HEDGE-IoT

Holistic approach towards Empowerment of the Digitalization of the Energy Ecosystem through adoption of IoT solutions

D2.3
HEDGE-IoT Reference Architecture (First Release)

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

DOCUMENT CONTROL SHEET

PROJECT INFORMATION

Project Number	101136216		
Project Acronym	HEDGE-IoT		
Project Full title	Holistic Approach towards Empowerment of the Digitalization of the Energy Ecosystem through adoption of IoT solutions		
Project Start Date	01 January 2024		
Project Duration	42 months		
Funding Instrument	Horizon Europe Framework Programme	Type of action	HORIZON-IA HORIZON Innovation Actions
Call	HORIZON-CL5-2023-D3-01-15		
Topic	Supporting the green and digital transformation of the energy ecosystem and enhancing its resilience through the development and piloting of AI-IoT Edge-cloud and platform solutions		
Coordinator	European Dynamics Luxembourg SA		

DELIVERABLE INFORMATION

Deliverable No.	D2.3							
Deliverable Title	HEDGE-IoT Reference Architecture (First Release)							
Work-Package No.	WP2							
Work-Package Title	Stakeholders' Requirements and System Specifications							
Lead Beneficiary	ED							
Main Authors	ED, TRIALOG							
Other Authors	ICCS, INESC, TNO, TAU, VTT, NESTER, IDSA, ABB, PPC, HEDNO, IPTO, HENEX, ARETI , APIO, AB, SONAE, OPR, JSI, KONC							
Due date	30/06/2025							
Deliverable Type	X	Document, Report (R)		Data management plan (DMP)		Websites, press & media action (DEC)		Other
Dissemination Level	X	Public (PU)		Sensitive (SEN)		Classified		
	PU: Public, fully open SEN: Sensitive, limited under the conditions of the Grant Agreement Classified R-UE/EU-R – EU RESTRICTED under the Commission Decision No2015/444 Classified C-UE/EU-C – EU CONFIDENTIAL under the Commission Decision No2015/444 Classified S-UE/EU-S – EU SECRET under the Commission Decision No2015/444							

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Document Revision History

Version	Date	Description of change	List of contributor(s)
0,1	16/08/2024	Table of Contents of Document	ED
0.2	02/12/2024	First Draft Literature Review	ED, EDAT, RWTH, ICCS, INESC, TAU, TRIALOG, IDSA, TUC, KONC
0.3	24/12/24	Added Draft Chapters 1-3	ED
0.5	02/06/25	Finalized Contributions from Partners in all Sections	ED, EDAT, RWTH, ICCS, INESC, TAU, TRIALOG, IDSA, TUC, KONC
0.6	18/06/25	Consolidation of Final Draft	ED
1.0	02/07/2025	Reviewed by WP leader	ED
1.1	08/07/2025	Reviewed and commented by appointed reviewers	IDSA, DST
1.2	10/07/2025	Final Draft for Submission	ED

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

PARTNERS

Participant number	Participant organisation name	Short name	Country
1	EUROPEAN DYNAMICS LUXEMBOURG SA	ED	LU
2	RHEINISCH-WESTFAELISCHE TECHNISCHE HOCHSCHULE AACHEN	RWTH	DE
~~3~~	~~ENGINEERING INGEGNERIA INFORMATICA SPA~~	~~ENG~~	~~IT~~
4	EREVNITIKO PANEPISTIMIAKO INSTITOUTO SYSTIMATON EPIKOINONION KAI YPOLOGISTON	ICCS	EL
5	INESC TEC - INSTITUTO DE ENGENHARIADE SISTEMAS E COMPUTADORES, TECNOLOGIA E CIENCIA	INESC	PT
6	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO	TNO	NL
7	TAMPEREEN KORKEAKOULUSAATIO SR	TAU	FI
8	TEKNOLOGIAN TUTKIMUSKESKUS VTT OY	VTT	FI
9	TRIALOG	TRIALOG	FR
10	CYBERETHICS LAB SRLS	CEL	IT
11	CENTRO DE INVESTIGACAO EM ENERGIA REN - STATE GRID SA	NESTER	PT
12	INTERNATIONAL DATA SPACES EV	IDSA	DE
13	ELIA TRANSMISSION BELGIUM	ETB	BE
14	HRVATSKI OPERATOR PRIJENOSNOG SUSTAVA D.D.	HOPS	HR
15	UNIVERSITATEA TEHNICA CLUJ-NAPOCA	TUC	RO
16	CLUSTER VIOOIKONOMIAS KAI PERIVALLONTOS DYTIKIS MAKEDONIAS	CLUBE	EL
17	F6S NETWORK IRELAND LIMITED	F6S	IE
18	SOCIAL OPEN AND INCLUSIVE INNOVATION ASTIKI MI KERDOSKOPIKI ETAIREIA	INCL	EL
19	ABB OY	ABB	FI
20	ENERVA OY	ENERV	FI

