk, **Open IoT**, Smart City Platform, Smart Data Platform, Traffic Information Center, Wubby
INTER-IoT	AWS, Azure, e-Care Tilab, Eclipse OM2M, **FIWARE**, I3WSN, **NodeRED**, **Open IoT**, SEAMS, Unical BodyCloud, UniversAAL
symbIoTe	KIOLA, MoBaaS, nAssist, Navigo Digitale IoT, **Open IoT**, Symphony
TagItSmart	Evrythng, **FIWARE**, RunMyProcess, SocIoTal
VICINITY	IoTivity, LinkSmart

3.3.5.2 Considerations for platforms selection and usage

The question of a choice of platform(s) by IoT system designers is complex. Some dimensions have to be considered:

- *Scope and breadth*: which kind of business sector and solution will the platform support?
- *Openness*: how is a platform going to comply with openness criteria such as those that define the work of standardisation or open source communities?
- *Origin and governance*: which entity is in charge of the definition of the platform and its evolution.
- *Ecosystem*: has the platform attracted several partners that can participate to the extension of its footprint?
- *Maturity*: how far can the platform support the implementation of effective and efficient implementations.
- *Standards support*: the available platforms can also have very different support to interoperability and to the standards in support of it.

The ETSI TR 103 536 (published in 2020, [35]) addresses the classification of IoT Platforms with the perspective of evaluating the possibility of using standardised platforms. From this standpoint, the question of origin and governance of the platform become a major choice factor. A typology of the platforms based on their origin is proposed in Table 4.

Table 4: A typology of IoT platforms

Type	Advantages	Drawbacks
SDO-based	• No dominant stakeholder • Open Source implementation availability • No dependency from a single company • Formal testing suites available • Global certification program available • Suitable for all the IoT services in the different region of the world • Strongly focused on interoperability • Strongly focused on integration of existing technologies • Global standardization • Competition on the platform is suitable for the users who reduce the associated costs	• A standard platform makes the platform a commodity • Competition on the platform is not suitable for the providers, who prefer to invest and focus on the IoT services
SSO-based	• There is usually an ecosystem of stakeholders representing the whole chain • Open Source solution often available, especially on device and gateway side • Some have certification programs • Some have global presence, even in vertical sectors	• Few of them are focusing on platform interoperability, while more are focused on protocol and devices, so integration effort if expected to be still predominant • There will be still a certain dependency from a specific ecosystem
Open Source-based	• No dominant stakeholder • Proven high TRL (e.g. TRL-9)	• Cover only parts of requirements • Limited focus on interoperability validation
Industry Group-based	• Usually reflect the needs of vertical sections of the industry • Usually well thought and helpful for the implementation of some interoperability interfaces • Sometimes no alternatives, either because of extremely widespread acceptance or because they are mandated by regulations in specific areas	• Cover only parts of manufacturers requirements • Need to be used in conjunction with other interoperability standards • May allow for specific extensions by individual manufacturers

Source: ETSI

In ETSI TR 103 536, a *standardised platform* is referring to the development of a set of components that support the development of a variety of (potentially competing) implementations. The components of the platform have been produced through a transparent and open development process in which all IoT stakeholders can participate. The main advantages of standardised platforms are to allow for multiple implementations, to offer controlled interfaces, provable and proven interoperability, maintenance over time with transparent control over the evolution of the features.

These platforms can be provided, for example, by an SDO or SSO that develop paper-based specifications with additional interoperability support such as plugtests (with the example of

oneM2M), or by an Open Source Software ecosystem that develop software components with openly available source-code with additional interoperability support such as APIs (with the example of Apache).

A standardised platform will typically encompass the provision of several elements such as:

- The description of a Reference Architecture (with potentially several models, the most frequently used being the Functional Model).
- A set of supported protocols.
- A set of interfaces or Reference Points (in particular Application Programming Interfaces).

3.3.5.3 The Service Platform

Amongst the many IoT platforms in use, with a very diverse scope of functionality, the IoT Service Platform plays an important role since its main objective is to provide an abstraction layer between the applications and the IoT devices and to provide a built-in support for a very large number of standards (existing or forthcoming).

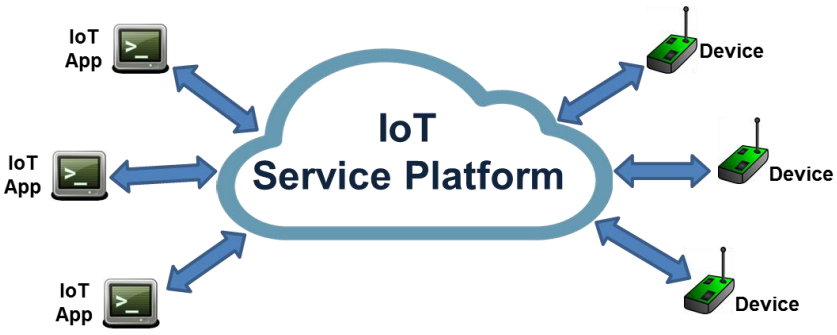


Figure 6: The IoT Service Platform

An IoT Service Platform is essentially:

- An Intelligent layer between applications, networks and devices.
- Offering a coherent set of standardized functionalities.
- And an enabler for communication and data interoperability.

The IoT service platform is the actual implementation/deployment of an abstract IoT architecture (entities and interfaces) like the ones outlined in the previous section.

3.4 The LSP Interoperability Framework: supporting convergence

3.4.1 The approach taken

The IoT LSPs form an ecosystem of 5 different project operating in 5 different sectors, where Technology, Stakeholders and Software Solutions may interact in a way that all together creates potential synergies stemming from data exchange, solutions or best practices, etc. The challenge for the LSPs has been to identify areas of commonality between projects that have different requirements, objectives and development logics.

Within an application domain, the development of effective solutions (including for data exchange) must follow specific patterns or standards. At the LSP level, the challenge of interoperability is to ensure that requirements and solutions are clearly specified, in order to guarantee the full integration of a solution and the correct provisioning of services across the multiple solutions in the LSP ecosystem. Within all LSPs, user-centric approaches have been followed and all solutions have been based on the definition, design and deployment of use cases which have been the main drivers for interoperable specifications (including the issue of data).

Each LSP has developed its own Interoperability Framework, based on the requirements of their applications (considering in particular the sector – e.g. health, transport, etc. – in which they operate), the selected Use Cases, or the concrete settings of the associated pilot sites (in particular the technology and platforms ecosystem). These parallel definitions have resulted in different Interoperability Frameworks (IF).

However, despite differences, several features of these IFs are similar or quite close, making their analysis and comparison a meaningful exercise. This has been the task of the LSP Activity Group 02 ("Standards, architectures and interoperability) which has gradually identified and assembled a set of common characteristics. As an example, an early analysis of the LSP reference architectures has led to the identification of a common set of functional layers (as presented in the LSP Brochure [12]) described in Figure 7.

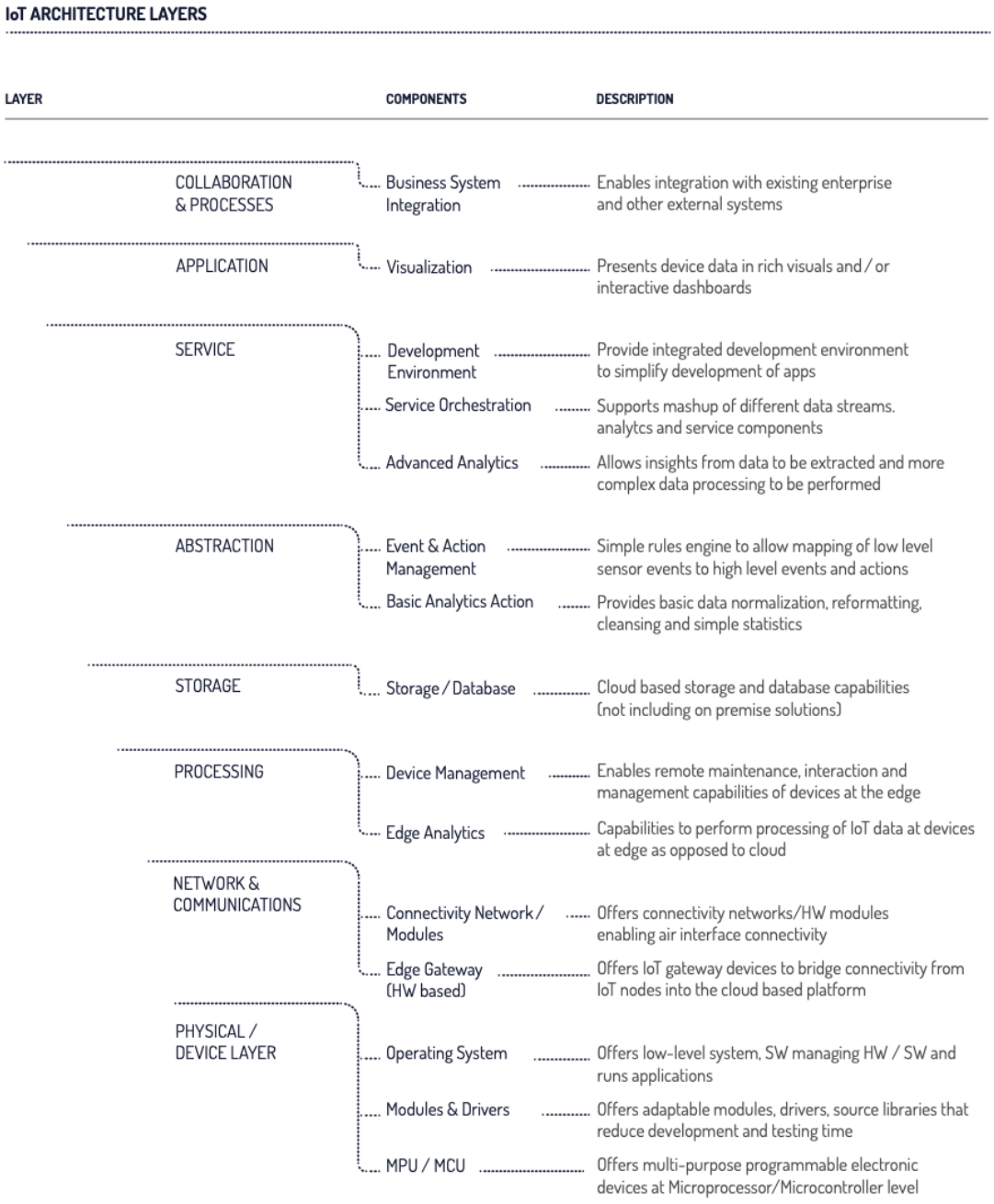


Figure 7: Common Functional Layers in the LSPs

In a subsequent step, a common identification of a reference set of use cases has been done. All the LSPSs have defined several Use Cases that have been developed in a number of pilot sites. All

these Use Cases have been gathered in a systematic and comparable manner by Activity Group 01 (IoT Focus Area Sustainability) that presents the main characteristics of these Use Cases in a common template. These results have been used by Activity Group 02 for the analysis of reference architectures, interoperability support mechanisms, and platforms and technologies (and presented in CREATE-IoT Deliverable D06.02 [2]).

The work of consolidation of the Interoperability Framework has been pursued and the common information has been gathered and discussed in several workshops held in 2018 and 2019 ([8], [9], [10] and [11]) whose main objective was to establish a common basis across the different IoT Large-Scale Pilots (LSPs) regarding topics such as: reference architecture models; interoperability framework and reference implementations based on use cases; analysis of components and standards, existing IoT platforms, etc.

3.4.2 The LSP Interoperability Framework

The first five EU IoT Large-Scale Pilots (ACTIVAGE, AUTOPILOT, IoF2020, MONICA and SynchroniCity) and the associated Coordination Support Action (the CREATE-IoT CSA) have addressed the definition of an LSP Interoperability Framework within the context of their Activity Group 02 on "Standardisation, Architecture and Interoperability".

The final status of the Interoperability Framework is described in the present document for its main aspects (reference architecture, technologies, platforms, interoperability mechanisms) whereas the standards aspects are described in the companion CREATE-IoT Deliverable D06.06 "Final report on IoT standardisation activities" [3].

The LSP Interoperability Framework has been developed by the Activity Group 02 participants and discussed during a set of Workshops that are summarized in the following CREATE-IoT deliverables:

- "Interoperability Framework Workshop", Deliverable D06.08, 2018.
- "Workshop on LSPs use cases: integration and standardisation alignment", Deliverable D06.09, 2019.
- "Workshop on IoT standardisation activities", Deliverable D06.10, 2019.
- "Workshop on common IoT standardisation framework", Deliverable D06.11, 2020.

During the development of the Interoperability Framework, the following CREATE-IoT deliverables have been produced:

- "Strategy and coordination plan for IoT interoperability and pre-normative and standardisation activities", Deliverable D06.07, 2018.
- "Recommendations for commonalities and interoperability profiles of IoT platforms", Deliverable D06.02, 2018.

The standards and pre-normative activities in support of the Interoperability Framework have also been addressed during its development in the following CREATE-IoT Deliverables:

- "Initial report on IoT standardisation activities", Deliverable D06.05, 2018.
- "Strategy and coordination plan for IoT interoperability and pre-normative and standardisation activities", Deliverable D06.07, 2018.

4. ASSESSMENT OF LSPS INTEROPERABILITY FRAMEWORKS

4.1 Introduction

This section presents the main aspects of the Interoperability Frameworks developed by the LSP during the course of the projects. The objective is to have a comparison point with respect to the frameworks defined and used by the IoT LSPs in the definition, design and implementation of a large variety of use cases across different pilot sites with various technological set-ups (e.g., platforms, legacy applications). Because of the inherent complexity and heterogeneity of their use cases, all the LSPs had to deal with all the interoperability levels defined in section 3.2 (see Figure 1), in particular regarding syntactic and semantic interoperability.

4.2 The ACTIVAGE Interoperability Framework

4.2.1 Interoperability Support in ACTIVAGE

ACTIVAGE [16] has tackled a major problem for IoT: the interoperability of the information and the associated challenge of defining how the things "talk" amongst other things and communicate with other systems in order to expose their capabilities and functionalities "services".

To this extent, ACTIVAGE has developed (and implemented) a High-Level Reference Architecture (HLA) described in Figure 8.

