OneNet Reference Architecture

D5.2

Authors:

Ferdinando Bosco (ENG)

Denisa Ziu (ENG)

Angelo Triveri (ENG)

Vincenzo Croce (ENG)

Vassilis Sakkas (ED)

Apostolos Kapetainos (ED)

Kostantinos Kotsalos (ED)

Maliheh Haghgoo (RWTH)

João Campos (ENERC)

Tiago Alves (ENERC)

Natalie Samovich (ENERC)

Carlos Damas Silva (E-REDES)

Alexandre Lucas (INESC)

Kalle Kukk (ELER)

Responsible Partner	ENG
Checked by WP leader	**Ferdinando Bosco (ENG)** - Date: 21/09/2021
Verified by the appointed Reviewers	**Mario Couto (EPRI)** – Date: 25/09/2021 **Kelsey Devine (Piclo)** – Date: 26/09/2021
Approved by Project Coordinator	**Stephan Gross (FhG)** – Date: 29/09/2021

Dissemination Level		
PU	Public	X
CO	Confidential, only for members of the consortium (including the Commission Services)	
CI	Classified, as referred to in Commission Decision 2001/844/EC	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Issue Record

Planned delivery date	30/09/2021
Actual date of delivery	29/09/2021
Status and version	V1.0 – Final Version

Version	Date	Author(s)	Notes
0.1	29/06/2021	Ferdinando Bosco (ENG) Denisa Ziu (ENG) Angelo Triveri (ENG)	First draft of the deliverable
0.2	30/08/2021	Ferdinando Bosco (ENG) Denisa Ziu (ENG) Joao Campos (ENERC) Tiago Alves (ENERC) Natalie Samovich (ENERC) Carlos Silva (E-REDES) Apostolos Kapetanios (ED) Kostantinos Kotsalos (ED) Kalle Kukk (ELER) Alexandre Lucas (INESC)	Chapter 3 and GAP analysis completed
0.3	13/09/2021	Ferdinando Bosco (ENG) Maliheh Haghgoo (RWTH) Apostolos Kapetanios (ED) Vassilis Sakkas (ED)	Chapter 4 and 5 drafted
0.4	21/09/2021	Ferdinando Bosco (ENG) Vincenzo Croce (ENG)	Chapters completed. Ready for internal review
0.5	27/09/2021	Mario Couto (EPRI) Kelsey Devine (Piclo)	Document merged with the reviews from partners
0.6	28/09/2021	Ferdinando Bosco (ENG)	Comments and feedback from reviewers addressed. Version ready for quality check.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

		Denisa Ziu (ENG) Apostolos Kapetanios (ED) Joao Campos (ENERC)	
1.0	29/09/2021	Ferdinando Bosco (ENG)	Final version of the document

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

About OneNet

OneNet will provide a seamless integration of all the actors in the electricity network across Europe to create the conditions for a synergistic operation that optimizes the overall energy system while creating an open and fair market structure.

The project OneNet (One Network for Europe) is funded through the EU's eighth Framework Programme Horizon 2020. It is titled "TSO – DSO Consumer: Large-scale demonstrations of innovative grid services through demand response, storage and small-scale (RES) generation" and responds to the call "Building a low-carbon, climate resilient future (LC)".

While the electrical grid is moving from being a fully centralized to a highly decentralized system, grid operators have to adapt to this changing environment and adjust their current business model to accommodate faster reactions and adaptive flexibility. This is an unprecedented challenge requiring an unprecedented solution. For this reason, the two major associations of grid operators in Europe, ENTSO-E and EDSO, have activated their members to put together a unique consortium.

OneNet will see the participation of a consortium of over 70 partners. Key partners in the consortium include: already mentioned ENTSO-E and EDSO, Elering, EDP Distribution, RWTH Aachen University, University of Comillas, VITO, European Dynamics, Ubitech, Engineering, and the EUI's Florence School of Regulation (Energy).

The key elements of the project are:

1. Definition of a common market design for Europe: this means standardized products and key parameters for grid services which aim at the coordination of all actors, from grid operators to customers;
2. Definition of a Common IT Architecture and Common IT Interfaces: this means not trying to create a single IT platform for all the products but enabling an open architecture of interactions among several platforms so that anybody can join any market across Europe; and
3. Large-scale demonstrators to implement and showcase the scalable solutions developed throughout the project. These demonstrators are organized in four clusters coming to include countries in every region of Europe and testing innovative use cases never validated before.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

List of Abbreviations and Acronyms

Acronym	Meaning
ACID	Atomicity, Consistency, Isolation, e Durability
AMPQ	Advanced Message Queuing Protocol
API	Application Programming Interface
ASP	Authentication Service Provider
BDVA	Big Data Value Association
BUCs	Business Use Cases
CGMES	Common Grid Model Exchange Specification
CIM	Common Information Model
CKAN	Comprehensive Knowledge Archive Network
CoAP	Constrained Application Protocol
COSMAG	Comprehensive Architecture for Smart Grid
CPS	Cyber Physical Systems
CSV	Comma-Separated Values
DEPO	Data Exchange Platform Operator
DEPs	Data Exchange Platforms
DHO	Data Hub Operator
DLMS	Device Language Message Specification
DMZ	Demilitarized Zone
DoA	Description of Actions
DSO	Distribution System Operator
EFI	Energy Flexibility Interface
EMS	Energy management system
ESOs	European Standardisation Organisations
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Electric Vehicle
FI-PPP	Future Internet Public Private Partnership
FSP	Flexibility Service Provider
FTP	File Transfer Protocol
GDPR	General data protection regulation
GUI	Graphical User Interface
HERM	Harmonised Energy Role Model
HTTP	Hypertext Transfer Protocol
HV	High Voltage

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

ICCP	Inter-Control Center Communications Protocol
ICT	Information and Communications Technology
IDAS	IDentification Authentication and Signature
IDPs	Industrial Data Platforms
IDS	International Data Spaces
IDSA	International Data Spaces Association
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
JDBC	Java Data Base Connectivity
JSON	JavaScript Object Notation
LEC	Local Energy Communities
LV	Low Voltage
M-BUS	Meter-Bus
MDA	Metered Data Administrator
MDO	Metered Data Operator
MDR	Metered Data Responsible
MO	Market Operator
MQTT	Message Queue Telemetry Transport
MV	Medium Voltage
NGSI-LD	Next Generation Service Interfaces – Linked Objects
OT	Operational Technology
P2P	Peer-to-Peer
PDPs	Personal Data Platforms
PPPs	Public Private Partnerships
PV	Photovoltaic
QoS	Quality of Service
RA	Reference Architecture
RAM	Reference Architecture Model
RDPs	Research Data Platforms
REST	Representational State Transfer
SAREF	Smart Applications REFerence
SGAM	Smart Grid Architecture Model
SO	System Operator
SUCs	System Use Cases
TSO	Transmission System Operator

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

UDPs	Urban/City Data Platforms
V2G	Vehicle-to-Grid
VPPs	Virtual Power Plants
W3C	World Wide Web Consortium
WG	Working Group
XML	eXtensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

Executive Summary

One of the key elements in the OneNet Vision is the "Definition of a Common IT Architecture and Common IT Interfaces enabling an open architecture of interactions among several platforms so that anybody can join any market across Europe".

Therefore, the results described in this document and in particular the OneNet Reference Architecture becomes of fundamental importance not only for the OneNet project but for the entire European Electricity System.

The design phase of the OneNet project includes several specifications and characteristics (Functional and non-functional requirements, OneNet Architecture, Functional and Technical specifications, Interoperable Interfaces, Data Governance, Cybersecurity and Regulatory aspects) for the reference implementation of the OneNet Solution.

The description of the OneNet Reference Architecture is part of this design phase, and it is the main result of this document. It has a twofold value: it is necessary for the implementation of the OneNet Solution in WP6 and at the same time paves the road for disseminating the OneNet concept as a pan-European solution to be adopted for interconnecting any smart energy platforms and involving energy stakeholders at any level (TSOs, DSOs, Customers, etc…).

In order to design the OneNet Reference Architecture a hybrid approach was followed. It includes a Bottom-Up approach, in which the use cases, requirements and specifications from the Demo Clusters was collected and analysed and a Top-Down approach in which detailed analysis were conducted starting from the results of the most promising and relevant EU projects, the reference architecture for a seamless integration of cross-platform services and the initiatives aimed at creating a data-based European ecosystem.

The result of these analysis activities brings to the definition of the OneNet Framework as a scalable, pluggable and well documented solution for facilitating the platform cooperation and integration, creating a unique ecosystem in which any energy stakeholder is able to participate.

From a technical perspective, the OneNet Framework leverage on fully decentralised approach for creating a P2P OneNet Network of Platform and exploits the most promising and used standard architectures and initiatives (IDSA and FIWARE) for implementing the OneNet Connectors.

In addition, the OneNet Framework intends to offer a series of Data Harmonization Services, tools for Data and Services Orchestration and evaluation, monitoring and analytics features, taking into account all the necessaries aspects related to the cybersecurity and data governance.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

1 Introduction

This chapter describes the context in which the activities of WP5, and more specifically the T5.2, activities are placed and how they are coordinated and linked within the other project activities. In addition, a detailed description of the structure and objectives of this document is provided.

1.1 Scope

OneNet will develop an open and flexible architecture to transform the actual European electricity system, which is often managed in a fragmented country- or area-level way, into a pan-European smarter and more efficient one, while maximizing the consumer capabilities to participate in an open market structure. According to OneNet Description of Action (DoA), WP5 contributes to the direction of fulfilling the OneNet envision by striving to attain two objectives; First, to design an open conceptual architecture for effective yet seamless operation of a smarter pan-European electricity system where market and network technical operations are coordinated closer to real-time across countries, and second to provide requirements, functional and technical specifications, together with interoperable and standardizable interfaces for an open scalable decentralized interconnection of platforms, technology agnostic adaptable and flexible IT reference architecture which fully support the OneNet concept and provides the necessary backbone for the WP6 subsequent implementation of the OneNet data sovereignty-preserving working space.

The WP5, together with WP6, act as IT pillar of the overall OneNet project. The IT pillar it is closely linked to all the other pillars of the project, as shown in Figure 1. It takes into consideration all the results provided in the Market Pillar (WP2 and WP3) as well as the Operation Pillar (WP4). In addition, the OneNet Solution, implemented in WP6 will be tested and evaluated in 4 Demonstration Clusters and the results of the evaluation will be used for adapting, improving, and enhancing the OneNet Solution.

The design of the OneNet Architecture is not strictly connected to the output of the other WPs but leverage on the output and results provided by them, collaborating with task T5.1 and analysing its results in D5.1, as described in the next section.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

WPs Interactions

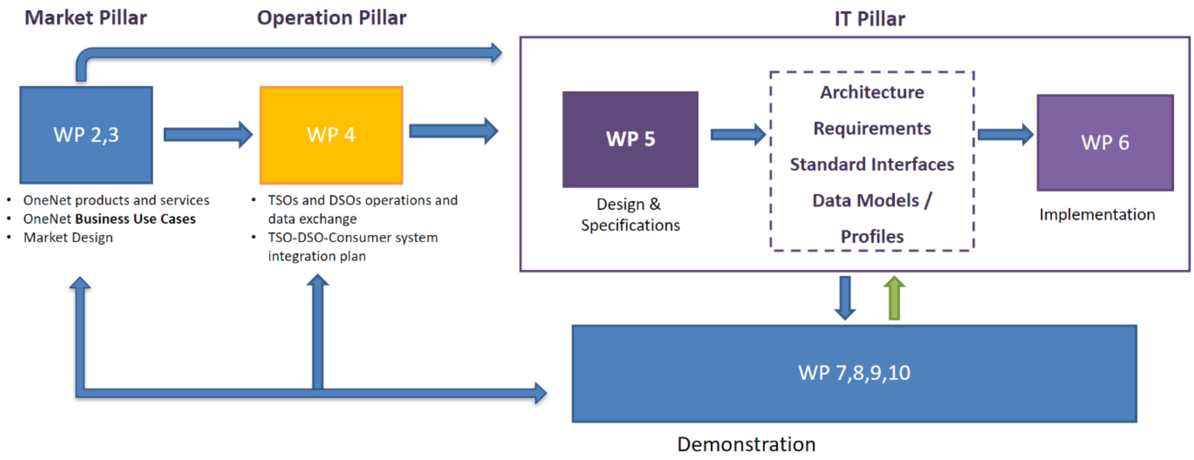

Figure 1: WP5 interdependencies

1.2 Task 5.2

Within the context just described in Section 1.1, the main goal of the Task T5.2 is defining the OneNet Platform and Data agnostic Architecture. This architecture will support the decentralized integration of existing legacy platforms and will be able to connect many stakeholders by enabling cross-platform services for market and grid operations.

The architecture will have to consider the specifications of existing projects, architectures and initiatives, to facilitate its adoption and dissemination.

Task 5.2 can be considered, together with T5.1, the starting task of the whole WP5. This task, started at M1 of the OneNet projects, collects all the necessary information for the definition of the OneNet Reference Architecture, which will be the basis not only for the implementation of the OneNet solution, as a reference implementation for the Demonstration Clusters, but also with a view to being used as a future reference for the implementation of a unique pan-European solution for the provisioning of coordinated multi-countries and multi-stakeholders' market and grid operations.

As shown in figure 2, the T5.2 is directly connected with the task T5.1 from which take as input all the Use Cases, functional and non-functional requirements, and other useful information for the definition of the OneNet Architecture.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

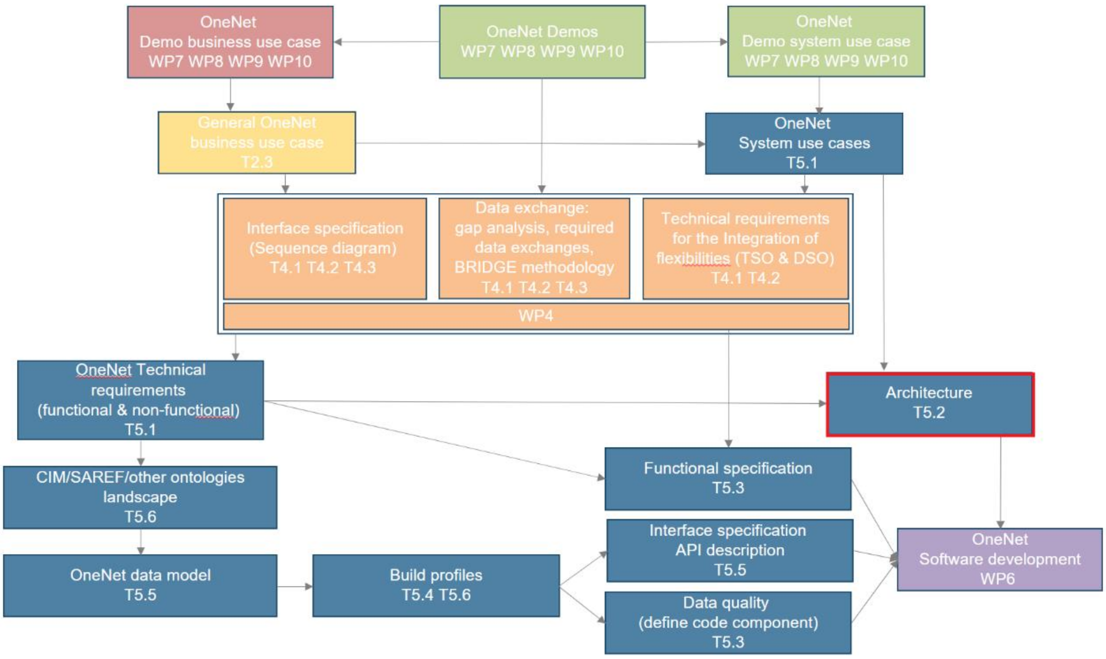

Figure 2: Coordination among WP5 tasks

In addition, T5.2 methodology approach, that is described in Ch.2, has foreseen a continuous interaction with the demos, as well as a detailed state-of-the-art analysis of projects and initiatives relevant to OneNet.

Finally, the T5.2 foresees two important results:

- the release of the **first version of the OneNet Reference Architecture** in the Deliverable D5.2 in September 2021, M12 of the project
- the release of the **final version of the OneNet Reference Architecture**, in the Milestone MS9 in September 2022, M24 of the project

1.3 Outline of the deliverable

This deliverable is structured in 6 different chapters.

Chapter 1 is the introductory one where the deliverable is contextualized within the WP5 and task T5.2.

Chapter 2 describes the methodology adopted for collecting the information necessary for the design of the OneNet architecture.

Chapter 3 describes the analysis activity in which all the information from other projects, data-driven initiative, reference architecture as well as demo architecture was collected. It concludes with an overall gap analysis.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Chapter 4 collects the information from task D5.1 and in particular the general OneNet concept (that take into accounts the OneNet Use Cases) and the OneNet functional and non-functional requirements to be taken into account for the implementation of the OneNet solution.

Chapter 5 is the main result of the document. It describes the OneNet Reference Architecture with a deeper detail on the architectural layers, components and technological solutions adopted downstream of the analysis phases.

Finally, chapter 6 concludes the document.

In order to facilitate the readability of D5.2, it might be useful to refer to D5.1 as well.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

2 Methodology

2.1 Methodology approach

The methodology applied for the definition of the first version of the OneNet Reference Architecture has been divided into four separate steps and bases the foundations on three pillars (see Figure 3): the evolution of the OneNet concept and the main objectives of the project (blue pillar); setting up an analysis of both the results already existing from the most relevant EU projects, architectures and initiatives in the field of Smart Energy and the TSO-DSO coordination platform for market and grid operations (green pillar); architectures, use cases and requirements coming from the OneNet demo clusters (yellow pillar).

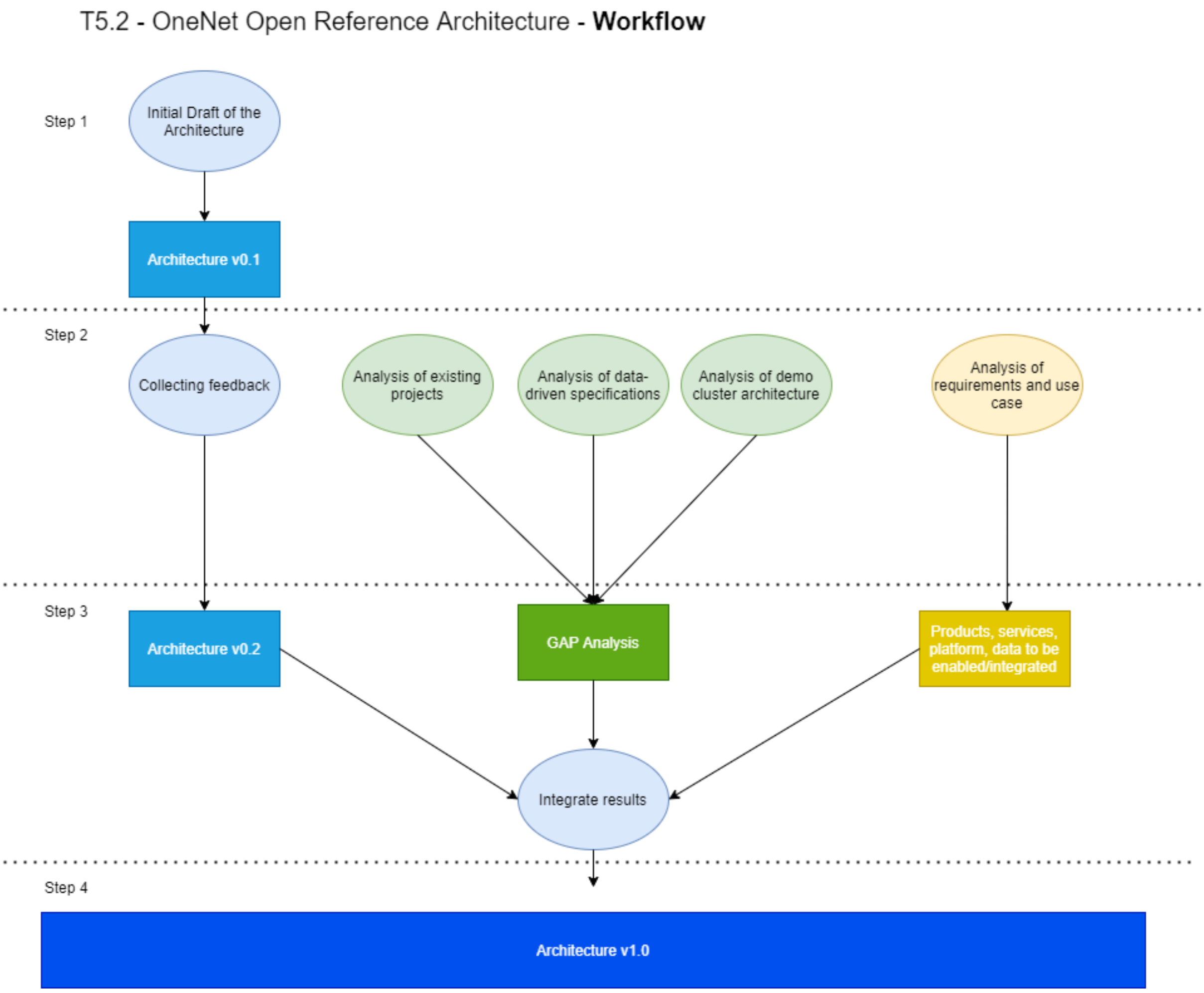

Figure 3: T5.2 The 4-steps methodology

Step 1 – Initial draft of the OneNet architecture

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The first step consists of the definition of a preliminary version of the OneNet Reference Architecture (v0.1). This early version of the architecture takes into consideration only the main objectives of the OneNet project and those that are the main features and characteristics of the architecture described in the OneNet DoA.

This preliminary version was used and discussed not only during specific meetings between the partners of the T5.2 task, but mainly during 2 specific Technical Workshops, organized under the supervision of the OneNet Technical Coordinator, in which the technical and demo partners have presented their vision on the OneNet concept, as well as on the architecture and expectations the demos have towards the OneNet solution for integrating their platforms.

Step 2 – Bottom-Up and Top-Down analysis

The second step of the methodology is probably the main one of the entire task activity, since it includes the analysis of all the information useful for the design of the OneNet Reference Architecture.

This analysis approach can be defined as a hybrid between Bottom-Up approach, in which the architecture of a software solution is designed starting from the use cases, requirements and specifications collected by the end user (in our case the demos cluster of OneNet) and a Top-Down approach in which the objectives already set and the results already consolidated are the main reference.

In this case, the first version of the architecture was used as a starting point for internal discussions and the collection of the first feedback, both from the technical partners and from the demos, as described before.

In parallel, detailed analysis were conducted starting from the results of the most promising and relevant EU projects, the reference architecture for a seamless integration of cross-platform services and the initiatives aimed at creating a data-based European ecosystem.

The architectures of the projects were mapped using the Bridge Reference Architecture Model which allowed us to collect comparable information also from the architectures provided within the demos.

Finally, the results of deliverable D5.1 were analysed, containing information from the Demos on Use Cases and the related requirements and specifications that the OneNet architecture should implement.

Step 3 – Integration of the results

All the information collected in step 2 was processed in a GAP analysis activity that allowed to identify similarities and divergences between projects, demos, architectures and initiatives, in order to find the main characteristics of the OneNet Reference Architecture.

At the same time, the first version of the OneNet architecture has been evolved (v0.2) integrating the first round of feedback and information provided by the partners.

Step 4 – Design of the OneNet Reference Architecture v1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The final step includes the design of the first consolidated version of the OneNet Reference Architecture (v1), taking into consideration all the information, requirements, specifications and concepts expressed during the various phases of analysis and design.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3 Architectures and Initiatives alignment

3.1 Relevant reference architectures

3.1.1 BRIDGE Reference Architecture

3.1.1.1 Introduction

BRIDGE [1] is an EU initiative launched by the European Commission in 2016 to foster collaboration and consolidate results between the research & innovation projects around smart grids, energy storage, islands and digitalisation of the energy system funded under the Horizon 2020 program. The BRIDGE initiative is structured with four permanent Working Groups (Data Management, Business Model, Regulation and Customer Engagement), responsible for preparing reports and formulating recommendations for the European Commission on various themes linked to the future of the energy sector.

On April 2021, the Data Management WG, whose purpose is to focus on the technical and non-technical aspects related to the exchange between stakeholders, including the handling of such data by each party, has published a report for the definition of an EU data exchange reference architecture [2].

Several BRIDGE projects have contributed to the results of the report. The reference architecture, mapped to the Smart Grid Architecture Model (SGAM), defines the building blocks required for cross-sector exchanges. Its goal is to be used by existing and future projects to enable cross-domain and cross-border interoperability.

3.1.1.2 Motivation for common European Architecture

The continuous growth of distributed renewable generation and energy storage systems, together with the expected increase in active customers engaged in demand response and electric mobility, poses several challenges in the current planning and operational practices of system operators. A key issue to be addressed on the road to energy transition is how to incorporate the demand flexibility services derived from these new assets and players into the energy market, using them for operational and ancillary services that can address any technical issues ensuring resilience, efficiency, and reliability for modern electricity grids. This last evolution is expected to bring flexibility products - also from residential consumers - to the forefront of system operation, allowing market uptake.

Both traditional retail processes and emerging flexibility services require data and information to be accessible to stakeholders and exchanged between a multitude of actors, networks, systems, devices, applications, and components. Existing and new systems need to cooperate and exchange data and information to enable existing,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

emerging, and future energy services. The definition of a common European reference architecture can serve as a key driver towards the essential commitment to demand flexibility, enabling utility coordination across national borders and reducing barriers to market entry.

A main element for the definition of a reference architecture is the correct designation of interoperable data exchange solutions. Bilateral point-to-point solutions between individual actors (decentralised approach), data hubs/warehouses (centralised approach) and data exchange platforms (distributed approach) all co-exist. All these solutions need to become interoperable with each other through comparability, appropriate standardisation, and governance. In addition to decentralised solutions, platform-type solutions (hubs, DEPs) have recently emerged across Europe to ensure efficient processes and better data quality and volume with minimal delay, initially in retail markets. Lately, the effort has been directed by the Clean Energy Package and other initiatives concerning the active incorporation of end-users in both retail and wholesale energy markets, increasing the requirement for data exchange between all stakeholders. The integrated data exchange architecture will play a vital role in the global energy system and point towards an integrated wholesale and retail market.

3.1.1.3 Reference Architecture Model

Figure 4 shows the reference architecture for European energy data exchange. 'European' refers to the cross-border data exchange capability. All the elements of the reference architecture are based on Smart Grid Architecture Model (SGAM) layers which are further split into sub-layers according to what is relevant to data exchange. SGAM originated from European M/490 smart grid mandate. It was then used at IEC level and a document was published in 2021 (IEC 63200) explaining SGAM and the usage of domains, zones and the five interoperability layers. It explains how SGAM can be used and more importantly how architecture is defined with focus on Function Layer described through the System Actors. It has been extended to Gas and Heat. SGAM has also been used to document Power System Management Reference Architecture (IEC 62357-1). The Business Layer is related to Business Use Cases, as Function Layer is associated to System Use Cases. The Information Layer hosts Canonical Data Models, data models and profiles, and semantics of exchanged data between systems, applications, equipment. Communication Layer refers to communication protocols (how the information is exchanged) and data formats (syntactics). The Component Layer represents the physical distribution of all participating components in the smart grid context.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

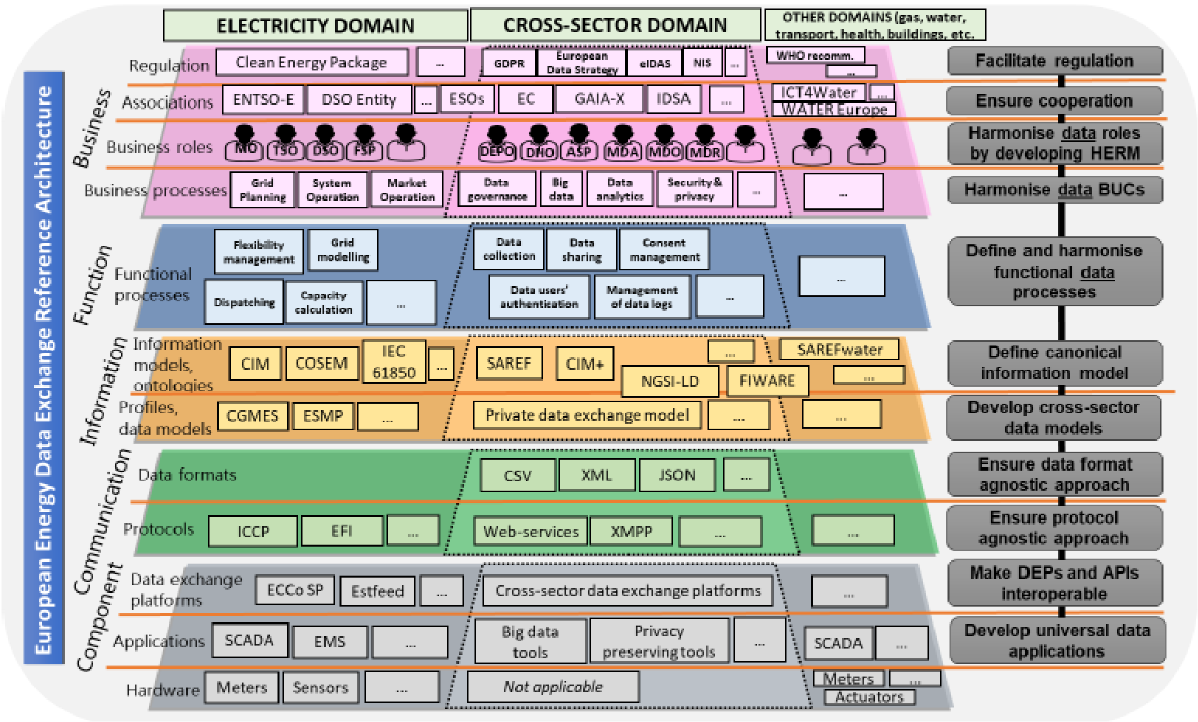

Figure 4 BRIDGE Reference Architecture Model

Highlighted on the left side of Figure 4 are the attributes related to electricity domain, while on the middle side are the elements related to the cross-sector domain. It is the cross-sector domain where biggest efforts in terms of interoperability are needed. It is the data exchange that can facilitate cross-sector interoperability. Data aspect is quite natural in information and communication layers. But it also can be and should be so in business, function, and component layers. Thus, the joint and well-coordinated actions should be dedicated to the elements in cross-sector domain. The figure concentrates on the elements which have been mentioned by BRIDGE projects or otherwise were retrieved as relevant for cross-sector domain. Obviously, the list of elements mentioned is not comprehensive.

Regulation sub-layer

While CEP (e.g., electricity market directive) is quite specific to electricity domain then for cross-sector interoperability GDPR, European Data Strategy (incl. Data Governance Act), regulation on electronic identification, authentication, and trust services (eIDAS), directive on security of network and information systems (NIS) and others need to be properly implemented, avoiding silo applications.

Associations sub-layer

ENTSO-E and soon to be established EU DSO Entity are for electricity. Cross-sector approach can be facilitated by European Commission but also by several initiatives (GAIA-X) and associations (IDSA). ESOs (European

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Standardisation Organisations) are in-between as some of them are more focused on electricity (CENELEC) and others are more generic (CEN, ETSI).

Business roles sub-layer

Some usual business roles in electricity are TSO, DSO, MO, FSP. But many data related roles can be highlighted which are relevant for several sectors: Data Exchange Platform Operator (DEPO), Data Hub Operator (DHO), Authentication Service Provider (ASP), Metered Data Administrator (MDA), Metered Data Operator (MDO), Metered Data Responsible (MDR).

Business processes sub-layer

Commonly generic processes in electricity are grid planning, system operation and market operation. For cross-sector domain data management related processes should have the priority, e.g., processes related to data governance, big data, data analytics, security & privacy.

Function layer

Examples of electricity sector functions are flexibility management, grid modelling, dispatching, capacity allocation. For cross-sector interoperability data related functions should be addressed: data collection, data sharing, consent management, data users' authentication, management of data logs.