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

21	JARVI-SUOMEN ENERGIA OY	JSE	FI
22	DIMOSIA EPICHEIRISI ILEKTRISMOU ANONYMI ETAIREIA	PPC	EL
23	DIACHEIRISTIS ELLINIKOU DIKTYOU DIANOMIS ELEKTRIKIS ENERGEIAS AE	HEDNO	EL
24	INDEPENDENT POWER TRANSMISSION OPERATOR SA	IPTO	EL
25	ELLINIKO HRIMATISTIRIO ENERGEIAS	HENEX	EL
26	HARDWARE AND SOFTWARE ENGINEERING EPE	HSE	EL
27	QUE TECHNOLOGIES KEFALAIOUCHIKI ETAIREIA	QUE	EL
28	ARETI S.P.A.	ARETI	IT
29	APIO S.R.L.	APIO	IT
30	ACEA ENERGIA SPA	AE	IT
~~31~~	~~VOLKERWESSELS ICITY B.V.~~	~~VWICI~~	~~NL~~
32	ARNHEMS BUITEN BV	AB	NL
33	STICHTING VU	VU	NL
34	COOPERATIVE ELECTRICA DO VALE DESTE CRL	CEVE	PT
35	REN - REDE ELECTRICA NACIONAL SA	REN	PT
36	MC SHARED SERVICES SA	SONAE	PT
37	ELES DOO SISTEMSKI OPERATER PRENOSNEGA ELEKTROENERGETSKEGA OMREZJA	ELES	SI
38	ELEKTRO GORENJSKA PODJETJE ZA DISTRIBUCIJO ELEKTRICNE ENERGIJE DD	EG	SI
39	OPERATO DOO	OPR	SI
40	SVEUCILISTE U ZAGREBU FAKULTET ELEKTROTEHNIKE I RACUNARSTVA	UNIZG	HR
41	INSTITUT JOZEF STEFAN	JSI	SI
42	KONCAR - DIGITAL DOO ZA DIGITALNE USLUGE	KONC	HR
43	DS TECH SRL	DST	IT
44	CYBERSOCIAL LAB S.R.L.	CSL	IT

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

DISCLAIMER

Funded by the European Union. Views and opinions expressed are those of the authors only and do not necessarily reflect those of the European Union. The European Commission is not liable for any use that may be made of the information contained herein.

COPYRIGHT NOTICE

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

EXECUTIVE SUMMARY

This document presents the first release of the Reference Architecture for the HEDGE-IoT project, a key milestone in advancing secure, efficient, and intelligent IoT-Edge service deployment integrated with the Data Space paradigm. The Horizon 2020 HEDGE-IoT project aims to create a next-generation edge-to-cloud continuum digital infrastructure that addresses the unique challenges of heterogeneous IoT-Edge environments—combining real-time responsiveness, data privacy, interoperability, security and scalability. HEDGE-IoT introduces an innovative Digital Framework conceptualized by the Proposed Reference Architecture designed to leverage IoT assets and Edge Services across multiple layers of the energy system—from behind-the-meter installations to the Transmission System Operator level. The framework enhances intelligence at both edge and cloud layers by leveraging advanced AI and machine learning tools, while bridging the cloud-edge continuum through federated applications governed by sophisticated computational orchestration.