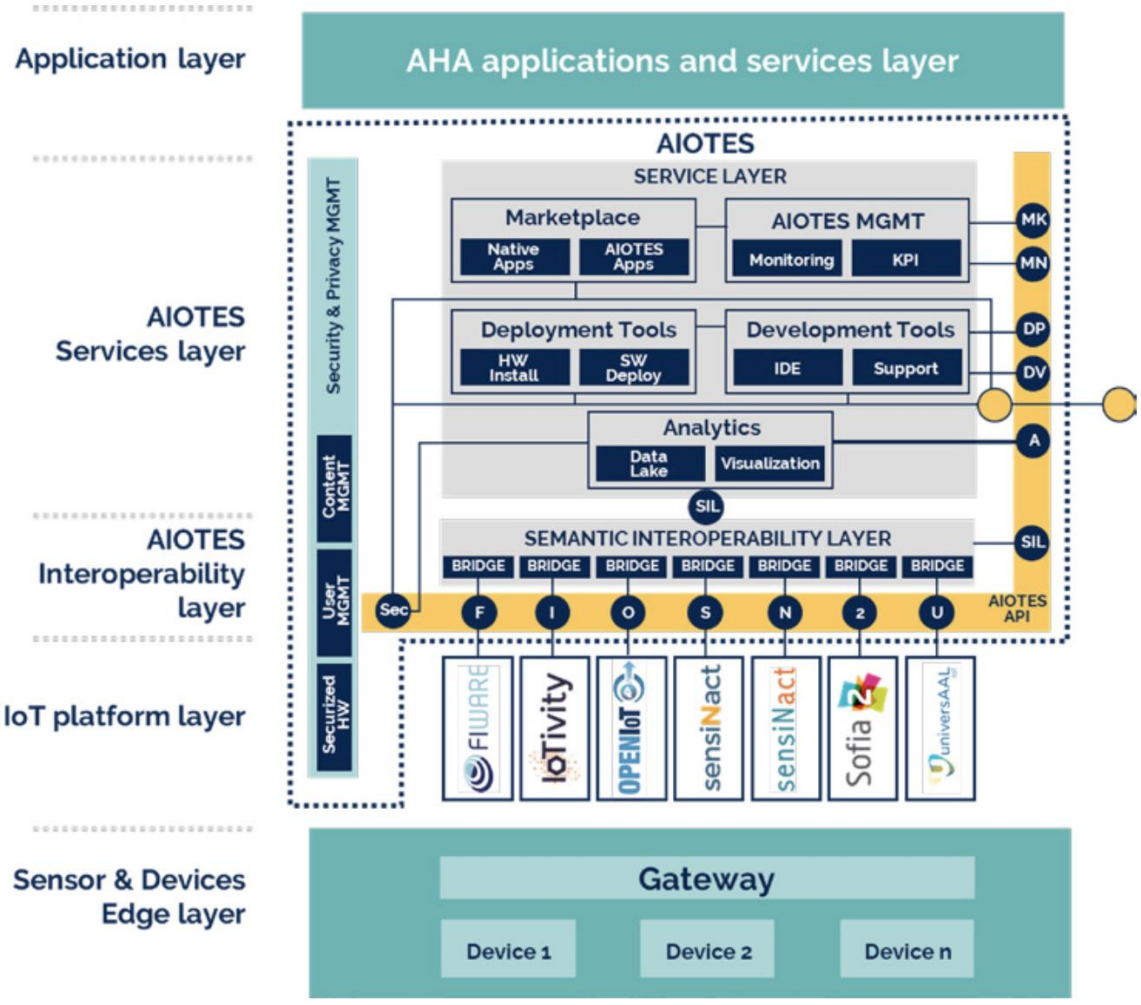


Figure 8: The ACTIVAGE Reference Architecture

This architecture is tailored to address the needs of AHA and relies on a layered model to ensure the intermediation between the intermediation between applications and the sensor devices (edge) layer. It is compliant with several architecture models (AIOTI WG03 HLA, ITU-T Y.2060 and IIC's IIRA).

Three main layers are involved:

- The (ACTIVAGE IoT Ecosystem Suites) *AIOTES Services Layer* is a set of software solutions, tools and methodologies in support of semantic interoperability, security, privacy and data protection.
- The *Interoperability Layer* is an abstraction layer in charge of ensuring interoperability through the ACTIVAGE platforms.
- The *IoT Platform Layer*. The IoT middleware in charge of connecting all the "things" involved in ACTIVAGE use cases is complex and heterogeneous. The Platform layer will serve as an abstraction layer that will ensure that different platforms can be supported, and a given service can be replicated across different pilot sites.

4.2.2 The AIOTES Service Layer

The main components of the AIOTES Service Layer and Interoperability Layer are summarized in Figure 9.

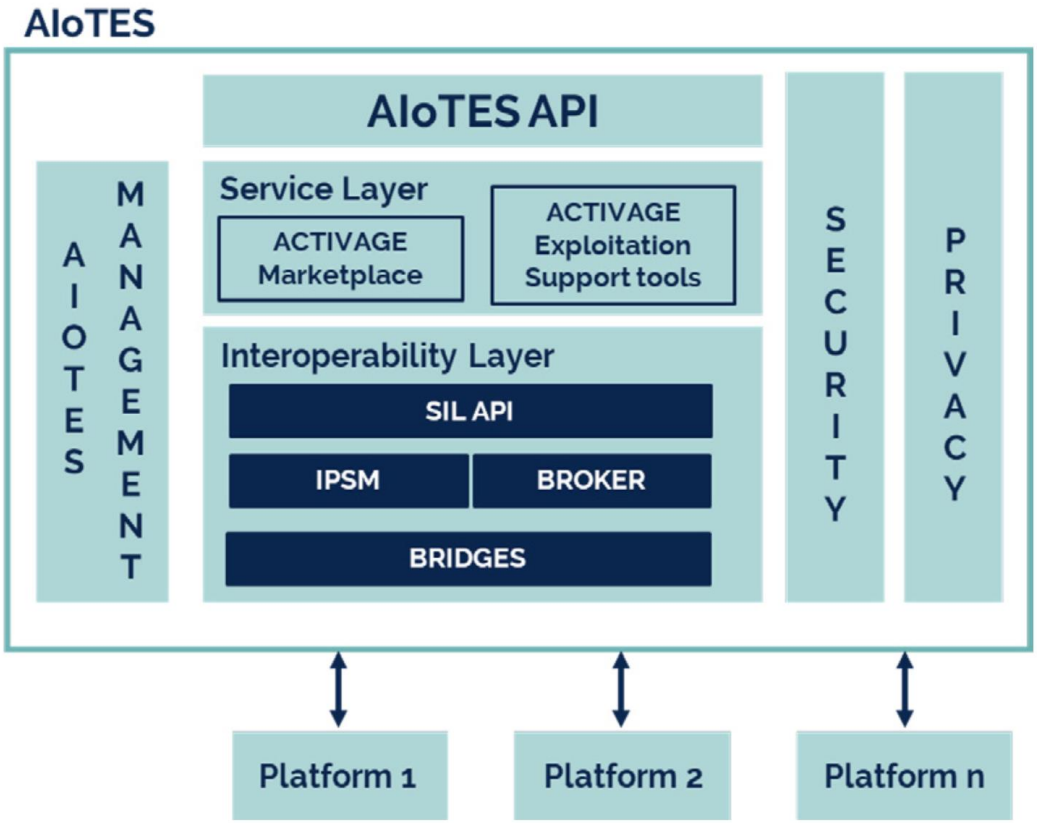


Figure 9: ACTIVAGE AIOTES Service Layer and Interoperability Layer

The main components of the AIOTES Service Layer are:

- The *AIOTES Development Toolkit* offer means for facilitating the use of existing applications by other developers, with available source code samples, browsing documentation, viewing available tutorials, testing sample code, etc. It also includes Data Lake tools to facilitate access to data available through the Data Lake.
- The *AIOTES Deployment Tools* allow IoT administrators and developers to register IoT components and applications and allow deployers to discover already existing ones.

- The *Data Analysis Tools* provide a bridge between the massive amounts of raw data collected from the IoT sensors and devices of multiple IoT platforms, as unified through the ACTIVAGE interoperability layer, and the human researcher and clinicians.
- The *ACTIVAGE Marketplace* is a deployment tool in support of a variety of stakeholders: any online user, deployment site or general healthcare professional, third party adopter, existing and potential developer, individual or business entity that want to develop, provide and obtain applications build for AIOTES.

4.2.3 The Interoperability Layer

The Semantic Interoperability Layer provides interoperability among platforms and allows other elements of ACTIVAGE to communicate with any platform through a common API (SIL API). It is divided into three main blocks:

1. The Broker is managing every communication in the IoT Interoperability Layer and can be divided, from a functional point of view, into four blocks:
    - The *API Requester Manager* handles the request received from the API proxy;
    - The *Platform Request Manager* prepares and sends requests to specific platforms through bridges, using already established permanent data streams (created during start-up with the help of Data Flow Manager) or newly created data streams;
    - The *Data Flow Manager* acts as orchestrator of data flows from the platforms (bridges) to the original caller, utilizing already established permanent data streams or creating new ones and ensuring that all intermediaries are included in the path
    - The *Message Queue* receives and provides the messages to the corresponding components, including ad-hoc temporary topics for single requests, and fixed platform channels.
2. The *IoT Platform Semantic Mediator* (IPSM) block manages the ontologies and provides semantic interoperability through the translation among the different platform ontologies and the ACTIVAGE ontology. This translation is performed by means of ontology alignment.
3. The information exchange is facilitated thanks to the use of platform *bridges*. These manage the communication with the subjacent platforms by translating its requests and answers. Different bridges might need to use HTTP, REST, sockets or other technologies to talk to the platforms, but these will be translated northwards into messages. The decision to connect the platforms directly to the abstraction layer instead of interconnecting all platforms among themselves, simplifies considerably the interoperability.

4.2.4 The ACTIVAGE IoT Platform Layer

The goal of the IoT platform is to provide the intelligent environment that interconnects the physical world with the digital world. In other terms, the IoT platform (IoT middleware) is an integrated physical/virtual entity system that enables the communication between the machines and devices and, consequently, the acquisition, processing, transformation, organization and storing machine and the sensor data.

The IoT platform employs various applications and components to provide fully interoperable IoT services and management of those. This includes, networks, IoT environments, IoT devices (sensors, controllers, actuators, tags and tag readers, gateways) and the attached physical devices, IoT operations and management, and external connectivity with suppliers, markets and temporary stakeholders of the IoT system.

The IoT platforms provide the ability on creating application and services in a structure environment that is formed by functional components. This IoT platform feature contributes to the development cycle and time to market while reduces the overall cost of the IoT implementation.

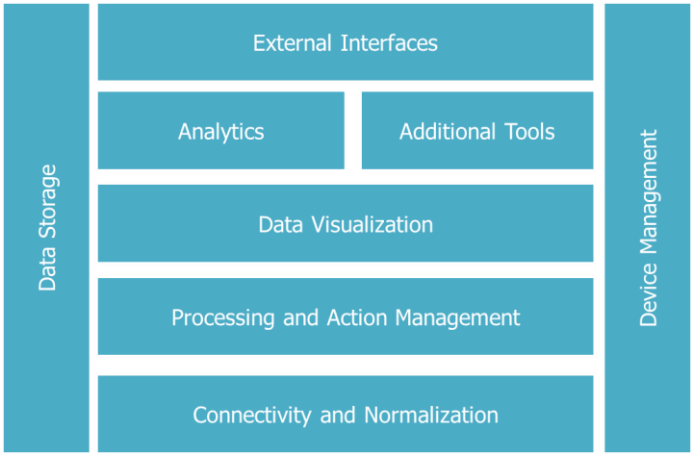


Figure 10. Functional components of IoT platforms [35]

The platform building blocks are usually common and repeated across many IoT applications and services as shown in Figure 10. More precisely:

- *Connectivity & normalization* eliminates the heterogeneous data as it brings different protocols and different data formats into one software interface ensuring accurate data streaming and interaction with all devices.
- *Device management* ensures the connected the network devices are working properly, seamlessly running patches and updates for software and applications running on the device or edge gateways.
- *Data Storage* scalable storage of device data brings the requirements for hybrid cloud-based databases to a new level in terms of data volume, variety, velocity and veracity.
- *Processing & action management* brings data to life with rule-based event-action-triggers enabling execution of intelligent actions based on specific sensor data.
- *Analytics* performs a range of complex analysis from basic data clustering and deep machine learning to predictive analytics extracting the most value out of the IoT data-stream.
- *Visualization* enables humans to see patterns and observe trends from visualization dashboards where data is vividly portrayed through line-, stacked-, or pie charts, 2D- or even 3D-models.
- *Additional tools* allow IoT developers prototype, test and market the IoT use case creating platform ecosystem apps for visualizing, managing and controlling connected devices.
- *External interfaces* integrate with 3rd-party systems and the rest of the wider IT-ecosystem via built-in application programming interfaces (API), software development kits (SDK), and gateways.

For the purpose of the ACTIVAGE project, two criteria have been applied: 1/ platforms focusing on the application layers, offering means to transform the information received from the devices and sensors into meaningful knowledge; and 2/ availability of the platforms, with open-source solutions preferred to proprietary solutions.

The platforms that have been used in ACTIVAGE are listed in Table 5. These platforms comprise a comprehensive set of open-source, application-oriented IoT platforms, covering a relatively wide range of functionalities. Furthermore, there is a past experience for using these platforms in other European projects.

Table 5: Platforms and Technologies Support in ACTIVAGE Use Cases

Platform or Technology	***#UC***	***Owner***	***Status***	***G/S***
FIWARE	*3,5,6*	*FIWARE Foundation*	*S/O*	*G*
IoTivity	*1,6,8*	*IoTivity*	*O*	*G*
OpenIoT	*1,5,7*	*OpenIoT*	*O*	*G*

Platform or Technology	*#UC*	*Owner*	*Status*	*G/S*
sensiNact	*1,3,4*	*LETI*	*O*	*G*
Seniorsome	*1,2,7*	*Finland Health*	*P*	*S*
SOFIA2 IoT Platform	*1,2,8*	*SOFIA2*	*O*	*G*
universAAL	*1,4,9*	*universAAL*	*O*	*G*

UC: use case; O: open source, P: proprietary, S: standards-based; G: generic or S: sector-specific

The IoT platform itself can be located in the cloud, located on premise or involve a combination of both. Cloud-based IoT platforms are significant as they are user based and has successful record of exploitation. Additional services of the IoT platform can include resource interchanges to enable access to resources outside of the IoT system, network services, cloud integration services and many other services as defined by the individual platform provider. A positioning of the functionality of IoT platforms is illustrated in Figure 11.

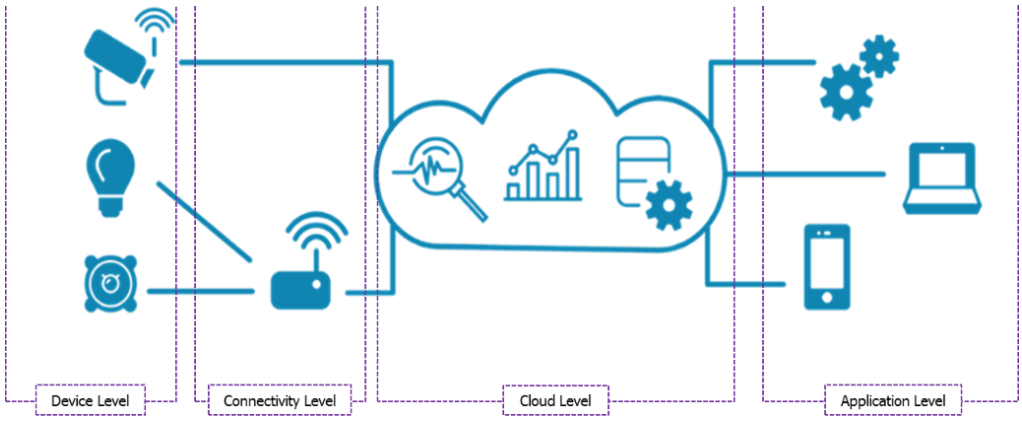


Figure 11. IoT platform levels.

4.3 The AUTOPILOT Interoperability Framework

4.3.1 Reference Architecture and Associated mechanisms in AUTOPILOT

In the AUTOPILOT [18] project, the IoT architecture was designed as a federation of IoT platforms, allowing it to be open and flexible [18]. Developers may plug their own (proprietary) IoT platforms or devices in the architecture and exchange data with existing IoT platforms and devices. As each IoT platform provides a different set of services (features) and may expose a different interface and use a different data exchange protocol, an effort is needed to achieve interoperability while allowing for openness and flexibility.

The interoperability framework in AUTOPILOT is achieved based on the following principles [18]:

- OneM2M Interoperability Platform and Interworking Gateways - As shown in Figure 12, proprietary IoT platforms are interconnected through interworking gateways and the oneM2M interoperability platform.
- Standardised IoT Data Models - IoT data requiring to be exchanged across the IoT platforms are standardized:
    - IoT Data Models specify the syntax, i.e. how the IoT data must be represented.
    - IoT Data Models also require agreement on the semantics of the data, i.e. what the data means. This may be defined in a written specification that developers must adhere to, or in form of an explicit ontology that is available in electronic form (e.g. the FIWARE NGSI-LD Broker refers to concepts identified by unique URIs, which may be defined in an ontology).