Information models and ontologies sub-layer

Most common information models in electricity are CIM, COSEM and IEC 61850. For sector agnostic approach SAREF and NGSI-LD could be applied. Also, CIM+ is there which could be the future enhancement of current CIM to support modelling of data management related process both inside and beyond electricity and which are not covered yet.

Profiles and data models sub-layer

Commonly used groups of electricity sector profiles are CGMES and ESMP. An example of cross-sector data model could private data exchange model since this is a challenge for many sectors.

Data format sub-layer

Data formats should generally not be sector specific. Commonly used formats are JSON, CSV, XML.

Protocols sub-layer

Protocols like ICCP, Energy Flexibility Interface (EFI) are for electricity sector only. Protocols like web-services and XMPP (Extensible Messaging and Presence Protocol) are of general nature.

Data exchange platforms sub-layer

Examples of DEPs which are focused on electricity sector today are message-based communication solutions like ECCo SP and Estfeed. For cross-sector interoperability these and other DEPs should be open to exchange data of any sector. Furthermore, these platforms need to be able to communicate with each other.

Applications sub-layer

SCADA and EMS are examples from electricity sector. Data management related systems like big data tools or privacy preserving tools should be addressed in cross-sector domain.

3.1.2 COSMAG

3.1.2.1 Introduction

Comprehensive Architecture for Smart Grid (COSMAG) refers to the analysis and collection of specifications, which can define the possible process of data exchange between various possible actors. The definition of COSMAG is based on some fundamental requirements:

- The set of interactions are defined to support the implementation of the vision of the European Commission as from the Clean Energy for all Europeans Package [3].
- The architecture is built to offer "open gates", i.e., data interaction points that can be used for future expansions and novel use cases.
- COSMAG does not introduce any new standards but rather exploits and collects results of previous projects or standardization activities.
- Interactions that create a single vendor or closed market situation should be avoided.

3.1.2.2 Data Flow analysis

Modern grid applications involve the interaction of a variety of actors. Figure 5 shows all the interactions envisioned in the modern electricity market and it is used as a starting point to identify all the possible data flows.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

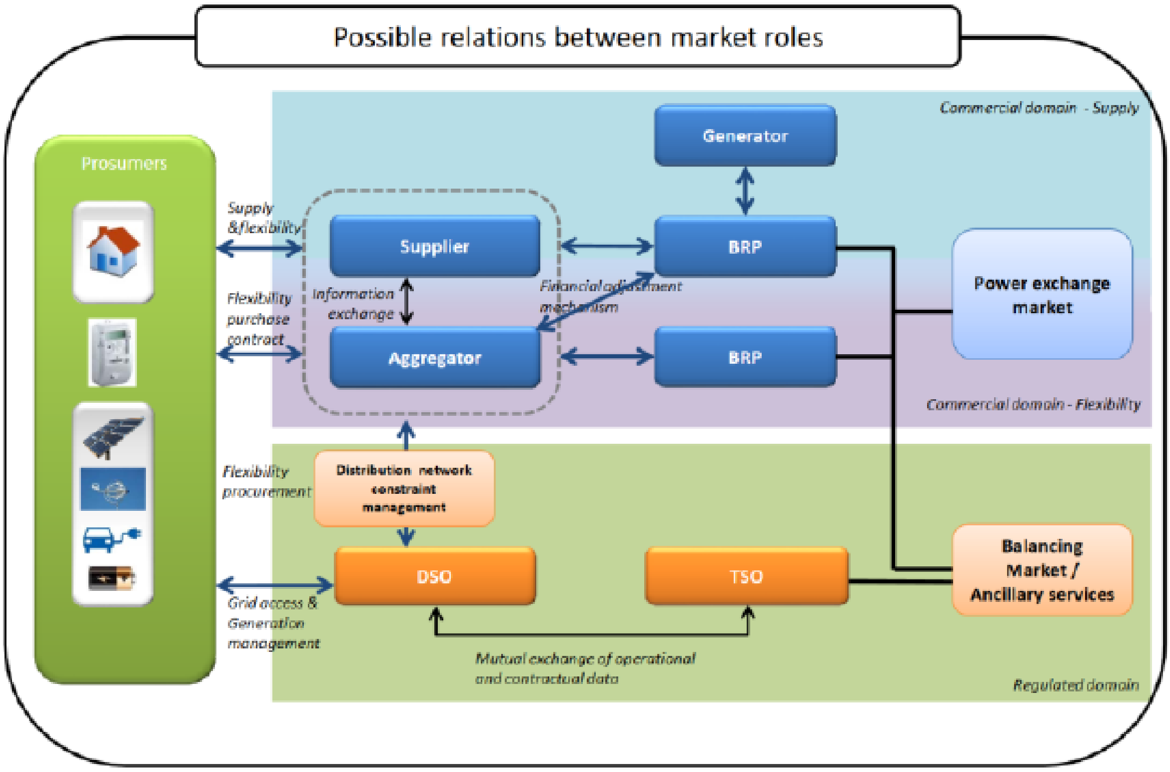

Figure 5 The structure of the market and actor interactions

Using this diagram as a reference, we can analyse each flow between actors to understand the current state of protocol definition and data models.

3.1.2.2.1 TSO

The internal data flow for TSO has been structured for a long time now and no need for incremental considerations is envisioned.

<u>TSO-Market</u>

This interface is already standardized even though it is evolving, for example through the network code on balancing [4].

<u>TSO-DSO</u>

This interface is currently under development. A significant amount of work is in progress in several ongoing H2020 projects, such as SMARTNET [5] or CoordiNet [6].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.1.2.2.2 DSO

The internal data flow for DSO can be considered well-structured. IEC61850 is considered an important standard as an automation protocol and as a data model for substations. Other key elements of data standardization are given by IEC61970-301 and IEC61968-11 that define the main element of the so-called Common Information Model (CIM). CIM is a complete data model for power system used to also exchange data among grid operators (both at TSO and DSO level). The adoption of all these standards should be encouraged within the DSO domain to support TSO-DSO interaction.

DSO-Local Market

This interface is not present as there are no local markets. Some reference solutions are proposed for this interface in the SMARTNET project [7].

DSO-Prosumer

This relation is still under development even though many experiments in this area have been already performed. The main reason for data exchange at this level is related to the generation control. Available solutions are given again by IEC61850-7 and in the case of wind turbines IEC61400-25. Communication between DSO and prosumers (or consumers) arises also due to programmed or unexpected service interruptions. Maintenance work operation, allocation of interruption or outages are events that should trigger data exchange between both actors, including schedules and estimation time to service recovery.

3.1.2.2.3 Aggregator

The role of the Aggregator is quite new. Some real cases are available, and they are mostly acting as link to the wholesale market.

Aggregator-Local Market

Currently there are no standards for such interactions given that local markets are not present yet. A set of tools for local market implementation has been proposed in the FP7 Project FINESCE [8]. A complete set of open-source APIs, compatible with the FIWARE platform, have been proposed and are publicly available [9]. An interesting extension to the already proposed solution could be given by adopting the SAREF data modelling to exchange the information.

Aggregator-DSO

This exchange is important to allow the integration of network constraints in the planning of an aggregator. In the FINESCE project, ESB Ireland implemented a complete solution based on FIWARE technology but using proprietary protocols for the network management part. This kind of data exchange is also covered in the USEF architecture [10].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

In Nobel Grid project [11] the interaction between aggregators and DSO was demonstrated in terms of demand response requests to solve congestions in the network through a negotiation process based on USEF and OpenADR 2.0 protocol [12].

Aggregator-Prosumer

In this area the emerging standard is given by OpenADR. IEC has approved OpenADR as Publically Available Standard (PAS) (IEC/PAS 62746-10-1) [13]. As part of this process OpenADR data model has been also mapped to CIM. This process is part of the wider IEC work PC118 (Smart Grid User Interface). Recent work from TNO has shown the possibility of integrating the OpenADR approach with SAREF. TNO has also released the so-called EFI (Energy Flexibility Interface) to model flexibility in support of all the market needs. Furthermore, a study published by the European Commission shown a great level of alignment of the SAREF approach with many existing standards [14].

3.1.2.2.4 Prosumer

Prosumer-Retail

The main exchange is related to metering data. Different standards have been proposed for metering data and tariffs. The Open Metering System specification has developed proposal of standardization in this area. Three protocols emerged as standard: M-BUS, DLMS/COSEM and SML.

Open-Source Domain Specific Enablers and API have been also proposed as open-source solution in the project FINESCE assuming a FIWARE based platform. This option would enable the possibility to integrate smart metering data in the larger context of Smart City.

Prosumer-Prosumer

Recently various project proposed solutions based on peer-to-peer markets models which require a direct link among the customers and the possibility to define direct contract among the parties. Most of the solutions proposed, assumed, in some way, the use of Blockchain technology for contract management. An example of development is proposed by eDream project [15] where self-enforcing smart contracts are exploited for the implementation of price-driven peer-to-peer energy marketplace allowing the local trading and consumption of energy produced at the micro-grid level [16].

3.1.2.3 Recommendations

COSMAG does not provide a reference architecture model. It provides a set of guidelines and recommendations to build scalable, interoperable, and replicable energy management systems. The following are a set of conclusions drawn by [17]:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- Many standards are available and data exchanges are already formalized. Nevertheless, emerging changes in the electricity market structure may bring some significant element of novelty (e.g., local markets)
- Most of the open points are around the customer/prosumers level. In the future, it is expected that a large amount of data will be related to the customer level. In this respect data platform able to aggregate data are an important part of the picture. Those data will play a key role in every element of the energy system.
- An important element to keep into account is the emerging role of sector coupling, making it critical to avoid data silos, not just between electricity, heat, gas etcetera within the energy sector, but also coupling of services with other sectors such as health, security, etcetera. In this respect new standards as emerged from the recent work of ETSI, e.g., the Context Broker, are an important piece of the puzzle.
- It is important that data platforms will be based on open standards to support open competition. In this respect solutions such as FIWARE can be considered as the right approach.
- Data models are also a critical aspect. In this respect, SAREF extended to cover the whole energy value chain is a very valuable candidate.

3.1.3 FIWARE Smart Energy Reference Architecture

3.1.3.1 Introduction

FIWARE is an Open-Source initiative defining a set of standards for context data management that facilitate the development of smart solutions for different domains such as Smart Cities, Smart Industry, Smart Agrifood, and Smart Energy. Founded through a partnership between Atos, Engineering, Orange, and Telefónica, the FIWARE Foundation encourages the adoption of a transparent, common, collaborative data sharing framework capable to reach its full potential in developing smart applications.

FIWARE was born in Europe from the Future Internet Public Private Partnership (FI-PPP), with the purpose of:

- accelerating the development and adoption of Future Internet technologies in Europe,
- advancing the European market for smart infrastructures, and
- increasing the effectiveness of business processes through the Internet.

3.1.3.2 FIWARE Components

FIWARE is a curated framework of Open-Source platform components that can be integrated with third party components to build smart solutions faster, easier, and cheaper. The main and only mandatory component of this open-source platform is the **Context Broker Generic Enabler**. It enables to manage all the whole lifecycle of context information including updates, queries, registrations, and subscriptions. FIWARE NGSI is the API exported by a FIWARE Context Broker, used for the integration of platform components within a FIWARE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

solution and by applications to update or consume context information. FIWARE NGSI API specifications have evolved over time, initially matching NGSI-v2 specifications, now aligning with the ETSI NGSI-LD standard [18].

Building around the Context Broker there are different other components (Figure 6) with the aim of:

- Interfacing with IoT, robots and third-party systems, to capture contextual information updates and translate required actuations.
- Context Data/API management, publication, and monetization, bringing support to usage control and the opportunity to publish and monetize part of managed context data.
- Processing, analysis, and visualization of context information implementing the expected smart behaviour of applications and/or assisting end users in making smart decisions.

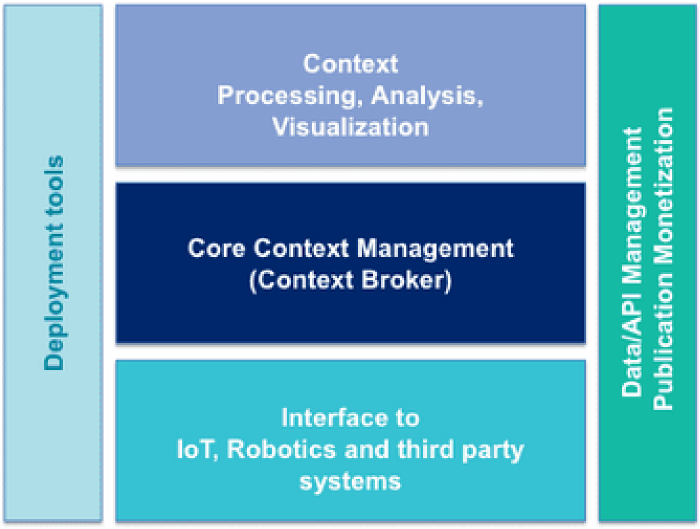

Figure 6 FIWARE components

FIWARE components can be deployed using standard containerization techniques. Most components are directly available as Docker Images, links can be found within the GitHub repository [19] of each generic enabler. Most of all, you are not forced to use these complementary FIWARE Generic Enablers but are free to combine them with other third-platform components to design the hybrid platform of your choice.

3.1.3.3 Technology Value Proposition

FIWARE is the result of a joined effort from different organisations to find common mechanisms supporting cities, industry, and communities to become interoperable and has gained relevance due to its vendor-neutral approach, defining standards that make it possible for all types of businesses and industries to build and share

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

portable and interoperable smart solutions around the globe. Its driven-by-implementation approach as opposed to a design-by-committee approach ensure an agile adoption.

Technology value proposition considers the specific needs of a wider range of ICT developers adopting FIWARE, as shown in Figure 7.

Customer Wants / Gains	FIWARE Benefits	Customer Needs	FIWARE Services/Features	Customer Pains	FIWARE Pain Reliever/Experience
1 **Quality**, Cost Effective – Freedom – Open Source is something ! want to contribute to and sign my name to it. 2. Simple yet Powerful (flexible)** 3.- easy to integrate and combine with other technologies 4.- Little Effort: Avoid debugging and writing from scratch 5.- I want to contribute 6.- Support / Community 7.- Sucess / CV	1 FIWARE is free open source technology - no cost to evaluate (there is community, the code is public , you can sign your name to it and add quality. 2. Defined with a simple interface with clear expectations, recommended by relevant initiatives and industrial bodies, used in multiple smart solutions. Well designed 3.- Standards Driven 4.- Track record in Smart Solutions, reliable, battle-tested. You can use FIWARE to quickly co-opt a large code base into your product at no cost. The modular nature means you can re-architect as your needs change.	1 Available to buy and market ready 2 Focus 3. If I have a well defined interface I can use a dummy object to produce test data (Mock) 4.- I want to pick an API that does one thing well – I need Context Management 5.- I need to build different things. I need freedom to take the existing components or write my own. 6.- I work with Context Data	1.- Not vaporware. Is not going to go away 2 No code rot, low maintenance, 3. Modular system of Generic Enablers - you can pick an choose the parts which apply to you switch and expand architect as necessary. Each element does one job well. 4.- it is easier to learn and keeps the purpose of the library simple. FIWARE do not include things you don't need. FIWARE does context management well 5. FIWARE offers lego bricks. FIWARE is defining the size and orientation of the studs and therefore all the different types of brick join together - it is up to YOU as the developer whether you want to build a House or a Toy Car. No-one forces you to take them all. You just need to stick to the standard.	1.I don't want things that I don't need. It means adding in more and more functionality which is tangential to the product. That diverges from main topic 2. Avoid Code Rot 3.- I want my job done with little effort 4.- 80% of development is maintenance and maintenance is boring. I don't want to have to keep rewriting my interfaces to your software just because your priorities has changed. 5.- I don't want to write everything from scratch. 6.- I want to avoid unnecessary Testing and Debugging	1.FIWARE is a focused solution based around context data only- no bloat to the API. 2. Code Rot is an issue that follows every project - a well defined modular framework like FIWARE should reduce it (if not eliminate it): • Other developers are still maintaining the Enablers. The simple interface does one thing well - and doesn't keep changing with iterations • The modular nature means that if you want to exchange elements you can do it bit by bit. 3.- NGSI is REST done right - FIWARE is therefore a fun tool-to-use. It is well designed and it gets my job done with little effort. It is easy to understand and based on existing well defined technology concepts 4. Well designed - No bloat, do one job well, rot slowly idea. The lack of unnecessary changes is emphasised by the adoption by standards bodies 5-6 FIWARE has already been tested in the wild. And provides a well defined modular framework

Figure 7 FIWARE adopters needs and FIWARE benefits [20]

Developers play an important role in any ICT-based company and corporate. Choosing to use one specific software rather than another, knowing the advantages or gaps of a specific system, recognising the value of services are important aspects that require the expertise of the developer. For this purpose, the value proposition of FIWARE Technology is primarily focused on to understand needs, problems, and desires of the developers in order to increase their interest in the adoption of FIWARE technology.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

STRATEGIC OBJECTIVE	**To increase developers' adoption: usage and contribution**		
VALUE PROPOSITION	FIWARE is open source technology with a great Community behind: no cost to analyze, test and use, with proper support. It drives standardization for a cornerstone problem in smart solutions: how context data can be modeled and managed. FIWARE is a fun tool-to-use: It is well designed and it gets your job done with little effort. It is easy to understand and modular, simple yet powerful, capable to integrate with best-of-the-breed technologies.		
KEY BENEFITS	**Simple yet Powerful** Gravitates around context management based on an API which is well designed, does just one concrete thing and does it well: FIWARE NGSI	**Open Source** FIWARE is open source - no cost to evaluate, test and use. You are able to contribute. The FIWARE Foundation warrants it will stay free, for all, for ever	**De-facto standard - Driving standardization** Recommended by relevant initiatives and industrial bodies. Driving standardization in context management. Growing number of smart solutions using it.
	High-quality software Avoid debugging and testing because QA processes is in place. FIWARE is reliable, battle-tested, accompanied by a comprehensive set of tutorials.	**Inclusive approach** Designed to integrate best-of-breed technologies as new GEs or to build hybrid platform solutions. The modular nature means you can re-architect as your needs change.	**Strong growing Community** Growing Community bringing support through well established channels. Community-supported sandbox environment where to test (FIWARE Lab)

Figure 8 FIWARE Technology value proposition [20]

Regarding the customer problems solved by FIWARE, here is a list of the most relevant ones:

- Avoidance of vendor lock-in.
- Easy Access to quicker, better, affordable technology solutions for the IoT.
- FIWARE Context Broker integrated with another component makes easier, faster, and free building up your smart application.
- A large open-source developers' community is maintaining and further developing the basic software components.
- Lowest cost of ownership for the end users.
- FIWARE Context Broker is since February 2018 a CEF Building Block. CEF is an initiative of the European Commission boosting the adoption of software components to build cross-border applications.

Regarding the benefits the various FIWARE components bring in, here is a list of the most relevant ones:

- Trust, in the access to validated (quality assured) versions of the FIWARE platform components.
- Sustainability and long-term liability, in the commitment to boost the FIWARE Ecosystem.
- Openness, by committing to an Open-Source model.
- Standards, by ensuring that FIWARE becomes a relevant standard in the Smart world. It enables interoperability.

3.1.3.4 FIWARE for the Smart Energy domain

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The Energy Transition is transforming the energy sector from straight supply chain to a complex ecosystem. Consumers are becoming prosumers, and supply and demand are optimized in real time and at a very granular level. The need for flexibility has grown, notably with the innovations of renewable energy sources, batteries, power electronics, electric mobility, blockchain, and rapid digitalization.

The digitalisation of the energy sector requires higher levels of operational excellence with the adoption of disruptive technologies to foster cross-sector data sharing and data-driven innovation. The following key aspects in data management must be fulfilled:

- Data model/semantics: Defining an appropriate data model appropriate data model beyond a single sector is a key ingredient for interoperability.
- Context information: Defining the context is a key ingredient for bridging the gap between different verticals.
- Data sovereignty: The ability of a data owner to define what a third party is allowed to do with its data.
- Open APIs: Closed solutions will not create a truly open and open and competitive market. Open APIs offer the perfect bridge between the private infrastructure spaces.

Modern grid applications need to accommodate the interaction of a multitude of actors. The main goal of a smart grid implementation is the creation of an automatic process. It is critical to define for every possible data exchange both the semantics of the information as well as the communication protocol. FIWARE can be a response to data flows in the smart energy sector, for example:

- Aggregators & DSO: this interface is yet to be defined, there are no dominating standards. In the FINESCE project, ESB Ireland implemented a complete solution based on FIWARE technology [8].
- Prosumers-retail & Power exchange market: a FIWARE-based platform for smart meter-based services can integrate smart metering data in the larger context of Smart Cities.
- Sector coupling: the main characteristics of a local energy community are the integration of different energy vectors to increase the level of local flexibility. Such a solution requires to go beyond the electricity sector. IEA has reported on what impact digitalization of energy brings to the transport, home, business, and industry domains [21]. The new business models should accommodate not only those incumbent energy actors (DSO, TSO, Service Providers, Energy retailers and the installation and maintenance providers), but also the new ones entering the domain (prosumers, aggregators, PV and smart meter manufacturers...). Solutions such as the FIWARE Context Broker support a seamless merging of sectors, extending the set of contexts present in the ETSI CIM standard. Such an extension could be built on top of the SAREF data modelling.
- Link to third parties: data platforms can create open interfaces that can be exploited by third-party providers, bringing innovative services to the energy domain. A complete set of APIs present in the FIWARE NGSI as well as extensions of the FIWARE Context Broker can be used to develop new energy domains.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- Link to smart city platforms: When coupling the Energy and E-Mobility sectors, FIWARE's open API and Context Broker technology can serve as a bridge to proprietary mobility solutions.

3.1.3.5 Reference Architecture Model

Figure 9 shows the FIWARE Reference Architecture for Smart Energy Management solutions.

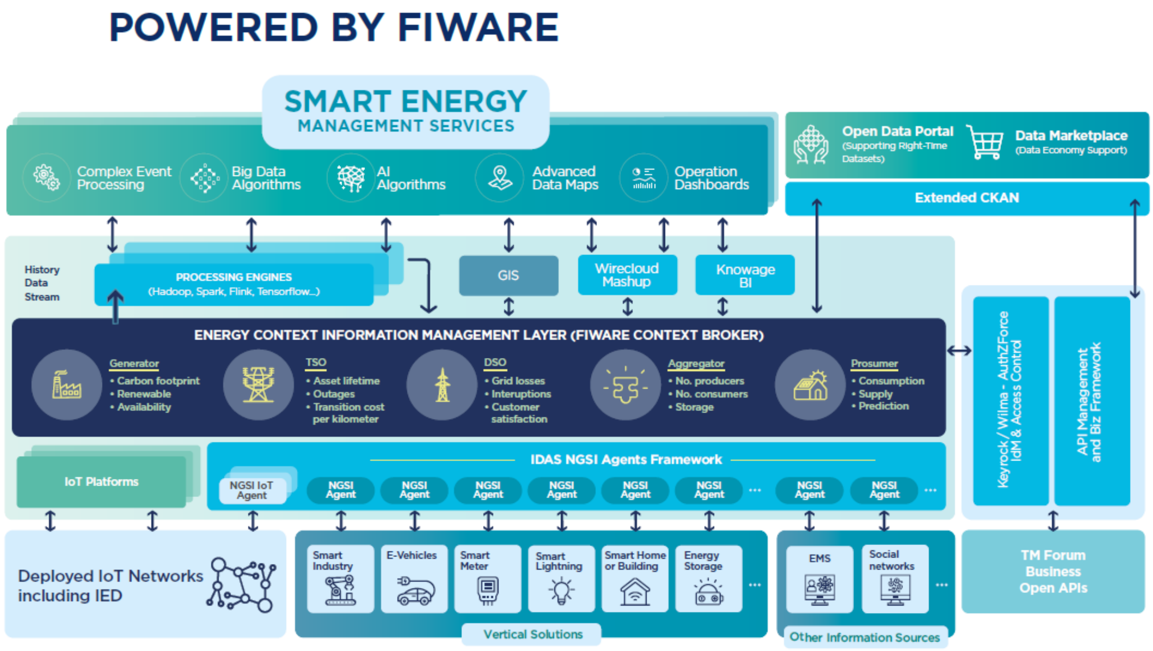

Figure 9 FIWARE Architecture Model

The architecture is designed to have several hierarchical levels. Starting from the bottom there is the layer of information sources coming from smart meters, sensors, and other devices, as well as vertical smart solutions and information systems. The FIWARE Context Broker (the core of the platform) integrates this information through the IDAS NGSI Agents Framework. IDAS IoT agents translate IoT-specific protocols (MQTT, CoAP/OMA-LWM2M, OneM2M…) into the NGSI context information protocol, which is the FIWARE standard data exchange model. Historical data can be processed using different processing engines (e.g., Hadoop, Spark or Flink) to extract valuable insights or derive smart actions. Complex Event Processing, Advanced AI or machine learning functions can be implemented on top of integrated processing engines. Part of the current and historical context data can be offered to third parties through an extended CKAN portal enabling publication of real-time data and the assignment of terms and conditions (including pricing) to data resources. Data/API access control functions ensure that context data is only accessible to those with the right privileges.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.1.4 ETIP SNET Holistic Architecture

Recent work by WG 1 of ETIP-SNET experts focused on the sector coupling and subsequent smart sector integration EU policies reflections within the environment protection policies which are fostering the deployment of the Sectors Coupling to provide greater flexibility to the energy system so that decarbonisation can be achieved cost-effectively (European Commission, 2018). This ambitious vision requires holistic architectures (ETIP SNET, 2019) that enables structured and effective coupling of different sectors by introducing the new control paradigms on a large- scale (European Commission, 2020) [22].

A long-term holistic architecture vision for future power systems is introduced in the ETIP SNET White Paper on Holistic Power System Architectures (2019), in which four different holistic architectures were described: Web of Cells, IDE4L, SmartNet and LINK-based holistic architecture [23].

A short overview of the architectures discussed in the Holistic Architecture paper are presented below.

- Web of Cells provides a decentralised control using non-overlapping geographical areas of the power system, known as cells, to maximise the utilisation of renewable sources. It is developed mainly for the electrical networks and needs to be extended to consider the Sector Coupling. IDE4L architecture enhances observability and controllability of the distribution networks and, therefore, enables more cost-efficient operation of the whole power system. Sector Coupling is not taken into account. It needs to be extended to consider the Sector Coupling.
- SmartNet focuses on the implementation of a flexibility market to provide optimised instruments and modalities to improve the coordination between the grid operators at national and local level (respectively the TSOs and DSOs). Five different coordination schemes were developed. Sector Coupling was not the focus of development, but the possibility of extending the coordination schemes will be examined. TDXAssist, EUSysflex & Interface projects also contributed to progressing in TSO-DSO key use case mapping as well as updates of the associated harmonised models.
- LINK-based holistic architecture reorganises the management of the grid, electricity production, energy storage facilities and consumers and harmonises with the market. It facilitates the description of all power system operation processes such as load, generation balance, voltage assessment, dynamic security processes, price and emergency driven demand response while enabling Sector Coupling.

Zooming in on wholistic architecture approach which is an umbrella concept of the LINK-based architecture the following concepts could be listed from the related work with relevance for the project.

"The purpose of architecture is to structure and organise the system in such a way that it is stable, usable, adapt to changes, and economical. When the architecture is sound, it helps to design better the system that is being described. The architecture of a system is a global model of it. It usually consists of a structure, properties of various elements involved, relationships between different components, and their behaviour and dynamics." It further states that "When we talk about Smart Grids, we must be clear that the giant

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

electromagnetic machine must be treated as a whole. So far, the power system's operation has been treated separately from that of the customer plants and their electrical equipment; their interaction was wasteful. But the picture changes with the increasing share of DGs. The exchange becomes very strong and cannot be ignored anymore."

"The design structure of Smart Grids consists of three complementary and consistent architecture types:
The holistic architecture of electrical appliances, including market to enable the processes required for the operation of Smart Grids;
The architecture of applications required to run the processes (soft- and hardware architecture); and
Information and communication architecture required for the smooth data exchange between applications.
The system can then be linked to another through an interface and viewed on various complementary and consistent abstraction levels." [24]

The above concepts are illustrated below:
Linked to the wholistic and enabling architectures are the main concepts discussed within the ETIP-SNET's paper on Smart Sector Integration [22]
The main concepts are listed below:

- Integrated view requires streamlined and System of Systems approach in order to avoid potential barriers
- Holistic architectures need to take the many to many interfaces and integrations into consideration
- ICT and the enabling technologies should facilitate the integration in a faster way while avoiding barriers, such as interoperability, lack of interfaces or fragmentation
- A holistic system view approach, including socio-economic parameters

The main policy recommendations communicated in the paper are listed below:

- Foster cross-sector and cross-countries level playing fields, removing unnecessary or double taxation on electricity, incentivising Power-to-X solutions (e.g. Gas, district heating, hydrogen generated from RES, and new flexibility solutions such as demand-side response including V2G). Decarbonization and carbon-free electrification are to become the pillars of the European Smart Sector Integration Strategy.
- Encourage stakeholder cooperation for platformization (TSO-DSO-aggregator cooperation on flexibility and storage) and a revamped EU Emission Trading Scheme, possibly extended to sectors such as fossil fueled heating and transportation, which would set the right signals and back Europe's sector coupling and decarbonization ambitions.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- Boost the imminent electricity and gas sector coupling for new products such as electrolytic hydrogen and renewable gases to become market-based solutions on a revised, functional, and transparent European gas market.
- Consider all vectors and enabling solutions within system of system approach in order to anticipate potential barrier, fragmentation and integrate lessons learnt.

An integrated approach requires streamlined System of Systems vision to overcome existing barriers. Holistic architectures need to take the many-to-many interfaces and integrations into consideration. ICT and other enabling technologies could facilitate integration in a faster way while avoiding barriers, such as interoperability, lack of seamless interfaces or fragmentation.

The ICT solutions should be supporting a decentralised and layered paradigm and nodal approaches while allowing connecting multiple stakeholders across energy vectors, facilitating "plug-n-play" despite legacy differences while facilitating platforms and services interoperability to achieve set integration goals.

3.2 Data-driven initiative specifications

3.2.1 BDVA

3.2.1.1 Introduction and mission

The Big Data Value Association (BDVA) [25] is an industry-driven international not–for-profit organisation with more than 200 members all over Europe and a well-balanced composition of large, small, and medium-sized industries as well as research and user organizations. BDVA is the private counterpart to the EU Commission to implement the Big Data Value PPP program [26], which aims at creating a functional Data Market and Data Economy in Europe, in order to allow Europe to play a leading role in Big Data in the global market.

The mission of the BDVA is to develop the Innovation Ecosystem that will enable the data and AI-driven digital transformation in Europe delivering maximum economic and societal benefit and achieving and sustaining Europe's leadership on Big Data Value creation and Artificial Intelligence.

To achieve this mission, in 2017 the BDVA defined four strategic priorities (Figure 10):

- **Develop Data Innovation Recommendations,** providing guidelines and recommendations on data innovation to the industry, researchers, markets, and policy makers.
- **Develop Ecosystem,** developing and strengthening the European Big Data Value Ecosystem.
- **Guiding Standards**, driving Big Data standardisation and interoperability priorities and influencing standardisation bodies and industrial alliances.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

•	**Know-How and Skills,** improving the adoption of Big Data through the exchange of knowledge, skills and best practices.

Figure 10: BDVA strategic priorities

One of the main goals of BDVA is collaborating with the European Commission, within the European research and innovation landscape of Horizon 2020, for developing and implementing a strategic roadmap for research, technological development and innovation in the Big Data Value and other ICT domains.

3.2.1.2 Enabling data exchange and unlocking AI potential

The BDVA position paper [27] describes the BDVA's vision on the necessity to develop and adopt a pan-European data sharing space. This is the primary driver, together with the opportunities presented by Artificial Intelligence (AI), for the evolution of the data economy.