To develop the HEDGE-IoT reference architecture, a step-by-step methodology definition is outlined, as some key processes and standards that are used to guide the design of the reference architecture. Building on that, the key EU programmes, standardisation efforts and flagship research projects to extract reusable patterns and gaps, are also analysed to establish an evidence base for the project's own choices. Following the review, the functional-specifications from the refined business and system use-cases, distils cross-pilot commonalities, defines interoperability profiles and lists the technical capabilities the system must deliver, while a set of transversal use-cases shows how those capabilities knit the pilots together. The narrative then shifts to cataloguing the software components, edge/cloud services and data connectors that will be assembled, before presenting the multi-layer reference architecture itself—its vocabulary, dataspace foundations, cloud-to-edge orchestration logic and mappings to SGAM and BRIDGE-DERA. Finally, dedicated sections follow on how identity, policy enforcement and usage-control patterns harden privacy and cybersecurity across that dataspace, and a forward-looking chapter flags upcoming work on AI at the edge, scalability and human-centric governance.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

TABLE OF CONTENTS

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

LIST OF TABLES

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

LIST OF FIGURES

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

ABBREVIATIONS

ABAC	Attribute-Based Access Control
ADF	Architecture Description Framework
ADL	Architecture Description Language
aFRR	Automatic Frequency Restoration Reserve
AI	Artificial Intelligence
AIOTI	Alliance for Internet of Things Innovation
API	Application Programming Interface
ALTAI	Assessment List for Trustworthy AI
BAL	Blockchain Access Layer
BDVA	Big Data Valuation Association
BMS	Building Management System
BSP	Balancing Service Provider
BTM	Behind The Meter
BUC	Business Use Case
CA	Consortium Agreement
CEM	Customer Energy Managers
CI/CD	Continuous Integration / Continuous Deployment
CIM	Common Information Model
CM	Congestion Management
CNN	Convolutional Neural Network
CRUD	Create-Remove-Update-Delete
CSA	Coordination and Support Actions
DEP	Data Exchange Platform
DER	Distributed Energy Resources
DERA	Data Exchange Reference Architecture
DESAP	Digitalising the Energy System Action Plan
DLR	Dynamic Line Rating
DMP	Data Management Plan
DMS	Distribution Management System
DoA	Description of the Action
DRL	Deep Reinforcement Learning
DSFM	Demand-Side Flexibility Management
DPP	Digital Platform Provider
DSC	Data Space Connector
DSO	Distribution System Operator
DSSC	Data Space Support Centre

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

DTR	Dynamic Thermal Rating
EaaS	Energy-as-a-Service
EC	European Commission
EC	Energy Community
EDC	Eclipse Dataspace Connector
eIDAS	electronic Identification, Authentication and Trust Services
EMS	Energy Management System
ESCO	Energy Service Companies
ETSI	European Telecommunications Standardization Institute
EU	European Union
FR	Flexibility register
FSP	Flexibility Service Provider
GA	Grant Agreement
GDPR	General Data Protection Regulation
GIS	Geographic Information System
HEDGE-IoT	Holistic Approach towards Empowerment of the DiGitalization of the Energy Ecosystem through adoption of IoT solutions
HEMRM	Harmonized Energy Market Role Model
HLA	High Level Architecture
HLEG	High Level Expert Group
HVAC	Heating, Ventilation, and Air Conditioning
IdPs	Identity Providers
IDSA	International Data Space Organization
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IETF	the Internet Engineering Task Force
IoT	Internet of Things
IoT-EPI	IoT European Platforms Initiative
IT	Information Technology
ISO	International Organization for Standardization
LCIM	Levels of Conceptual Interoperability Model
LFM	Local Flexibility Market
LV	Low Voltage
M2M	Machine-to-machine
mFRR	Manual Frequency Restoration Reserve
ML	Machine Learning
MO	Market Operator
MQTT	Message Queuing Telemetry Transport

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

MV	Medium voltage
NEMO	Nominated Electricity Market Operator
NGSI	Next-Generation Service Interface
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance
OBJ	Objective
ODRL	Object Description Registry Language
OCF	Open Connectivity Foundation
PEP	Policy Enforcement Points
PGUI	Power Grid User Interface
PMH	Project Management Handbook
PV	Photovoltaic
QoS	Quality of Service
RA	Reference Architecture
RAM	Reference Architecture Model
RBAC	Role-Based Access Control
RES	Renewable Energy Sources
RR	Reserve Resource
SaaS	Software-as-a-Service
SAREF	Smart Applications REFerence Ontology
SCADA	Supervisory Control And Data Acquisition
SD	Self-Description
SG	Smart Grid
SGAM	Smart Grid Architecture Model
SME	Small and Medium-sized Enterprises
SO	System Operator
SoC	System on Chip
SUC	System Use Case
T&D	Transmission and Distribution
TLS	Transport Layer Security
TSO	Transmission System Operator
UC	Use Case
UI	User Interface
UML	Unified Modelling Language
WG	Working Group
WP	Work Package