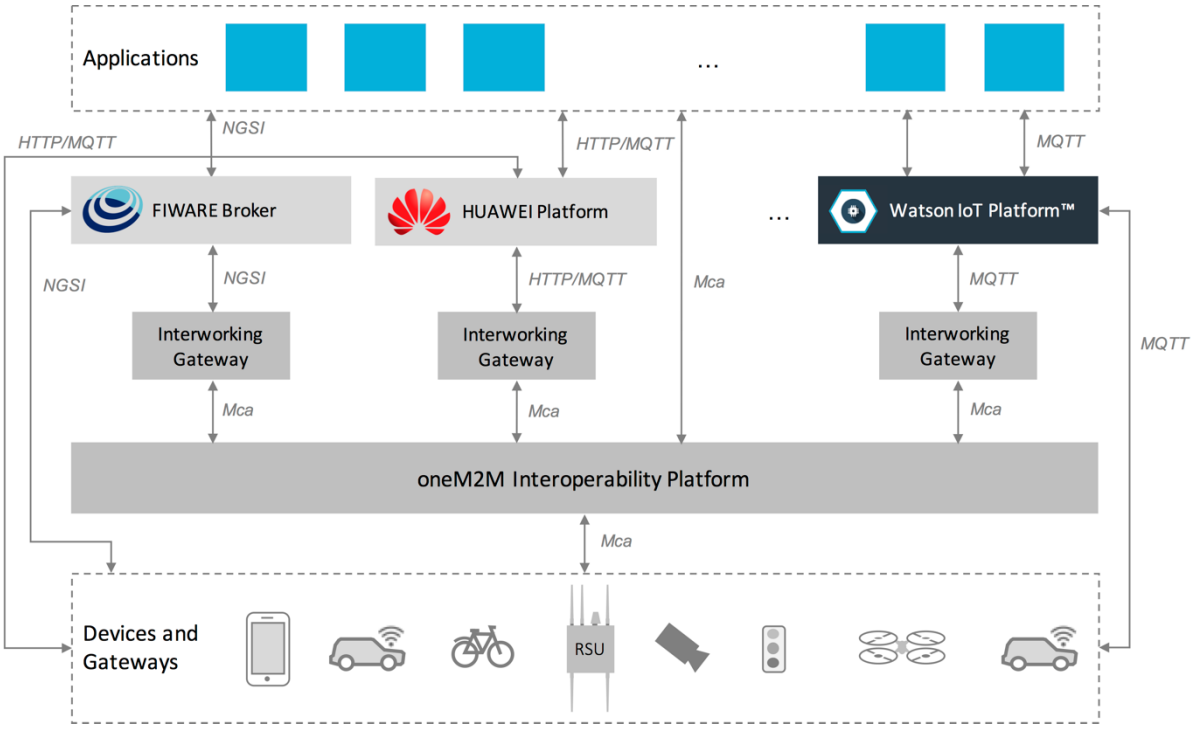


Figure 12: AUTOPILOT federated IoT architecture [18]

4.3.2 Overview of Platforms and Supporting technologies in AUTOPILOT

Each of the above interoperability principles is discussed in the two following sections.

4.3.2.1 OneM2M Interoperability Platform and Interworking Gateways

In the AUTOPILOT project, an interworking gateway is considered as a oneM2M wrapper belonging to a proprietary IoT platform, which enables to expose a oneM2M interface and to be connected to the oneM2M interoperability platform [18]. The AUTOPILOT project refers to the gateway between Watson IoT and oneM2M platforms as SMG (Watson-oneM2M Interworking Proxy and to the gateway between FIWARE and oneM2M as "Semantic Mediation Gateway) or MMG (Morphing Mediation Gateway). MMG is a more dynamic and advanced version of SMG.

The oneM2M platform serves as the bridge for interoperability, allowing data to flow from one IoT platform to another in both directions. Using this architecture, an IoT platform may push data to other IoT platforms and receive data from them. Mapping between the internal data representation of an IoT platform and the oneM2M message contents are specified in the interworking gateways. These gateways also act as filters allowing only selected data to be exchanged.

In this architecture, the applications may use any of the available IoT platforms according to their requirements [18]. For instance, a data provider may publish data to Watson IoT platform and this data can be shared with FIWARE through the oneM2M platform, so that an application developer who uses FIWARE can access it through the FIWARE platform.

This approach offers flexibility to the project pilot sites and the application developers. However, to enable this oneM2M interoperability platform data flow; data providers and consumers need to exchange data using standard data models and vocabularies.

4.3.2.2 Standardised Data Models

OneM2M provides a standard protocol for exchanging IoT messages, but it does not specify the content of the messages as this is domain specific. To achieve interoperability in AUTOPILOT,

we standardised the contents of the oneM2M messages exchanged between the IoT platforms, devices, applications, and vehicles, through the oneM2M interoperability platform. A Data Modelling Activity Group (DMAG) was created in AUTOPILOT for this purpose.

The scope of the data model standardisation activity in the AUTOPILOT project, covers the IoT messages and data fields required to implement the project's use cases uniformly across the project pilot sites [18]. On the one hand this includes the syntactic structure of the messages (e.g. if a certain field expects a number or a string) and on the other hand the semantics is specified (e.g. that the number expected by a certain field is a speed in kilometres per hour).

All standardized data models are described in a written specification. Some may have an alternative representation (e.g. according to the NGSI-LD model) for use with the FIWARE platform with a corresponding ontology representation.

Standardised data models allow Autonomous Driving (AD) vehicles to access the same types of data regardless of their locations (pilot sites), and to be able to process the data and work with it [18]. For instance, a message notifying AD vehicle about a hazard on the road, or instructing them to avoid a given road lane, should be the same in all pilot sites, allowing vehicles to consume these messages and react to them correctly as they are moving from one place to another.

The intention of the AUTOPILOT project was not to standardise all the data across all the use cases and pilot sites [18]. Rather, the scope of this work covers only the IoT messages used for exchanging information or instructions between IoT devices, services, and the AD vehicles. This includes, for instance, messages notifying AD vehicles about the presence of a hazard, or object, or instructions for AD vehicle to avoid a given road lane.

Raw sensor data (e.g. LiDAR, camera images, etc.) and service internal data models (e.g. parking data, user accounts, etc.) were beyond the scope of the data modelling activities.

The work carried out, was based on reusing, and possibly extending, existing standards rather than creating new models. A list of IoT messages under standardisation by the AUTOPILOT project is provided in Table 6 [18]. In the AUTOPILOT project we were aiming to standardise the IoT messages regardless of the originating sensor or application.

Table 6: AUTOPILOT use cases IoT messages selected for standardisation [18]

Message types	Pertaining use cases
Vehicle Probe Data (GPS position, speed, status)	Car/ride sharing, AVP
Notifications about detected objects	AVP, highway pilot, urban pilot, platooning, car/ride sharing
Notifications about VRUs	AVP, highway pilot, urban pilot, platooning, car/ride sharing
Notifications about hazards and obstacles	AVP, highway pilot, urban pilot, platooning, car/ride sharing
Notifications about traffic conditions	Highway pilot, urban pilot, platooning, car/ride sharing
Notifications about environmental conditions	Highway pilot, urban pilot, platooning, car/ride sharing
Traffic light states and time to red/green	Highway pilot, urban driving, platooning
Notifications about parking space availabilities	AVP, parking, car/ride sharing
Notifications about charging spot availabilities	AVP, parking, car/ride sharing
Routing instructions	Highway pilot, urban driving, AVP, car/ride sharing
Platoon instructions	Platooning

As an example, the interoperability with other LSPs were demonstrated at a workshop [19]. The AUTOPILOT and SynchroniCity projects demonstrated interoperability of AUTOPILOT data with the architectures deployed in SynchroniCity. As an example, the visualisation of data related to parking spaces published by the AUTOPILOT pilot sites could be use by the SynchroniCity deployment, as illustrated in Figure 13 [19].

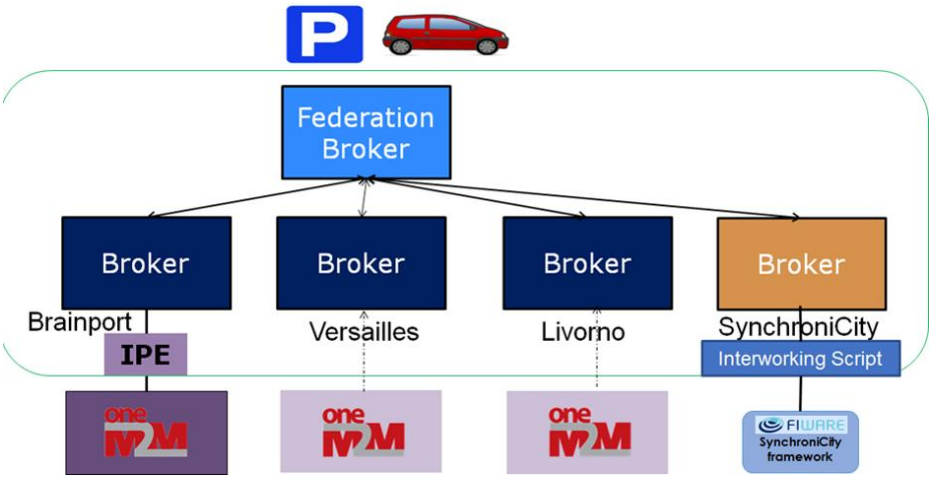


Figure 13: Visualisation of AUTOPILOT parking information in SYNCHRONICITY [19]

4.4 The IoF2020 Interoperability Framework

4.4.1 Interoperability Support in IoF2020

Building on the experience being generated on the field, the initial plan in IoF2020 [21] was to establish a common view, for each of the 19 Use Cases with the aim of ensuring that deployed components and solutions can prospectively inter-operate so to deliver added-value functionalities to various stakeholders – possibly maximizing re-use of common IoT enablers across different Use Cases and trials.

This has been achieved by leveraging common interoperability endpoints and data models and allowing secure and controlled exchange of information and capabilities across heterogeneous components. As part of the general guidelines for Use Case Architecture analysis, each Use Case has been specified by defining and analysing a minimal set of architectural views.

The resulting approach is described in [21] and [22], and presented in Figure 14.

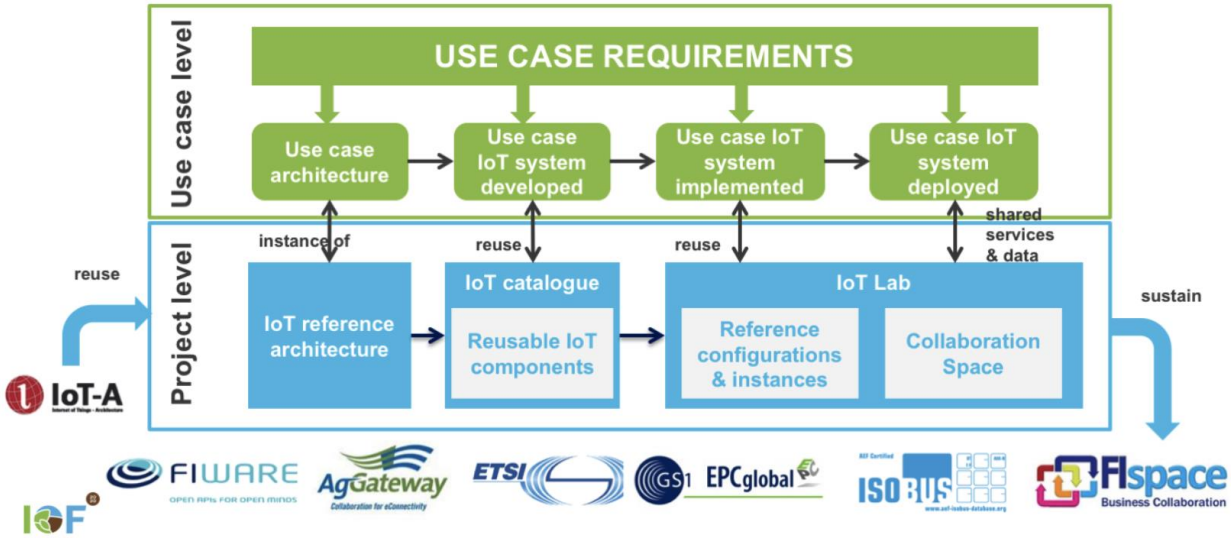


Figure 14: IoF2020 Large Scale Pilot approach

4.4.2 The Interoperability Endpoints

One of the guidelines for the use case analysis was the description of the Interoperability Endpoints. The main resulting Interoperability Points (IOPs) described in Figure 15 are:

- Interoperability Point 0 (IOP 0). It is realized as a connectivity enabler for IoT Devices and agricultural machinery.
- Interoperability Point 1 (IOP 1). It is situated in between the IoT Service Layer and the Mediation Layer, enabling the exposition of the data and services offered by IoT Devices through well-known programmatic interfaces.
- Interoperability Point 2 (IOP 2). It is situated in between the Information Management Layer and the Mediation Layer. On the one hand it enables the transformation, aggregation, harmonization and publication, as context information, of harmonized data coming from IoT Devices, agricultural machinery or other sources of information (open data portals, web services providing contextual data, etc.). On the other hand, it exposes a unified way to send commands and to mediate with IoT Devices or agricultural machinery, regardless the interface exposed by the IoT Service Layer or the Physical Machinery.
- Interoperability Point 3 (IOP 3). Situated between the Application Layer and the Information Management Layer, it is intended to provide access to all the data of interest to smart farming applications, including, but not limited to, real or right-time data, historical data or analytics results.
- Interoperability Point 4 (IOP 4). This interoperability point enables the Application and Mediation Layers to consume public Geo-Services, enriching the smart farming applications with geospatial data and off-the-shelf visualizations.
- Interoperability Point 5 (IOP 5). It is a cross-cutting interoperability point that facilitates the secure interchange of information between the different layers and actors.

The Interoperability Endpoints View summarizes the main endpoints, which can be exploited to integrate available systems to other systems.

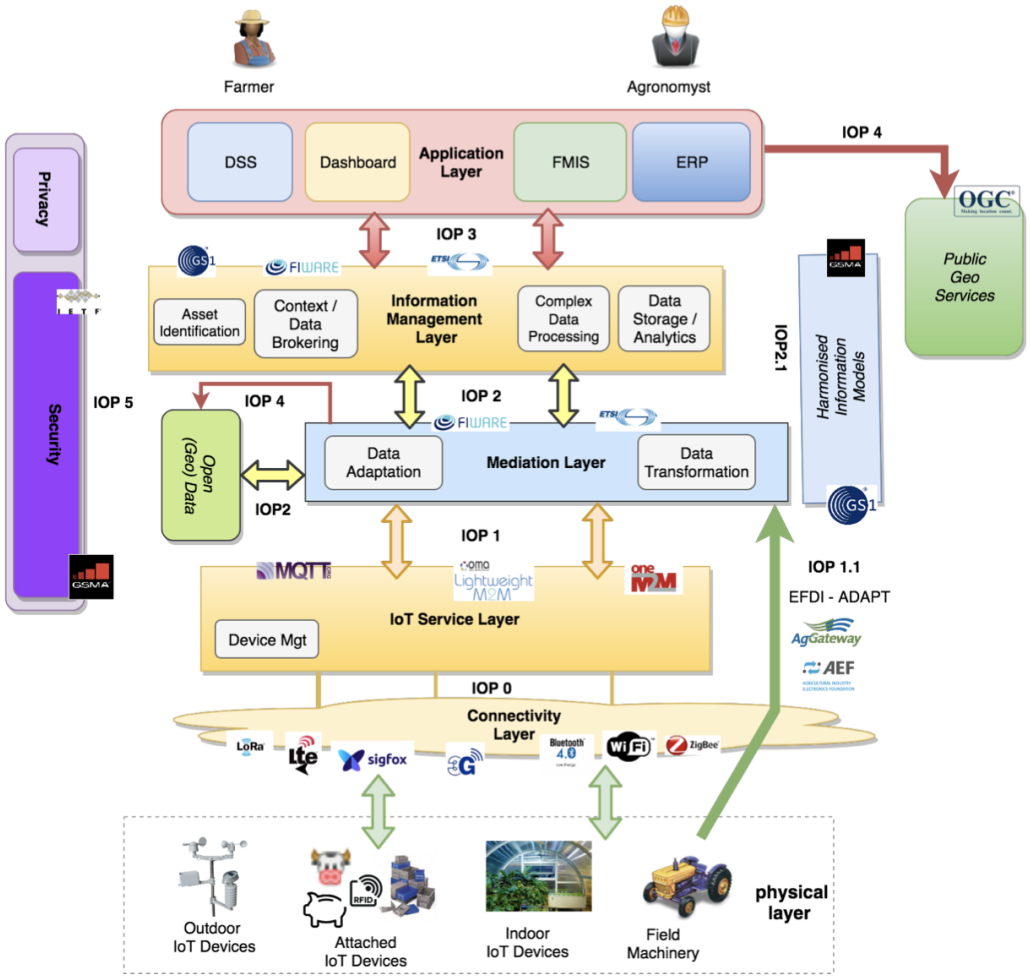


Figure 15: Overview of IoF2020 End Points and their relationship to standards

Its main purpose is to help identifying the most suitable entry points to access available legacy and IoT systems, deployed in each UC, referencing the standards and protocols, which must be implemented to perform such integration. While this is not a "standard" view (such information is typically spread across the information, communication and deployment views), it has been adopted to facilitate the identification of technical synergies.