BDVA provides a list of recommendations for the successful development, implementation, and adoption of a European Data Sharing Space that:

1. allows new and existing vertical, cross-sectoral, personal, and industrial data spaces to interoperate
2. offers services and experimentation opportunities to all stakeholders
3. promotes European values.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

In particular, BDVA recommends:

- To create the conditions for the development of a trusted European data sharing framework.
- To incorporate data sharing at the core of the data lifecycle for greater access to data.
- To provide supportive measures for European businesses to safely embrace new technologies practices and policies.
- To assemble a European-wide digital skills strategy to equip the workforce for the new data economy.

3.2.1.3 BDV Reference Model

The BDV Reference Model has been developed by the BDVA, considering input from technical experts and stakeholders along the whole Big Data Value chain, as well as interactions with other related PPPs. The BDV Reference Model may serve as common reference framework to locate Big Data technologies on the overall IT stack [28].

It addresses the main concerns and aspects to be considered for Big Data Value systems. The BDV Reference Model distinguishes between two different elements. On the one hand, it describes the elements that are at the core of the BDVA; on the other, it outlines the features that are developed in strong collaboration with related European activities.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

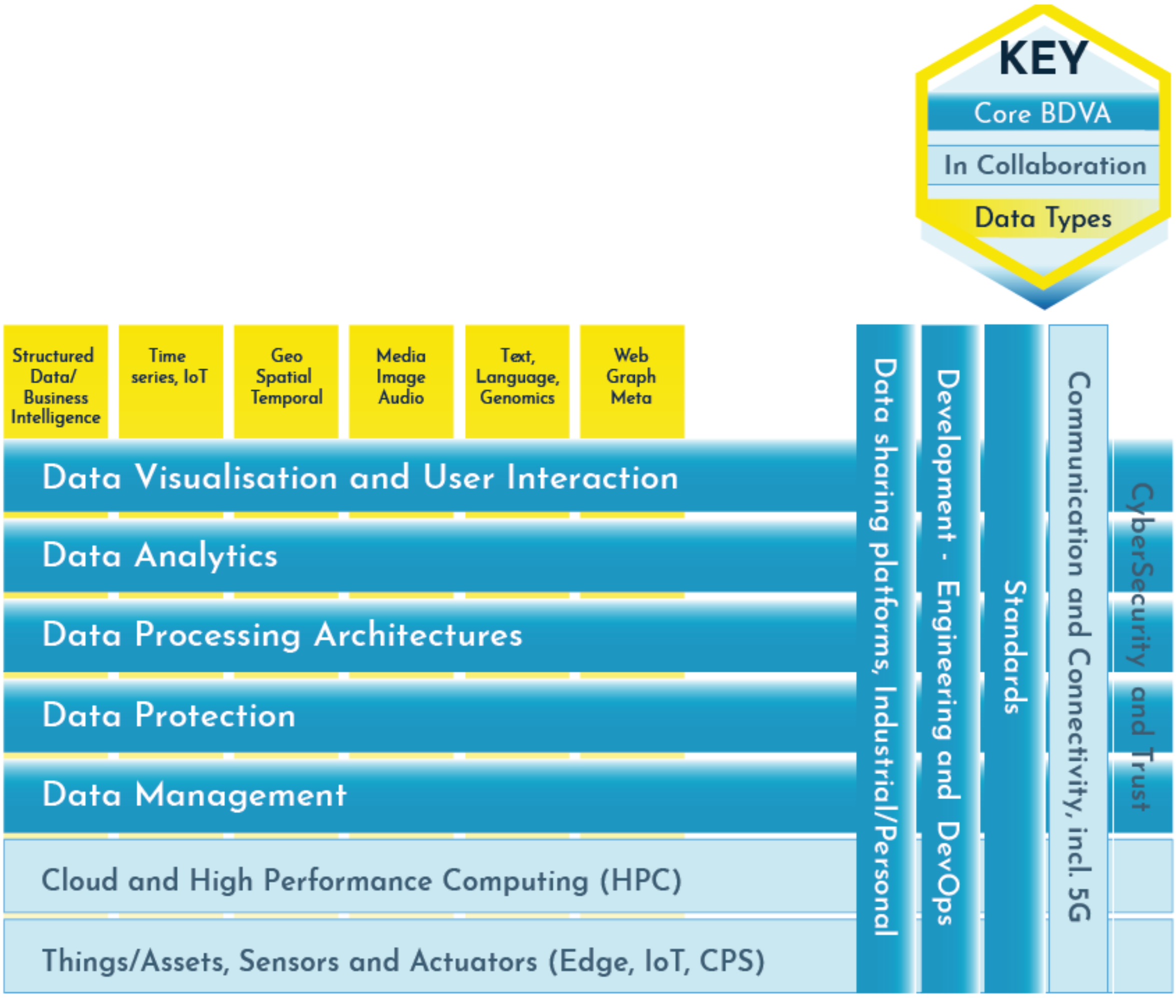

Figure 11: BDV Reference Model

The BDV Reference Model is structured into horizontal and vertical concerns.

Horizontal concerns cover specific aspects along the data processing chain, starting with data collection and ingestion, and extending to data visualisation. It should be noted that the horizontal concerns do not imply a layered architecture. As an example, data visualisation may be applied directly to collected data (the data management aspect) without the need for data processing and analytics.

Vertical concerns address cross-cutting issues, which may affect all the horizontal concerns. In addition, vertical concerns may also involve non-technical aspects.

Horizontal concerns

- Data Visualisation and User Interaction: Advanced visualisation approaches for improved user experience.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- Data Analytics: Data analytics to improve data understanding, deep learning and the meaningfulness of data.
- Data Processing Architectures: Optimised and scalable architectures for analytics of both data-at-rest and data-in-motion, with low latency delivering real-time analytics.
- Data Protection: Privacy and anonymisation mechanisms to facilitate data protection. This is shown related to data management and processing as there is a strong link here, but it can also be associated with the area of cybersecurity.
- Data Management: Principles and techniques for data management.
- The Cloud and High Performance Computing (HPC): Effective Big Data processing and data management might imply the effective usage of Cloud and High Performance Computing infrastructures.
- IoT, CPS, Edge and Fog Computing: A main source of Big Data is sensor data from an IoT context and actuator interaction in Cyber Physical Systems. In order to meet real-time needs it will often be necessary to handle Big Data aspects at the edge of the system.

Vertical concerns

- Big Data Types and Semantics: The following 6 Big Data types have been identified, based on the fact that they often lead to the use of different techniques and mechanisms in the horizontal concerns, which should be considered, for instance, for data analytics and data storage: (1) Structured data; (2) Time series data; (3) Geospatial data; (4) Media, Image, Video and Audio data; (5) Text data, including Natural Language Processing data and Genomics representations; and (6) Graph data, Network/Web data and Metadata. In addition, it is important to support both the syntactical and semantic aspects of data for all Big Data types.
- Standards: Standardisation of Big Data technology areas to facilitate data integration, sharing and interoperability.
- Communication and Connectivity: Effective communication and connectivity mechanisms are necessary in providing support for Big Data.
- Cybersecurity: Big Data often need support to maintain security and trust beyond privacy and anonymisation. The aspect of trust frequently has links to trust mechanisms such as blockchain technologies, smart contracts, and various forms of encryption.
- Engineering and DevOps for building Big Data Value systems
- Marketplaces, Industrial Data Platforms and Personal Data Platforms (IDPs/PDPs), Ecosystems for Data Sharing and Innovation Support: Data platforms for data sharing include, in particular, IDPs and PDPs, but also other data sharing platforms like Research Data Platforms (RDPs) and Urban/City Data Platforms (UDPs). These platforms facilitate the efficient usage of a number of the horizontal and vertical Big Data areas, most notably data management, data processing, data protection and cybersecurity.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

It should be noted that the BDV Reference Model has no ambition to serve as a technical reference structure. However, the BDV Reference Model is compatible with most relevant data reference architectures, e.g., the emerging ISO Big Data Reference Architecture [29].

3.2.1.4 Alignment with OneNet vision

The ambition of OneNet to realise a cross-border, cross-sectoral sharing data space and enable platforms to interconnect each other in a in interoperable way, is also very relevant in the BDVA.

In particular, BDVA identifies and analyses several technical and non-technical challenges (business, organizational, legal compliance and skills-related challenges) that need to be tackled during the implementation.

The Technical challenges are the most relevant ones that can have the greatest impact in defining the OneNet reference architecture.

TC1. Sharing by design: Data life-cycle management that is not designed around sharing.

TC2. Digital Sovereignty: Enforcing data usage rights.

TC3. Decentralisation: Decentralised data sharing and processing architectures.

TC4. Veracity: Weak verification and provenance support.

TC5. Security: Secure data access and restrictions.

TC6. Privacy Protection: Maturity of privacy-preserving technologies for big data.

3.2.2 IDSA

3.2.2.1 Introduction

The International Data Spaces Association (IDSA) [30] is a non-profit organization founded jointly by business, politics, and research with the mission of establishing both the development and the use of a Reference Architecture Model for secure data spaces and sovereign data sharing on a European and International level. More than 130 members from different kind of industries, sizes and organizations aim to establish a worldwide standard for data exchange.

3.2.2.2 Mission and Goals

International Data Spaces (IDS) can be considered as a Virtual Data Space whose mission is to leverage existing standards and technologies, as well as Governance Models, in order to facilitate and establish a secure, standardized and sovereign system of data exchange in a trusted Business Ecosystem. This way IDS forms a basis for creating Smart Service Business Processes and at the same time helps participants realize the full value of their data. IDSA realizes this vision by defining and delivering a new reference architecture for a new ecosystem, which guarantees security, sovereignty and trust. This Reference Architecture Model (RAM) connects data clouds/hubs, enterprises, business applications and IoT devices thus creating the IDS ecosystem. This is achieved through a dedicated software component named IDS Connector as shown in Figure 12, which works as an interface between the participating actors.

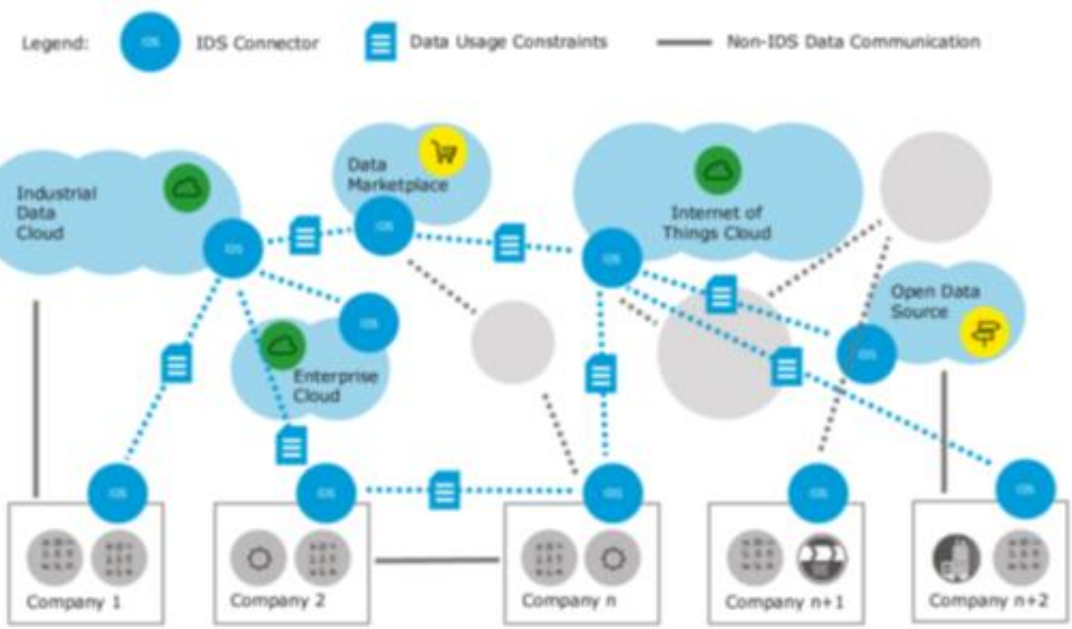

Figure 12: IDS connectors

The Goals of IDSA can be summarized as follows [31] :

- The design, continuous development, and evolution of the core principles of the Reference Architecture Model through an increasing number of research activities conducted by various partners.
- Testing the model's implementation through various industry specific uses cases.
- Materialize the standard in the IDS-RAM itself, but also in defined methods for secure data exchange and data sharing facilitated by the IDS Connector, the central technical component of the IDS.
- Ensure the international ambition of the initiative, through the establishment of Regional Hubs in different countries.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- To supporting the adoption of IDS concepts and technologies in the market.

3.2.2.3 Key features of International Data Spaces

Guided by the demand for digital sovereignty, International Data Spaces aims to create a network of trusted data. Key features of IDS are:

- Sovereignty of data assets: The data owner establishes individual usage policies for their data assets, regarding both data usage and data users (such as the specific release or blocking of data for certain users).
- Security of data exchange: A protection level concept regulates the data protection requirements, in particular during the exchange of data.
- Decentralized organization and federal architecture: International Data Spaces combines all end points that use an IDS connector for participation in the data space of International Data Spaces. Thus, there is no central authority for data management or data governance tasks. This makes International Data Spaces an alternative architecture design, compared for example to central data management concepts (including data lakes) on the one hand and decentralized data networks without shared rules on the other hand.
- Governance and shared rules: Due to the decentralized architecture of International Data Spaces and thus the lack of a central supervisory authority, data governance principles are developed as shared rules. They determine the rights and obligations for data management and are derived from the requirements of the users.
- Network of platforms and services: International Data Spaces connects data providers and data users. Data providers can be companies, but also individual entities on the Internet of things such as vehicles, machines, means of transport, and equipment.
- Scaling and network effects: International Data Spaces provides data services for the secure exchange and straightforward linking of data. By connecting the participants via the IDS connectors, the infrastructure has a decentralized character which makes International Data Spaces scalable without a central authority. Furthermore, the scaling and network effects as such develop through the growing availability of data, not only from individual participants but also entire ecosystems.
- Openness: The International Data Spaces initiative is user-driven and based on a participative development process, organizationally bundled in the International Data Spaces Association.
- Protection of trust: International Data Spaces participants must be able to rely on the identity of data providers and data users, and on the technical implementation of data sovereignty. To this end, a mandatory certification of the software ensures the protection of trust. Special IDS connectors with extended encryption are also available for the secure exchange of data.

3.2.2.4 Strategic Requirements

The International Data Spaces is a peer-to-peer network of participants who are obliged to adhere to the specified rules. For this effort to be a success, the following Strategic Requirements have to be met:

- **Trust:** Trust is the basis of the ecosystem. Each participant is evaluated and certified by a trusted authority before participating in the process.
- **Security and Data Sovereignty:** All technical components used are evaluated and certified. Also, a data owner attaches usage restriction information to their data before it is transferred to a data consumer. To use the data, the data consumer must fully accept the data owner's usage policy.
- **Ecosystem of Data**: By pursuing the idea of storage decentralization, there is no need for central data storage capabilities. Data physically remain with the respective data owner until it is transferred to a trusted third party.
- **Comprehensive Data Source description.**
- **Integration of domain-specific data vocabularies.**
- **Real-time data search services.**
- **Standardized Interoperability:** The main technological component of the RAM is the IDS connector, which is not unique implementation wise. Every connector though, is able to communicate with each other or any other technological component.
- **Value Adding Apps:** The integration of IDS connectors with business applications provides a series of services on top of data exchange processes (data processing, data format alignment, data exchange protocols, data analytics).
- **Data Markets:** The International Data Space can provide clearing mechanisms, billing functions, domain-specific broker solutions and marketplaces, usage restriction information and legal information.

All research and development activities are driven by the following guidelines:

- **Open Development Process:** IDSA is a non-profit organization open to every participant who adheres to the common principles of work.
- **Re-Use of existing Technologies:** One of IDSA guidelines is to re-use existing technologies and standards as much as possible.
- **Contribution to Standardization:** Aiming at establishing an international standard itself, the International Data Spaces initiative supports the idea of standardized architecture stacks.

3.2.2.5 Reference Architecture Model

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The IDSA defines a framework and governance principles for the Reference Architecture Model (RAM) [32], as well as interfaces aiming at establishing an international standard. The main RAM purpose is to provide a higher abstraction level than common architecture models of concrete software solutions do, by focusing on the generalization of concepts, functionality, and overall processes involved in the creation of a secure "network of trusted data". In accordance with common system architecture models and standards (e.g., ISO 42010, 4+1 view model), the Reference Architecture Model uses a five-layer structure that express stakeholder concerns and viewpoints at different levels of granularity as illustrated in Figure 13:

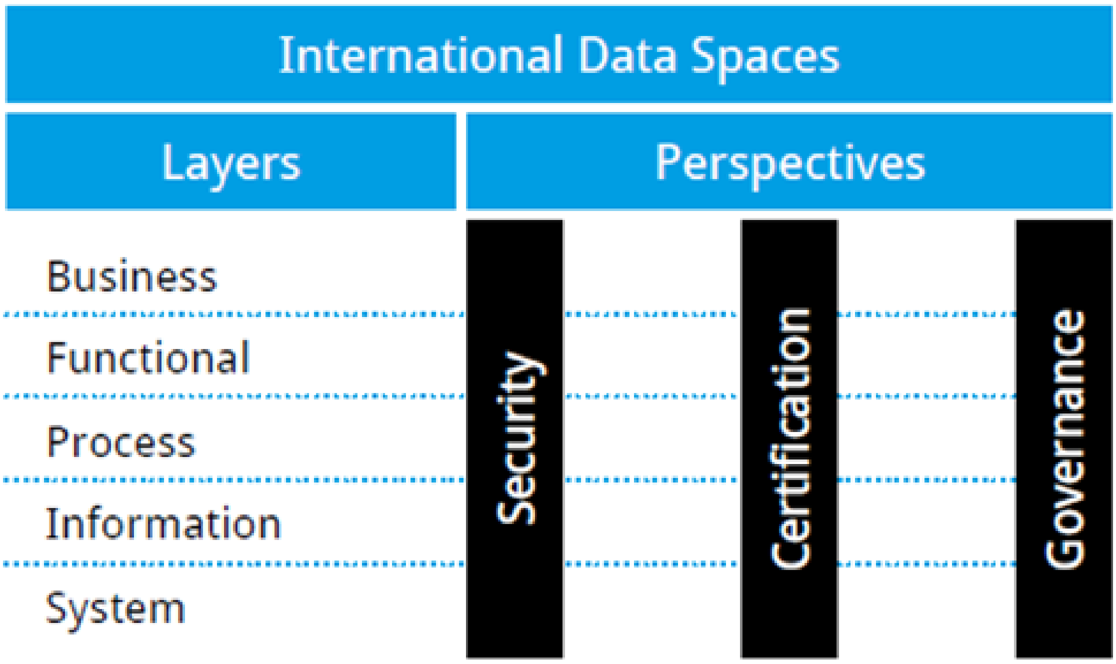

Figure 13: IDSA Reference Architecture Model

The ***Business Layer*** specifies and categorizes roles, main activities, and interactions for the IDS participants. The ***Functional Layer*** defines the functional requirements of the International Data Spaces, plus the features to be derived from them. So, in other words this layer defines the software components functionality. The ***Process Layer*** is responsible for the specification of interactions taking place between the different components by using the BPMN notation, so that to provide a dynamic view of the Reference Architecture Model. The ***Information Layer*** defines a conceptual model by using linked-data principles for describing both the static and the dynamic aspects of the International Data Space's constituents like data endpoints, data apps or datasets. The ***System Layer*** defines the logical software components, considering aspects such as integration, configuration,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

deployment, and extensibility. In addition to the layer view, the Reference Architecture Model comprises of three perspectives that need to be implemented across all five layers: ***Security, Certification, and Governance.***

Business Layer

As previously stated, the Business Layer specifies and categorizes roles, main activities and interactions for the IDS participants. This abstract description can be considered a high-level technical blueprint.

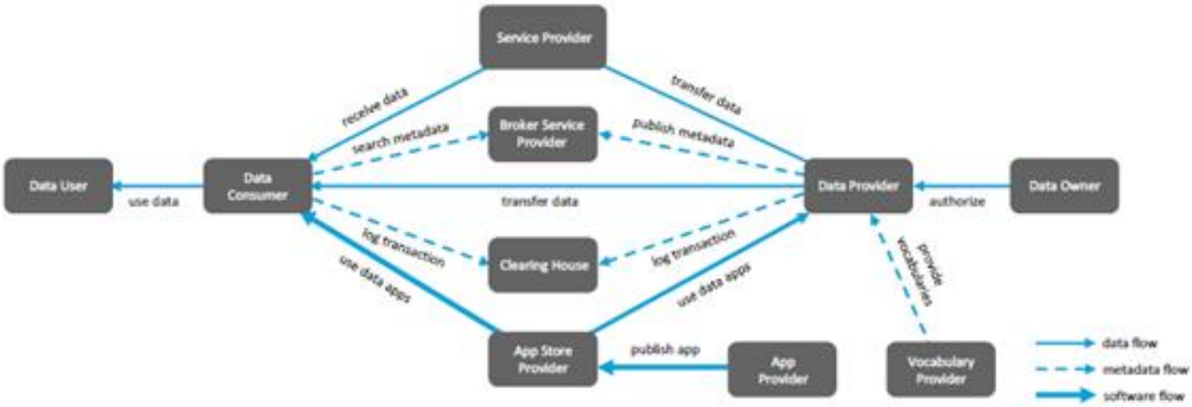

Figure 14: IDS Technical Blueprint

As per the Business Layer Roles:

The **Data Owner** holds the legal rights of its data meaning that has complete control over it but is not necessarily is the one who makes the data available, enter the **Data Provider.** Usually, a participant acting as Data Owner automatically assumes the role of the Data Provider as well.

The **Data Consumer** receives data from a Data Provider. As a mirror entity of the Data Provider, the Data Consumer performs similar activities. However, the Data Consumer does not necessarily need to be the one who uses the data. It is the **Data User**, who has the legal right to use the data as specified by the access policy.

Service Provider makes data available to other IDS participants or process raw data before transferring towards a Data Consumer and Data User. Companies that cannot be participants in the IDS ecosystem, transfer their data to a Service Provider.

Broker Service Provider provides and manages information about potential data sources available in the IDS, by focusing on the metadata regarding the actual data. If a Data Provider is not known, Data Consumer can search for data through the use of a Broker Service Provider.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The **Clearing House** is an intermediary that logs all activities performed in the course of data exchange in the IDS and it therefore provides clearing and settlement services for all financial and data exchange transactions. Based on the logging information reports we have billing and conflict resolution services.

The **App Store** provides data apps. The functionality of an app varies but generally an app facilitates data processing workflows. Also, the App Store provide interfaces for publishing and retrieving Data Apps plus corresponding metadata. The apps themselves are built by an **App Provider**, who publishes its apps via the App Store, as long as the apps are compliant with IDS System Architecture.

The **Vocabulary Provider** is responsible for managing and offering vocabularies (i.e. ontologies, reference data models and metadata elements) that are used to annotate and describe datasets. Vocabulary Provider provides also the Information Model of IDS.

Other roles in the IDS are the **Identity Provider** which validates the identity of each IDS participant, the **Software Provider** that provides software components not for the App Store and the **Certification Body and Evaluation Facility**, which are in charge of the certification of the participants and the technical core components.

Functional Layer

The Functional Layer defines – irrespective of existing technologies and applications – the functional requirements of the International Data Spaces, and the features to be implemented resulting thereof. Figure 15 shows the functional architecture of the IDS, which is divided into six functional groups that have to be provided.

Figure 15: IDS Architecture Functional Layer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The 1st group **Trust** comprises of three main categories (roles, identity management, and user certification), which are complemented by governance aspects:

- **Roles:** Each Role has certain rights and duties depending on the service they have to deliver and the level of trust it is required.
- **Identity Management**: Every connector has to have a unique identifier and a valid certificate. Each connector must be able to verify the identity of other connectors.
- **User Certification:** Each participant in the International Data Spaces must undergo certification in order to establish trust among all participants.

The 2nd group **Security and Data Sovereignty** can be split into the following categories:

- **Authentication and Authorization**: Each connector has to have a valid X.509 certificate, so that IDS participants can identify each other's identity.
- **Usage Policies and Usage Enforcement:** Each Data Owner & Data Provider can define usage control policies for their data, attached to the outbound data. Therefore, IDS participants can be sure, that their data are treated according to their usage policies.
- **Trustworthy Communication and Security by Design:** Connectors, the App Store, and Brokers can check if the Connector of the connecting party is running a trusted and therefore certified software stack. Any communication between Connectors can be encrypted and integrity protected.
- **Technical Certification:** The core components of the IDS and especially the Connector require certification from the certification body in order to establish trust among all participants.

The 3rd functional group is the **Ecosystem of Data** which is split in three categories:

- **Data Source Description:** Participants of the IDS must be able to describe, publish, maintain and manage different versions of metadata that describe the syntax and serialization as well as the semantics and the application domain of the data source. Further aspects that can be described are the price model and the usage policy.
- **Brokering:** The operator of a Connector must be able to provide an interface for data and metadata access. Each Connector must be able to transmit metadata of its data sources to one or more brokers. Every participant must be able to browse and search metadata in the metadata repository, as long as the participant has the right to access the metadata. Furthermore, each participant of the IDS must be able to browse the list of participants registered at a Broker.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- **Vocabularies:** Vocabularies are used in order to create and structure metadata. It is possible to either use standard Vocabularies, create your own vocabularies or to work together with other participants on the creation of new vocabularies.

The 4th functional group is the **Standardized Interoperability** which is split into two categories:

- **Operation:** Participants should run an IDS Connector in their own IT environment. Alternatively, they can make use of a mobile or embedded device. The operator of a Connector must be able to define the data workflow inside the Connector. Users of the Connector must be identifiable and manageable. Passwords and key storage must be protected. Every action, data access, data transmission, incident, etc. should be logged so that it is possible to draw up statistical evaluations on data usage etc.
- **Data Exchange:** The Connector must receive data from a backend system, either by a push-pull mechanism. The data can be provided via an interface or pushed directly to other participants. To do so, each Connector must be uniquely identifiable. Other Connectors can subscribe to data sources or pull data from these sources. Data can be written into the backend system of other participants.

The 5th functional entity **Value Adding Apps** is split into four categories:

- **Data Processing and Transformation:** A data processing app must provide a clearly defined processing service applied on the input data and produce an expected output. A data transformation app must be able to transform a specific input format to a different output format, in compliance with the requirements of the Data Consumer/User without changing substantially the information contained in the data.
- **Data App Implementation:** Developers of a data app must annotate the app with appropriate metadata (functionality and interfaces, pricing model and licensing etc.)
- **Providing Data Apps:** An authorized developer of Data Apps can initiate a software provision process meaning publish a Data App on an App Store. The Apps to be published can be undertaken a certification process that is performed by the Certification Body. The App Store supports participants in searching for Data Apps that fit the need of the participant.
- **Installing and Supporting Data Apps:** A dedicated Connector service should support authorized users in (un-)installing Data Apps not originating from an official App Store. In addition, it should support authorized users in searching, installing, and managing (e.g., removal or automated updates) Data Apps retrieved from an App Store.

The 6th and last functional group **Data Markets** is split into three categories:

- **Clearing and Billing:** The Data Owner is able to define the pricing model (e. g. pay per transfer, pay for access per day or month) and the price of the data. Any transaction is logged in the Clearing House.
- **Usage Restrictions, and Governance:** Governance in the International Data Spaces comprises five aspects: data as an economic good, data ownership, data sovereignty, data quality, and data provenance.
- **Legal Aspects:** Trading data on a data marketplace requires legal contracts and conditions that can be negotiated in an automated way. Therefore, standard contracts for typical data exchange transactions are necessary.

Process Layer

The Process Layer of the IDS RAM specifies the interaction that takes place between the different components of the IDS, providing a dynamic view. It is split into three main processes/subprocesses, which are:

Onboarding, which is the process required to be granted access to IDS as Data Provider or Data User.
Exchanging data, i.e., searching for a suitable Data Provider and invoking the actual data operation.
Publishing and Using Data Apps

These three processes are related to the International Data Space's key value propositions and involve most of the roles introduced in the Business Layer.

Information Layer

The Information Layer specifies the Information Model, as a generic model with no commitment to any particular domain which facilitates compatibility and interoperability. The primary purpose of this formal model is to enable semi-automated exchange of digital resources within a trusted ecosystem, while preserving data sovereignty of Data Owners. The Information Model therefore supports the description, publication and identification of data products and reusable data processing software (both referred to hereinafter as "Digital Resources", or simply "Resources"). Once the relevant Resources are identified, they can be exchanged and consumed via semantically annotated, easily discoverable services. Apart from those core commodities, the Information Model describes essential constituents of the International Data Spaces, its participants, its infrastructure components, and its processes.

Information Layer can be formalized in different levels of representation (Figure 16):

The **Conceptual Representation** is a high-level overview of the main concepts by means of textual document and visual notations. It targets a general audience, management boards, and media, as it provides basic information and promotes a shared understanding of the concepts

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The **Declarative Representation** adds a semantic level to the description of concepts. Based on a stack of W3C Semantic web technology standards and standard modelling vocabularies it therefore provides a formal, machine-interpretable specification of the IDS concepts.

The **Programmatic Representation** is meant for software providers as target group and therefore aims to seamlessly integrate the Information Model with familiar development infrastructures. It provides best-effort mapping of the IDS Ontology onto native structures of a target programming language.

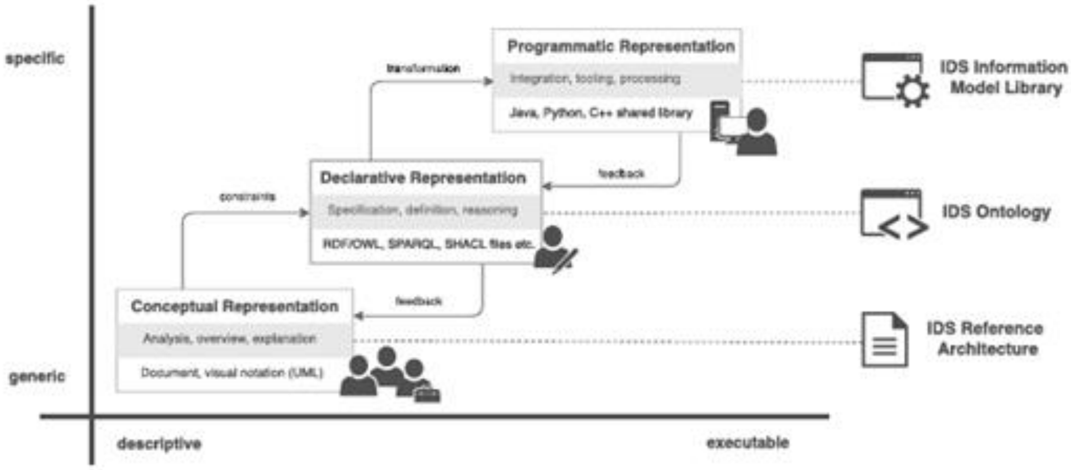

Figure 16: IDS Architecture Information Layer

System Layer

The System Layer maps the roles that are defined in the Business Layer with a concrete data and service architecture in order to meet the requirements of the Functional Layer. There are three major technical components, which are required to realize an IDS ecosystem: The Connector, the Broker and the App Store. The interaction of these three components is depicted in Figure 17. Besides that, the System Layer also describes the architecture of the core components, e. g. for the connector.