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

1 INTRODUCTION

1.1. HEDGE-IOT PROJECT INTRODUCTION AND SUMMARY

HEDGE-IoT (Holistic Approach towards Empowerment of the Digitalization of the Energy Ecosystem through adoption of IoT solutions) is a Horizon Europe Innovation Action (Grant Agreement No. 101136216) aimed at transforming the European energy system through an advanced digital framework. The project addresses the deployment of IoT assets across all levels of the energy value chain—from behind-the-meter devices to Transmission System Operators (TSOs)—to enhance intelligence, flexibility, and resilience.

Central to HEDGE-IoT is the development of a federated edge-cloud architecture that enables real-time data processing and advanced services through AI/ML, federated learning, and orchestration solutions. This architecture supports a scalable and interoperable environment for diversified energy services.

The project is structured around four core pillars:

- **Technology Facilitator**, enabling edge-based intelligence through computational sharing;
- **Interoperability**, ensuring semantic and technical compatibility using data space architectures;
- **Standardisation**, promoting cross-domain adoption of standards like SAREF;
- **Ecosystem Enabler**, fostering stakeholder engagement, ethics, and trust.

HEDGE-IoT will be validated through six national pilots and extended via Open Calls targeting Small-Medium Enterprises (SMEs) and innovators. It aligns with EU policy goals on digitalisation and decarbonisation by increasing Renewable Energy Resource (RES) hosting capacity, unlocking flexibility, and promoting secure data sharing in the energy sector.

1.2. D2.3 SCOPE AND OBJECTIVES

Deliverable D2.3, as part of Work Package 2, represents a critical milestone in the HEDGE-IoT initiative, detailing the project's reference architecture (RA) and underlying functional specifications. Specifically, this deliverable provides a comprehensive description of the RA developed to ensure seamless interoperability between heterogeneous IoT devices, services, and platforms. It highlights architectural guidelines for implementing federated data spaces, secure data exchange, semantic interoperability, and intelligent orchestration mechanisms, supporting diverse industrial and utility scenarios addressed within the project's demonstrators.

This deliverable therefore serves multiple purposes: it acts as a blueprint for subsequent technical implementation efforts, guides integration processes within pilot demonstrators, and offers valuable insights to stakeholders—including developers, system integrators, and decision-makers and ensures alignment with technical standards and ongoing EU-initiatives.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

1.3. WP2 – STAKEHOLDERS REQUIREMENTS AND SYSTEM SPECIFICATIONS

Work Package 2 (WP2) provides the methodological and architectural foundation for the HEDGE-IoT project. It ensures that system specifications and architectural design are grounded in the operational realities and strategic needs of energy stakeholders. WP2 progresses through a coherent sequence of analytical and technical tasks, structured across four core deliverables: D2.1, D2.2, D2.3, and D2.4.

The work began with D2.1 "Requirements on an IoT Cloud/Edge System for the Energy Ecosystem"[73], which compiled comprehensive stakeholder requirements across six pilot sites. These were formalised through Business Use Cases (BUCs), capturing the functional objectives, actors, and high-level processes relevant to national and cross-border energy contexts.

D2.2 "Functional Specifications of the HEDGE-IoT System" [74]extended this work by deriving System Use Cases (SUCs) from the BUCs, using the IEC 62559-2 template [41]. These SUCs detail specific system functionalities, interactions, information flows, and constraints—forming the first version of functional specifications for the HEDGE-IoT system. D2.2 also introduced a preliminary set of technical requirements.

D2.3 "HEDGE-IoT Reference Architecture (First Release)", the current deliverable, synthesises these outputs to produce a modular, scalable, and interoperable reference architecture. It defines the methodology, the architecture development process, and links to key European interoperability frameworks such as BRIDGE DERA, SGAM, and IDSA. It also incorporates the definition of key system components, transversal use cases, and the mapping of actors and data sources. D2.3 includes a first refinement of interoperability profiles and identifies common semantic and cybersecurity considerations to be addressed across use cases.

As the project evolves, this architecture will be continuously updated and validated through implementation feedback, with a final, consolidated version to be delivered in D2.4 "HEDGE-IoT Reference Architecture (Final Release)".