4.4.3 The IoF2020 IoT Catalogue

IoF202 has developed a catalogue of IoT components [24], initially with the objective of supporting the IoF2020 use cases, and later to support a wider audience of IoT users and providers, in identifying and re-using components that were successfully developed, integrated, deployed and validated. The approach to reuse is described in Figure 16.

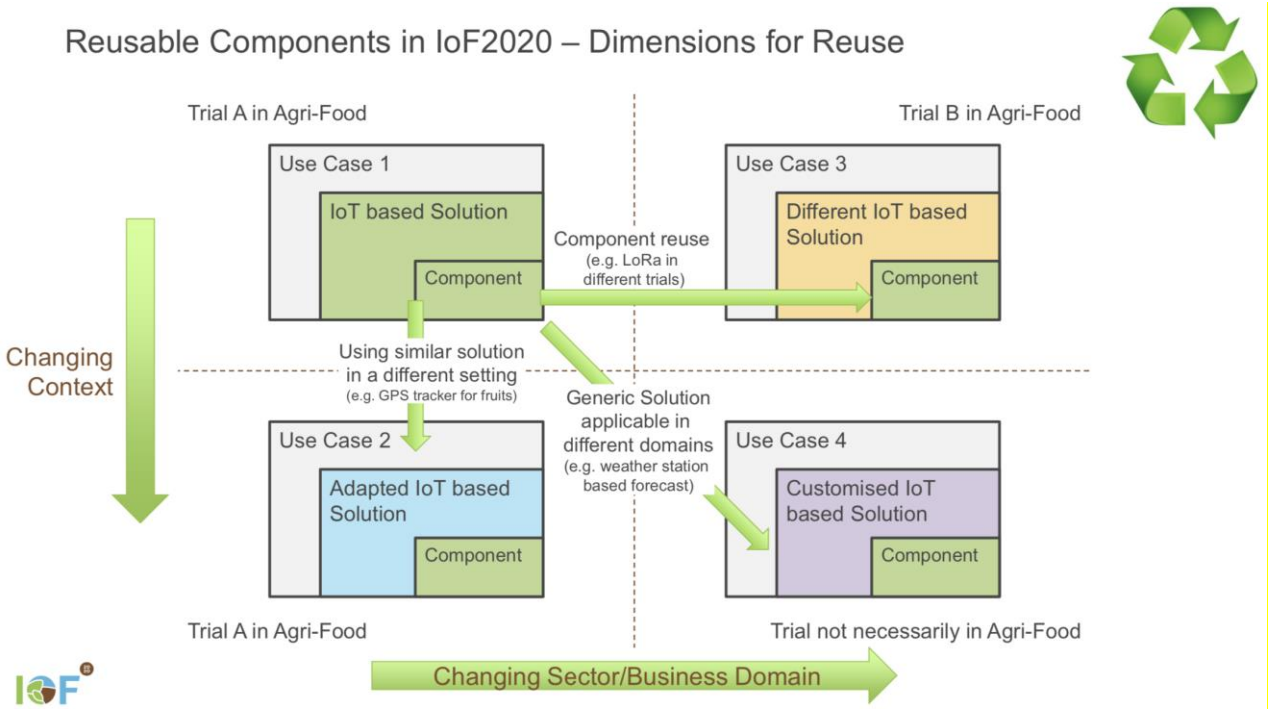


Figure 16: Dimensions for reuse in IoF2020

The 'catalogue of IoT (reusable) components' is aimed especially at IoT users (particularly at advisors working close to the farmers) and technology providers/integrators of IoT solutions. The catalogue is intended to include all the features as to allow users to access the information in order to identify and choose (reusable) components for their applications/projects.

The 'catalogue of IoT (reusable) components' enables to showcase the results of two WP3 objectives:

- Identify common platform APIs and generate common information models, context adaptors and components, which can be integrated into different IoF2020 use cases;
- Facilitate identification, coordination and realization of synergies in use cases. Identify and/or develop platform and IoT device related common components relevant for several use cases in WP2.

Instead of developing a platform from scratch, it was chosen to use and improve the already existing IoT-Catalogue (available at http://www.iot-catalogue.com). The IoT-Catalogue is a result of the H2020 research project WAZIUP, where it was used to present its use cases. The IoT-Catalogue is a web- based catalogue for Internet-of-Things (IoT) solutions. It brings IoT users and technology providers together, from the domain needs to IoT products (and back) via validated solutions with components, assembly guides, and more.

4.4.4 Platforms and Technologies in IoF2020

4.4.4.1 Use Cases and the support of Platforms and Technologies

IoF2020 has developed (and documented) 19 Use Cases. The platform and technologies in support of these Use Cases are listed in Table 7.

The fact that the field of IoT platforms is unconsolidated and this is reflected in the choices made in the IoF2020: the use cases use many platforms, though a relatively high number of use cases report they use 365FarmNet and/or FIWARE. Additionally, aspects such as device management, enrolment, firmware deployment/upgrades and decentralized security models are important and have required early consideration when deploying IoT at scale. The configuration management strategies that are completely feasible when deploying tens of devices, break when a solution is scaled to thousands of devices.

Regarding FIWARE, which as been used relatively often and is a very modular platform, the following components from the FIWARE ecosystem are used specifically:

- Context broker - A broker that allows sharing objects and their properties, and supports updates, queries, registrations and subscriptions.
- Device management and IoT Agent - This component collects data from devices using heterogeneous protocols and translates them into the standard platform language suitable for the context broker.
- Identity management - A generic component that supports authentication tasks for users' access to networks, services and applications, including secure and private authentication from users to devices, networks and services.

Table 7: Platforms and Technologies Support in IoF2020 Use Cases

Platform or Technology	***#UC***	***Owner***	***Status***	***G/S***
365FarmNet	*6*	*365FarmNet*	*P*	*S*
AgroSense	*1*	*Corizon*	*O*	*S*
Apache Cassandra	*1*	*Apache*	*O*	*G*
Apache Flink	*1*	*Apache*	*O*	*G*
Apache Spark	*1*	*Apache*	*O*	*G*
Arvalis IoT Platform	*1*	*Arvalis*	*P*	*S*
Atland FMIS	*2*	*Atland*	*P*	*S*
Connecterra IoT	*1*	*Connecterra*	*P*	*S*
Cygnus	*1*	*FIWARE*	*O*	*G*
EBBITS	*1*	*ISMB*	*O*	*G*
EPCIS	*3*	*GS1*	*S*	*G*
FIWARE (in particular Broker)	*8*	*FIWARE Foundation*	*O*	*G*
FISpace	*1*	*FISpace*	*P*	*S*
LinkSmart (Free, Open Source IoT Platform)	*1*	*Fraunhofer*	*O*	*G*
MongoDB	*1*	*mongoDB*	*P*	*G*
OpenStack	*1*	*OpenStack*	*O*	*G*
Qlip platform for automatic calibration and validation	*1*	*Qlip*	*P*	*S*
ThingWorx IoT	*1*	*ThingWorks*	*P*	*G*
VIRTUS (XMPP Based Architecture for Secure IoT)	*1*	*ISMB*	*O*	*G*

UC: use case; O: open source, P: proprietary, S: standards-based; G: generic or S: sector-specific

4.5 The MONICA Interoperability Framework

4.5.1 Interoperability Support in MONICA

MONICA [25] has developed and documented 4 Use Case Groups (UCGs), namely:

- Sound Monitoring and Control
- Crowd and Capacity Monitoring and Management
- Missing Persons/Locate Staff Members
- Health/Security Incidents

MONICA has adopted and integrated different IoT platforms and technologies to demonstrate the 4 Use Case Groups (UCGs). These UCGs have been demonstrating in 6 EU cities (Turin, Bonn, Hamburg, Copenhagen, Leeds, Lyon) and in many different events including concerts, festival and sports event.

To ensure interoperability and all levels (from devices to applications), MONICA has designed the architecture following the AIOTI-High Level Architecture that is shown in Figure 17.

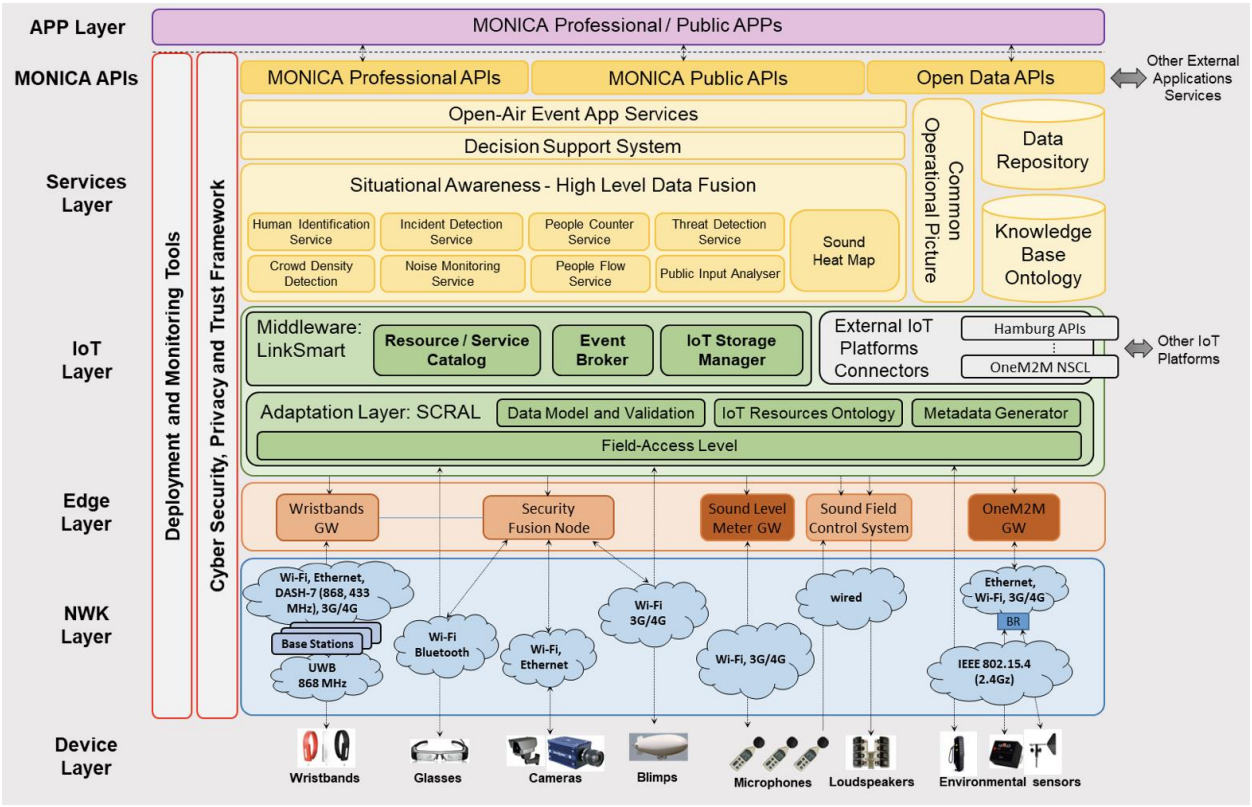


Figure 17: MONICA Functional Architecture

The role of the main layers is the following:

- The *APIs Layer* provides service access points for MONICA application developers and external application developers that want to access MONICA functionalities and information streaming from the platform.
- The *Services Layer* is where the intelligence of the platform is implemented, and specific processing modules are integrated. The services modules are combined with knowledge base components and decision support tools to assist human operators in gathering context-sensitive information and decision making
- The *IoT Layer* is in charge of guaranteeing interoperability. It is essentially comprising two open source frameworks: the LinkSmart (IoT middleware) and the SCRAL (IoT abstraction layer). The SCRAL framework provides interoperability over devices. In fact, applications can

access any kind of devices whichever proprietary protocol they may speak, over a uniform web-service based interface. In addition, the SCRAL framework exposes available metadata and semantic information for connected devices and streams; thus, enabling the Service Layer to access such an information when needed. More specifically, the SCRAL performs data modelling according to the open standard OGC SensorThings API; thus, addressing the syntactic interoperability of the IoT. Finally, the MONICA IoT Layer integrates the oneM2M modules allowing the platform exposing to external platforms the IoT data according to the oneM2M standard.

- The *Edge Layer* includes a set of processing modules that process real-time data directly from the Device Layer. Examples are the Wearables Gateway running localization algorithms, the Processing Units executing video-based algorithms, the Sound Field Control System (SFCS) for managing the sound quality and noise reduction). These modules need to be deployed locally in the pilot site to avoid the latency introduced by the upper layers.
- The *Network Layer* allows the effective communication between the heterogeneous IoT wearables, IoT devices and the IoT platform modules.

The *Device Layer* includes all IoT wearables (g., wristbands and glasses) and IoT sensors, which can be fixed (e.g., sound level meters, loudspeakers, cameras, environmental sensors) or mobile (e.g., wireless sound level meters, cameras installed in a helium inflated balloon).

4.5.2 The MONICA Toolbox

MONICA has developed an open software development toolbox and generic enablers that allow developers to rapidly develop new applications to be deployed on the MONICA platform. The development platform consists of a toolbox and a set of tutorials and guidelines.

The MONICA Toolbox [26] is divided into three different categories:

- Software Developer Tools. These are packaged tools with user interfaces intended to be used by developers. They have been developed by the MONICA project. They are described in Chapter 3.
- Generic Enablers. These are re-usable software components developed by the MONICA project. MONICA generic enablers are made available in an Open Source GIT repository and can be used by entrepreneurs, start-up and established companies alike.
- Third Party Services and Tools. These are some openly available third-party tools that are recommended by the MONICA project to use when building Large Scale IoT applications. MONICA Tools and Generic Enablers have available interfaces for these third-party tools and services. They are described in Chapter 5.

The toolbox can be used to integrate various resources into the IoT Platform and hides the complexity of the communication with IoT devices. It features model-driven development of services that use the MONICA platform, also in connection with available Open Data sources. It will be based on a structure of service ontologies where a conceptual domain model describes the application, the services to be deployed and the objects involved (devices, users, rules, repositories, etc.).

4.5.3 Platforms and Technologies in MONICA

MONICA has opted for an integrated platform the developed IoT platform is the same used in all UCGs. It is composed of the LinkSmart middleware and the SCRAL adaptation framework and integrates the GOST (Go-SensorThings) IoT server that implements the sensing profile (part 1) of the OGC SensorThings API standard including the MQTT extension.