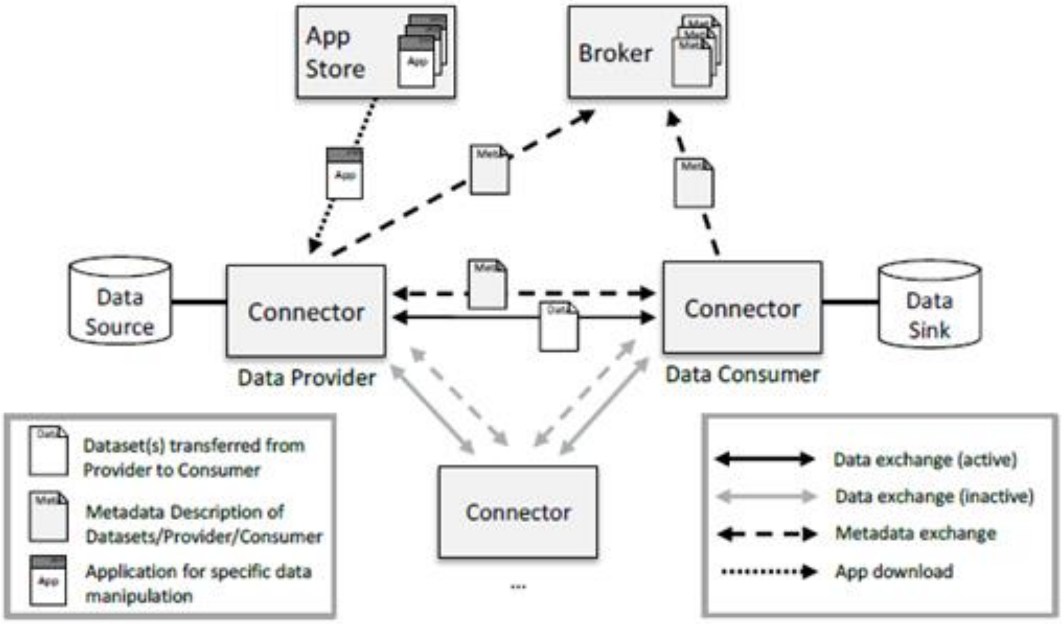

Figure 17: IDS Connector, Broker and App interactions

The Connector, the Broker, and the App Store are supported by four additional components (which are not specific to the International Data Spaces, but specified for the International Data Spaces): the **Identity Provider** as defined in the Security Perspective, the **Vocabulary Hub** currently as defined outside the IDS, the **Update Repository** (i.e. the source for updates of deployed Connectors) depending on the connectors technology, and the **Trust Repository** (i.e. the source for trustworthy software stacks and fingerprints as well as remote attestation checks) as discussed in the Security Perspective.

3.2.2.6 IDSA Connector

International Data Spaces as a distributed network relies on the connection of different member nodes where Connectors or other core components are hosted. The Connector is responsible for the exchange of data or acts as a proxy in the exchange of data, executing the complete data exchange process from and to the internal data resources and enterprise systems of the participating organizations. The Connector provides metadata to the Broker, which include description of the technical interface, authentication mechanism, exposed data sources, and associated data usage policies. Data is transferred between the Connectors of the Data Provider and the Data Consumer (peer-to-peer network concept).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

There are different types of Connector implementations, based on different technologies and depending on what specific functionality is required regarding the purpose of the Connector. Two fundamental variants are the Base Connector and the Trusted Connector as they differ in the capabilities regarding security and data sovereignty. Connectors can be further distinguished into External Connectors and Internal Connectors:

An **External Connector** executes the exchange of data between participants of the International Data Spaces. The International Data Spaces network is constituted by the total of its External Connectors. Each External Connector provides data via the Data Endpoints it exposes. Applying this principle, there is no need for a central instance for data storage. An External Connector is typically operated behind a firewall in a specially secured network segment of a participant (so-called “Demilitarized Zone”, DMZ). From a DMZ, direct access to internal systems is not possible. It should be possible to reach an External Connector using the standard Internet Protocol (IP), and to operate it in any appropriate environment. A participant may operate multiple External Connectors (e.g., to meet load balancing or data partitioning requirements). External Connectors can be operated on-premises or in a cloud environment.

An **Internal Connector** is typically operated in an internal company network (i.e., a network which is not accessible from outside). Implementations of Internal Connectors and External Connectors may be identical, as only the purpose and configuration differ. The main task of an Internal Connector is to facilitate access to internal data sources in order to provide data to External Connectors.

Connector Architecture

The Connector Reference Architecture (Figure 18) uses application container management technology to ensure an isolated and secure environment for individual data services which offer an API to store, access or process data. Any data pre-processing (e.g., filtering, anonymization, or analysis) should be performed by Internal Connectors. Only data intended for being made available to other participants should be made visible through External Connectors.

Data Apps are bundled as container mages for simple installation by application container management. Using an integrated index service, the Broker manages the data sources available in the International Data Spaces and supports publication and maintenance of associated metadata. Furthermore, the Broker Index Service supports the search for data resources. Both the App Store and the Broker are based on the Connector architecture in order to support secure and trusted data exchange with these services.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

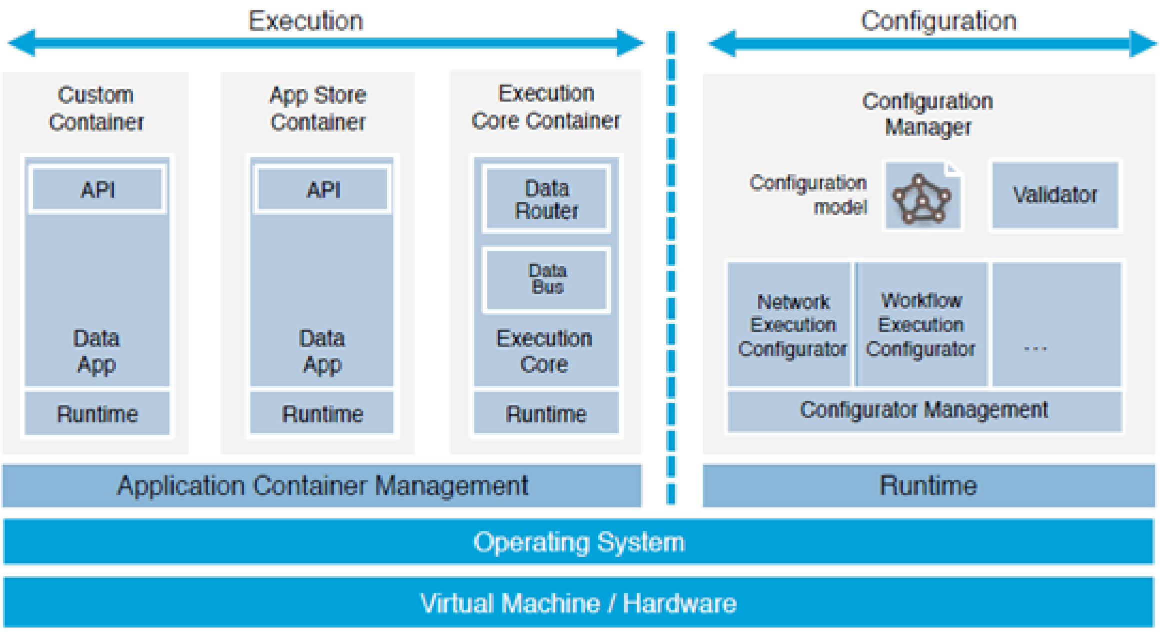

Figure 18: IDS Connector Reference Architecture

3.2.2.7 GAIA-X: A federated infrastructure for Europe [33]

Driven by the conviction that we can push forward the development of a sustainable and innovative data economy in Europe, the GAIA-X project was launched in autumn 2019 [34].

GAIA-X is a project initiated by Europe for Europe and beyond. Its aim is to develop common requirements for a European data infrastructure. Therefore openness, transparency and the ability to connect to other European countries are central to GAIA-X. Representatives from several European countries and further international partners are currently involved in the project. We want to invite other European and international partners to join the project and to contribute to its development. Many dialogues are already underway and will be further intensified. Furthermore, GAIA-X is in continuous exchange with the European Commission.

With GAIA-X, representatives from business, science and politics on a European level create a proposal for the next generation of a European data infrastructure: a secure, federated system that meets the highest standards of digital sovereignty while promoting innovation. This project is the cradle of an open, transparent digital ecosystem, where data and services can be made available, collated and shared in an environment of trust.

Gaia-X Architecture overview [34]

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The Gaia-X project was started with the aim to enable a secure, open and sovereign use of data. It´s motivated by challenges to the European digital economy, such as:

- Decentralized processing locations
- Lack of transparency and sovereignty over stored and processed data and infrastructure.
- Sector specific data spaces and lack of ontology

According to the vision and objectives of the architecture, the core architecture principles include openness and transparency, interoperability, federation as well as authenticity and trust. The following technical guidelines enforce these principles and assure compliance with the GAIA-X vision:

- Security-by-design
- Privacy-by-design
- Enabling federation, distribution and decentralization
- User-friendliness and simplicity
- Machine-processability
- Semantic representation

It is important to mention that the Gaia-X reference architecture is formed by an infrastructure ecosystem, where infrastructure services are provided, connected or consumed, and a data ecosystem, that deals with data as the main business asset. Both ecosystems are connected via the federation services and cannot be viewed separately. They include Identity and Trust Services, Compliance Services, Federated Catalogues and Sovereign Data Exchange Services.

This architecture serves as an underlying framework common to all domains.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

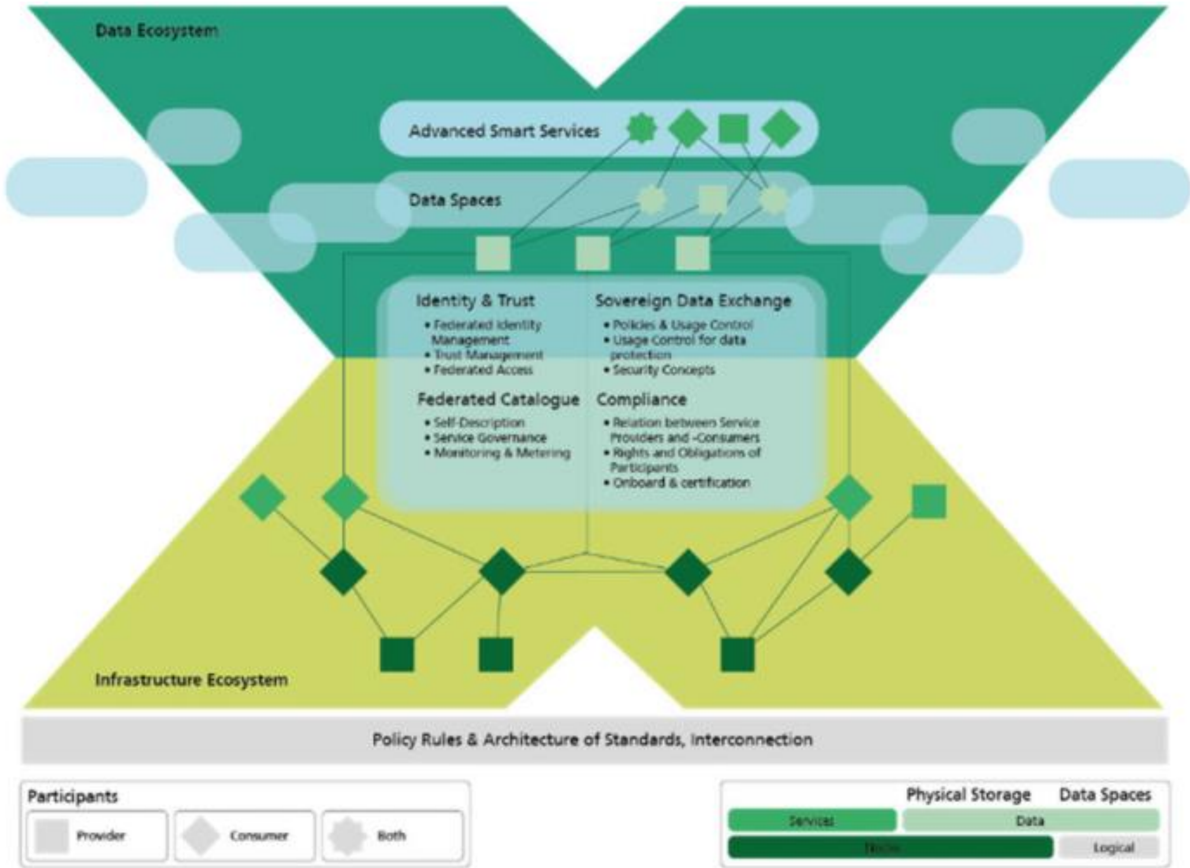

Figure 19: GAIA-X Architecture (own adaption based on BMWI 2020, GAIA-X Technical Architecture)

To ensure high-level data protection, security, transparency and portability within the Gaia-X ecosystem, a framework of Policy Rules is being developed.

Integration & Differences between GAIA-X and IDS [34]

The combined architecture of GAIA-X and IDS supports and enables data spaces and builds advanced smart services in industry verticals. GAIA-X focuses on sovereign cloud services and cloud infrastructure, while IDS focuses on data and data sovereignty. The interaction of GAIAX and IDS has three main tasks: self-sovereign data storage, trustworthy data usage and interoperable data exchange. This way, GAIA-X is developed in accordance with the European Data Strategy and supports smart data applications and innovations across industry sectors. For this purpose, GAIA-X and IDS complement each other to ensure cloud and data sovereignty for end-to-end data value chains in federated ecosystems.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The below image presents a mapping of IDS components into the GAIA-X architecture. The Data Provider and Data Consumer are mapped into the GAIA-X Data Ecosystem, while the App Store Provider, App Provider and Service Provider are rather located in the GAIA-X Infrastructure Ecosystem. The IDS Connectors can be integrated in the GAIA-X Nodes, as they work as secure gateways. It is important to note, that Connectors do not restrict to the GAIA-X Data Ecosystem but reach down the whole stack including the GAIA-X Infrastructure Ecosystem for security reasons.

The four Federation services are also congruent to various IDS concepts: A key element is the GAIA-X Federated Catalogue, which leverages the IDS Broker, Vocabulary Provider and Information Model. The Federation Service of Sovereign Data Exchange is represented by the IDS Clearing House and Usage Control concept. Further, the GAIA-X Federation services of Identity & Trust and Certification can take advantage of the IDS Identity Provider and IDS Certification Body. Figure 20 shows the mapping of the IDS components into the Gaia-X Architecture.

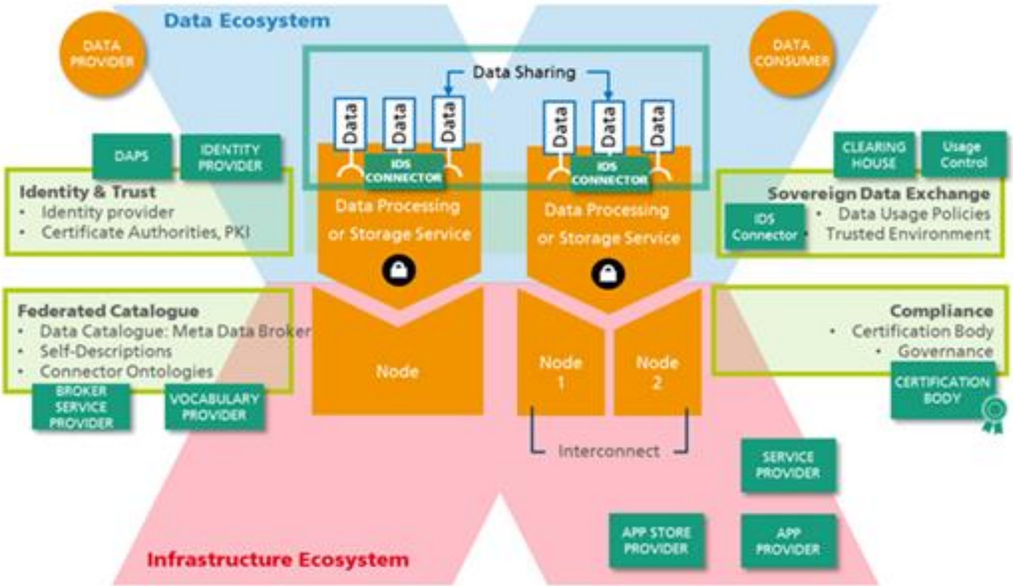

Figure 20: Mapping of IDS Components into the GAIA-X Architecture (source: GAIA-X initiative)

3.3 Interoperability achievements of other major projects (ENG)

One of the goals of the OneNet Architecture is to facilitate a seamless cross-stakeholders interoperability, by incorporating latest interoperability achievements from major projects.

The Bridge Initiative on Data Management and Reference Architecture (described in Ch.3.1.1) provides us a very useful tool for identifying the interoperability achievements of existing architectures based on the SGAM reference architecture.

This high-level SGAM based reference architecture for European energy data exchange (Figure 4), defines the building blocks required for implementing an interoperable cross-border and cross-stakeholder data exchanges and here was used for mapping all the architectures designed or implemented in the identified projects.

Below the list of the mapped projects:

- CoordiNet
- Platone
- INTERRFACE
- InterCONNECT
- EUniversal
- eDREAM
- EU-SysFlex

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.3.1 CoordiNet

The purpose of the project is to establish different collaboration schemes between transmission system operators (TSOs), distribution system operators (DSOs) and consumers to contribute to the development of a smart, secure, and more resilient energy system. Special emphasis will be on the analysis and definition of flexibility in the grid at every voltage level ranging from the TSO and DSO domain to consumer participation.

Three different architectures are provided, one for each demonstrator: Greece, Spain and Sweden.

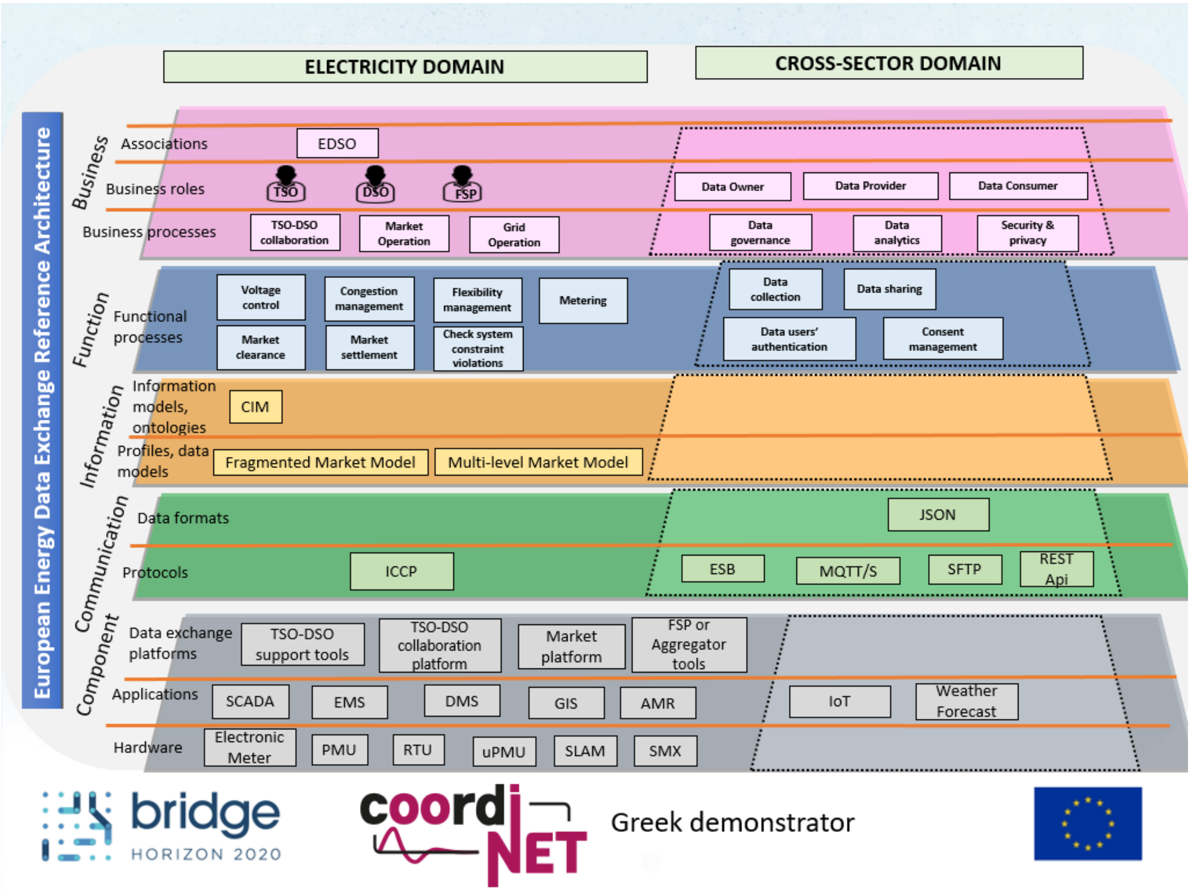

Figure 21: Coordinet Bridge RA Mapping - Greek demo

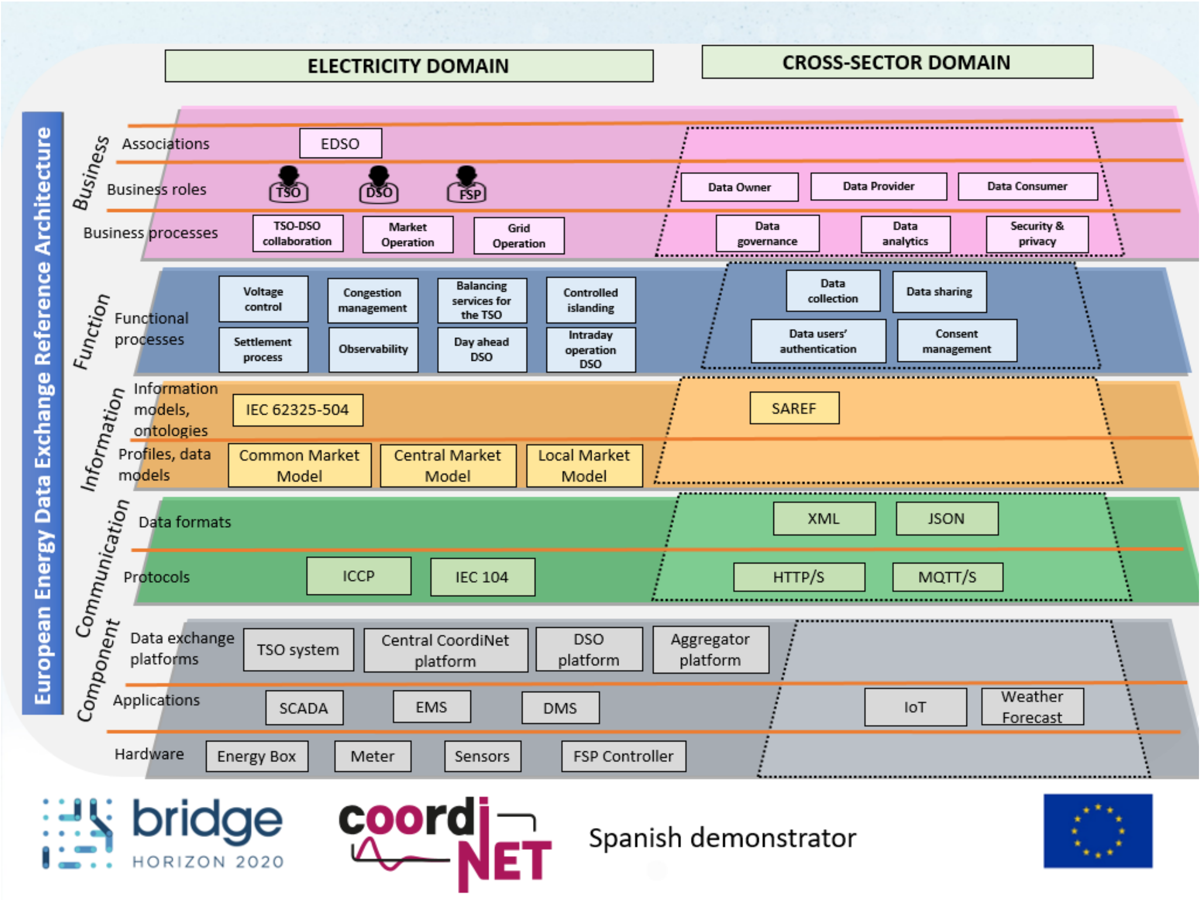

Figure 22: Coordinet Bridge RA Mapping - Spanish demo

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

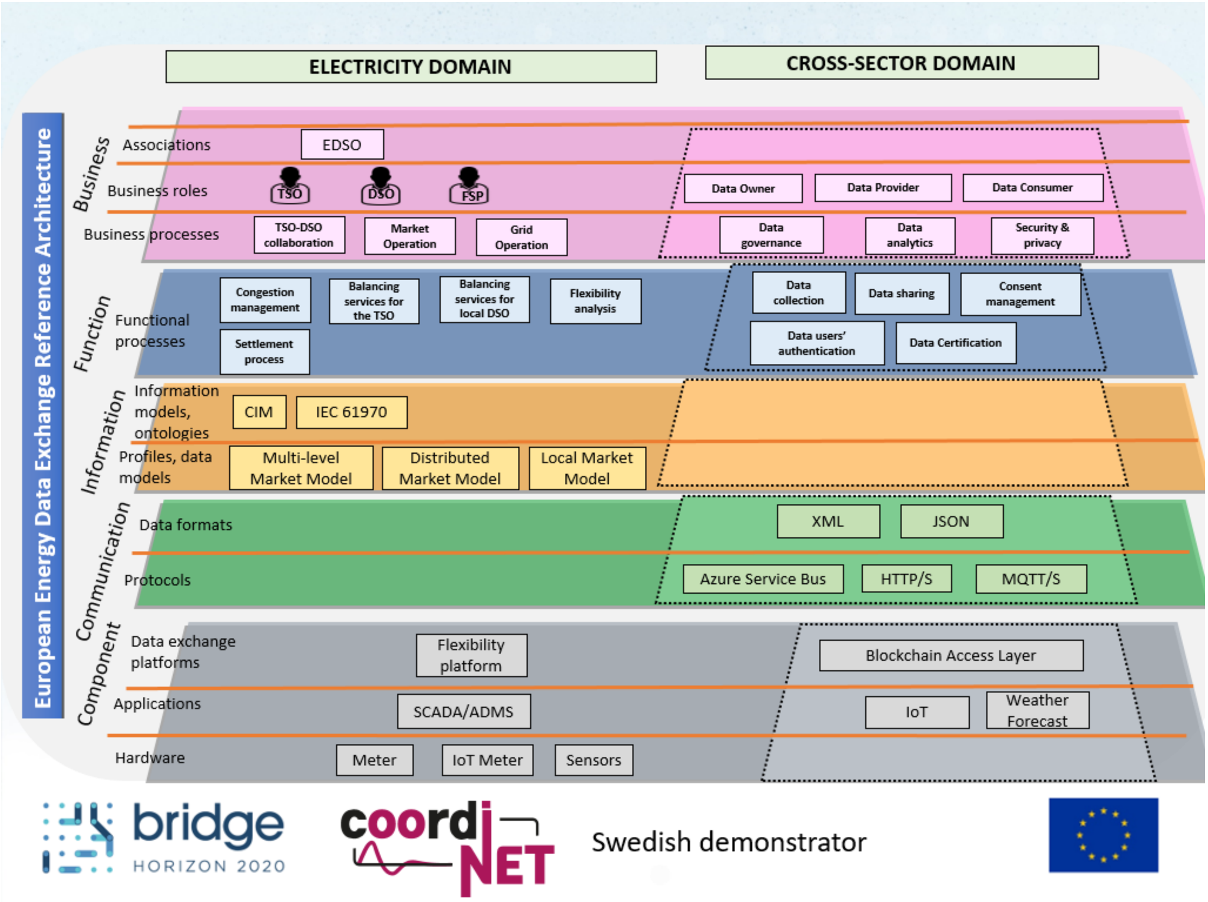

Figure 23: Coordinet Bridge RA Mapping - Swedish Demo

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.3.2 Platone

The project aims at defining new approaches to increase the observability of renewable energy resources and of the less predictable loads while exploiting their flexibility.

Platone project provides a unique mapping based on the Platone Open Framework architecture.

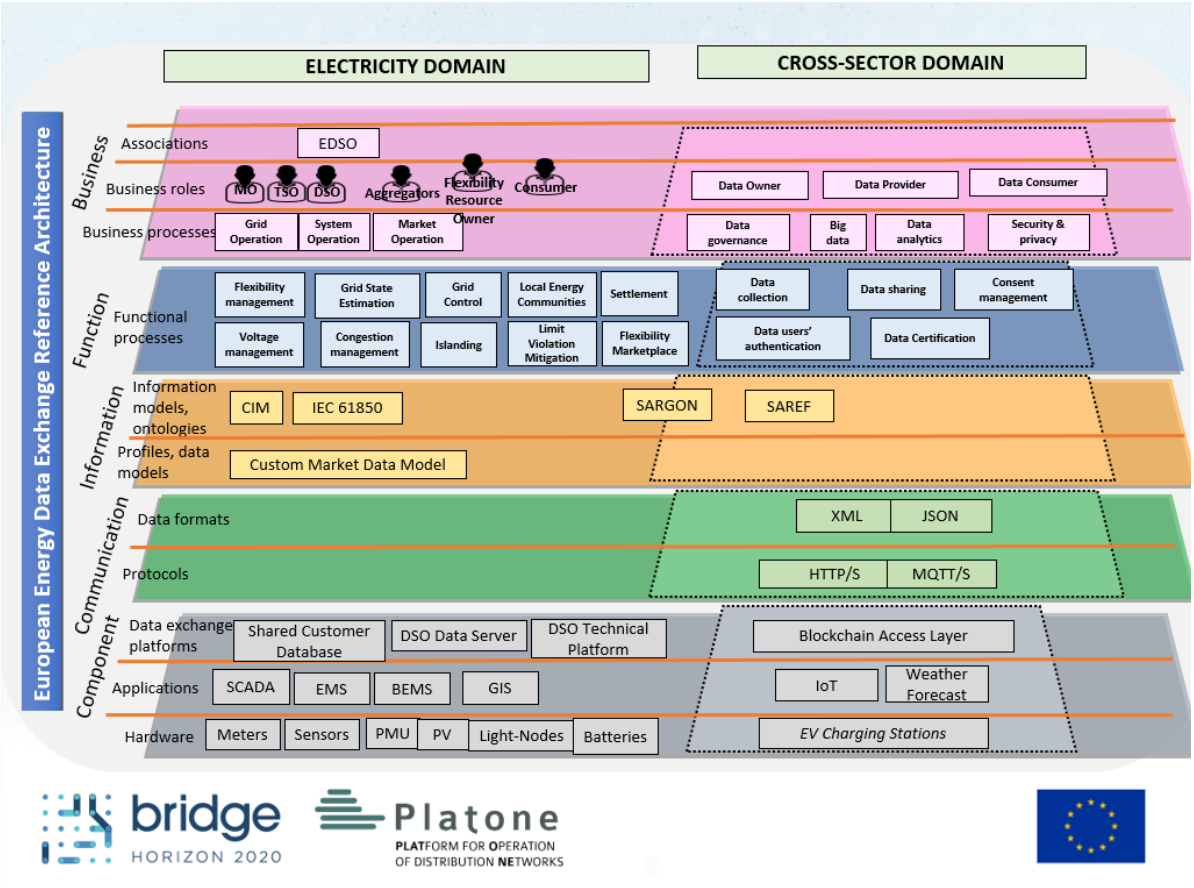

Figure 24: Platone Bridge RA Mapping - Platone Open Framework

3.3.3 INTERRFACE

The project aims to design, develop, and exploit an Interoperable pan-European Grid Services Architecture (IEGSA) to act as the interface between the power system (TSO and DSO) and the customers and allow the seamless and coordinated operation of all stakeholders to use and procure common services.