The LinkSmart middleware enables search and discovery of these devices and their resources by platform services and applications. Moreover, it provides unified APIs and protocols for historical and (near) real-time data access between the lower layers (i.e. Device Layer and Edge Layer) and

the upper one (i.e. Service Layer and App Layer) as depicted in MONICA architecture. The main components of the LinkSmart middleware are:

- The *Event Broker* that provides a message bus for efficient asynchronous communication of sensor data streams implementing the publish/subscribe communication pattern. The Message Queue Telemetry Transport (MQTT) is recognized as the de-facto standard for Publish/Subscribe communication in the IoT messaging domain, and provides several features like topic wildcards, different level of quality of service, retained messages, last will and testament, and persistence sessions;
- The *Resource Catalog* exposes a lightweight JSON-based RESTful API and provides a registry of integrated ICT data sources, their basic meta-information and deployment configuration, including information on how their data can be accessed. The SCRAL is supposed to register the available devices and their resources so that applications and services can discover these devices and learn how to communicate with them.
- The *Service Catalog* has similar functionality as the described above Resource Catalogue with the difference that it provides a registry for middleware and Monica Platform services.
- The *Historical Datastore* provides a repository with historical data from integrated sensor systems compliant with the OGC SensorThings v1.0, allowing access to the historical data from integrated sensor systems is one of the main functional requirements from applications to the middleware.

The IoT Layer components as well as the upper layers ones have been deployed on a cloud platform (MCP) that uses virtual machines as level of virtualization. The MCP uses two levels of virtualization - virtual machines and containers. The base virtual machine is CentOS 7, and the base container technology is Docker 1.12.6.

Various IoT devices have been integrated thanks to the MONICA platform, such as Sound Level Meters from B&K through its GW, and environmental sensors (based on RIOT) through its GW running in the Raspberry PI platform. Regarding the wearable devices, wristbands (based on the UWB standards and 868 MHz radio chip) and smart glasses have been integrated too. In addition, other IoT systems such as the AFCS (used to control the sound in the concert area and to reduce the sound limit in the neighbourhood), the Security Fusion Node (used to collect results from different video-based algorithms) and other external IoT smart city platforms have been integrated. One of these smart city platforms is the Hamburg one that will be integrated thanks to the oneM2M module of the MONICA platform.

4.6 The SYNCHRONICITY Interoperability Framework

4.6.1 Interoperability Support in SYNCHRONICITY

4.6.1.1 Reference Architecture and Interoperability Points

Based on a careful analysis of existing architectures and on the interoperability requirements of the different “Reference Zones” (RZ, i.e. the pilot cities) [28], SynchroniCity [27] has developed a Reference Architecture (updated in [29]) that strongly relies on the notion of “Interoperability Points”: *the main interfaces that allow applications to interact with the supporting platform*.

The Reference Architecture follows the OASC principles listed above that are strong guidelines for commonality that help creating more interoperable solutions:

- *A common standard API for context information management*: the context data manager (Context Data Broker) is a key component of the SynchroniCity architecture and the implementation of its API (compliant with NGSI API) is considered an “interoperability point” to enable cities to participate to the SynchroniCity platform.

- *A common set of information models*: semantic interoperability, achieved through the adoption of common data models, is introduced in the architecture as a basic requirement to enable reuse of applications in different cities and domains.
- *A set of common standards data publication platforms*: the role of data is crucial in SynchroniCity. For this reason, the reference architecture includes specific data management components that aim to provide, through standard interfaces, all the functionalities related to data life cycle management.

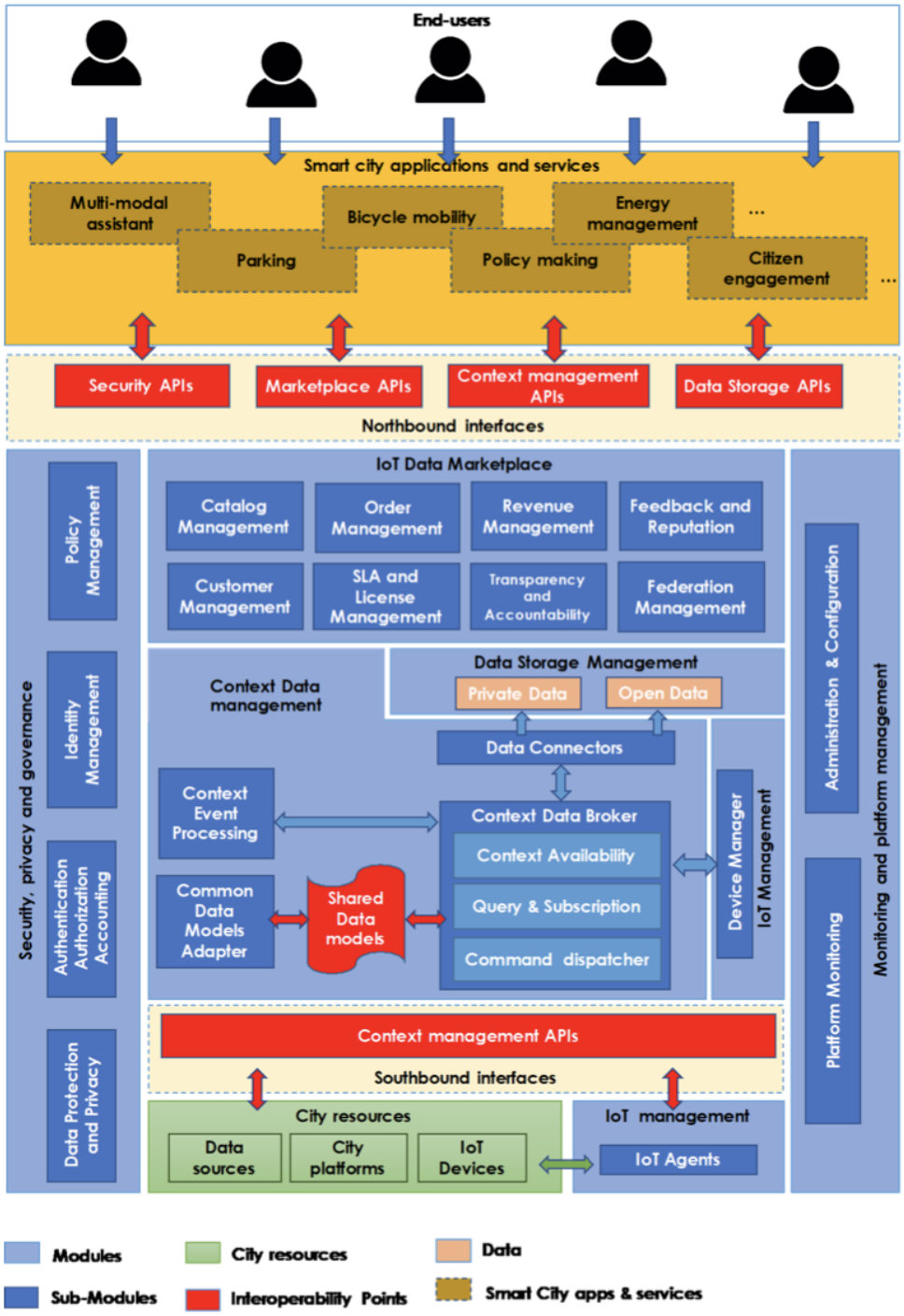


Figure 18: The SynchroniCity Reference Architecture and the Interoperability Points

Within the Reference Architecture presented in Figure 18, a crucial role is devoted to the Interoperability Points and the Interoperability Mechanisms (the actual interface specifications at the Interoperability Point). The Interoperability Mechanisms are listed in Table 8.

Table 8: SynchroniCity Interoperability Mechanisms

	Description	Specification document	Related Standards [and Baselines]
Context Management API	The API to access to real-time context information from the different cities.	Reference Architecture for IoT Enabled Smart Cities (D2.10)	FIWARE NGSIv2, ETSI NGSI-LD API, ITU-T SG20*/FG-DPM*
Shared data models	Guidelines and catalogue of common data models in different verticals to enable interoperability for applications and systems among different cities	Guidelines for the definition of OASC Shared Data Models (D2.2) Catalogue of OASC Shared Data Models for Smart City domains (D2.3)	[FIWARE, GSMA, schema.org, Saref , SynchroniCity RZ + partner data models]
Ecosystem Transaction Management ("Marketplace")	An API to expose functionalities such as catalogue management, ordering management, revenue management, SLA, license management etc.	Basic Data Marketplace Enablers (D2.4) Guidelines for the integration of IoT devices in OASC compliant platforms (D2.6)	[TM Forum API]
Security API	An API to register and authenticate user and applications in order to access to the SynchroniCity-enabled services.	Reference Architecture for IoT Enabled Smart Cities (D2.10)	OAuth2
Data Storage API	An API to allow access to historical data and open data of the reference zones.	Reference Architecture for IoT Enabled Smart Cities (D2.10)	ETSI NGSI-LD, DCAT-AP [CKAN]

4.6.1.2 The Synchronicity IoT Data Marketplace

The SynchroniCity architecture includes an IoT Data Marketplace component (a brokerage site that favours the meeting between demand and supply of goods and services) to encourage and foster the sustainable commercial viability of data by developing an added value that goes beyond traditional rights-based licensing models of data sets.

The Conceptual view of the Data marketplace is shown in Figure 19.

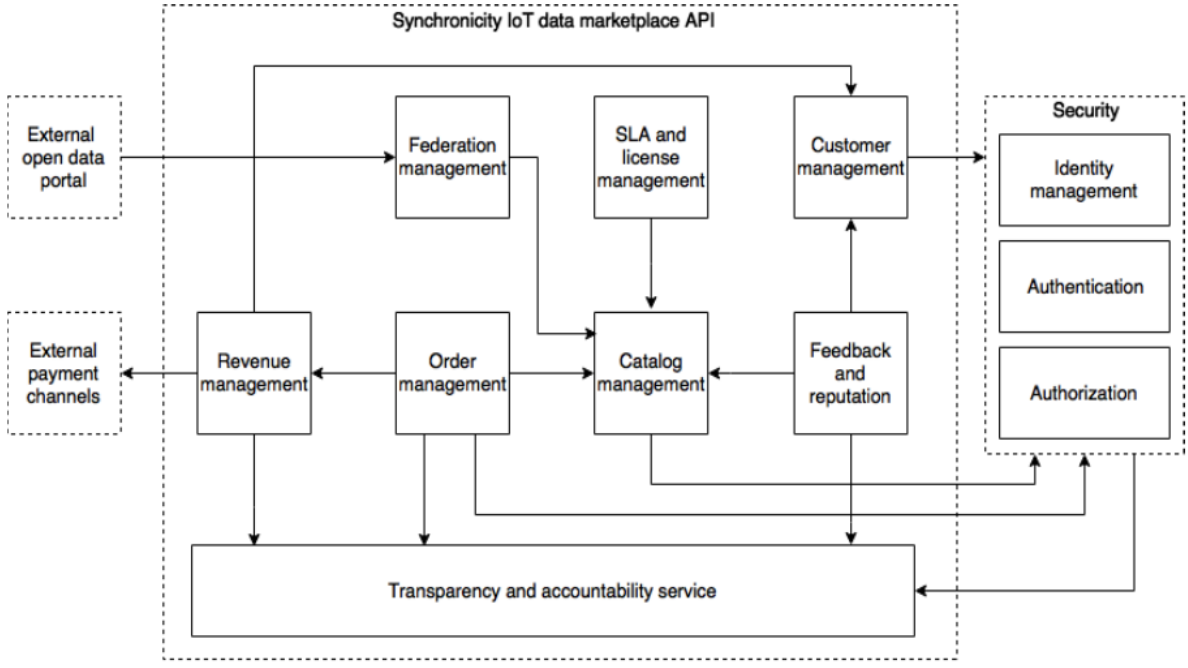


Figure 19: Conceptual model of the SynchroniCity IoT data marketplace

The marketplace platform consists primarily of the following components:

- The *Marketplace API* is the core element of the platform. It allows data providers to register or import data sources into the platform, to publish offerings containing its description, and allows data consumers (e.g., service developers) to discover and purchase offerings.
- The *Marketplace portal* is an optional component providing a user interface through which data providers and data consumers can interact with the platform, use the Marketplace API, and manage their accounts and information.

The basic functionalities of the current implementation of the marketplace APIs and marketplace portal are provided by adapting/extending the FIWARE/TMForum BAE components and by developing new components.

4.6.2 Platforms and Technologies in SYNCHRONICITY

SynchroniCity proposes a reference implementation of the logical architecture in order to provide open-source, ready to use components to the deployment sites.

The adoption or usage of the proposed technical components are not mandatory but should be considered as one of the possible implementations of the SynchroniCity architecture.

The pilot sites (RZ) can choose the best approach related to their technical and business requirements and adopt or integrate only a part of the components proposed in the reference implementation.

The main elements of the Reference Implementation are shown in Figure 20 with the Interoperability Points supported.

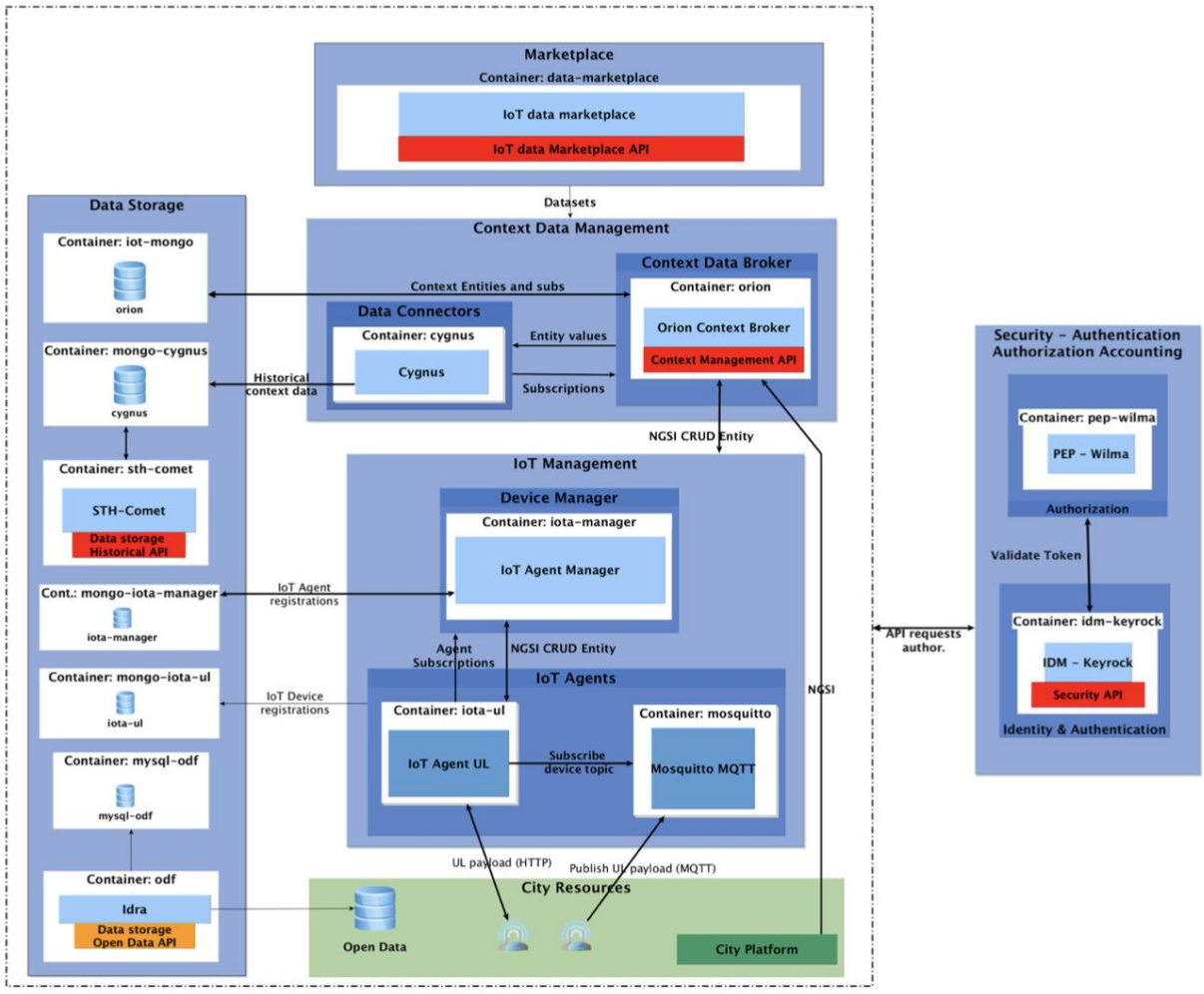


Figure 20: Overview of the Reference implementation architecture

4.7 Commonalities of LSPs IoT Interoperability Frameworks

For several IoT projects, those who span large domains (e.g., Smart Cities), cross-domain interoperability is a key requirement for achieving large scale deployment of IoT-enabled services.

Some commonalities have been identified across the Reference Architectures of the LSPs. This has already been highlighted in section 3.4, in particular regarding the identification of a common approach to functional layering (as shown in Figure 7). The work of the LSP Activity Group 02 (Standardisation, Architecture and Interoperability) has shown that other commonalities can be identified within the existing architectures (e.g., regarding the "Cross-cutting Functions" such as security for which the LSPs have defined relatively similar frameworks). In addition, new common elements have been addressed by Activity Group 02 such as the additional "Properties" dimension. The 3D Reference Architecture model presented in section 5 is capturing these commonalities.

5. A COMMON REFERENCE ARCHITECTURE MODEL

5.1 A common view of the IoT LSPs Reference Architectures

For the specification and development of their use cases, all the LSPs have produced several specific Reference Architectures that correspond to the needs of their specific domain, their technology and platform choices, etc.

The work of the LSP Activity Group 02 (Standardisation, Architectures and Interoperability) has addressed the identification of commonalities across their different approaches.

The (3D) IoT Reference Architecture proposed in the present section is reflecting the common view of LSPs and has been completed by an analysis by the LSP of one significant use case using the 3D Reference Architecture model.

As already pointed out (in section 3.4.1), an early analysis of the functional architecture had shown a similarity of approaches regarding the layers they used (summarised in Figure 7).

In addition, most architecture also had to consider issues such as security and privacy (the latter having emerged as a very critical aspect regarding trust in the IoT systems).

Such cross-cutting approaches have appeared as another are of possible commonality between the LSPs and a possible extension to a common Reference Architecture model.

This initial blueprint of the 3D Reference Architecture Model will be further elaborated and is meant to be fed to the discussion initiated by ISO/IEC JTC1 on Meta-Architectures.

5.2 A 3-dimensional Reference Architecture Model

5.2.1 A model in support of stakeholders' viewpoints in IoT system development

The LSP 3 dimensional (3D) Reference Architecture model (developed in the IoT Large Scale Pilots Activity Group 02 "Interoperability and Standardisation") offers an extension of current Reference Architectures and is aiming at ensuring a common view of the different layers of the IoT systems from Physical up to Business; and providing additional viewpoints to the different stakeholders (not just to the developers);

This architecture consists of a 3D representation presenting the key components for IoT/IIoT applications under 3 dimensions that support shared analysis of some between different stakeholders.

- The "Layer" dimension in support of the functional view of the system. The 8 layers defined are common to all the Reference Architectures that the 5 LSPs have developed.
- The "Cross-Cutting Functions" dimension considering transversal technologies such as security, privacy or safety and properties (e.g., integrability)
- The "Properties" dimension addresses the global properties of the IoT system that re (or not) provided b y a proper implementation of functions (at all layers) and cross-cutting functions. As an example, trustworthiness is resulting in particular from the proper implementation of the security and privacy cross-cutting functions.

The applications may require different components presented in the architecture depending on the requirements and specifications.

Two of the 3D Model's dimensions, namely the "Layer" and "Cross-Cutting Functions", provide viewpoints that are present in most of the Reference Architecture model, though in a more systematic approach.

The additional third dimension of "Properties" is a new way to discuss the properties of the IoT system between different involved parties (e.g., users, contractors, designers) and identify the elements in support (e.g., functional building blocks, APIs) and those missing.

The 3D architecture is generic and offers a representation that can include the different IoT/IIOT applications across different sector domains (e.g. automated/autonomous vehicles, smart farming, wearables, smart cities, energy, manufacturing, health, etc.).

The architecture includes the function by design concept with end-to-end functions addressed across the 8 layers.

This allows to address the heterogeneous applications including different IoT platforms and processing at the edge, fog and cloud.

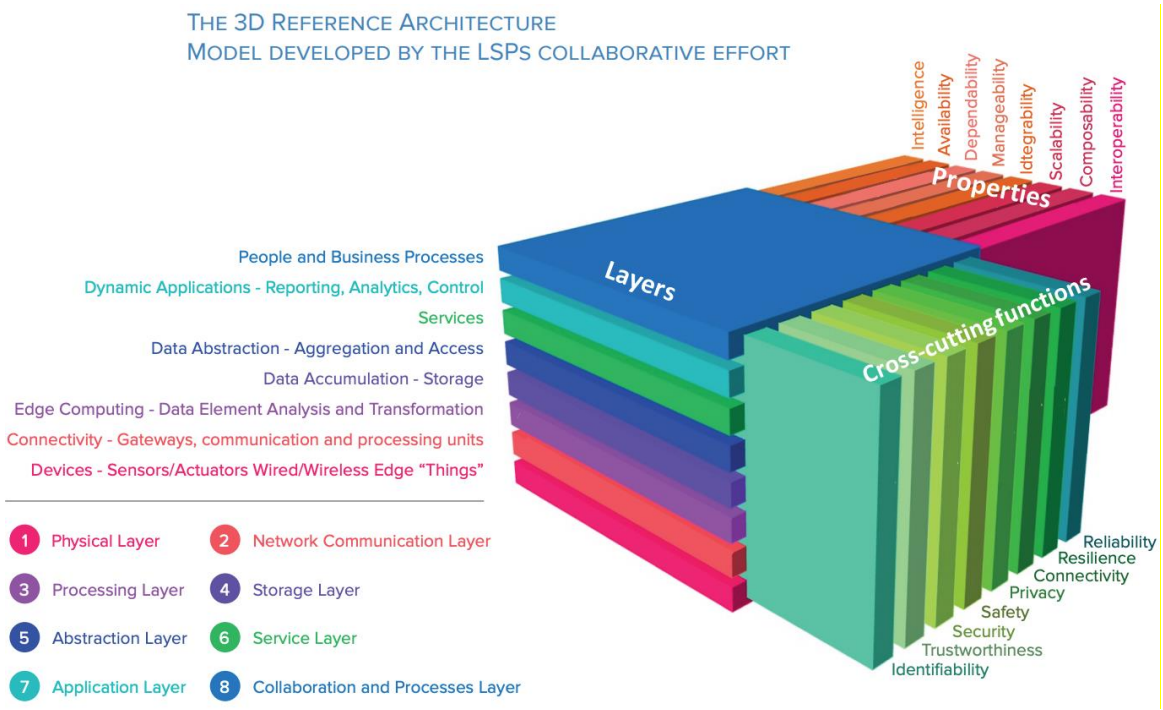


Figure 21: The 3D Reference Architecture Model

5.2.2 Benefits of the 3-dimensional approach

The architecture allows to address the device management, capabilities, including command/control of devices and the inclusion of various gateways for implementation of the different functions across the 8 layers.

The services that ingests events from IoT devices and the message broker functions implementations between devices and backend services can be highlighted using this new 3D architectural views.

The 3D architecture provides an optimised view of the stream processing across the 8 layers allowing to evaluate the rules and functions for analysing the information streams.

By including the system properties view elements as intelligence, dependability, manageability, integrability, composability, interoperability can be specified and implemented across the 8 layers.

The intelligence system property allows defining for example machine learning components across the 8 layers for predictive algorithms to be executed over historical IoT data, enabling scenarios such as predictive maintenance.

Information transformation across the 8 layers and the aggregation of IoT data stream can be specified for different applications including protocol transformation and interoperability interfaces.

5.2.3 Supporting complementary points of view of an IoT system

The 3D architecture model has 6 faces which can, in principle, offer a given view of the IoT system under analysis. Amongst them, three (marked by the arrows in Figure 22) have been particularly found useful in support of the discussion amongst various involved roles:

1. The “Layers” view
2. The “Cross-cutting view
3. The “Properties” view

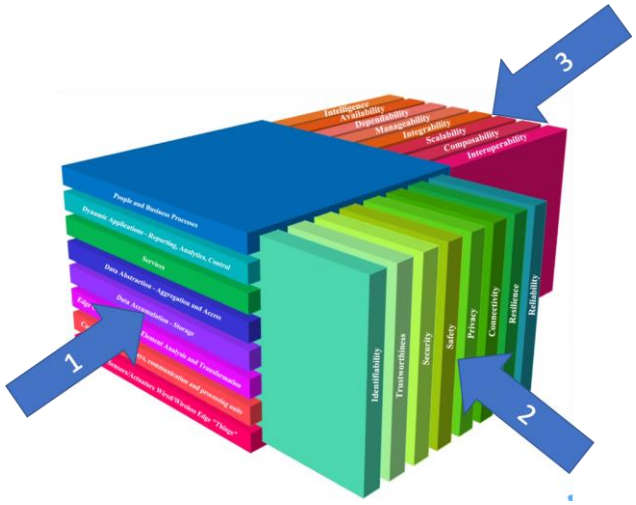


Figure 22: Three perspectives on an IoT system

Their main purpose and the stakeholder’s roles involved are described below. These views are used further in the section with the different examples. They are described in 2 dimensions as shown in Figure 23. In each of the 2D views, some elements are identified such as applicable standards, mandatory interfaces or Reference Points, APIs, codes of conduct, conformance schemes, etc.

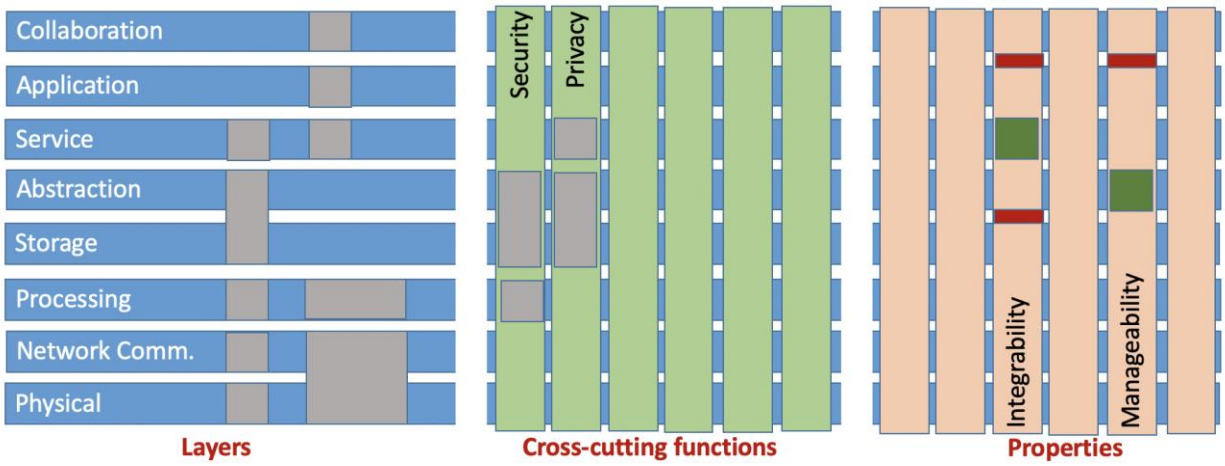
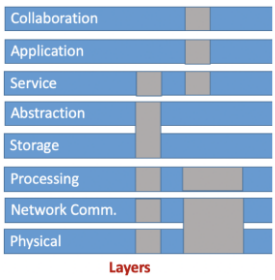


Figure 23: Three views of an IoT system

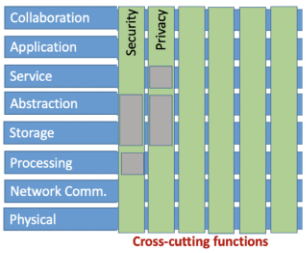
5.2.3.1 The “Layers” view



- A “Functional” view
  - Identification of functional blocks
    - And possibly associated components
  - Characterisation of interoperability
    - Data Models
    - Information models
    - Interworking standard
- Main supported roles
  - IoT System Designers
  - IoT System Developers
  - Application developers

The “Layers” view in the 3D model refers to the overall characteristics of IoT Systems from a functional and operational perspective, it includes aspects from physical devices, networking, cloud infrastructures, data, services and applications but also collaboration. The main usage of this layer is to facilitate the identification of necessary functional blocks for interoperability at the different “layers” in IoT systems.

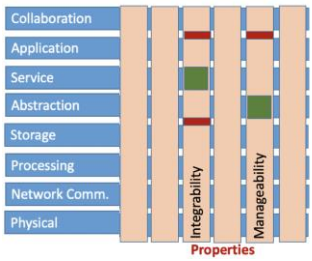
5.2.3.2 The "Cross-cutting Functions" view



- A "specialized expertise" view
  - Identification of functional blocks
    - Functional blocks and APIs
    - Applicable process-oriented schemes
      - E.g., security or data protection assessment
  - A support for exchange of information
    - Mapping designers and experts views
    - Identification of constraints
    - Clarification of applicable standards
- Main supported roles
  - Domain experts (security, safety, ...)
  - IoT System Designers and developers
  - Application developers

The "Cross-cutting Functions" view refers to properties of the IoT system which are not resulting from just functional components but more from the interactions amongst these components. It includes security, safety & resilience, trust and privacy, connectivity, interoperability, dynamic composition and automated interoperability. The main usage of this layer is to support the protected and reliable exchange of information.

5.2.3.3 The "Properties" view



- An "all stakeholders" view
  - Identification of expected properties
    - Expected non-functional figures
      - E.g. availability, latency; legacy support; ...
    - Applicable frameworks and standards
      - E.g., codes of conduct, specific regulation
  - A support for exchange of information
    - Expressing the decision-makers and users views
    - Confronting them with the designers/experts
    - Resolving discrepancies upstream
- Main supported roles
  - Project owners and supervisors; (end-)users
  - IoT System designers and developers
  - Application developers
  - Domain experts (security, safety, ...)

The "Properties" view refers to features and characteristics of the IoT systems associated with the administration and management aspects of the IoT infrastructure and the system itself. It includes intelligence, availability, dependability, manageability, integrity, scalability composability and Interoperability. The main usage of this layer is for identification of the properties characterising IoT systems or applications.

5.2.4 The "Properties" dimension of IoT systems

As already pointed out in section 5.2.1, the third dimension of "Properties" in the 3D Reference Architecture Model is a new way to support the discussion about the expected properties of the IoT system between different involved parties (e.g., users, contractors, designers) and identify the elements in support (e.g., functional building blocks, APIs) and those missing.

To some extent, the notion of property has a more "open" character than the "Layers" and "Cross-cutting Functions" dimensions. In particular, given the nature of the IoT system under consideration (e.g., business domain, integration with legacy), the list of "properties" could be defined on a more "IoT project-oriented" basis than the other two dimensions. In addition, it should be noted that there is no commonly agreed upon definitions for some of the "properties" analysed below.

Secondly, the "properties" dimension is not only directed to the identification of applicable standards: the discussion between stakeholders may also lead to the identification of applicable codes of conduct or policy directives.

5.2.4.1 Interoperability

Interoperability is a characteristic of a product or system, whose interfaces are perfectly able, to work with other products or systems, at present or future, in either implementation or access, without any restrictions [15]. More specifically, interoperability is defined as the degree to which two or more IoT systems/platforms, can exchange information/knowledge and use the information/knowledge that has been exchanged.