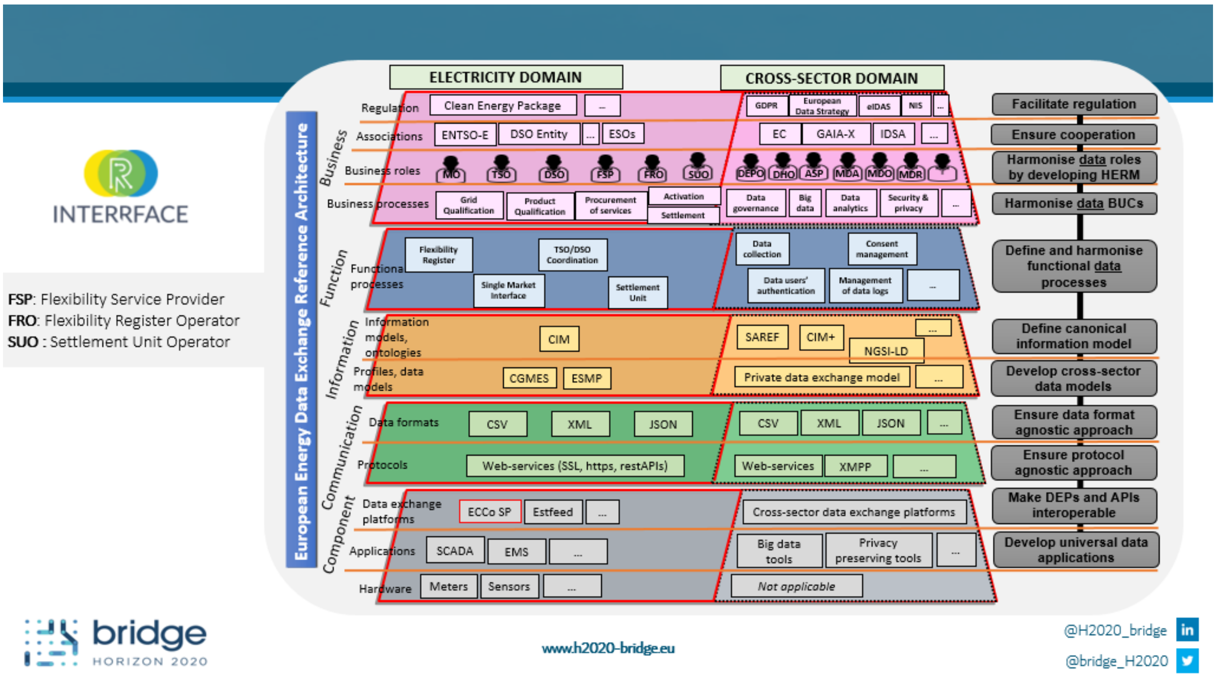

Figure 25: INTERRFACE Bridge RA Mapping

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.3.4 InterCONNECT

The project gathers 50 European entities to develop and demonstrate advanced solutions for connecting and converging digital homes and buildings with the electricity sector, with the main goal of bringing efficient energy management within reach of the end-users.

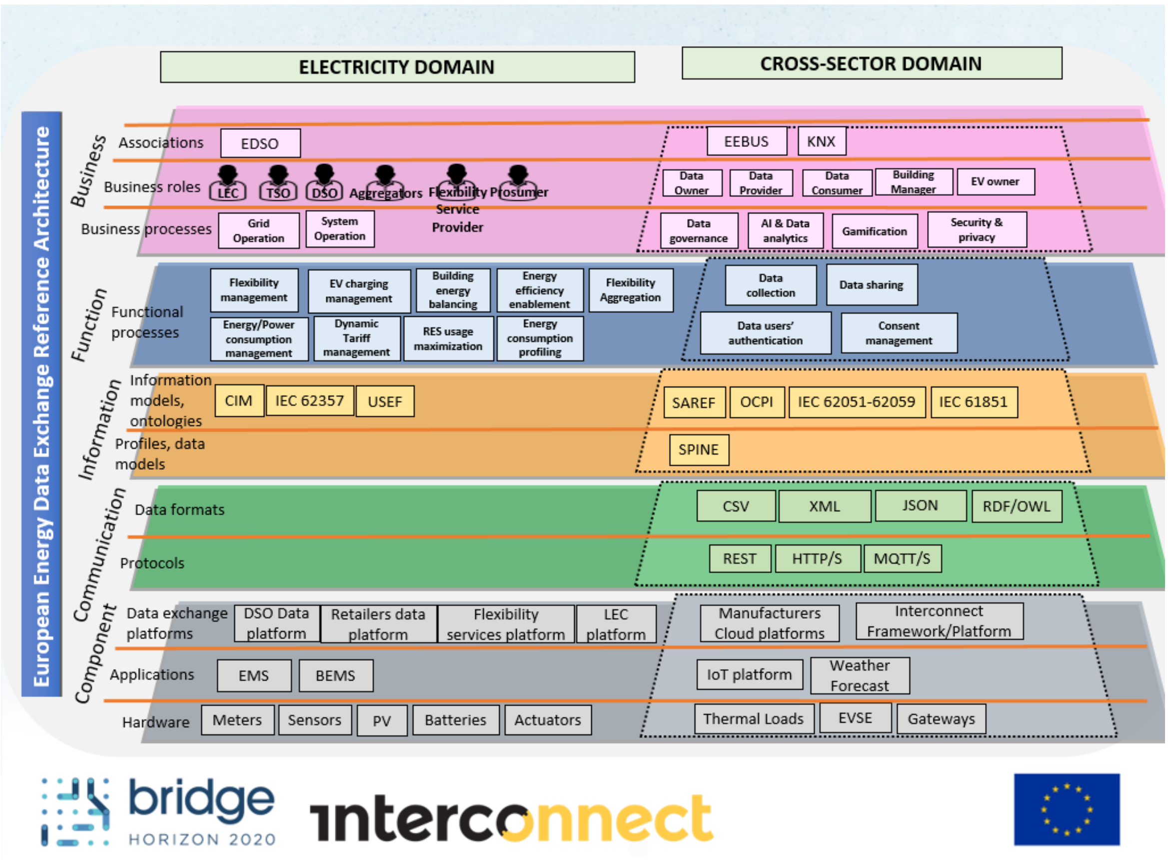

Figure 26: InterCONNECT Bridge RA Mapping

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.3.5 EUniversal

The project aims to develop a universal approach on the use of flexibility by Distribution System Operators (DSO) and their interaction with the new flexibility markets, enabled through the development of the concept of the Universal Market Enabling Interface (UMEI) – a unique approach to foster interoperability across Europe.

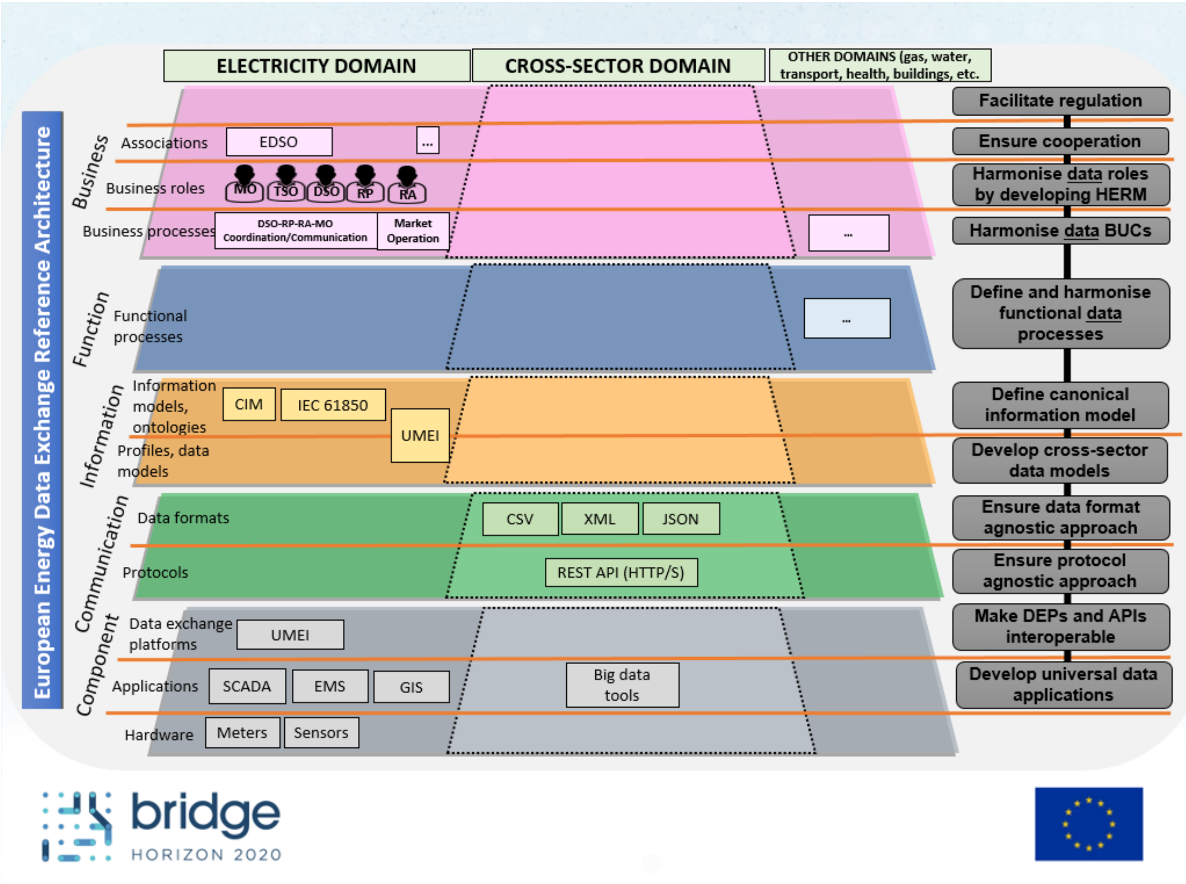

Figure 27: EUniversal Bridge RA Mapping

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.3.6 eDREAM

The project aims to develop new solutions for DSOs, as well as improving decision-making of aggregators and energy retailers using a new decentralized and community-driven energy ecosystem by fully integrating the micro-grid and VPPs (Virtual Power Plants) to local power disruption network.

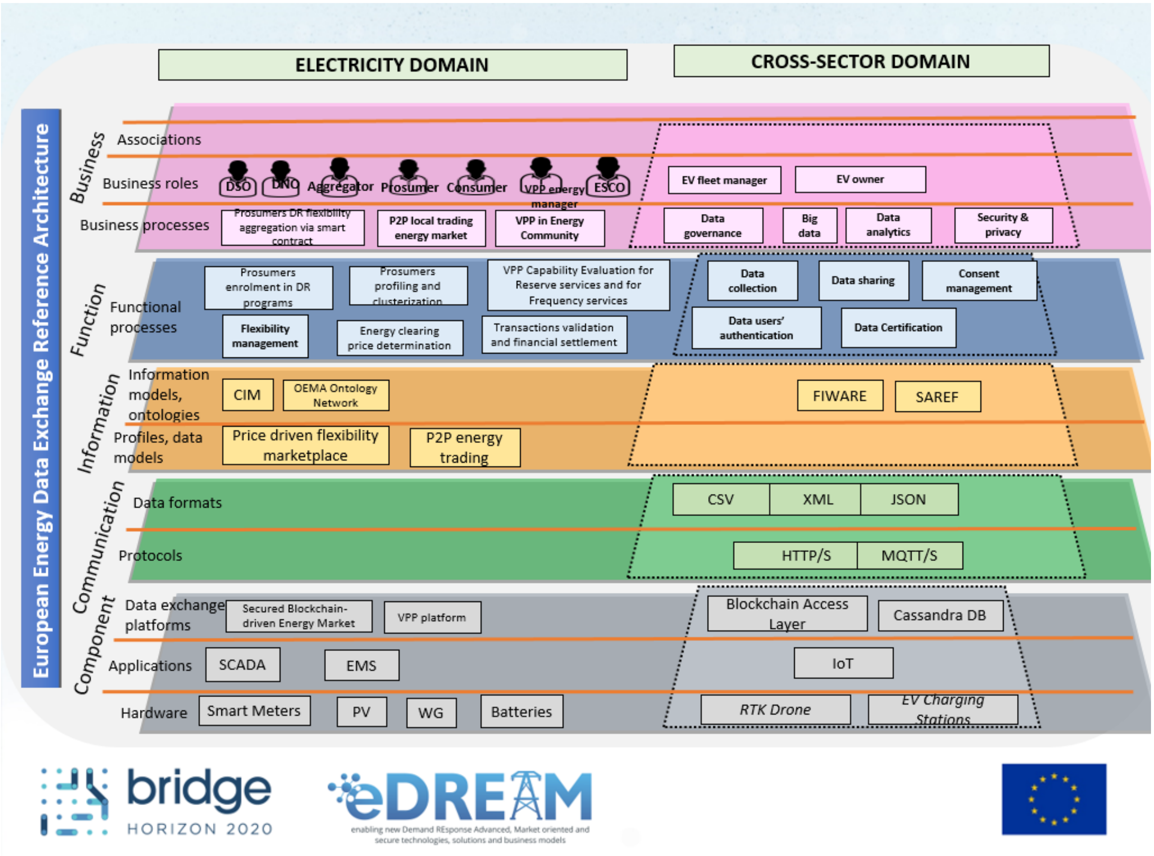

Figure 28: eDREAM Bridge RA Mapping

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.3.7 EU-SysFlex

The project will test a high level of integration of renewable energy sources in the pan-European electricity system. The aim of the project is to identify issues and solutions associated with integrating large-scale renewable energy and create a plan to provide practical assistance to power system operators across Europe. This should ultimately lead to identification of a long-term roadmap to facilitate the large-scale integration of renewable energy across Europe.

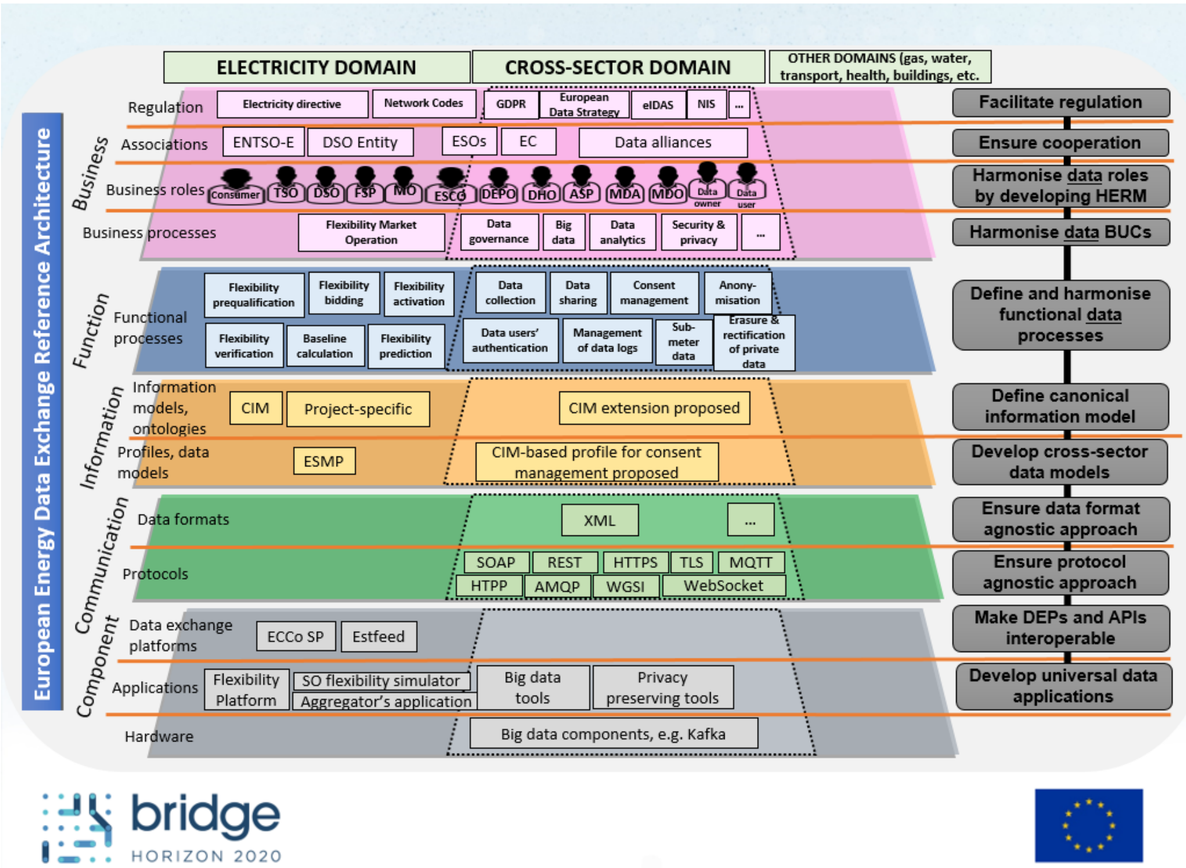

Figure 29: EU-SysFlex Bridge RA Mapping

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.4 OneNet Demo Architectures

The analysis of existing projects was accompanied by that of the OneNet Demo architectures. This additional activity allowed to extend this analysis and have more information to be taken into consideration for the design of the OneNet Architecture.

The mapping was conducted based on the Demo BUCs at the country level, except for the Northern, which is working since the beginning at a cluster-level.

The information collected from the projects and demos were processed and compared in a GAP analysis activity (Section 5.3), which made it possible to identify some fundamental characteristics to be taken into consideration in the implementation of the OneNet Architecture.

Furthermore, the result of this mapping allows to create a shared repository of architectures described using a single tool (the Bridge RA), maintainable, versionable and easily comparable.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.4.1 Northern Cluster

The Northern Demonstrator is an integrated effort by multiple TSOs and DSOs to enable market driven flexibility uptake by these networks in a coordinated way through multiple markets where liquidity can be reached due to scope or existing trading volumes. Through this demonstration, the project will be able to show mapping and management of network needs in multiple use cases over multiple networks. Instead of single network or single network pair dynamics, the demonstrator will focus on how joint and shared mechanisms can be used by multiple networks to demonstrate scalability and contribution towards a pan-European solution.

With this in mind, the Northern Cluster Demonstrator foresees a unique architecture.

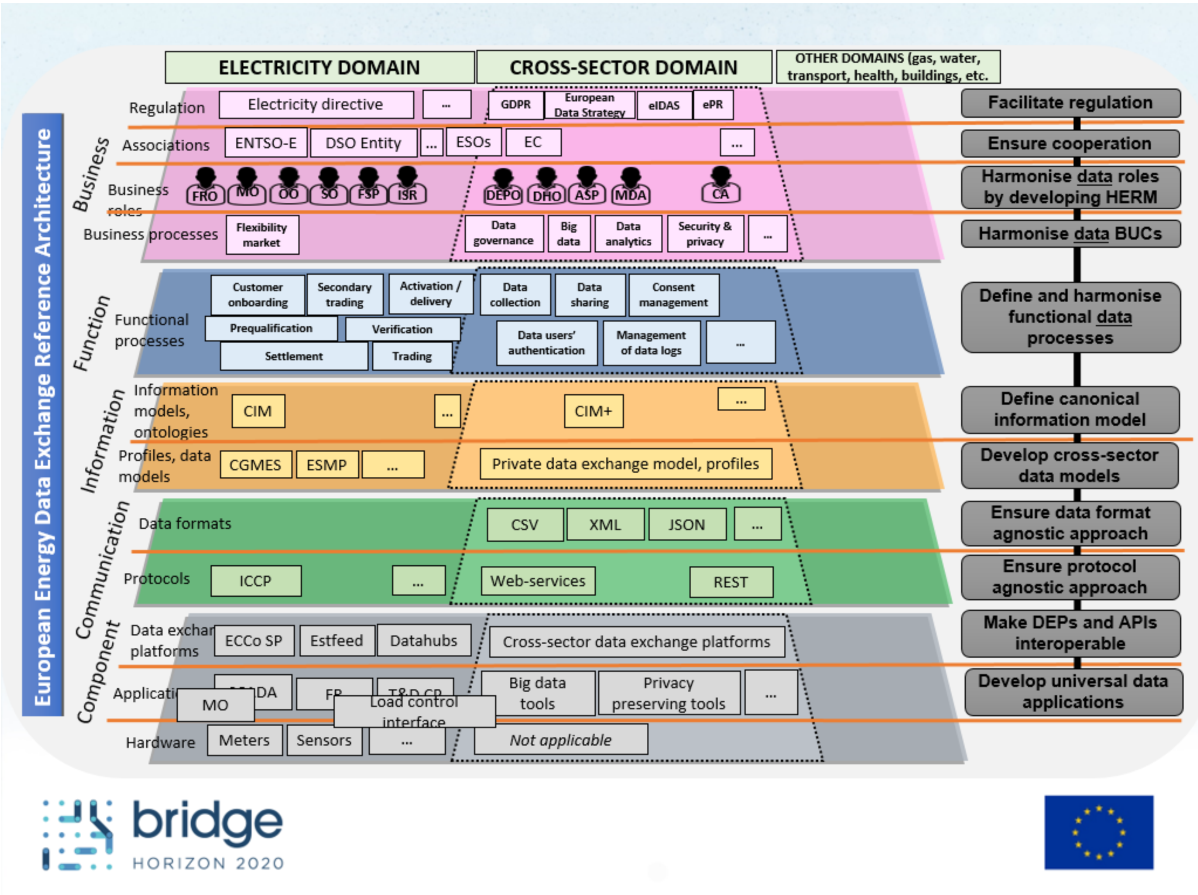

Figure 30: OneNet Northern Cluster Bridge RA Mapping

3.4.2 Southern Cluster

The main objective of the Southern Cluster is to design, develop, implement, and evaluate two pilot projects in Greece and Cyprus dealing with balancing and congestion management challenges facing system operators in the clean energy era, in compliance with the OneNet overall architecture. The TSOs and DSOs in both countries will share flexibility resources and coordinate their efforts to meet their augmenting regional challenges through grid services stemming from prosumers, aggregators, suppliers, producers, while at the same time they are optimizing the use of network assets and big data processing tools for network predictability and observability.

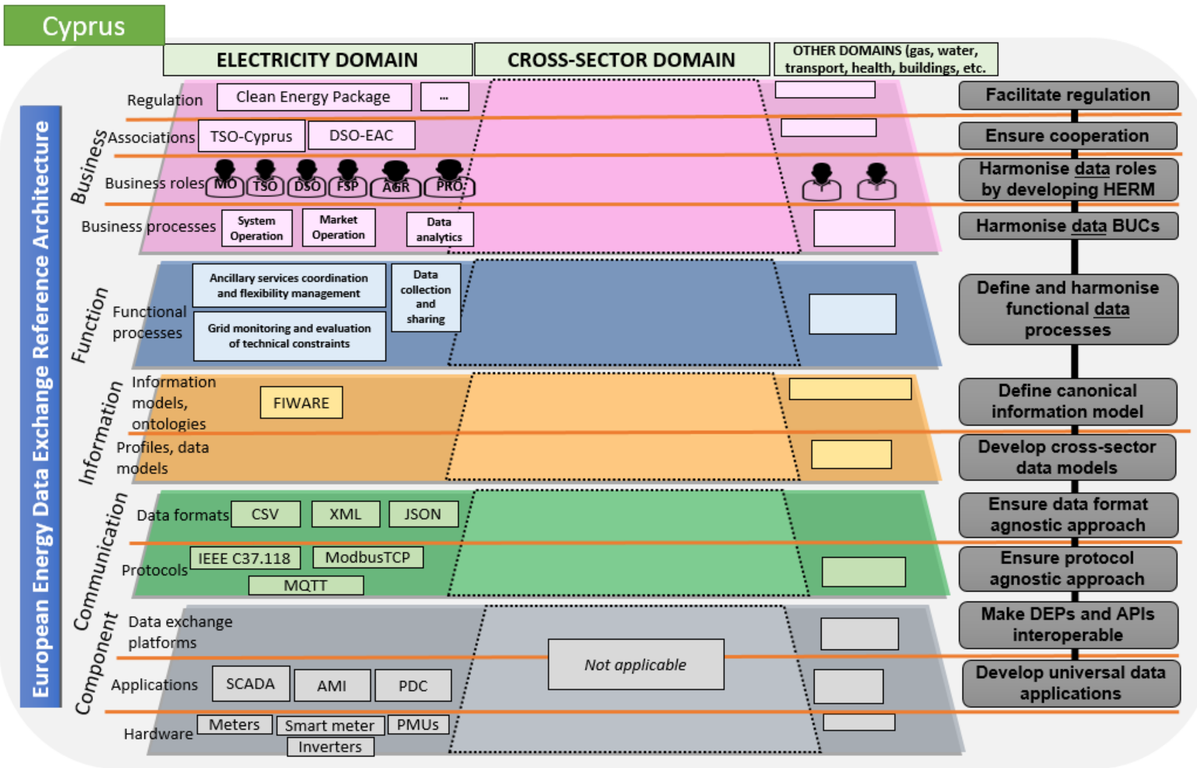

Figure 31: OneNet Cyprus Demo Bridge RA Mapping

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

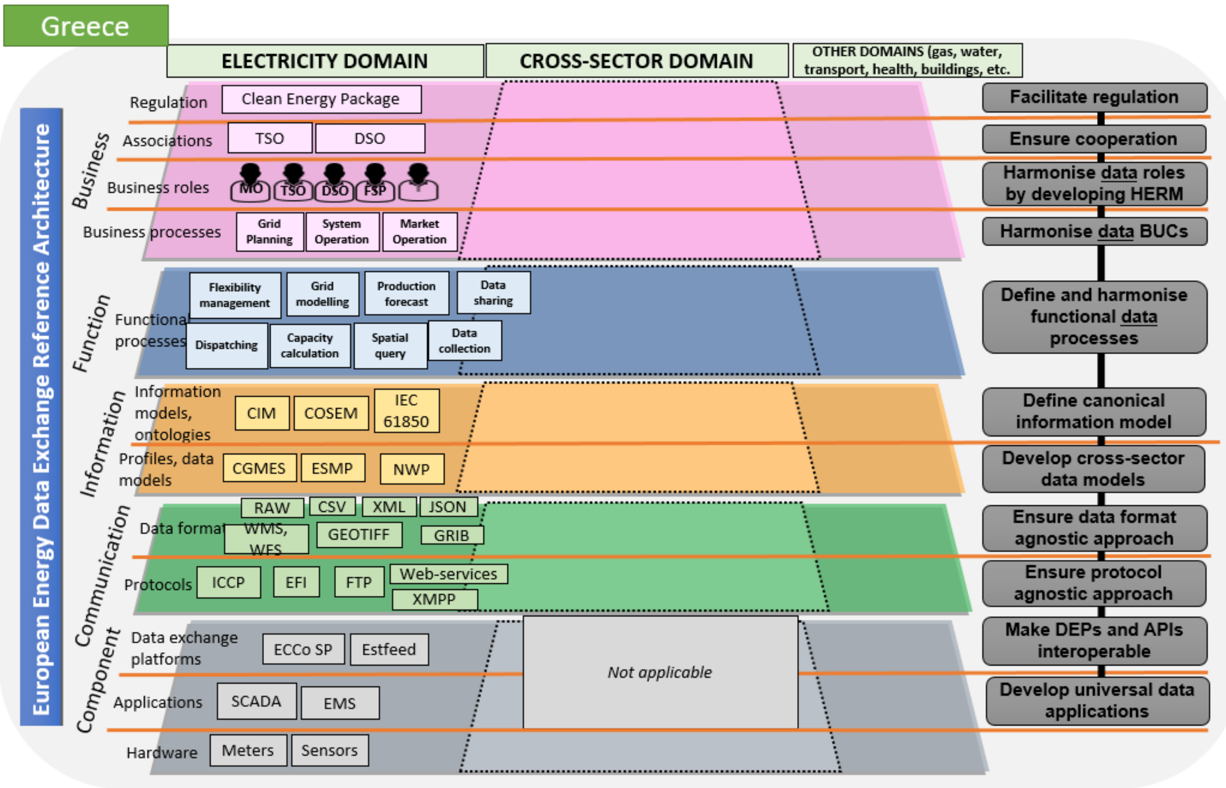

Figure 32: OneNet Greek Demo Bridge RA Mapping

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.4.3 Western Cluster

The Western Cluster foresees three different demo countries – Portugal, Spain and France - and aims to allow for the implementation of a wide range of flexibility mechanisms to address both DSO and TSO needs, including coordination between market mechanisms and the planning and real-time operation of the grids.

Within the different demos will be demonstrated several distinct approaches for the feasibility of solving different system operation needs in a coordinate environment that favours the active participation, direct or indirectly, of consumers and prosumers.