This refers to the approaches taken to ensure interoperability at different layers, as explained in section 3.1. Interoperability is key to enabling data spaces with ecosystems of providers and consumers of data. Of particular note, semantic interoperability depends on the availability of standard vocabularies, and the number of vocabularies is potentially unlimited. This makes semantic interoperability more challenging than interoperability at other layers, e.g. technical and syntactic where fewer standards are needed.

5.2.4.2 Composability

Composability is defined as an IoT system property that address the inter-relationships of components, with composable IoT systems integrating components that can be selected and

assembled in various combinations to satisfy specific user requirements. In IoT the features required for a composable IoT system is to be self-contained (modular) and can be deployed independently and to be stateless and can treat each data request as an independent transaction, unrelated to any previous requests. The IoT composable systems are considered more trustworthy than non-composable systems because the IoT system can be decompose and evaluate the individual parts. The complex IoT implementations represent systems of systems with different systems and sub-systems developed by diverse teams, often from different stakeholders. For the IoT systems compositionality, is defined as the ability to combine modules and to understand and composite system by defining the components and how they are combined, while modularity represents the degree of designing subsystems (modules) with well-defined interfaces that can be used in a variety of contexts.

Composability is the capability for creating services as the combination of other services. Using an analogy, an architect creates a design that can be used to build many buildings, whilst a builder creates a particular building. Composability of services thus takes two forms:

- *Architect:* Using the metadata for software components to design a combination that will satisfy a given design goal when applied to matching data feeds. The new design can be sold on the marketplace for the customers to instantiate according to their needs.
- *Builder:* Combining existing data feeds to create a derived data feed that will be of value to one or more customers.

In both cases rich metadata is essential for ensuring that the components will work together as specified. Composability is coupled to **Searchability**, i.e. the means to discover components that match a given set of characteristics.

5.2.4.3 Scalability

Scalability is the ability of a process, network, software or organization to grow and manage increased demand [15]. Scalability is often a sign of stability and competitiveness, as it means the network, system, software or organization is ready to handle the influx of demand, increased productivity, trends, changing needs and even presence or introduction of new competitors.

Scaling can refer to the ability to support increasing numbers of devices, e.g. millions of cars or billions of smart phones. It can also refer to the amount of data and its throughput. Cloud based solutions are often cheaper and more flexible than systems hosted by an organisation in its own computing centre. Containerisation is a commonly used means to deploy and run distributed cloud-based applications without the need to launch a new virtual machine for each app.

A centralised cloud-based system may be the easiest design to deploy but can run into problems when the number of IoT devices scales up and up. This can be addressed by federating the service across a server farm or a peer to peer scale free network. It may also be possible to move much of the burden of processing and storage to the network edge – so called *edge computing*. The use of intermediate sized systems in between the edge and the cloud is sometimes referred to as *fog computing*.

5.2.4.4 Integrability

Integrability is defined as the degree of effectiveness and efficiency with which an IoT system can be successfully integrated within heterogeneous IoT systems/platforms and sub-systems or other types of systems including platforms. This can be contrasted with composability of IoT services.

5.2.4.5 Manageability

Manageability is the ability to manage the IoT system to ensure continuous operation. This is important to being able to handle very large numbers of IoT devices in a convenient and cost-effective manner. That includes, for instance, the installation of new devices, software upgrades

to fix vulnerabilities, and the transfer of ownership of individual devices, and re-establishment of trust.

5.2.4.6 Dependability

Dependability is the ability to deliver a service that can justifiably be trusted [14]. Another definition of dependability is the ability to avoid service failures that are more frequent and more severe than is acceptable. This relates to quality of service commitments, and the speed with which vulnerabilities can be fixed by rolling out software updates. It also relates to resilience and the dependability of the system in the face of faults, cyberattacks and demand spikes.

5.2.4.7 Availability

Availability is defined as the degree to which an IoT system/platform is operational and accessible when required for use. The ability of the IoT system to deliver services and information when requested [14].

5.2.4.8 Intelligence

Intelligence in the meaning of Artificial Intelligence (AI) and AI features, algorithms, techniques and methods used in different IoT layers of a system to provide different levels of intelligent functions and behaviours. It can be contrasted with analytics that is the systematic computational analysis of data or statistics, and which can be used to better understand the functioning of a system. AI is also related to machine learning, including *deep learning* based upon multi-layer artificial neural networks, which can be contrasted with techniques based upon reasoning over symbolic representations. Today's AI is narrow in scope *(weak AI)* and designed to handle specific tasks. In future, strong AI will be capable of handling a much wider range of tasks including those it has not seen before. Strong AI is expected to be based upon advances in the cognitive sciences, i.e. our understanding of the human mind and brain.

5.3 Examples of use of the 3D Reference Architecture Model

The 3D Reference Model has been used in the context of the LSP Activity Group 02 to analyse some Use Cases.

5.3.1 The AUTOPILOT analysis

The LSP and AUTOPILOT architecture approaches are illustrated in Figure 24 including the application, IoT, and network layers, together with IoT reference architectures, architecture patterns, and characteristic features of IoT.

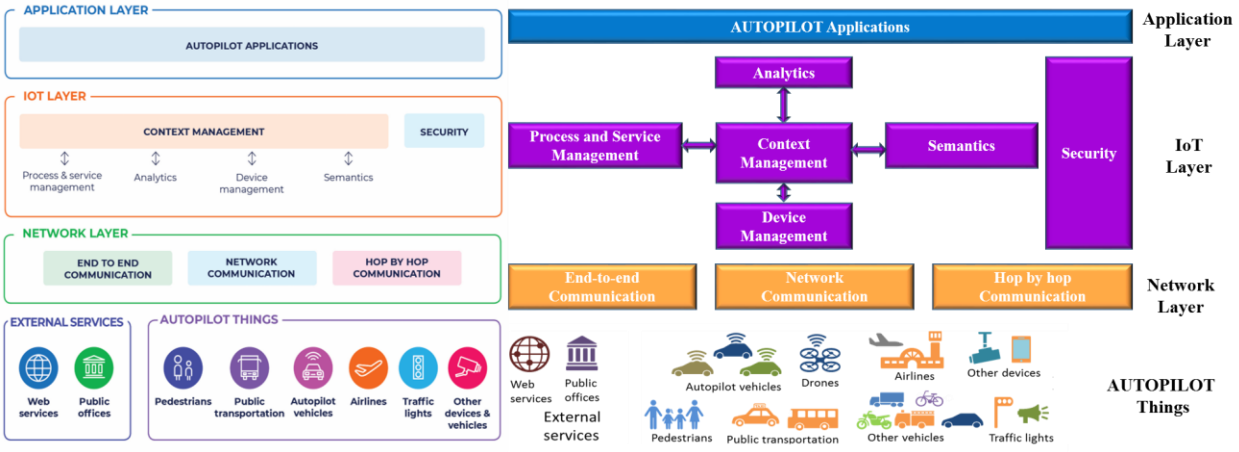


Figure 24: LSP architecture approach

AUTOPILOT has been the first LSP to make an initial analysis of a use case (in the context of the Versailles pilot) with the 3D Architecture Model.

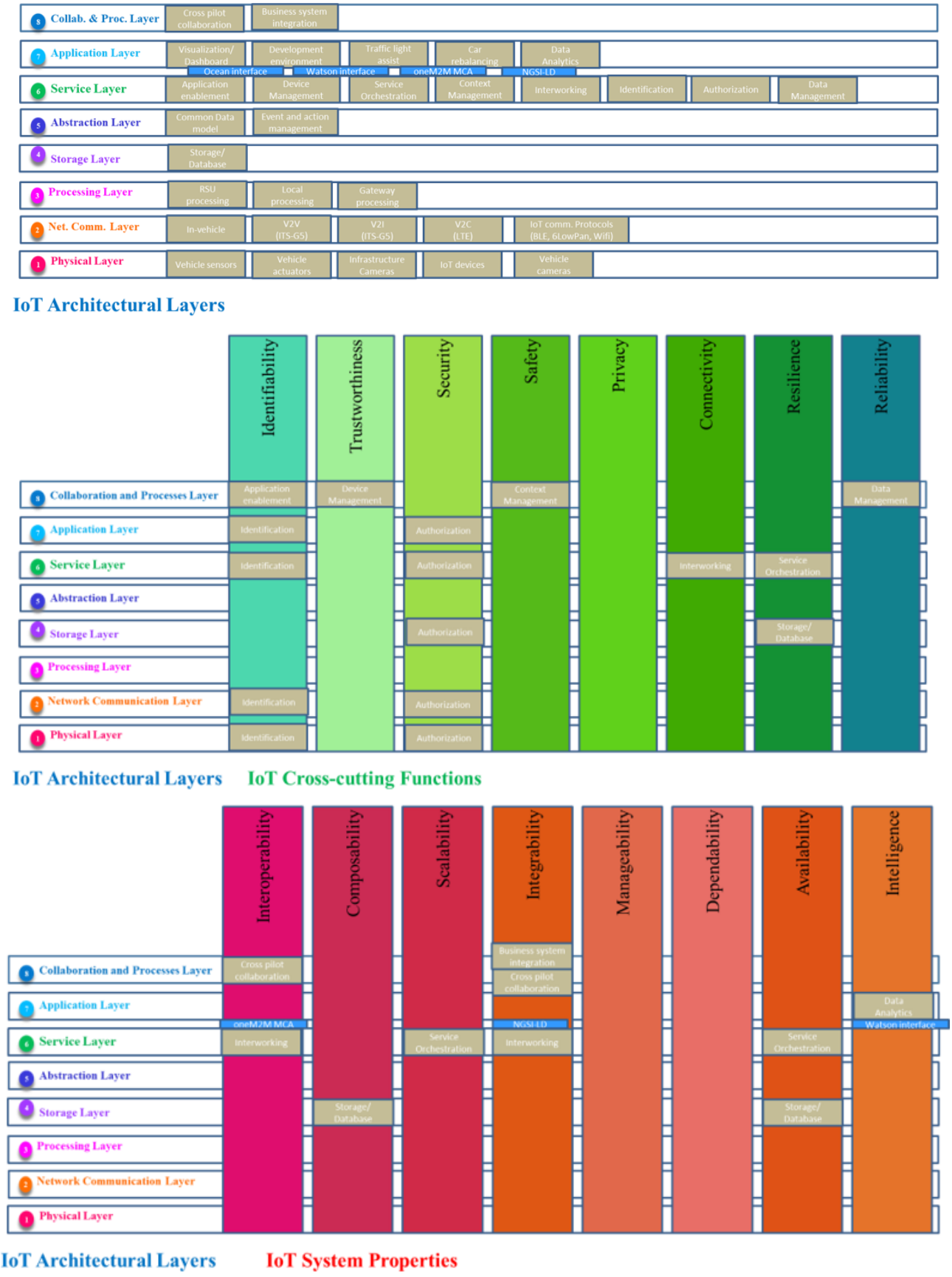


Figure 25: AUTOPILOT use case mapping

This example has served to the LSPs as a basis for the development of their own example. The approach taken is to fill the three main views (Layers; Cross-cutting Functions"; and "Properties") from the point of view of the application designers and developers in order to identify the concrete elements of the implementation. In particular, it has addressed the identification of the functional constraints linked to the various platforms utilised.

As an illustration, the analysis of the IoT system properties related to the use case of the Versailles pilot site is shown in Figure 25. The northbound interfaces between the Service Layer and the Application layer involved in the provision of properties are identified, with the example of the oneM2M Mca Reference Point for interoperability.

5.3.2 The ACTIVAGE analysis

The ACTIVAGE architecture (illustrated in Figure 26) is by design semantic-oriented and that this is a feature that address the requirement for cross domain interoperability. The role of the AIOTES Semantic Interoperability Layer (SIL) is to provide flexibility with respect to the deployment of applications in such a way that they are interoperable and, as such, they are not constrained by the closed environment of cloud service providers and that at the same time this approach enables the full interoperability from a semantic layer perspective allowing to bridge variety of IoT platforms as shown in Figure 26.

In ACTIVAGE the diversity of IoT technology is an element to consider all the time and particularly when different interoperability scenarios outline the need for a very precise role of data in the architecture. A significant part of the issues to handle are regarding data management (cross-platform sharing; cross-applications and cross-services reuse; data lakes; etc.) but also data usage consent. The possible support of the BDVA approach has been discussed.

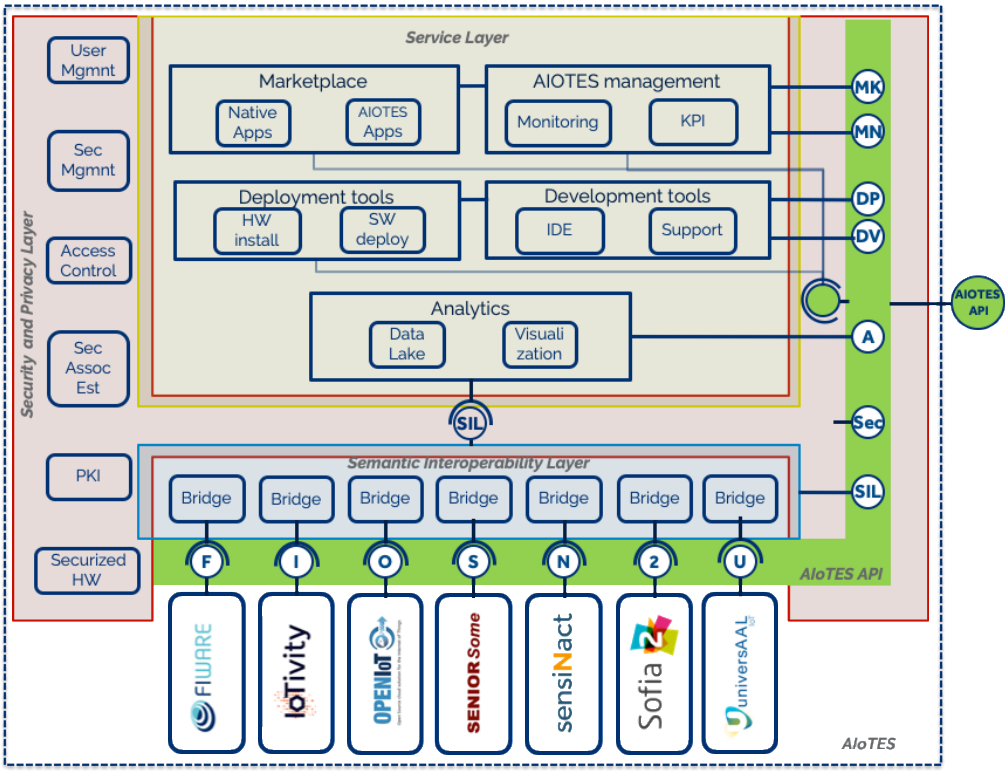


Figure 26: ACTIVAGE Functional Architecture

The analysis of the IoT system properties related to the use case of the Versailles pilot site is shown in the three pictures of Figure 27.

A preliminary revision and analysis of the mapping with the 3D Model to ACTIVAGE use case has started by aligning the current AIOTES layers and the cross-cutting functions for the semantic layer (SIL) from AIOTES architecture.