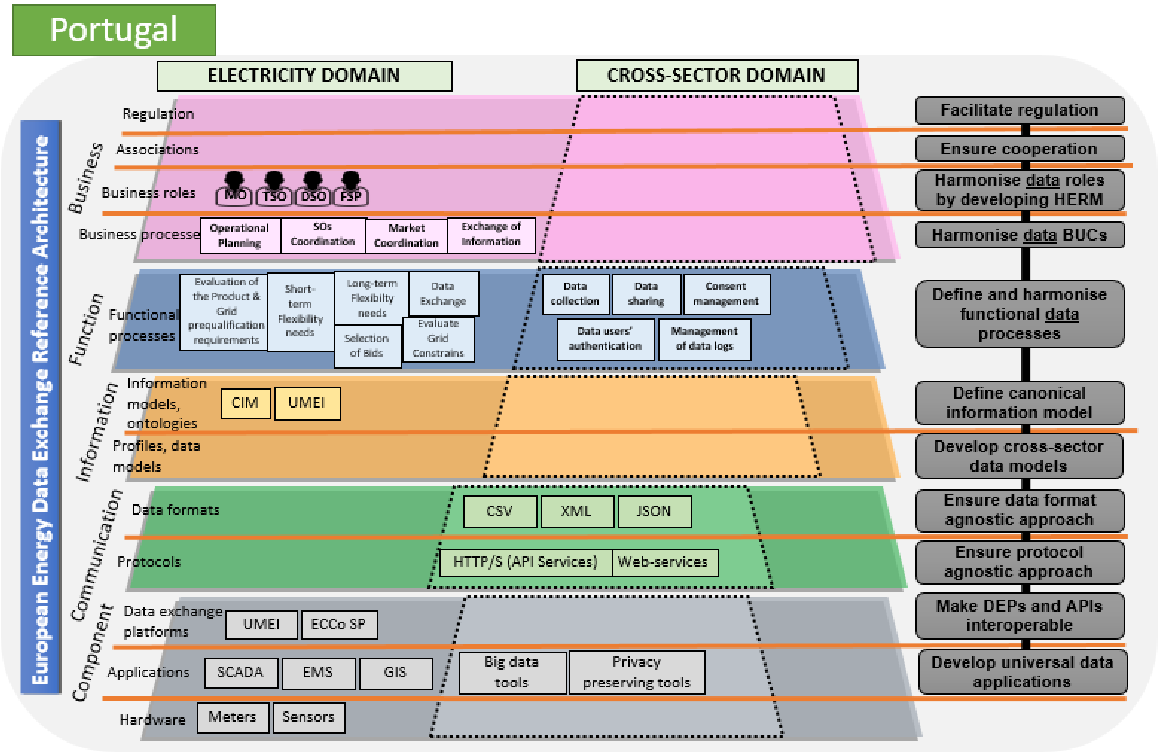

Figure 33: OneNet Portuguese Demo Bridge RA Mapping

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

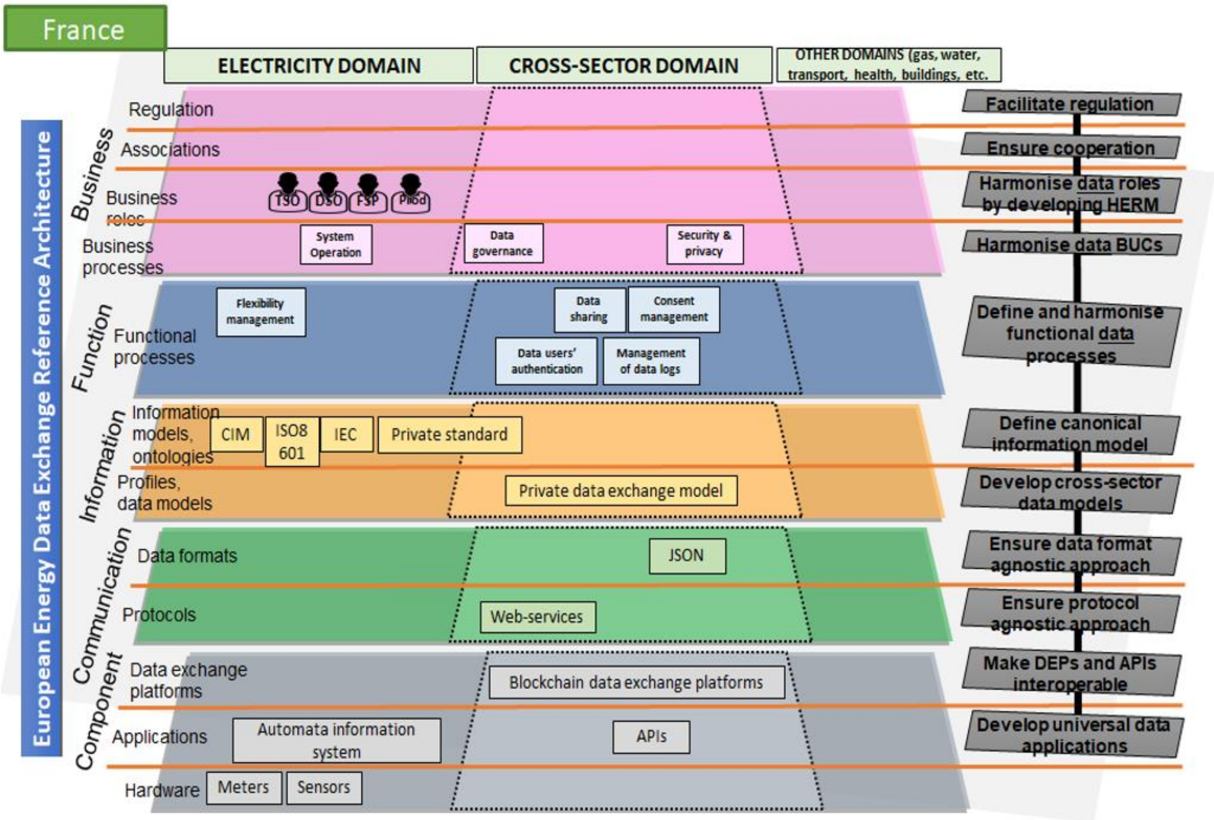

Figure 34: OneNet French Demo Bridge RA Mapping

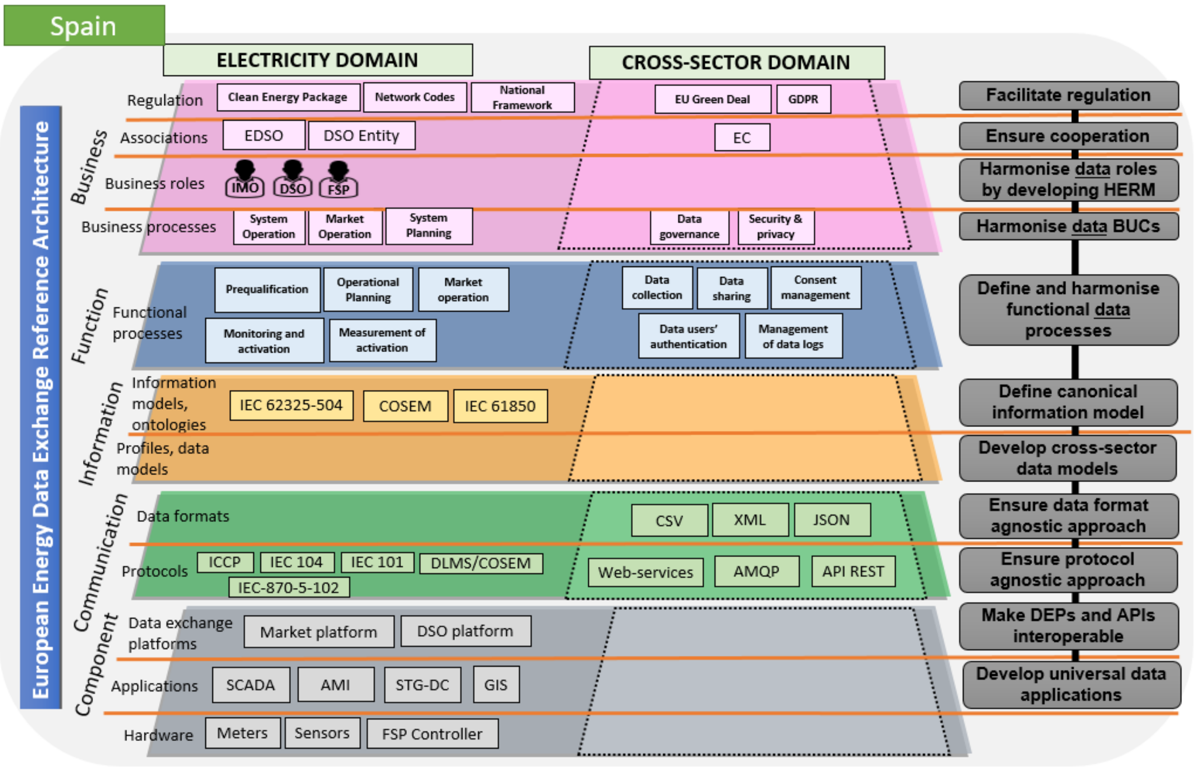

Figure 35: OneNet Spanish Demo Bridge RA Mapping

3.4.4 Eastern Cluster

The Eastern Cluster Demonstrator aims to develop an interoperable network of flexibility platforms to support the utilisation of various flexibility services, service integration and interaction, as well as the related data exchange.

Within the Eastern Cluster Demo will be developed and extended capabilities of existing flexibility market platforms for TSO and DSO grid services, which will be standardized to an appropriate European format. The development will be focused in particular on four areas: definition of new standardized flexibility services, elaboration of related market-based product and grid prequalification processes, the conceptualisation of location-based service activation and the coordination of access to local and system-level services. It will also include the definition of technical requirements for flexibility providers and aggregators offering flexibility services. Demo coordinators will perform pilot testing of flexibility services for DSOs and the TSO utilizing a varied mix of providers and resources. The Demo Cluster East will be focusing on the coordinated activation of flexibility services for congestion management and balancing (TSO, DSO) as well as for new market based non-frequency flexibility services addressing local issues. This will be achieved by establishing a combined and digitalized TSO-DSO flexibility process for balancing, congestion management and other non-ancillary/ancillary services, commonly procured and activated to deliver services for TSOs and DSOs. The cluster will address these services

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

as standardized market products provided in market-based environment. Various middleware solutions covering power system and related domains (e.g. smart city) have been developed in recent years and will serve as a basis for the abovementioned development.

At the time this document was drafted, the Hungarian demo has not yet defined the technical specifications of its architecture and therefore has not been able to provide the mapping in the Bridge RA.

The architecture of the Hungarian demo will anyway be taken into consideration as soon as it is defined, and the information will be collected and included in the updated version of this deliverable.

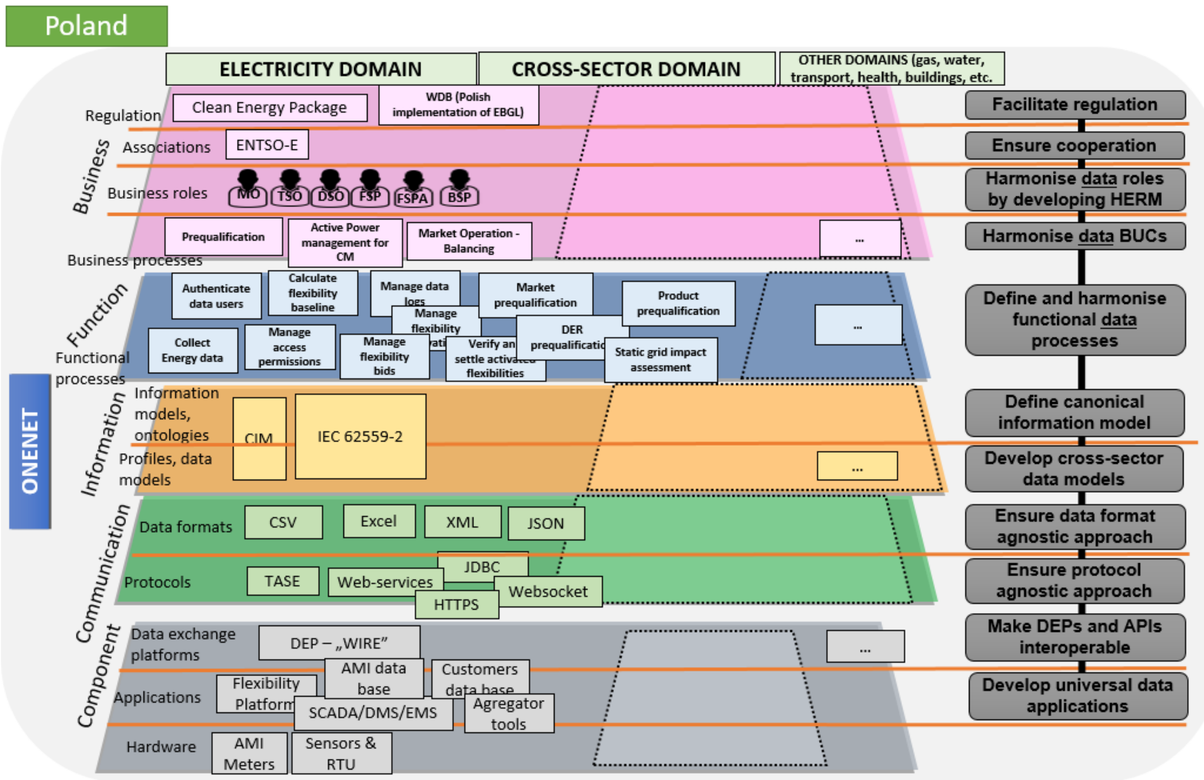

Figure 36: OneNet Polish Demo Bridge RA Mapping

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

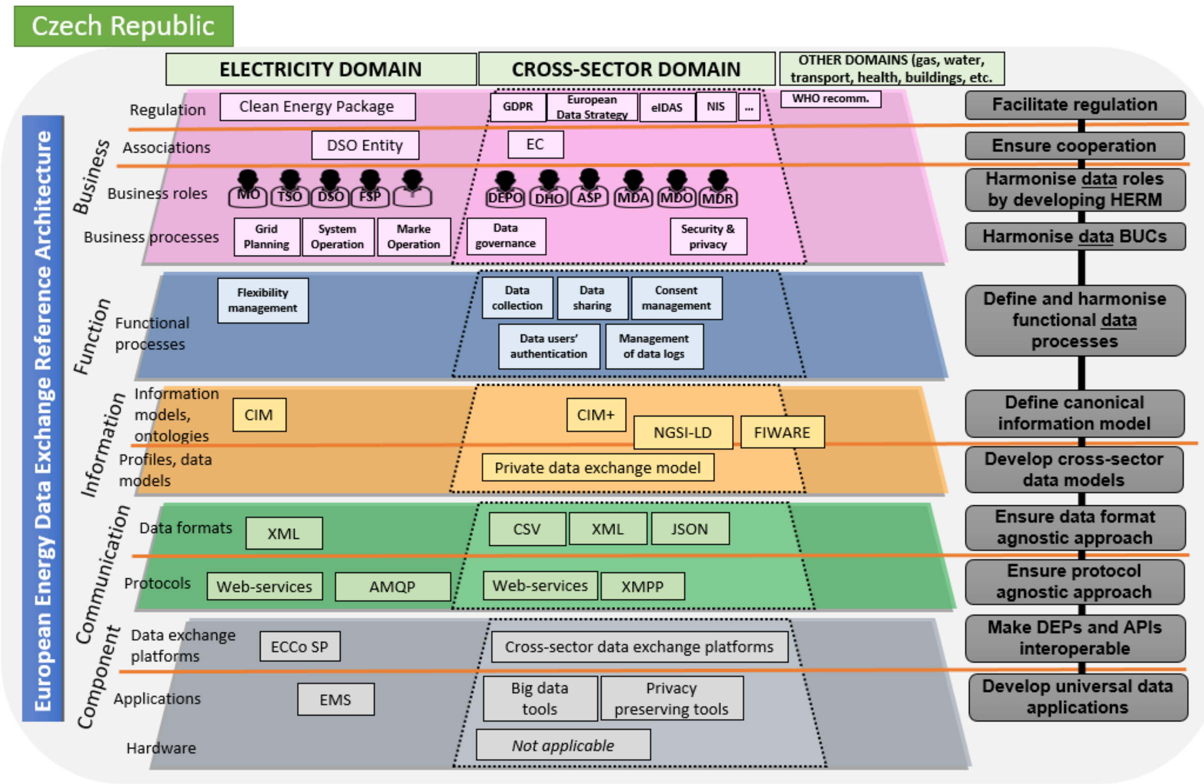

Figure 37: OneNet Czech Demo Bridge RA Mapping

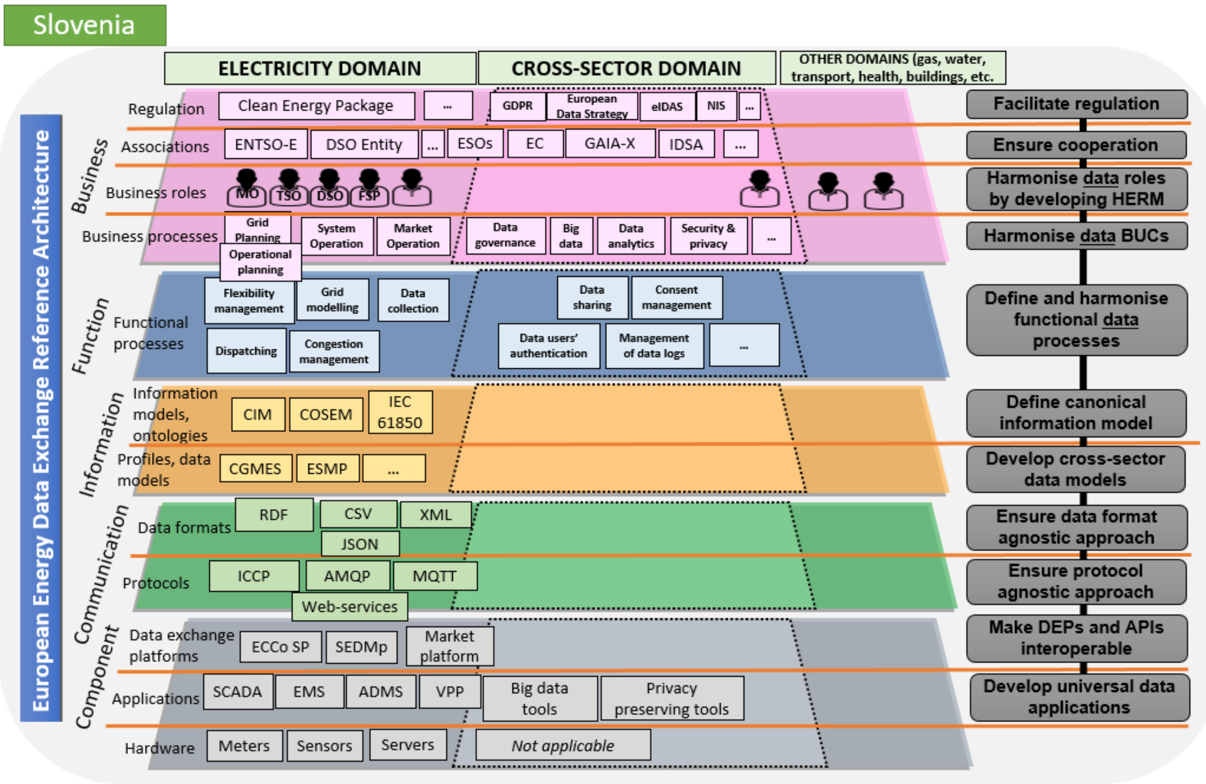

Figure 38: OneNet Slovenian Demo Bridge RA Mapping

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

4 Analysis of OneNet Requirements and Specification

This chapter will analyse the results of the activities carried out within the T5.1 task and in particular the objectives and the general concept of the OneNet system as well as the functional and non-functional requirements identified for its implementation.

4.1 OneNet Concept analysis

Task T5.1 is closely connected with T5.2. In fact, the objectives and the general concept of the OneNet system are the result of various activities, including the preliminary analysis on the OneNet Reference Architecture, which was conducted at the beginning of this task and is reported in paragraph 5.

This allowed us to have a continuous alignment on the main objectives of OneNet and that these were expressed and implemented correctly in the OneNet Reference Architecture.

As described in D5.1, the key feature of the OneNet Framework is to make available a data interoperability mechanism to all platforms to support data exchange for facilitating market and network operations and the cooperation between network operators, like TSOs and DSOs as well as the involvement of other players like prosumers and aggregators.

This key concept could be summarized in a set of fundamental characteristics:

- the adoption of open standards and interfaces to allow the seamless participation of various users,
- data privacy control and data access according to regulations for each stakeholder,
- definition of standard models and protocols for data exchange,
- the provision of data management features like data harmonization, data quality assessment, semantic annotation,
- dataflow monitoring and logging,
- Identification, Authentication and Authorization mechanisms for ensuring secure and trusted data exchange and platforms integration.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Analysing these characteristics, it is evident that a scalable, secure and standard approach is necessary to implement the multi-countries and multi-stakeholder interoperability mechanisms, declared as the main goal of OneNet.

The decentralized approach and the use of standardized interfaces and mechanisms therefore assume fundamental importance to satisfy all these characteristics and in particular to ensure the necessary scalability for the near real-time data integration and management enabling multi-country and multi-stakeholder near real-time services.

From this first analysis, it is therefore clear how the core component of the OneNet Framework, the OneNet Middleware, must leverage on a decentralized approach as well as on the most used and promising Data and Smart Energy open architectures (FIWARE Smart Energy grid Reference Architecture, IDS Reference Architecture Model), implementing standardized components for the platform integration (e.g., NGSI Standard Context broker). Technical details for the implementation of the OneNet Middleware are described in Section 5.4.3.1.

4.2 OneNet Requirements analysis

One of the main results described in D5.1 is the list of functional and non-functional requirements to be met for the implementation of the OneNet framework.

Obviously, in addition to the implementation of components in WP6, the Open Reference Architecture must also take these requirements into account, so that they can be satisfied by any implementation of the reference architecture.

In fact, we recall that the framework implemented in WP6 is only a reference implementation of the OneNet architecture, which however has the aim of being an Open Reference Architecture that can be implemented and adapted by anyone.

For convenience, below is reported the list of functional and non-functional requirements, provided in D5.1. Downstream of this, a general analysis of the requirements will be presented and how these are reflected in the design choices of the OneNet architecture.

Table 1: OneNet Functional Requirements

Requirement ID	Requirement Name	Description
OneNet_FUR_01	The OneNet system must enable exposure of list of data/ services from vertical WPs to third parties	System of the OneNet Participant has many features/roles and data. Those can be accessed through API's by third party. The list of services/data and their properties can be retrieved automatically by special API - "Catalogue service". This list can be provided by API to OneNet system, in order to be exposed to potential third parties.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

OneNet_FUR_02	The OneNet system must enable role-based access for data/service to authenticated users.	Every data/service responds to authenticated requests only. In case third party need the access then the authentication/secure channel needs to be established.
OneNet_FUR_03	The OneNet system must visualize and provide analysis tool for activity logs.	User activity trace logs, technical performance or problem related logs are generated and could be exposed from demonstrator's implementation to third parties, through the OneNet system
OneNet_FUR_04	The OneNet system must facilitate the communication of the SO's flexibility needs to external interested stakeholders	The SOs, i.e., DSO and TSO, shall be able to make available to stakeholders their flexibility needs in different timeframes, e.g., Day-ahead and Intra-day, through the utilization of the OneNet system.
OneNet_FUR_05	The OneNet system must facilitate market results to be disseminated to external interested stakeholders	The local market platform publishes collected market results through OneNet system to external interested parties.
OneNet_FUR_06	The OneNet system must facilitate data exchange amongst SOs, MOs, and FSPs participating in the market-based flexibility procurement process, for prequalification, market clearing, evaluation and real-time control purposes.	Prequalified limits in the interface between the HV/MV (TSO) and MV/LV (DSO) that FSPs exist are sent to the market (TSO market or local DSO market) in order to be taken into consideration by the market operator in the allocation of the awarded bids to the FSPs. In addition, MO publishes the awarded bids to the operators through the OneNet. After the activation of the flexibility, evaluation report of the FSP's performance is sent to the market operator through the OneNet platform. Finally, communication between the DSO control centre (ABCM-D platform is develop in the context of Cypriot Demonstrator) and the local FSPs connected to the distribution grid through the OneNet system
OneNet_FUR_07	The OneNet system must connect the involved in the Demo parties to external actors responsible for TSO-DSO coordination	TSO/DSO coordination process takes place through the utilization of OneNet. This specifically includes: DSO demand finalization, flexibility registration, bid prequalification and market result broadcasting
OneNet_FUR_08	OneNet system must be able to manage and certificate the identity of each OneNet Participant	OneNet system manage the identities of all the OneNet participants offering an Identity Provider
OneNet_FUR_09	OneNet system must be able to register/unregister a OneNet connector	OneNet Connector need to register itself before starting any data exchange process
OneNet_FUR_10	Each OneNet Participant must be uniquely identified using certification	OneNet Participants are uniquely identified within the OneNet ecosystem, using certification process and establishing trust among all participants.
OneNet_FUR_11	Each OneNet Connector have a unique certificate and identifier	
OneNet_FUR_12	Each OneNet Connector is able to verify the identity of the other OneNet Connectors	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

OneNet_FUR_13	OneNet participant must be able to run the OneNet connector in its own environment	OneNet Middleware leverage on the IDS decentralized approach. The OneNet Connector provided by OneNet must be deployable in any environment
OneNet_FUR_14	The OneNet Participant must be able to configure its own OneNet Connector	OneNet connectors are configurable by the OneNet participants using specific interfaces
OneNet_FUR_15	The OneNet connector must be able to send metadata of a data source to one or more Brokers	Once the connector is configured it is able to connect the Brokers for starting data exchange. The connector is able to provide and/or search metadata as well as discover for new data sources and participants.
OneNet_FUR_16	The OneNet Participant must be able to search and discover other OneNet Participants	
OneNet_FUR_17	The OneNet Connector must be able to search for metadata connecting to a Broker	
OneNet_FUR_18	The OneNet Connector must be able to exchange data with other connectors using pull and/or push mechanisms	The data exchange process happens end-to-end exploiting pull or push mechanisms.
OneNet_FUR_19	The OneNet system must be able to support the creation, management and usage of vocabularies	A feature provided by OneNet system is the Vocabulary Provider. It manages and offers vocabularies (i.e., ontologies, reference data models, or metadata elements) that can be used to annotate and describe datasets.
OneNet_FUR_20	The OneNet participant could use vocabularies for creating and structuring its metadata	
OneNet_FUR_21	The OneNet system should offer data services/apps for data processing and transformation	One of the main features of the OneNet system is the possibility to enrich, transform, validate and harmonize the data processed. In addition, the OneNet allow to log all the data transaction.
OneNet_FUR_22	The OneNet system should be able to log any data transaction between any OneNet participant	
OneNet_FUR_23	The OneNet system should be able to assess the quality of data processed	
OneNet_FUR_24	The OneNet system should be able to perform a semantic validation of the data processed	
OneNet_FUR_25	The OneNet system could use AI mechanism for empowering Data services	For improving the Data Services offered by the OneNet system, some AI mechanism could be implemented.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

OneNet_FUR_26	The OneNet system should be able to integrate any kind of data sources using Context Broker	The usage of the FIWARE context broker could facilitate the integration of any kind of data source, using a standard API based approach.
OneNet_FUR_27	The OneNet Orchestration Workbench must be able to manage data and service orchestration	The OneNet Orchestration Workbench aims to support the data orchestration for the evaluation of the performance and scalability of the AI, IoT and Big Data cross-platform services for market and grid operations.
OneNet_FUR_28	The OneNet Orchestration Workbench must be able to integrate data using the OneNet Middleware	The OneNet Orchestration Workbench allows to integrate data coming from the OneNet middleware and implement a data pipeline orchestration. It also should include: • Job Scheduling • App/Service registry and discovery • Error/Retries management • SLAs tracking, alerting and notification
OneNet_FUR_29	The Service Provider must be able to register its service in the OneNet Orchestration Workbench	
OneNet_FUR_30	The Service Provider must be able to create a data workflow using the Orchestration Workbench	
OneNet_FUR_31	The Service Provider must be able to evaluate the performance of its own service	
OneNet_FUR_32	The OneNet Orchestration Workbench should provide a service catalogue to the OneNet Participants	
OneNet_FUR_33	The OneNet system should offer a UI dashboard to OneNet Participants for monitoring and analytics	The OneNet system should implement a GUI for facilitating the OneNet Participants in the management, monitoring and analytics of the data transactions.

Table 2: OneNet Non-Functional Requirements

Requirement ID	Requirement Name	Category	Subcategory	Description
OneNet_NFR_01	Coverage of objectives	Functional Suitability	Completeness	The OneNet system shall at least cover all the objectives and envisioned utilization of it from the demonstrators, satisfying all the functional requirements and implementing all the functionalities and tool expected.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

OneNet_NFR_02	Correctness level	Functional Suitability	Correctness	The OneNet system shall implement the functionalities envisioned in the proper way.
OneNet_NFR_03	Regulation update compatibility	Reliability	Maturity	The OneNet system shall be compatible regarding the updates in energy data security according to EU and national EU members' regulation.
OneNet_NFR_04	System failure	Reliability	Fault tolerance	The OneNet system shall ensure a low level of system failure.
OneNet_NFR_05	Recovery ability	Reliability	Recoverability	The OneNet system should be able to recover the data that have been directly affected by an undesirable interruption.
OneNet_NFR_06	Timing execution errors	Performance Efficiency	Time behaviour	The OneNet system shall be able to monitor and alert for timing execution errors.
OneNet_NFR_07	Resource Utilization issues	Performance Efficiency	Resource utilization	The OneNet system is able to monitor and alert for resources utilization issues.
OneNet_NFR_08	Capacity limitations	Performance Efficiency	Capacity	The OneNet system is able to monitor and alert for capacity limitations.
OneNet_NFR_09	Documentation for the integration	Usability	Learnability	The OneNet system shall provide a comprehensive documentation for the integration of the platform/services.
OneNet_NFR_10	Documentation for the operations	Usability	Operability	The OneNet system shall provide a comprehensive documentation for all the envisioned operations.
OneNet_NFR_11	User initialization error	Usability	User error protection	The OneNet system shall be resilient to user initialization error.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

OneNet_NFR_12	Privacy of grid data	Security	Confidentiality	The OneNet system must ensure the privacy and the security of grid data.
OneNet_NFR_13	Privacy of customer's personal data	Security	Confidentiality	The OneNet system must ensure the privacy and the security of customers' personal data.
OneNet_NFR_14	Secure integration to critical energy infrastructure	Security	Integrity	Secure one point of connection between the OneNet platform and the legacy systems of the energy domain stakeholders.
OneNet_NFR_15	Penetration testing	Security	Integrity	Penetration security test should be performed before the final release of the OneNet system of platform in order to identify potential security branches and fix them before the final release.
OneNet_NFR_16	Data flow tracking	Security	Non-repudiation	The OneNet system shall track all the data and process flows.
OneNet_NFR_17	Link data to user	Security	Accountability	The OneNet system shall link all the data and process flows to a specific user.
OneNet_NFR_18	User Authentication	Security	Authenticity	The OneNet system must identify uniquely the involved users in the system.
OneNet_NFR_19	Facilitation of connection to multiple external platforms and stakeholders	Compatibility	Co-existence	Existence of several connections simultaneously to OneNet system should be considered, without deteriorating the system overall performance
OneNet_NFR_20	Interoperability of OneNet solution	Compatibility	Interoperability	Interoperability of the solution should be considered towards avoiding the risk of creating a closed environment that does not allow integration of other technologies

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

				and the expansion of the pan-European energy marketplace.
OneNet_NFR_21	Connection to the platform of multiple stakeholders at the same simultaneously	Maintainability	Modularity	OneNet System shall be able to service multiple connections at the same by having multiple connections to the external platforms and stakeholders, without deteriorating the performance overall.
OneNet_NFR_22	Modification capability	Maintainability	Modifiability	The OneNet system shall be modifiable based on the feedback collected during the evaluation phase of the demonstrations.
OneNet_NFR_23	Testing process	Maintainability	Testability	The OneNet system shall be testable and evaluable within the demonstrators' architecture.
OneNet_NFR_24	Agnostic	Portability	Adaptability	The OneNet system must be platform and environment agnostic.
OneNet_NFR_25	Deployability	Portability	Installability	The OneNet system must be deployable in any environment (e.g., using Docker container or similar approach)

The analysis conducted highlighted that not all the Demo SUCs reports a clear interaction with the OneNet System at the time this document is drafted.

The collection of information from Demos will then be continued, in order be able to draw up a complete list of: platforms/applications to be integrated into OneNe; data exchanged between the different actors; functionalities to be implemented in the various tools of the OneNet system. These activities will be carried out in the other tasks of WP5 and reported in the subsequent deliverables.

Anyway, the functional requirements extracted from the OneNet General System Use cases and the few that refer to the demos allow to clearly identify some specific features and/or components that the OneNet Architecture should implement

Below are reported a list of main characteristics and features that OneNet Architecture will take into considerations. A more detailed view is described in the specific architecture paragraphs (Ch. 5).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- Enable a secure and managed data flow between the end points
- Manage data access and consent mechanisms
- Provide standard authentication and authorization methods
- Provide standard methods and technologies for a seamless platform integration
- Provide Data and Services Catalogue
- Implement an administration portal
- Provide Monitoring and Analytics features
- Track and monitor data processes
- Allow integration, security, and deployment test
- Allow configuration mechanisms
- Provide a scalable and flexible solution
- Ensure Data privacy
- Provide standard and readable documentation
- Encourage the adoption and reuse of the solution

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

5 OneNet Open Reference Architecture

5.1 Vocabulary

In the table below was collected all the concepts and terms that the OneNet system refers to, in order to create a common vocabulary for all the OneNet Stakeholders and avoid any misunderstanding and lack of clarity.

Table 3: OneNet common vocabulary

Term	Description
Generic Terminology	
Platform	Complex collection of systems, interfaces and processes integrated with each other for providing a set of functionalities and services
Reference Architecture	A reference architecture provides a template solution for an architecture for a particular domain. It also provides a common vocabulary for all the stakeholders involved.
Use Case	Is a list of actions or steps that describes the interactions between actors and systems to achieve a goal.
Business Use Case	It describes the business process that is used by its business actors for achieving a business goal
System Use Case	It describes behavior of a system that implements a business use case at the system functionality level, specifying the function or the service that the system provides.
Requirement	A requirement is a single documented physical or functional need that a particular design, product or process aims to satisfy.
Functional Requirement	Functionalities, behaviour, and information that the solution needs
Non-Functional Requirement	The conditions under which the solution must remain effective, qualities that the solution must have, or constraints within which it must operate (reliability, testability, maintainability, availability, performance)
Actor	An actor classifies a role played by an external entity that interacts with the subject (e.g., by exchanging signals and data), a human user

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

	of the designed system (Person) some other system or hardware using services of the subject.
Component	A Component represents an encapsulation of functionality aligned to implementation structure, which is modular and replaceable. A Component is a self-contained unit. As such, it is independently deployable, re-usable, and replaceable. A Component performs one or more Application Functions. It encapsulates its contents: its functionality is only accessible through a set of Application Interfaces.
Device	A Device represents a physical IT or OT resource upon which system software and artifacts may be stored or deployed for execution. A Device is a specialization of a Node that represents a physical IT or OT resource with processing capability. It is typically used to model hardware systems such as mainframes, PCs, or routers. Usually, they are part of a node together with system software
Application Programming Interface (API)	Is a software interface that allow the connections between components, tools, and platforms. A document or standard that describes how to build such a connection or interface is called an API specification. The term API may refer either to the specification or to the implementation.
Interoperability	Characteristic of a system to work with other systems in a clear and standardized way, without any restrictions.
OneNet Terminology	
Demo Cluster	Is a cluster of geographically close demonstration sites that collaborates for aiming a goal beyond the small regional problems facing use cases that also go across several countries at all the levels of the grid. In OneNet there are four demo clusters: Northern, Southern, Eastern and Western.
Demo Use Case	Use Case derived directly from the demonstrators.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Regional Use Case	Use Case derived on a demo cluster level to showcase the connectivity amongst demonstrators belonging to the same cluster through OneNet system of platforms
OneNet Use Case	Use Case derived by following two processes; first, we identify and classify the data exchanges and used services between actors/platforms in both Demo and Regional SUCs with the OneNet system of platforms. Second, we include SUCs identified in other H2020 projects, based on the work conducted in the context of T5.3, that are relevant to the OneNet, in order to have a complete list of General SUCs that will be implemented through the OneNet system of platforms.
OneNet Framework	Is the core layer of the OneNet Architecture. It consists of three main components: the OneNet Decentralized Middleware, the OneNet Orchestration Workbench and the OneNet Monitoring and Analytics Dashboard.
OneNet Decentralised Middleware	The core component of the OneNet system. It is implemented using a decentralized approach based on the more used and promising standard architecture and interfaces, namely IDS and FIWARE. It allows the integration and collaboration of the OneNet participants, facilitating the cross-platform market and network operations, ensuring scalability and interoperability, while maintaining the data ownership.
OneNet Connector	Is a specific instance of the OneNet Decentralized Middleware, will be placed inside each platform and will allow an easy integration and cooperation among the platforms, maintaining the data ownership and preserving access to the data sources.
OneNet Orchestration Workbench	One of the components of the OneNet system. It acts as a data orchestrator to evaluate the performance and scalability of the cross-platform services that aims to use near real-time IoT metering and Big Data at consumer and/or network level.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

OneNet Participant	Any kind of actor involved in the OneNet ecosystem. Can be divided into: data source, data provider, data consumer and service provider.
Data Source	The more generic source of data that could be integrated within OneNet system. It could be represented by a Data Provider (see below), a single database, an IoT device, a file system etc.
Data Provider	A specific OneNet participant that provide data to the system. To submit metadata or exchange data with a Data Consumer, the Data Provider uses software components (OneNet connector) that are compliant with OneNet System.
Data Consumer	A specific OneNet participant that receives data from a Data Provider. From a business process perspective, the Data Consumer is the mirror entity of the Data Provider; the activities performed by the Data Consumer are therefore similar to the activities performed by the Data Provider. Before the connection to a Data Provider can be established, the Data Consumer can search for existing datasets by making an inquiry at Broker Service Provider.
Service Provider	A specific OneNet participant that provides services or tools. The Service Provider registers its services in the OneNet Framework in order to be used, integrated and tested within any cross-platform integration or orchestration process.

5.2 Concept Architecture

As described in the methodology approach in Ch.2, three versions of the architecture were designed during Task T5.2, two draft versions and the final one. The step-by-step approach allowed us to have an incremental evolution and the improvement of the draft versions, including all the feedback, comments and results coming from technical partners, demo partners and other tasks and WPs of the OneNet projects.

OneNet Architecture v0.1 – It is the first initial draft of the architecture, starting from OneNet main objectives and OneNet Solution described on the OneNet DoA. It includes: the OneNet solution, named OneNet Framework first concept; different layers of data exchange for enabling cross-platform integration and cooperation; specific Layer for cybersecurity and data privacy aspects, following also D5.8 guidelines.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

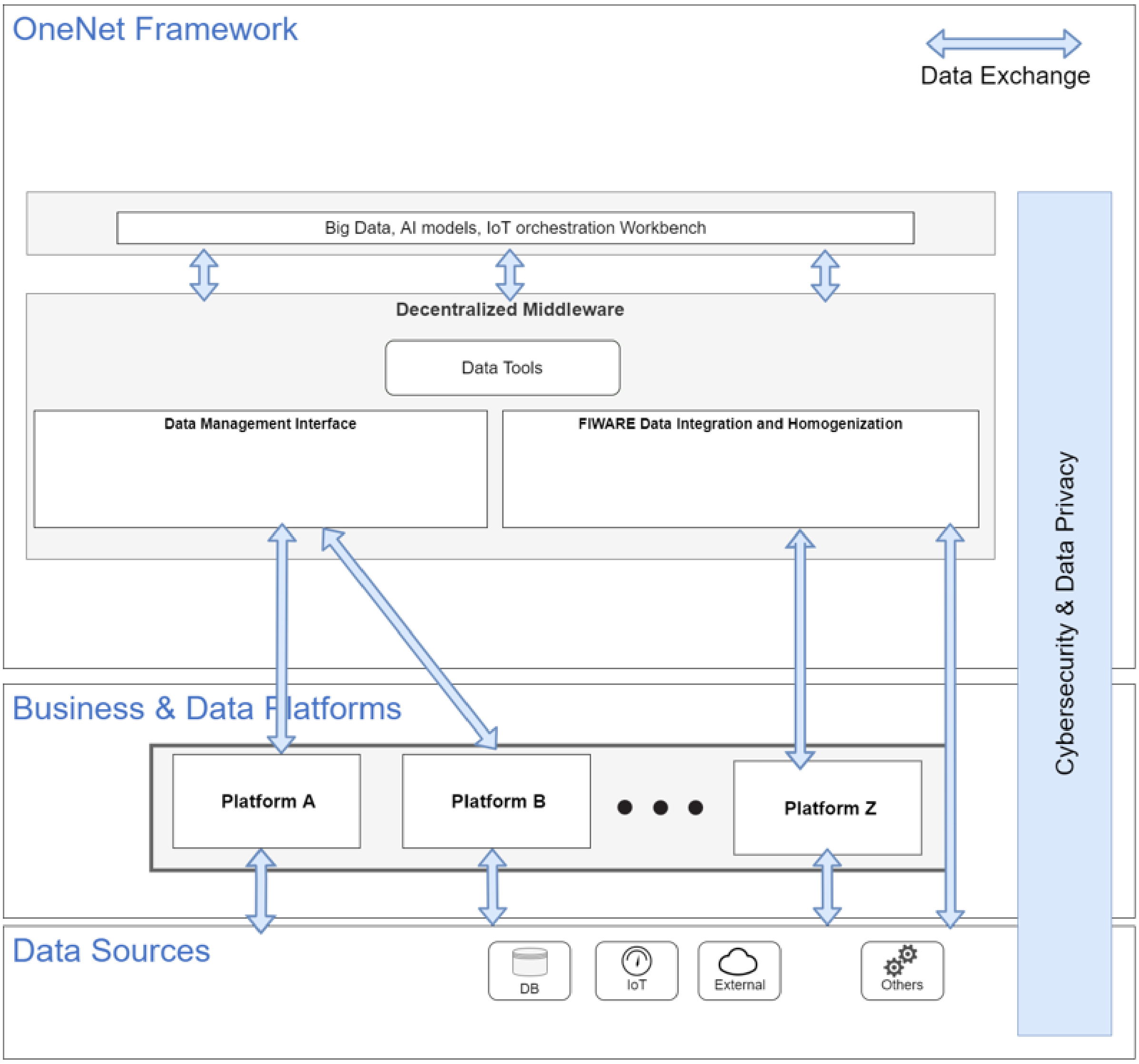

Figure 39: First draft of OneNet Architecture (v0.1)

OneNet Architecture v0.2 – It is the second intermediate version of the architecture. It includes: the first round of feedback from demo and technical partners; the results on the first analysis on the alignment of reference architectures and technologies that brought to the definition of the decentralised approach and the usage of Standard Data Architecture (IDS and FIWARE).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

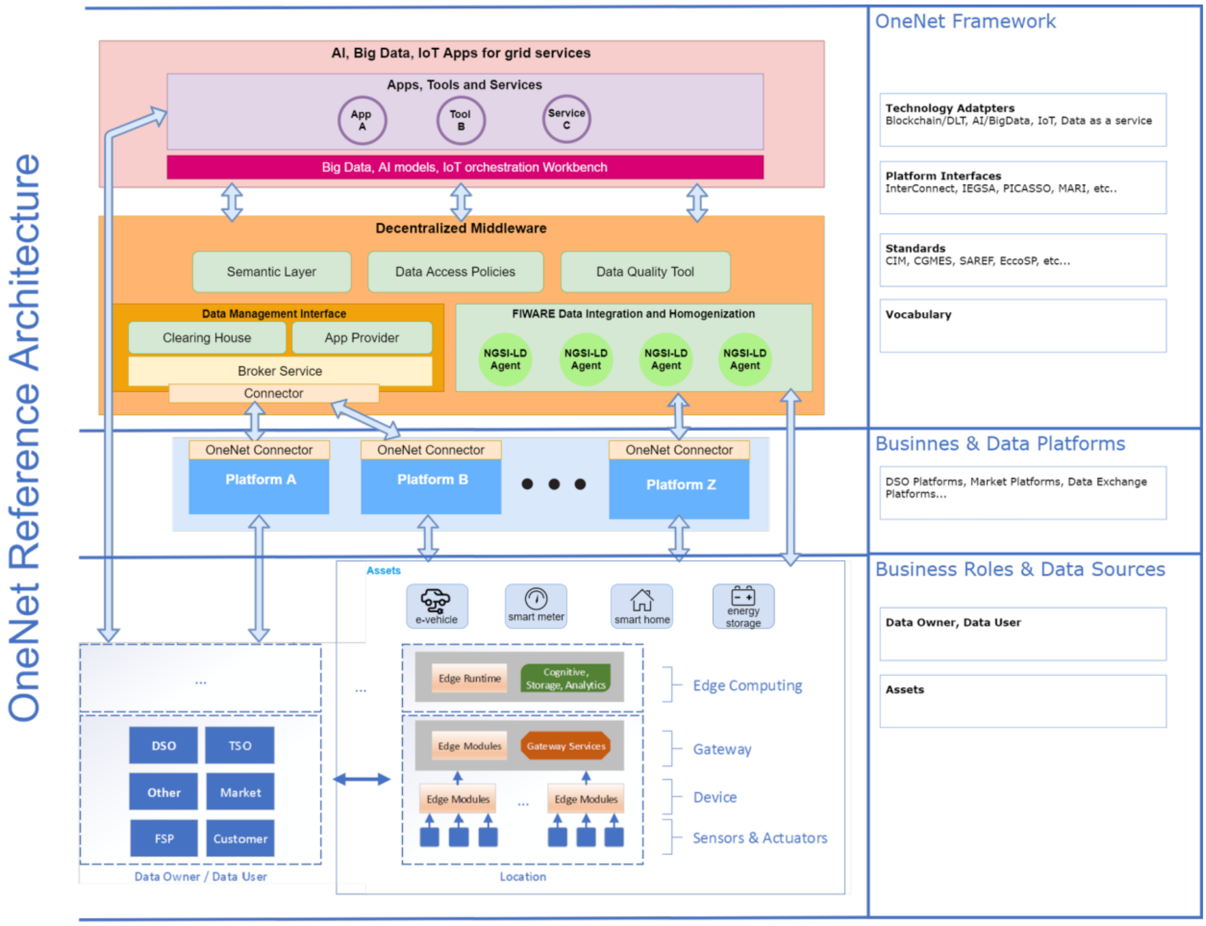

Figure 40: Intermediate draft of the OneNet Architecture (v0.2)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

5.3 GAP Analysis

5.3.1 GAPs between OneNet and the relevant projects

The objective of the OneNet project is not set to deliver a services platform but instead to create a platform to integrate existing ones. The relevant projects identified deal with interoperability between energy sector actors and so these interoperability achievements should be taken into consideration when creating the OneNet platform.

First, analysing the similarities between the preliminary versions of the OneNet RA and the results of the Bridge RA mappings analysis of the relevant projects (conducted in subchapter 3.3), the following similarities can be seen in Table 4:

Table 4: Similarities between OneNet RA and Bridge RA mapping of relevant projects

Business Layer	• Associations: FIWARE, IDSA • Roles: DSO, TSO, FSP, Data Owner, Data Provider, Data Consumer. • Processes: Data Governance, Big Data, Security/Privacy
Function Layer	• Data collection, Data Sharing, Data Certification, Anonymization, Erasure & rectification of private data (compliance with GDPR)
Information Layer	• Info Models: CIM, SAREF, NGSI-LD, CGMES
Communication Layer	• Protocols: REST APIs
Components Layer	• Data Exch. Platf.: DSO platforms, market platforms, data platforms, blockchain platforms, OneNet Framework Platform • Hardware: EV, Meter, Sensors, Energy Storage

Second, analysing the similarities and other specific features of the Bridge RA projects mappings and comparing them to the OneNet alignment (architecture and objectives), the following possible gaps on the SGAM layers can be seen in Table 5:

Table 5: Gaps between OneNet RA and Bridge RA mapping of relevant projects

Business Layer	• Association: GAIA-X • Roles: Aggregators, Local Energy Communities (LEC), Prosumers • Processes: VPP Operation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Function Layer	• Stakeholder Coordination/Communication (DSO-TSO-Services providers-customers)
Information Layer	• SARGON – ontology to extend SAREF to achieve better monitoring and controlling in applications to digitize Smart Grids and implement Building Automation projects • SPINE – Spine Toolbox is an open-source software to manage data, scenarios and workflows for modelling and simulation • UMEI – "UMEI is a set of evolving and universal rules that allow electricity systems to seamlessly interacting with flexibility markets […] The UMEI development will promote the standardization of an open and safe communication environment between Distribution System Operators (DSO), market agents as well as Transmission System Operator (TSO) platforms."
Communication Layer	• Protocols: MQTT/s and HTTP/s
Components Layer	• Secured Blockchain-driven Energy Markets • TSO platforms • Aggregator platforms • Flexibility platforms • VPP & LEC platforms • APPs: Weather Forecast, SO flexibility simulator

5.3.2 Comparisons of the OneNet Demos

Utilizing information gathered from the Clusters Demos Bridge RA mappings (section 3.4), this section will focus on identifying and comparing the different cluster's demos in order to find possible gaps that could be interesting to be addressed in OneNet.

Analysing the Demos mappings, the following similarities found in most of the demos can be seen in Table 6:

Table 6: Similarities between OneNet RA and OneNet Cluster Demos

Business Layer	• Regulations: GDPR • Associations: DSO Entity • Roles: MO, FSP

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

	• Processes: Data Analytics
Function Layer	• Prequalification, Flexibility Management, Data Collection, data sharing
Information Layer	• Info Models: CIM
Communication Layer	• Data formats: CSV, XML, JSON • Protocols: ICCP, Web-services
Components Layer	• Data Exch. Platf.: ECCo CP • APPs: SCADA • Hardware: Meters, sensors

Analysing the Clusters Demos Bridge RA mappings, these are all standards, protocols, and overall communication mechanisms being that the OneNet platform should be able to integrate:

- **Regulations:** GDPR, European Data Strategy, NIS, eIDAS
- **Info Models:** CIM, COSEM, UMEI, FIWARE
- **Data Models:** CGMES, ESMP, NWP
- **Protocols:** ICCP, Web-services, REST, HTTPS, MQTT, XMPP, AMPQ, JDBC, DLMS, ModbusTCP, EFI, FTP
- **APPs:** SCADA, Big Data tools, Privacy preserving tools, EMS, AMI, GIS, VPP, DMS

5.3.3 Architectures and Initiatives alignment

Using Relevant Reference Architectures and Data driven initiative models (descriptions made in sections 3.1 and 3.2) the OneNet alignment with these will be identified, further identifying components that OneNet could benefit from.

Relevant Reference Architectures:

The BRIDGE RA can be used as a relevant tool to help structure the OneNet project within the SGAM layers model. Many of such considerations are already being accounted in the project but some gaps can be related to:

- Facilitate regulation for cross-sector exchange of data
- Ensuring cooperation between appropriate associations to work on cross-sector and cross-border data management
- Harmonise data roles across electricity and other energy domains by developing HERM – Harmonised Energy Role Model.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- Create a central repository for roles used by the OneNet project
- Define and harmonise functional data processes for cross-sector domain.

COSMAG alignment with OneNet is relevant since it exploits and collects results of previous projects or standardization activities. It is a collection of specifications able to define any possible data exchange among all the possible energy actors (TSO, DSO, prosumers, aggregators, local markets). Several COSMAG recommendations are already being considered to be integrated in the OneNet project such as FIWARE and SAREF. However, a gap to have in mind, could be the integration of data platforms able to aggregate data (mainly on the customer level).

FIWARE is a working part of the OneNet project specifically in the Data Integration and Homogenization of OneNet, using the NGSI-LD agents to connect to the FIWARE context broker. These agents can translate IoT-specific protocols that can be used directly without the need for “OneNet connectors”.

ETIP SNET mentions interesting considerations that could be beneficial for the OneNet project such as using the OneNet platform to help asset planning and decommissioning, in cross-sector (between transmission and distribution level) and cross-border (limiting the decommissioning of assets beneficial to neighbouring Member States) coordination, in order to foster interoperability across markets and borders.

ETIP SNET warns about the cybersecurity level of equipment in use across the energy sector since a large part of the equipment today does not incorporate security measures that are required for connected electronic devices performing critical functions. This is part due to recommendations and guidelines being very general, not binding, and long waits at the national implementation level. It is suggested raising cybersecurity to minimum standard as a feature, for example adopting the ISO 27001 standard.

Data Driven Initiatives

The BDVA initiative aligns with OneNet in their vision to develop a pan-European data sharing space. It is clear that OneNet will need integrate a multi-country data sharing space in order to accomplish its vision. One of BDVA’s recommendations is a core of the OneNet architecture, which is the development of a trusted European data sharing framework and the offer of services and business opportunities to all the stakeholders of data space.

The BDVA reference model provides common reference framework for the application of Big Data technologies, and it has many similarities with the OneNet architecture such as focus on Data Management, Data Protection, Data Analytics, Data sharing platforms, Cybersecurity and Standardization.

Some of the gaps identified are technical challenges that might arise when implementing the OneNet architecture:

TC1. Sharing by design: Data life-cycle management that is not designed around sharing.

TC2. Digital Sovereignty: Enforcing data usage rights.

TC3. Decentralisation: Decentralised data sharing and processing architectures.

TC4. Veracity: Weak verification and provenance support.

TC5. Security: Secure data access and restrictions.

TC6. Privacy Protection: Maturity of privacy-preserving technologies for big data. "

The alignment of IDSA with the OneNet project is obvious with interoperability and connectivity between various different participants as a main focus. At the same time the IDSA initiative has a strong focus in data security, governance and trust. For this reason, the IDSA model and components are working parts in the OneNet architecture, specifically the Data Management Interface, where the IDS connector - the central technical component of IDS, and other components such as the broker service, clearing house and app provider are envisioned to be part of.

Similarly, to the BRIDGE RA, the IDSA initiative also lists and defines the roles of the participants in the data space in the IDS Data Governance Model, which outlines a decision-making framework regarding the definition, creation, processing, and use of data for the participants. This reinforces the idea that the same should be done for the participants and data processes in the OneNet system.

The GAIA-X architecture aligns with the core of the OneNet project on openness and transparency, interoperability, federation as well as authenticity and trust. Their services include Identity and Trust Services, Compliance Services, Federated Catalogues and Sovereign Data Exchange Services.

GAIA-X and IDS are a good fit for the data spaces ecosystem, since they complement each other. GAIA-X focuses more on sovereign cloud services and cloud infrastructure, while IDS focuses on data and data sovereignty. Their interaction focuses on self-sovereign data storage, trustworthy data usage and interoperable data exchange. A key element from the GAIA-X that could be considered for the OneNet Project could be the GAIA-X Federated Catalogue, which leverages the IDS Broker, Vocabulary Provider, and Information Model.

5.4 OneNet Reference Architecture v1

The OneNet Reference Architecture v1 is the first consolidated version of the architecture. Starting from the draft versions, it also includes: the definition of OneNet role and actors; the analysis of Demo and General System Use Cases as well as the requirements from D5.1; a final round of feedback from technical partners.

The analysis of IDS reference model and FIWARE interfaces, bring to a hybrid solution using both the standard models for implementing the OneNet Decentralized middleware and the OneNet Connector. The usage of IDS

Connector and FIWARE Context Broker was identified as the best solution to be adopted for ensuring a high level of standardization, interoperability, scalability and reuse of OneNet solution.

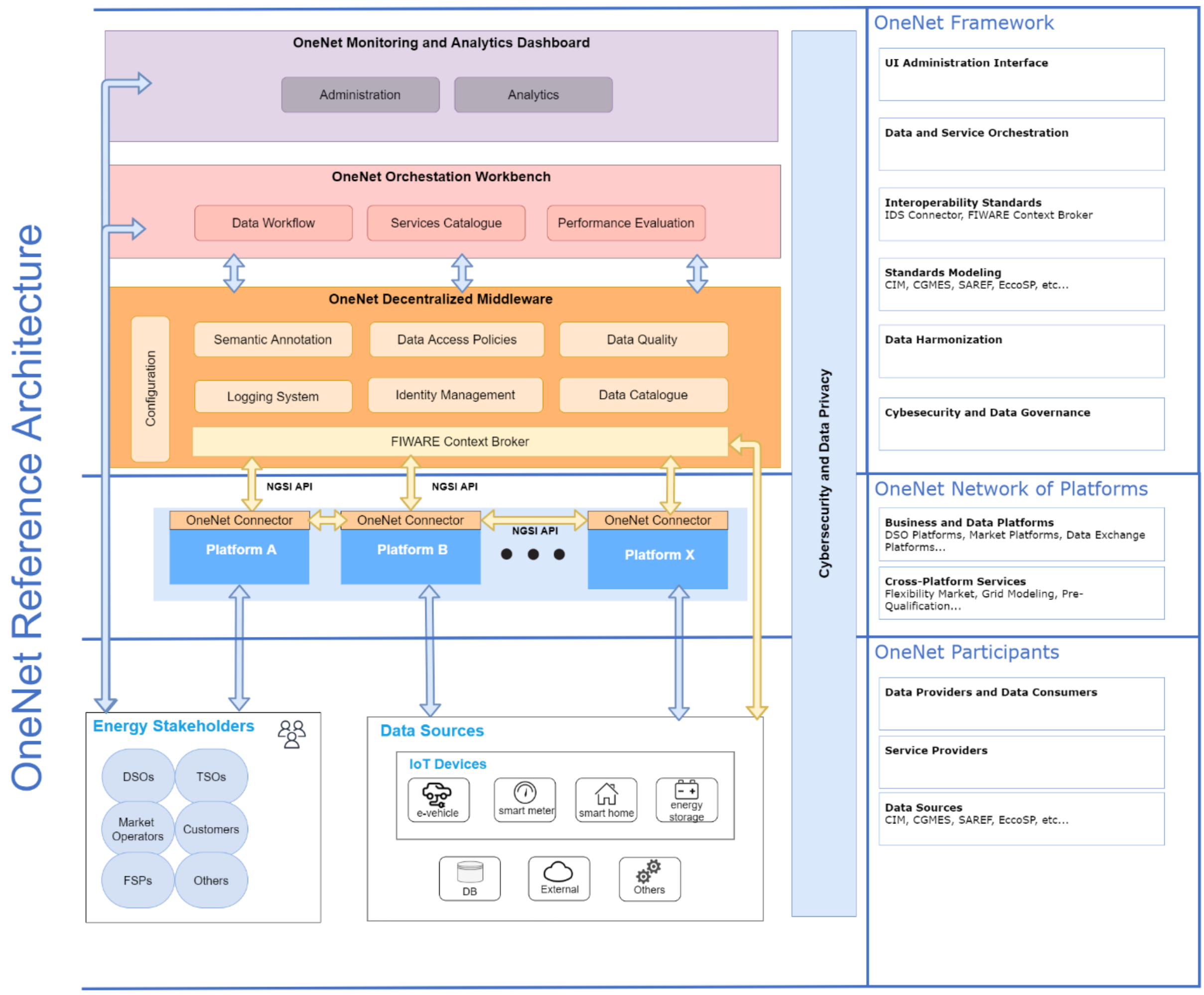

Figure 41: OneNet Reference Architecture v1

The OneNet Reference Architecture consists of three logical layers:

- the bottom layer includes data sources and energy stakeholders, the **OneNet Participants**;
- the middle layer is the one that in the OneNet ecosystem allows the creation of a **OneNet Network of Platforms** and includes all the platforms that participate in data exchange and the use of cross-platform services. In this layer there is the first component provided by OneNet, the OneNet connector;
- the top layer is the one properly defined as **OneNet Framework**. This is the core of the OneNet Architecture. It includes all the components that will be implemented in the reference implementation in WP6,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

as well as all the necessaries specifications for data harmonization, ontologies, data modelling, service orchestration, workflow monitoring, analytics, etc.
In the next paragraphs we will see more in detail how each single layer plays a fundamental role in the entire OneNet ecosystem.

5.4.1 OneNet Participants: Data Sources and Business Actors

The OneNet Participants layer includes all the actors and data sources involved in the OneNet system.

The Business Actors are named according to their business role, and this can be DSO, TSO, Market, FSP, Customer or others. Due to the focus of the architecture in the Data exchange, these actors can be further classified as Data Owner, User, Consumer, Provider, and others.

The list of Business Actors will be clearly identified in T5.3 following the analysis conducted in WP2, WP3 as well as the result of the information collected from the Demos in T5.1

The data sources refer to all the assets that produce or process data. These can be sensors, actuators, gateways, edge computing nodes and they can come from various energy sectors like electric mobility, energy storage and residential energy monitoring.

Following the Actors and Roles identified in the OneNet System Use Cases in D5.1 a OneNet Participant can be:

- **Data Source** is the more generic source of data that could be integrated within OneNet system. It could be represented by a Data Provider (see below), a single database, an IoT device, a file system etc.
- **Data Provider** is a specific OneNet participant that provide data to the system. To submit metadata to a Broker, or exchange data with a Data Consumer, the Data Provider uses software components (OneNet connector) that are compliant with OneNet System. To facilitate a data request from a Data Consumer, the Data Provider should provide proper metadata about the data the Broker Service Provider (see below).
- **Data Consumer** receives data from a Data Provider. From a business process perspective, the Data Consumer is the mirror entity of the Data Provider; the activities performed by the Data Consumer are therefore similar to the activities performed by the Data Provider. Before the connection to a Data Provider can be established, the Data Consumer can search for existing datasets by making an inquiry at Broker Service Provider. The Broker Service Provider then provides the required metadata for the Data Consumer to connect to a Data Provider.
- **Service Provider** is a specific OneNet participant that provides services or tools. The Service Provider registers its services in the OneNet Framework in order to be used, integrated and tested within any cross-platform integration or orchestration process.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

This layer is connected with the OneNet Network of Platforms layer since it represents the source of data for all the business and data platforms, as well as any integrable services or applications. It could be also directly connected to the OneNet Framework, since based on needs and requirements, there may be a need to integrate a data source directly into the OneNet Framework, using the OneNet Middleware and its interoperability mechanisms based on the FIWARE architecture and on the FIWARE Orion Context Broker.

Furthermore, the business actors will have the possibility to access the Orchestration Workbench for the evaluation and testing of apps, tools and services and the OneNet Monitoring Dashboard for exploiting monitoring and analytics features offered by the OneNet Framework.

5.4.2 OneNet Network of Platforms: Business and Data Platforms, Application, Services

The OneNet Network of Platforms layer focuses on the integration of external platforms, such as DSO platforms, Market platforms and other data exchange platforms into the OneNet system. This integration is to be made regardless of the technology of these platforms in order to remain platform-agnostic. From a technical point of view, the term platform means any software environment (e.g., applications, services or tools) able to connect with the OneNet Middleware using the OneNet Connector.

The main goal of this layer is to create a P2P **fully decentralised system for interoperability**. In such an infrastructure, two systems (OneNet Participants) can interact directly with each other, without intermediation by a third party. The results of this fully decentralised approach will create the OneNet Network of Platforms.

From the OneNet perspective, the more important component included in this layer is the OneNet Connector.

A **OneNet Connector** is a specific instance of the OneNet Decentralized Middleware, will be placed inside each platform and will allow an easy integration and cooperation among the platforms, maintaining the data ownership and preserving access to the data sources. The OneNet Connector is essential for connecting and integrating a platform within the OneNet ecosystem.

The OneNet connector will be developed following a decentralised approach, ensuring the necessary scalability for the near real-time data integration and management enabling multi-country and multi-stakeholder near real-time decision-making services. More details in the decentralised approach are described in the next chapter, Ch.5.3.3.1.

Based on the requirements analysed from D5.1, the OneNet connector will be based on IDS connector specification and will follow all the IDS specifications and requirements. Furthermore, the Broker included in the OneNet Connector will follow the FIWARE Context Broker specification.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The FIWARE context Broker will offer the FIWARE NGSI APIs and associate information model (entity, attribute, metadata) as the main interface for sharing data by the OneNet Participants. Data Providers will use the APIs to publish or to expose the data they offer, and Data Consumers will retrieve or subscribe (to be later notified) to the data offered.

5.4.3 OneNet Framework

The OneNet Framework is the core of the OneNet Architecture. This solution will be implemented in WP6 following the requirements and specification identified in WP5.

It consists of three main components: the OneNet Decentralized Middleware, the OneNet Orchestration Workbench and the OneNet Monitoring and Analytics Dashboard.

5.4.3.1 OneNet Decentralised Middleware

A significant part of the OneNet Interoperable Network of Platforms is a decentralized edge-level middleware which will be used as a middleware layer on top of the common IT infrastructure enabling the exchange of information between all assets and other various components that will be integrated in OneNet network. But what exactly constitutes an edge-level middleware?

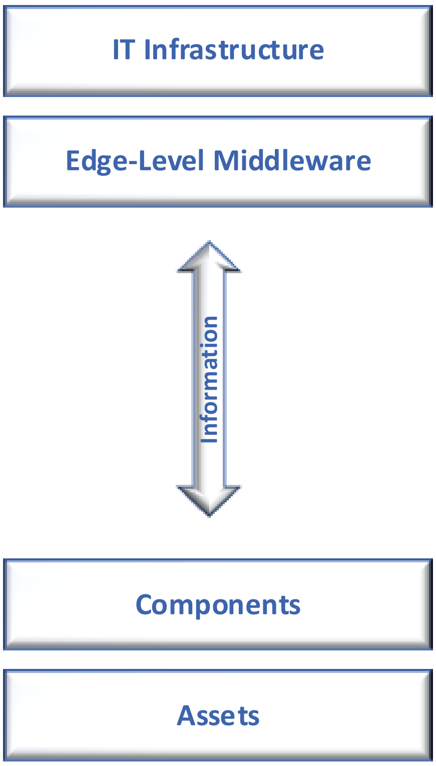

Figure 42: Middleware Concept

One of the most widespread concepts of our era is the Internet of Things paradigm. IoT integrates edge devices via Internet providing a plethora of applications. In recent years, the number of connected devices has grown significantly, along with the volume and variety of data that is being generated by these devices at the edge of the network [35] . An edge-based middleware is a software application that serves as an interface or message bus between IT resources and IoT devices/sensors enabling communication between components. Thus, an edge-based (or edge-level) middleware is required to provide the necessary functional components for sensor registration, discovery, workflow composition, and data pre-processing. The importance of this

paradigm in conjunction with the necessity of these applications and the new technical capabilities in our disposal, result in a landscape of edge middleware platforms which is growing exponentially, with different platform requirements, architectures, and features.

Implementations wise the edge-level middleware will rest on three pillars:

- A suitable common data model so that all data and request types can be satisfied, whether they come from data writers or data readers.
- A set of clearly defined QoS low-level tasks, such as discovery, reliability, security, discovery, performance, accessibility, ACID transaction etc.
- Basic middleware interfaces/modules

○ Data management interface between involved actors.

○ Semantics layer interface which will provide information on the definition of data sharing requirements and how these will be implemented in system components.

Based on the analysis of similar projects performed in WP4 in conjunction with the BUCs collection (WP2) and the work performed (so far) in other tasks of WP5, a comprehensive catalogue of services, actors, roles and business objects is being built up. Such catalogue will feed WP5 in order to create the definitive cross-platform services catalogue, the appropriate semantic models and the categories of shareable data needed for a standardized data exchange. This information along with functional requirements influences the reference architecture and participates in the step-wise approach of middle-ware development.

Methodologically our approach will be step wise, based on OneNet reference architecture, generic edge-level middleware architectures and best practices:

- **Step 1: Development of Semantic models**

During this step necessary semantic models (conceptual data model which includes semantic information) will be developed in order to assist the IT systems of stakeholders with the interpretation of the exchanged information between organizations and to invoke action of these systems, if applicable. Taking into account from current demo SUCs the actors, roles, business objects etc. WP5 will conclude to a harmonized model that serves

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

their needs and that will facilitate the exchange of information between them in a homogeneous form and content.