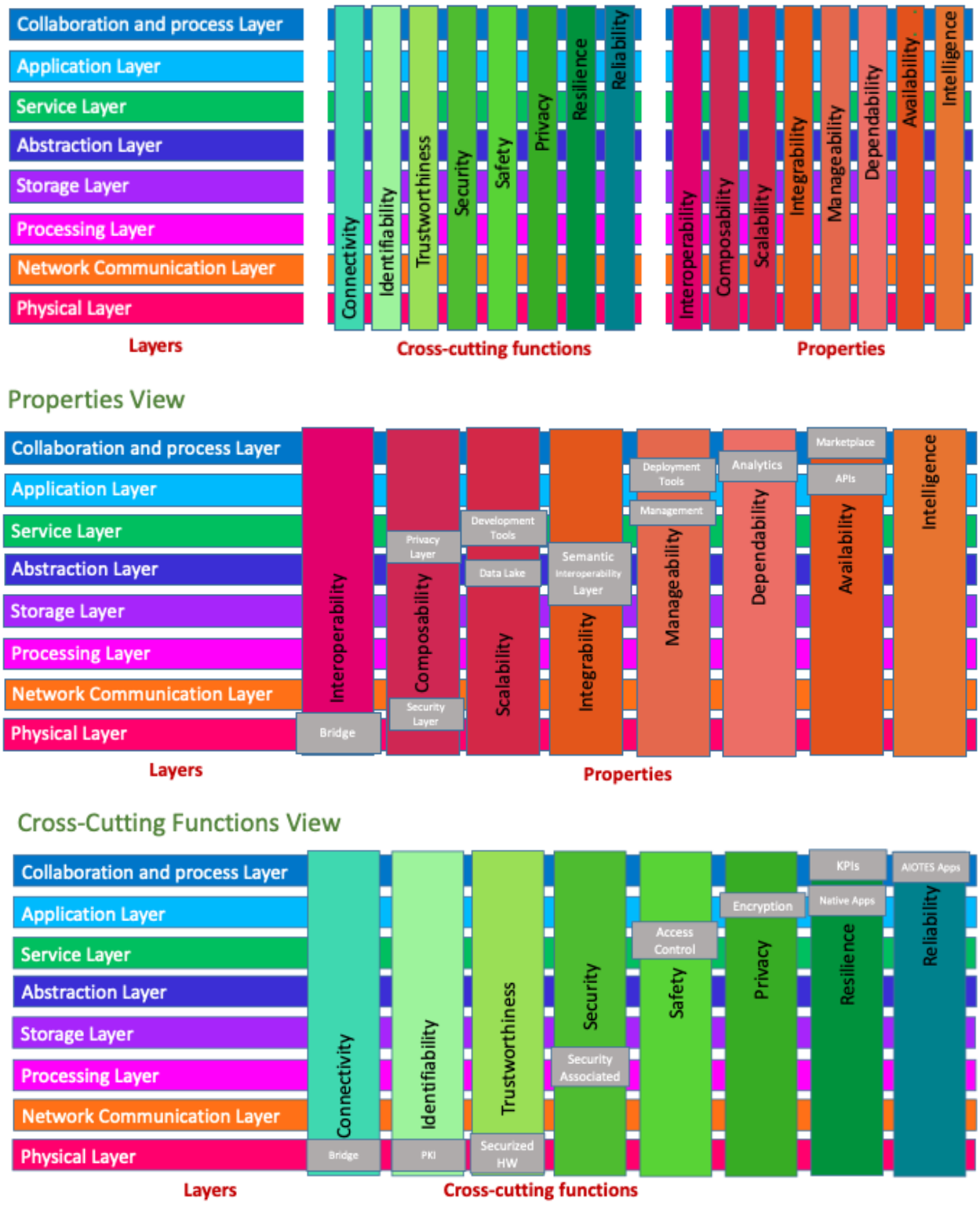


Figure 27: ACTIVAGE preliminary Architecture Mapping

The preliminary analysis has also focused on the identification of the processes at the AIOTES level and the services for mapping with the properties layer in the 3D model, from a designer/developer perspective, of the different functional blocks used the 3D model and the LSP ACTIVAGE AIOTES architecture can be mapped.

In ACTIVAGE the interoperability level follows the definition provided from the IoT interoperability manifesto [39] which reflects the IoT community contribution. The mapping with the 3D model also re-organises the properties and cross-domain functions following the interoperability levels.

5.3.3 The MONICA analysis

A preliminary analysis of a MONICA use case, based on a similar approach than that of AUTOPILOT, has focused on the identification, from a designer/developer perspective, of the different functional blocks used.

Figure 28: MONICA Use Case mapping on 3D Architecture

A follow-up should address the other elements involved in the 3D models such as the interoperability points and mechanisms, the APIs, etc. A short feedback on the lessons learned will be also provided.

5.3.4 The SYNCHRONICITY analysis

A preliminary analysis of the application of the 3D Model to a SYNCHRONICITY use case, based on a similar approach than that of AUTOPILOT, has insisted on the role of the Interoperability Points in the context of the Use Cases and of the open calls, and how they provide interoperable, replicable and reusable solutions across cities and sectors.

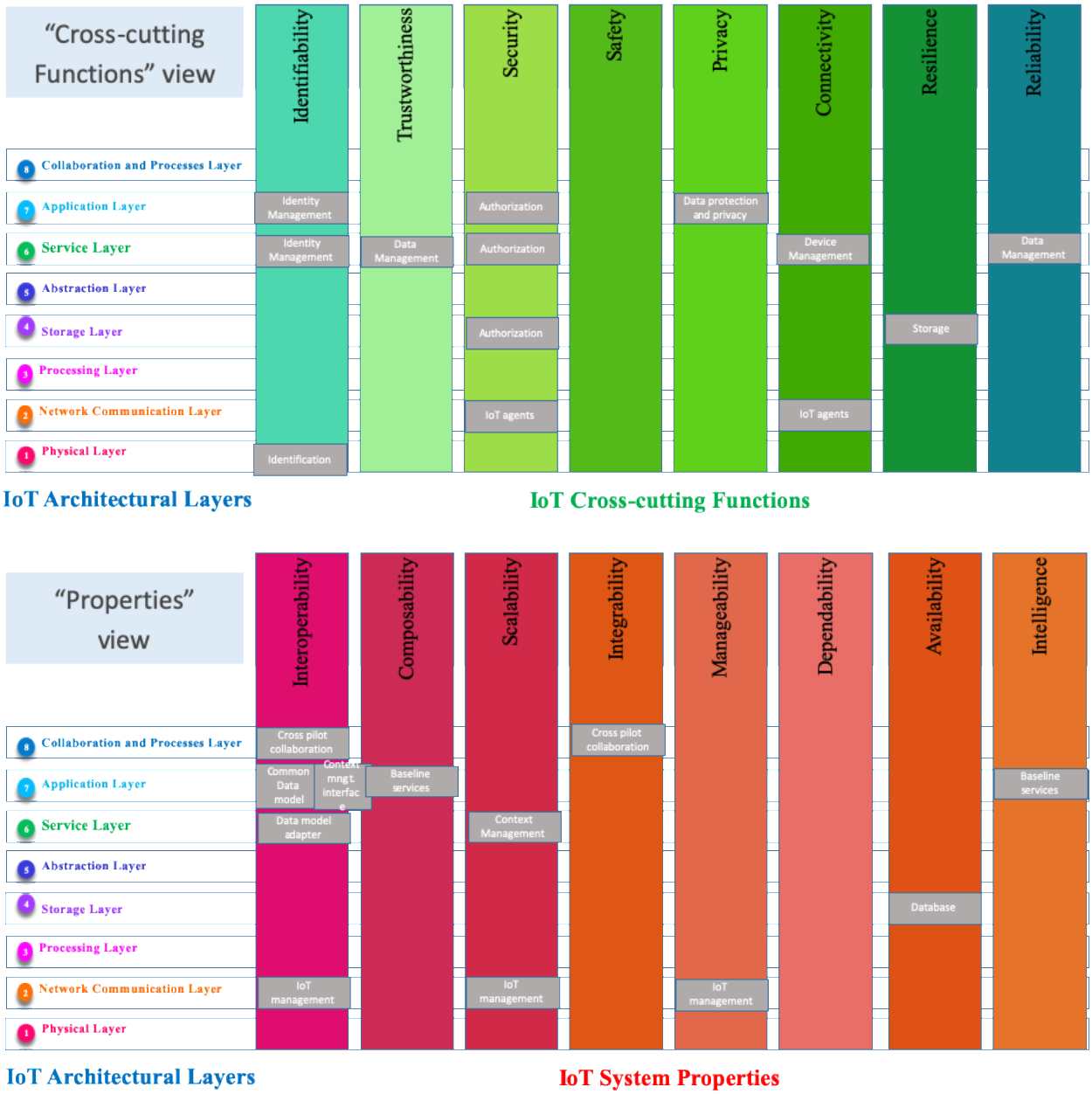


Figure 29: SYNCHRONICITY Use Case mapping on 3D Architecture

5.3.5 Feedback from usage and potential areas of evolution

The four above use case analysis have been presented in the context of one of the Workshops organised by the Activity Group 2 (see). Some remarks and suggestions have been made during the discussion, in particular regarding the 3D Reference Architecture approach:

- The role of data in the architectures (the 3D reference Architecture model as well as the LSP ones) is becoming more and more important and it needs to be clarified (e.g., as a specific element within the Cross-cutting functions). Additionally, the way the 3D model maps with the BDVA approach requires additional investigation.
- The model may seem difficult to use for some of the stakeholders involved in its potential usage. Even if it seems that the designers and developers may use it easily (though with a strong focus on functionality rather than on properties), it is probably more difficult to handle for the project owners and supervisors or the (end-)users. Some clarification, more detailed examples and guidelines will be needed.

6. FINDINGS AND FUTURE WORK

The 5 LSPs (of the first generation of LSPs) have addressed the development of a large variety advanced use cases in a variety of sectors. To this extent, they had taken the state of the art in IoT systems development and made several additions that have been validated in a large number of pilot sites using various technologies and platforms.

Amongst these contributions, a certain number have been related to a given sector with the objective to ensure common approaches and reusable solutions. Some others have the potential of being applicable beyond the borders of the sector in which they have been defined.

Some examples are listed below:

- The collaborative development by LSPs of a 3D Reference Architecture model.
- The Minimum Interoperability Points (MIMs).
- The definition and early implementation of Data marketplaces.
- The definition and development of (open source based) Reference implementations.
- The IoT Catalogue that collects components to be used/reused in implementation projects.
- The methodology for launching Open Calls and following their implementation.

Innovation in the IoT field is continuing at high pace and priorities have somehow shifted, in particular due to the central role of data in IoT systems and the growing role of Artificial Intelligence in dealing with all issues related to the management and processing of data. Some topics have been clearly identified (see deliverable D06.11 [11]) as priorities by several projects of the second generation of LSPs.

A short list of these topics is the following:

- Supporting the efficient adoption of new technologies such as Distributed Ledger Technologies or Artificial Intelligence, across all parts of the IoT systems from physical to business layers, in support of cross-cutting functions such as security, privacy or safety.
- Developing solutions (including the necessary infrastructure) for secure data management in support Open Access to data and the creation of generic or sector-specific data spaces.
- Addressing the challenges of industrial adoption for semantic interoperability together with improving the efficiency of organizational interoperability solutions.
- Strengthening the provision of privacy and security for resilient services.
- Taking full benefits of communications scalability, reliability, latency (e.g., 5G).
- Boosting the efficiency of edge solutions (data privacy, federation, AI, etc.).
- Proposing robust solutions for privacy-preserving federated machine learning.
- Fostering the emergence of the Intelligent autonomous IoT.
- Defining the Sentient Web (web of digital twins, cognitive AI and open marketplaces).

By using some of the results of the first generation of LSPs, the next generation of LSPs may contribute to the progress in IoT standardisation, even on a larger scale than the first generation has. In order to make this most effective, there is a need, across the new LSPs, for collaboration, information exchange, as well as identification and promotion of common approaches and best practices, fostering the development of common visions (e.g., through White Papers).

7. REFERENCES

CREATE-IoT WP06 Deliverables

[1] "Strategy and coordination plan for IoT interoperability and standard approaches", Deliverable D06.01, 2017.

[2] "Recommendations for commonalities and interoperability profiles of IoT platforms", Deliverable D06.02, 2018.

[3] "Assessment of convergence and interoperability in LSP platforms", Deliverable D06.03, 2020.

[4] "IoT pre-normative activities", Deliverable D06.04, 2017.

[5] "Initial report on IoT standardisation activities", Deliverable D06.05, 2018.

[6] "Final report on IoT standardisation activities", Deliverable D06.06, 2020.

[7] "Strategy and coordination plan for IoT interoperability and pre-normative and standardisation activities", Deliverable D06.07, 2018.

[8] "Interoperability Framework Workshop", Deliverable D06.08, 2018.

[9] "Workshop on LSPs use cases: integration and standardisation alignment", Deliverable D06.09, 2019.

[10] "Workshop on IoT standardisation activities", Deliverable D06.10, 2019.

[11] "Workshop on common IoT standardisation framework", Deliverable D06.11, 2020.

Other CREATE-IoT Deliverables

[12] "IoT European Large-Scale Pilot Programme – Large-Scale Pilots", eBrochure. https://european-iot-pilots.eu/wp-content/uploads/2018/03/220315_SD_IoT_Brochure_A4_LowRes_final-1.pdf

[13] "Reference Architecture for Federation and Cooperation Between IoT Deployments", Deliverable D2.02, 2018.

[14] "IoT Policy Framework", Deliverable D05.01, 2017.

LSP References and Deliverables

[15] Handbook to the IoT Large-Scale Pilots Programme. Online at: https://european-iot-pilots.eu/resources/iot-european-large-scale-wiki/

ACTIVAGE

[16] ACTIVAGE (ACTivating InnoVative IoT smart living environments for AGEing well); https://european-iot-pilots.eu/project/activage/

[17] "ACTIVAGE IoT Ecosystem for Smart Living Environments", ACTIVAGE Brochure

AUTOPILOT

[18] AUTOPILOT (AUTOmated driving Progressed by Internet Of Things); https://european-iot-pilots.eu/project/autopilot/

[19] "Standardisation plan", AUTOPILOT Deliverable D5.7, May 2017.

[20] "Standards and conformance of IoT in AD", AUTOPILOT Deliverable D5.8

IoF2020

[21] IoF2020 (Internet of Food and Farm 2020); https://european-iot-pilots.eu/project/iof2020/

[22] "Opportunities and Barriers in the present regulatory situation for system development", IoF2020 Deliverable D3.3

[23] "Hosting Environment and IoF2020 Lab", IoF2020 Deliverable D3.8

[24] "The IoT Catalogue", http://www.iot-catalogue.com

MONICA

[25] MONICA (Management Of Networked IoT Wearables); https://european-iot-pilots.eu/project/monica/

[26] "The MONICA Development Toolbox", Deliverable D7.5

Synchronicity

[27] SynchroniCity (Delivering an IoT enabled Digital Single Market for Europe and Beyond); https://european-iot-pilots.eu/project/synchronicity/

[28] "Reference Architecture for IoT Enabled Smart Cities", SynchroniCity Deliverable D2.1

[29] "Reference Architecture for IoT Enabled Smart Cities, update", SynchroniCity Deliverable D2.10

Other References

[30] IoT European Large-Scale Pilots Programme Team. Large-Scale Pilots Projects. Online at: https://european-iot-pilots.eu/resources/iot-lsps-brochures/

[31] "IoT Platforms Interoperability Approaches", White Paper, IoT-EPI Platform Interoperability Task Force.

[32] "Advancing IoT Platforms Interoperability", River Publishers, Gistrup, 2018, 978-87-7022-005-7 (ebook), IoT European Platforms Initiative (IoT-EPI) White Paper, online at: https://iot-epi.eu/wp-content/uploads/2018/07/Advancing-IoT-Platform-Interoperability-2018-IoT-EPI.pdf

[33] "Guidelines for using semantic interoperability in the industry", ETSI TR 103 535.

[34] "Market Drivers and High- Level Architecture for IoT- enabled Data Marketplaces", AIOTI WP11 contribution, https://aioti.eu/wp-content/uploads/2019/02/IoT-data-market-places-drivers-and-architechtures-white-paper-Elloumi-De_Block-Samovicz.pdf

[35] "Report on IoT platform activities", Deliverable D03.01, UNIFY-IoT.

[36] "Analysis on IoT Platforms Adoption Activities", Deliverable D03.02, UNIFY-IoT.

[37] "Interoperable IoT Platforms Standards Framework", Deliverable D05.01, UNIFY-IoT.

[38] "Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms", ETSI TR 103 536.

[39] "Semantic Interoperability Manifesto" IERC 2015, Online at http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Semantic_Interoperability_Final.pdf