- **Step 2: Categorization of sharable data**

Sharable data will be classified in unstructured (text data), semi-structured (e.g., XML/JSON formalized data) and structured (e.g., data in the operators' Data Hubs and Energy Data Management Systems).

- **Step 3: Data exchange**

Based on a data-driven development of semantic models and sharable data categorization we implement an improved data exchange.

- **Step 4: Development of added value services**

The added value services which will be developed will support and build upon the semantic models and shall include data quality checking, data consolidation and aggregation.

- **Step 5: Development of semantic interoperable framework**

A framework for orchestrating semantic interoperability e.g., based on the International Data Spaces for data sharing will be generated to describe the data exchange interfaces for read/write access and import/export of available data and output analytics. A common edge-middleware architecture approach (edge-to-edge) comprising of four separate layers (resource management, data processing, service, and security) can be visualized as follows:

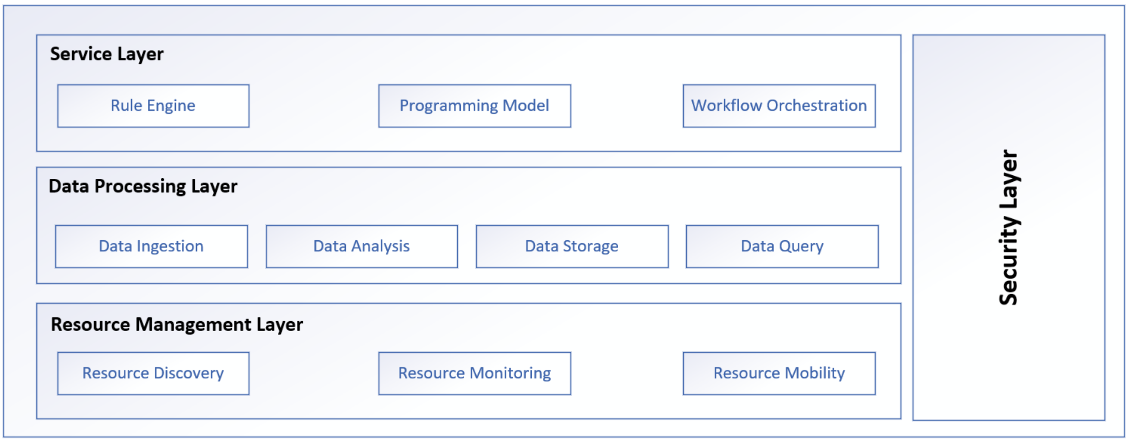

Figure 43: Edge Level Middleware Architecture [35]

1. The resource management layer is responsible for the discovery, identification, and allocation of available resources. The end goal of the resource management layer is to manage these limited and geo-distributed resources in an efficient manner. The resource management layer consists of the following components: resource discovery, resource monitoring, and resource mobility.

2. The data processing layer consolidates data from multiple data owners, along with basic wrangling and delivery functionality. The data processing layer consists of four components: ingestion, analysis, storage, and query.

3. The service Layer defines an application's set of available functionalities to the end user. The service layer is composed of three components: rule engine, programming model, and workflow orchestrator.

Based on OneNet RA, general considerations regarding potential cloud-centric platform capabilities instead of edge-to-edge and Dataspace implementation approach will differentiate the architecture (e.g., Context Broker component will be responsible for Resource management).

OneNet Decentralised Approach

First, we start with a definition of "Scalability". Neuman defines [36]: "A system is said to be scalable if it can handle the addition of users and resources without suffering noticeable loss of performance or an increase in administrative complexity."

In this part, we propose a decentralised scalable Peer-to-Peer architecture. The number of data providers /consumers and spatial data sources (e.g., geo-sensor networks) increases rapidly.

Scalability is challenging for today's Internet-connected architectures. From literature and existing systems, there are mainly two types of architectures: (1) Client-Server (C/S) architecture, and (2) Decentralized architecture. Both architectural designs have centralized components, i.e., the central server of the C/S and the central directory/registry of the Decentralized systems [2]. When a system shall scale in users and data sources, its centralized components make the system unreliable in that they are single points of failure. They also become system performance bottlenecks in that all additional system loads are added to the central components [37]. Furthermore, they result in poor flexibility of administration because the system is controlled by the providers of central components. For the above reasons, we need a "fully" decentralized – a "distributed" -architecture without any central components.

Our goal is to find a P2P architecture that is applicable and useful to build a distributed (i.e. fully decentralized) system for interoperability. In such an infrastructure, two individuals can interact directly with each other, without intermediation by a third party. The figure presents the first result of OneNet fully decentralised architecture, where the OneNet connector opens a channel to an interoperable network for data providers and consumers.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

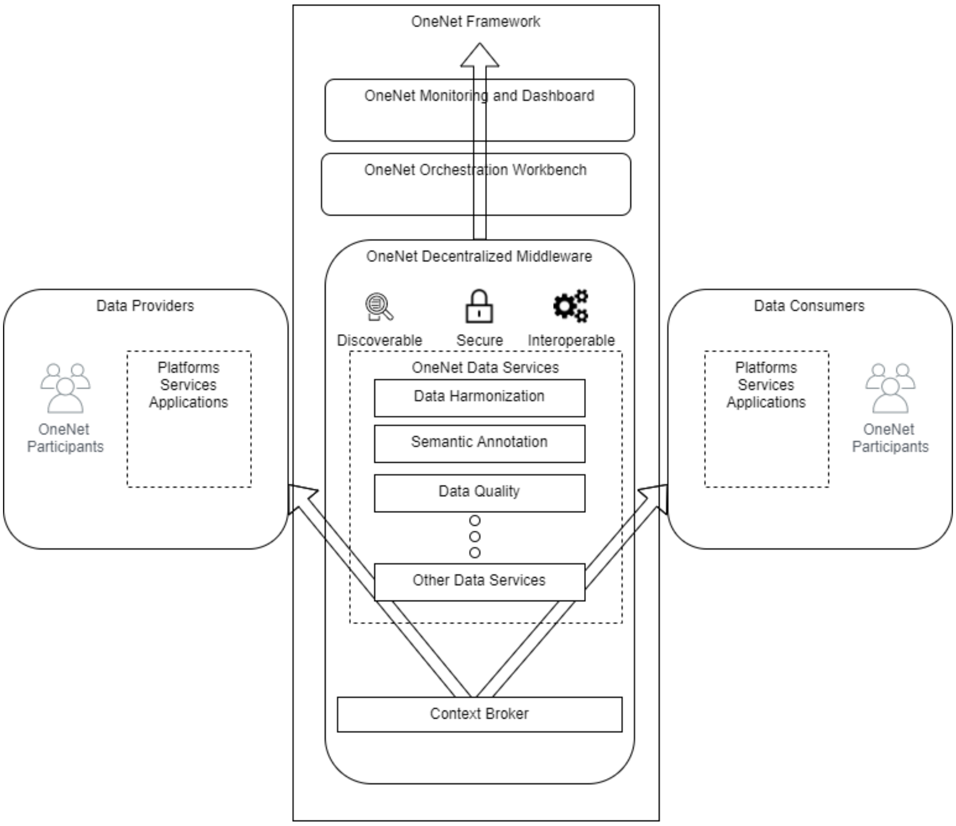

Figure 44: OneNet Interoperable Network Concept

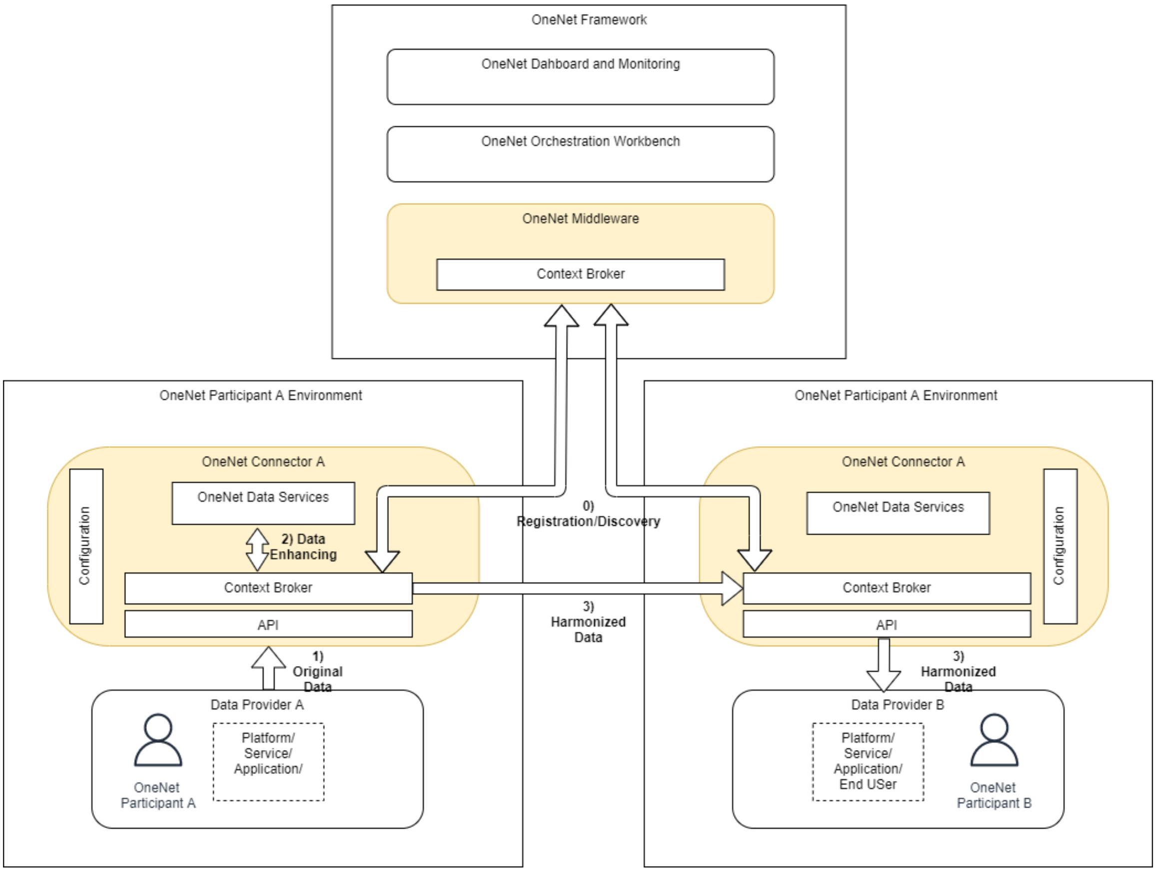

Figure 45: OneNet Decentralised approach

OneNet Connector – IDS and FIWARE specifications

One important parameter for a Reference Architecture design and implementation is the adoption of best practices and initiatives within the European (or Global) community such as the Data Spaces. A **Data Space** [38] refers to a decentralized data ecosystem built around commonly agreed Building Blocks (components) enabling an effective and trusted sharing of data among participants. From a technical perspective, a number of technology Building Blocks are required ensuring:

- Data interoperability. Data Spaces should provide a solid framework for an efficient data exchange among ecosystem participants, supporting full decoupling of data providers and consumers. This requires the adoption of a common language between uses, materialized in the adoption of common APIs for the data exchange, and the definition of common data models. Common mechanisms for traceability of data exchange transactions and data provenance, are also required.
- Data sovereignty and trust. Data Spaces should verify that participants in a Data Space can trust each other and exercise sovereignty over data they share. This requires the adoption of common standards for

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

managing the identity of participants, the verification of their truthfulness and the enforcement of policies agreed upon data access and usage control.

- Data value creation. Data Spaces should provide support for the creation of multi-sided markets where participants can generate value out of sharing data (i.e., creating data value chains). This requires the adoption of common mechanisms enabling the definition of terms and conditions (including pricing) linked to data offerings, the publication and discovery of such offerings and the management of all the necessary steps supporting the lifecycle of contracts that are established when a given participant acquires the rights to access and use data.

Based on the above, a fundamental component of the OneNet Network of platforms will be the one which facilitates trusted data exchange among participants, so that the participants involved in the data exchange are verified, and that the data exchange adheres to agreed rules.

Therefore, the OneNet platform should make sure that data providers and data consumers can rely on the identity of the members of the data ecosystem between different security domains. The IDS Connector as described in the IDS Reference Architecture Model (RAM) [32] adopts this logic. FIWARE [39] Community has incubated an open-source implementation of this technology that has already been tested how it can integrate with the rest of core FIWARE components.

IDSA is providing several architecture components necessary to create data spaces with trust and data sovereignty being some of the most important aspects. These are necessary but not sufficient to create real living data spaces which are accepted and adapted on the market. Standard APIs, standard data models as well as marketplace functionalities are also necessary. The complementarities of both initiatives regarding technology building blocks are illustrated in below image. As the FIWARE Context Broker technology was adopted in 2019 as one of the Building Blocks of the Connecting Europe Facility (CEF) program and has proven to integrate smoothly with other relevant CEF Building Blocks for the creation of Data Spaces (e.g., eIDAS, EBSI), this allows the alignment between these initiatives. Integration between FIWARE and IDSA is guaranteeing the aligned contribution of both ecosystems to the success of data spaces and can be a contributing factor to OneNet implementation (relying on open-source implementation of the IDS Architecture based on Fiware enablers, compatible with Fiware Architecture principles).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

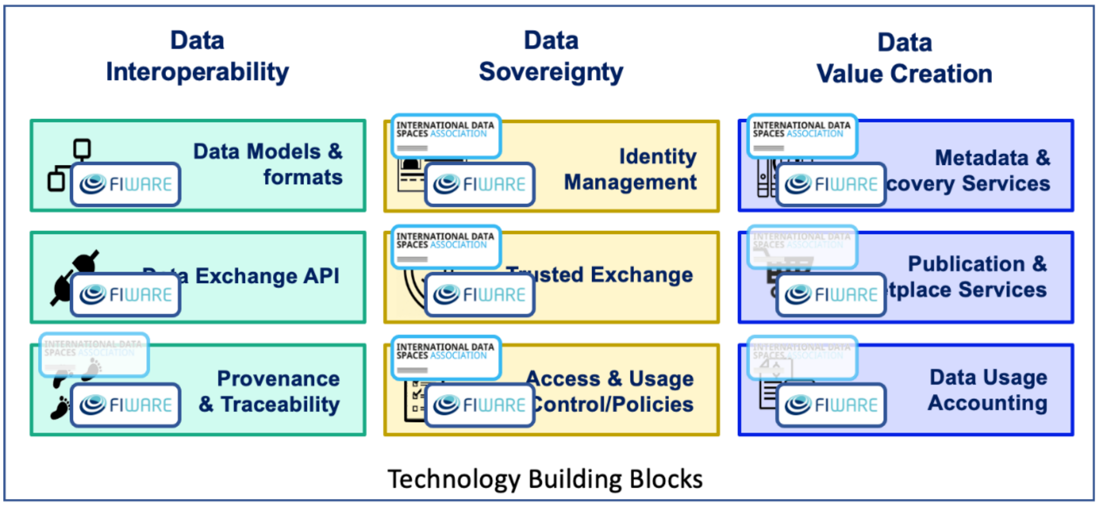

Figure 46: IDSA and FIWARE positioning to create Data Spaces [38]

In the below image we can see how an AI service provider application and an AI service consumer application, each hosted in different organizations and participating in a common Data Space "powered by FIWARE", may interact with each other. It shows the role of components that are part of the incubated FIWARE IDS Connector implementation and their integration with other FIWARE components.

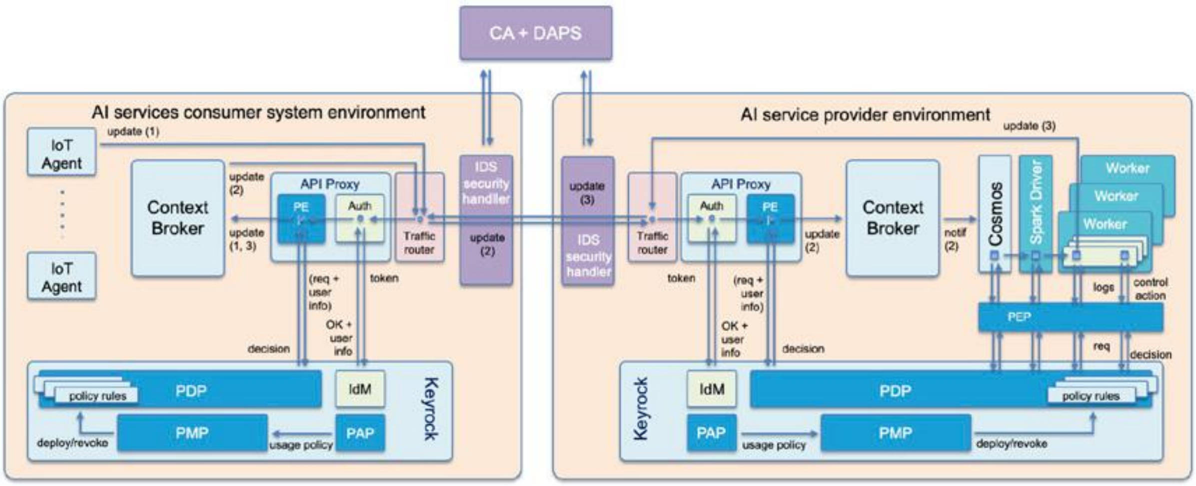

Figure 47: Integration of FIWARE IAM and IDS Connector functionalities [38]

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Another approach for IDS Connector implementation using FIWARE is visualized in the below image which is presenting how a data exchange (end to end communication) between a Data Provider and Data Consumer can be achieved through dedicated connectors.

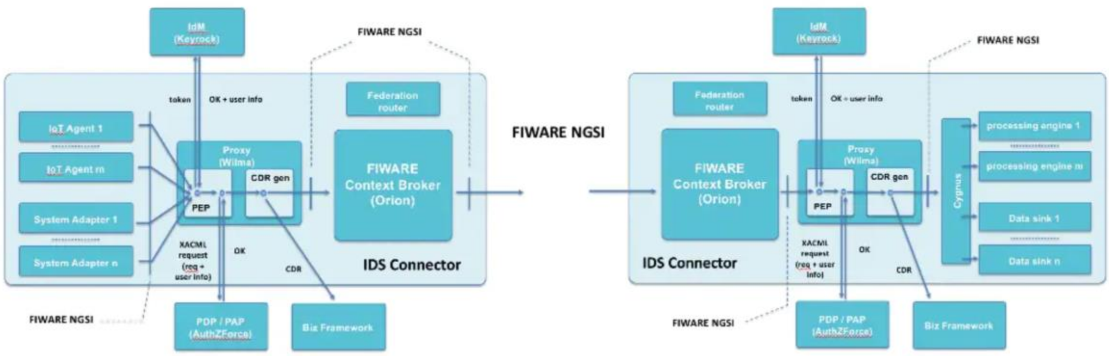

Figure 48: IDS/FIWARE End to End Communication [40]

OneNet Data Services

The integration of services from different providers using different data formats hinders interoperability; a secure and trustworthy data exchange is needed to preserve the rights of beneficiaries on the shared data.

To provide interoperability, a series of data services are expected that enable simpler interoperability between disparate information systems. The main objective of these services is to receive transactions from a different platform, application, or device, coordinates the interaction between them, and to provides common core functionality to simplify the data exchange between systems.

The main function of data services is to allow disparate smart energy information systems to share information more easily. This means that it should handle the common, mundane tasks such as logging and security and performs message transformations such that systems may communicate with it in a native messaging format.

At its core, the interoperability data services should provide a single point of entry into the services of the smart energy system. It can be powered by AI-based algorithms to log/audit messages and handle authentication and authorization and the routing of data to the correct service provider. In addition, it may provide additional mediation functions for transactions within the smart energy system in an attempt to simplify the business logic required by service consumer systems to interact with the smart energy system. These functions may include mediation tasks such as the transformation of messages and message orchestration.

Furthermore, interoperability data services can rely on the semantic-based approach to produce a harmonized data network and enable connectivity of the existing data providers/consumers in the smart energy system

5.4.3.2 OneNet Orchestration Workbench

OneNet Orchestration Workbench is one of the core components of the OneNet Framework. It acts as a data orchestrator to evaluate the performance and scalability of the cross-platform services that aims to use near real-time IoT metering and Big Data at consumer and/or network level.

Any OneNet Participant and in particular the Service Providers will be able to test and evaluate its own service exploiting the OneNet Orchestration Workbench, that allows to integrate data coming from the OneNet Middleware and to implement a data pipeline orchestration.

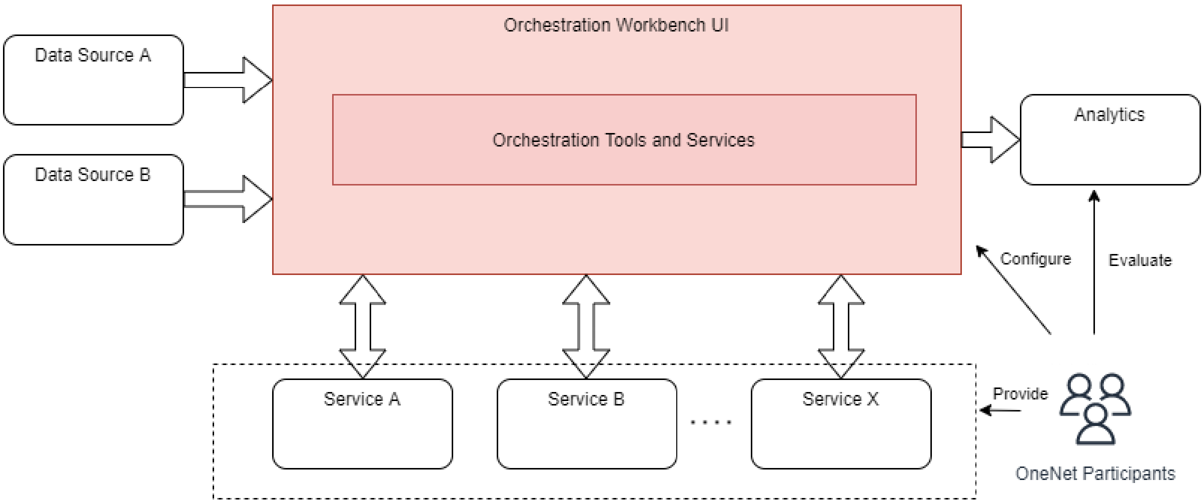

Figure 49: OneNet Orchestration Workbench Concept

The OneNet Orchestration Workbench will also include a series of tools and services:

- Graphical User Interface
- Job Scheduling
- App/Service registry and discovery
- Error/Retries management
- SLAs tracking, alerting and notification

5.4.3.3 OneNet Monitoring and Analytics Dashboard

Several features offered by OneNet Framework need a direct user interaction and following the requirements collected in D5.1, the OneNet system should implement a GUI for facilitating the OneNet Participants in the management, monitoring and analytics of the data transactions.

This component is foreseen on top of the architecture and should provide UIs to all the OneNet components.

Main features of the OneNet Monitoring and Analytics should be:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- administrative and configuration tools;
- easy integration with the OneNet Orchestration Workbench and OneNet Middleware;
- data-analytics dashboard;
- monitoring and alerting dashboard for data processes and platform integrations;
- user-friendly selection of data sources and services from the catalogues;

5.4.3.4 Cybersecurity and Data Privacy

The analysis of the result of the D5.1 in terms of security and data privacy clearly describes the need to have a specific component for addressing these aspects. In particular, the OneNet non-functional requirements provides the references for the implementation of this component.

As detailed in Ch.4.2, the Cybersecurity and Data Privacy components must:

- Ensuring the security and privacy of data exchanged;
- Tracking all the data processes and flows;
- Ensuring that all the processes can be uniquely identified and related to a specific user;
- Providing a testing environment to identify and solve potential security breaches;

Furthermore, according to results described in the D5.8, pan-European innovation in grid operations creating a Decentralised Network of Platforms is a complex technical challenge, which requires special attention to cybersecurity, privacy and regulatory requirements.

The D5.8 provides a series of guidelines and recommendation for addressing cybersecurity and data privacy challenges. In terms of data privacy, the principles of GDPR must be followed, especially so when dealing with customer data and other personally identifiable information. Also, data controller obligations and data subject's rights in terms of GDPR have been reviewed and must be considered. In addition, from ethics perspective, collection and processing of personal data should be non-invasive.

In terms of security, comprehensive requirements provided in NISTIR 7628 are recognized as the most relevant guidelines for going forward with OneNet project. Based on this, more detailed recommendations and suggestions have been provided, also taking into account SGIS report, ENISA cybersecurity guidelines for smart grids and OWASP ASVS security verification standard.

The work conducted in T5.8 will be extended in T4.4, in which a complete list of cybersecurity, data privacy and regulatory requirements will be provided. These requirements will be integrated which non-functional

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

requirements collected in T5.1 and used for the implementation of the Cybersecurity and Data Privacy component in T6.6.

6 Conclusions

The work done at this stage, allowed to have a complete overview of the characteristics of the OneNet System and to design the first version of the OneNet Reference Architecture.

The mapping of the architectures of the other projects together with which of the OneNet demos using the Bridge Reference Architecture model was important for identifying the similarities and the differences among the results already achieved and what will be used within the OneNet project. These results will also be used in the other tasks of the WP5 for defining the functional and technical specifications and identifying data standards, ontologies, communication protocols and others interoperability building blocks that need to be considered in the OneNet implementation phase.

Through the analysis of the relevant reference architectures and data-driven initiatives, was identified fundamental characteristics, specifications, and challenges to be addressed in the OneNet Architecture.

More in detail, it's clear from the analysis that the decentralisation, the harmonization of data processes, the security and the data governance, play a fundamental role in the creation of a pan-European solution for the cross-countries and cross-stakeholder cooperation and integration.

For the implementation of the OneNet Decentralised Middleware and OneNet Connector the usage of the IDS Reference Architecture Model and FIWARE Context Broker was identified as the best solution to be adopted for ensuring a high level of standardization, interoperability, scalability and reuse of OneNet technologies.

The OneNet Reference Architecture takes into account all the results of this analysis as well as the requirements and the overall concepts defined in D5.1. It will be the base for the implementation phase and the integration within the demo sites architecture. Each demo site will integrate, test, and evaluate the OneNet System. The iterative approach will allow us to learn from the implementation, execution, and evaluation phase, enriching and improving the OneNet Reference Architecture throughout the project.

Furthermore, the Openness of the OneNet Reference Architecture will support a better outreach, adoption and re-use of the results as well as an increment of the impact of the OneNet project on the scientific community and in particular on the energy stakeholders.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

7 References

[1] «BRIDGE EU initiative,» [Online]. Available: https://www.h2020-bridge.eu/.

[2] «BRIDGE - Data Management Working Group - EU Reference Architecture,» [Online]. A
https://ec.europa.eu/energy/sites/default/files/documents/bridge_wg_data_management_eu_reference_architcture_repo
2021.pdf.

[3] E. Union, «Clean Energy for all Europeans,» 2019. [Online]. Available: https://op.europa.eu/en/pu
en?WT.mc_id=Searchresult&WT.ria_c=null&WT.ria_f=3608&WT.ria_ev=search.

[4] E. Commission, «Electricity network codes and guidelines,» [Online]. Available: https://ec.europa.eu/energy/en/topics/marl

[5] «The SmartNet project,» [Online]. Available: http://smartnet-project.eu/.

[6] «The CoordiNet project,» [Online]. Available: https://coordinet-project.eu/projects/project.

[7] «SmartNet Project - D1.3,» [Online].

Available: http://smartnet-project.eu/wp-content/uploads/2016/12/D1.3_20161202_V1.0.pdf.

[8] «Finesce project,» [Online]. Available: http://www.finesce.eu/.

[9] F. Project, «API documentation,» [Online]. Available: http://finesce.github.io/api_table.html.

[10] «Universal Smart Energy Framework,» [Online]. Available: https://www.usef.energy/.

[11] «The NobelGrid project,» [Online]. Available: https://nobelgrid.eu/.

[12] «Universal Smart Energy Framework,» [Online]. Available: https://www.usef.energy/.

[13] IEC, «IEC PAS 62746-10-1:2014 Withdrawn - Systems interface between customer energy management system and the powe
2.0b Profile Specification),» 19 02 2019. [Online]. Available: https://webstore.iec.ch/publication/7570&preview=1.

[14] C. a. T. (. C. ,. D.-G. ,. E. ,. T. Directorate-General for Communications Networks, «Study on ensuring interoperability for enab

[15] «The eDREAM project,» [Online]. Available: https://edream-h2020.eu/.

[16] C. Pop, M. Antal e T. Cioara, «5.2 Self-enforcing smart contracts for DR tracking and,» 2019.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

[17] E. Commission, «COSMAG - Background Document on big data and energy,» [Online]. Available: http://ec
background_document_on_big_data_and_energy_en.pdf.

[18] D. Bees, L. Frost, M. Bauer, M. Fisher e W. Li, «ETSI White Paper. NGSI-LD API:
https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp31_NGSI_API.pdf.

[19] «FIWARE GitHub Repository,» [Online]. Available: https://github.com/Fiware/catalogue.

[20] A. Tejado, «FIWARE Go-to-market strategy Y2,» 2018. [Online]. Available: https://ec.europa.eu/research/participants/docur

[21] «https://www.iea.org/reports/digitalisation-and-energy,» [Online]. Available: https://www.iea.org/reports/digitalisation-an

[22] E. SNET, «Position Paper - Smart Sector Integration, towards an EU System of Systems - Building blocks, enablers, archite
https://www.etip-snet.eu/wp-content/uploads/2021/03/ETIP-SNET-PP-Sector-Coupling-towards-an-EU-System-of-Systems-

[23] E. SNET, «White Paper - ETIP SNET Holistic Architecture,» March 2019. [Online]. Available: https://www.etip-snet.eu/wp-co

[24] A. S. D.-L. Ilo, A Holistic Solution for Smart Grids based on LINK– Paradigm, Springer, 2021.

[25] B. D. V. Association. [Online]. Available: https://www.bdva.eu/about.

[26] B. D. V. Association, «Big Data Value Public-Private Partnership,» [Online]. Available: https://www.bdva.eu/PPP.

[27] B. D. V. Association, «TOWARDS A EUROPEAN-GOVERNED DATA SHARING SPACE - Enabling data
https://www.bdva.eu/sites/default/files/BDVA%20DataSharingSpaces%20PositionPaper%20V2_2020_Final.pdf.

[28] B. D. V. Association, «BDV SRIA - European Big Data Value - Strategic Research and Innovation Agenda,» 10 2017. [Online]. A

[29] ISO, «ISO/IEC 20547-3:2020 - Information technology — Big data reference architecture — Part 3: Reference architecture,»

[30] IDSA, «IDSA,» [Online]. Available: https://internationaldataspaces.org/.

[31] IDSA, «IDSA publications,» [Online]. Available: https://internationaldataspaces.org/publications/most-important-document

[32] IDSA, «Reference Architecture Model,» April 2019. [Online]. Available: https://internationaldataspaces.org/wp-content/upl

[33] «GAIA-X: Driver of digital innovation in Europe,» [Online]. Available: https://www.data-infrastructure.eu/GAIAX/Navigation/

[34] IDSA, «GAIA-X and IDS - Position Paper,» 01 2021. [Online]. Available: https://internationaldataspaces.org/wp-content/uplo

[35] D. B.-T. M. P. EDUARD GIBERT RENART, «Challenges in designing edge-based middlewares for the Internet of Things,» Rutge

[36] S. e. a. Ratnasamy, «A scalable content-addressable network.,» *Proceedings of the 2001 conference on Applications, technol*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

[37] B. C. Neuman, «Scale in Distributed Systems,» in *Readings in Distributed Computing Systems*, IEEE Computer Society Press, 1

[38] FIWARE, «FIWARE for Data Spaces Position paper,» 2021.

[39] FIWARE, «Fiware Community,» [Online]. Available: https://www.fiware.org/.

[40] C. F. F. Juanjo Hierro, «FIWARE Global Summit - FIWARE Implementation of IDS Reference Architecture Concepts,» 15 M summit-fiware-implementation-of-ids-reference-architecture-concepts .

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

This paper reflects only the author's view and the Innovation and Networks Executive Agency (INEA) is not responsible for any use that may be made of the information it contains.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739