1.4. REFERENCE AND APPLICABLE DOCUMENTS

The general guidelines for the project implementation are defined in the HEDGE-IoT Grant Agreement (GA), the Consortium Agreement (CA), the Project Management Handbook (D1.1 - PMH), and the Data Management Plan (D1.4 – DMP).

Therefore, this deliverable "HEDGE-IoT Reference Architecture (First Release)", does not replace any of these applicable documents. Project partners should adhere to the following order of precedence:

- Grant Agreement
- Consortium Agreement
- D1.1 "Project Management Handbook" [71]

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- D1.4 "Data Management Plan" [72]
- D2.1 "Requirements on an IoT Cloud/Edge System for the Energy Ecosystem"[73]
- D2.2 "Functional Specifications of the HEDGE-IoT system"[74]
- D3.1 "HEDGE-IoT Interfaces and Tools for Interoperability"[75]
- D3.3 "HEDGE-IoT Technological Enablers (First Release)"[76]

1.5. STRUCTURE OF THE DOCUMENT

This deliverable is structured into nine chapters:

Chapter 1 provides the introduction, contextualizing the deliverable within WP2, outlining its scope and objectives, and describing the structure.

Chapter 2 explains the reference architecture methodology adopted, detailing the architectural views and connections with other work packages.

Chapter 3 reviews relevant EU initiatives, reference architectures, data-driven initiatives, and related projects to establish a solid foundation and identify potential gaps.

Chapter 4 presents the refined functional specifications of the HEDGE-IoT system, aligning business and system use cases, and detailing interoperability profiles.

Chapter 5 describes the components and services of HEDGE-IoT, including the functional requirements matrix.

Chapter 6 outlines the detailed reference architecture, including vocabulary definitions, methodologies, alignment with other architectures, and mappings.

Chapter 7 addresses cybersecurity considerations and AI safety measures pertinent to the architecture.

Chapter 8 highlights future considerations for the final release of the reference architecture.

Chapter 9 concludes the deliverable.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

2 REFERENCE ARCHITECTURE METHODOLOGY

2.1. REFERENCE ARCHITECTURE APPROACH

The HEDGE-IoT Reference Architecture (RA), aims to create a functional, interconnected environment that supports the dynamic cloud-edge ecosystem. The key objectives include leveraging Data Space principles to manage data sovereignty and ensure compliance with EU regulations and initiatives, as well as promoting the decentralization of operational services, to improve system scalability. The RA will support interoperable and integrated solutions while ensuring regulatory-preserving data sharing and secure control over data. To ensure the RA aligns with ongoing EU efforts and global standards, the design process will integrate concepts and outcomes from several initiatives and projects, as detailed in Table 1.

These efforts provide a foundation for the architectural framework, ensuring that the RA follows the latest regulatory, technological, and operational best practices (e.g., BRIDGE and AIOTI focus on interoperability and smart energy systems, while IDSA addresses data sovereignty). Similarly, related projects such as OneNet, Enershare, and Platone contribute to the understanding of distributed energy systems, data integration, and advanced market participation. By referencing these initiatives, the RA design remains at the forefront of technological advancements, ensuring seamless integration across platforms and regulatory compliance. As mentioned above, Table 1 lists the full set of EU initiatives and projects relevant to the design of the HEDGE-IoT RA, which will be further analysed in Chapter 3.

The approach to the HEDGE-IoT RA design will focus on establishing a cost-effective and easy-to-install middleware layer that integrates IoT/edge devices and fog/cloud platforms. As illustrated in Figure 1 presents a first high-level conceptual Reference Architecture, the HEDGE-IoT Interoperability Middleware will be central to this design, enabling communication between IoT Edge Services, data sources, and the HEDGE-IoT stakeholders via HEDGE-IoT Data Connectors. Core concepts like semantic interoperability, data access policies, identity management, and a Context Broker will ensure secure, regulatory-compliant data flows in line with EU regulations. Tools such as the Data Catalogue and App Store will manage data and service access, supporting interoperability across diverse platforms. The HEDGE-IoT Services Layer will provide essential services such as Federated Learning Services, User-centric Services, and Horizontal Services. These services are supported by the middleware layer and integrated into a Service Catalogue. Federated learning will emphasise the decentralised nature of the system, allowing distributed nodes to collaborate while maintaining data privacy and security, crucial for regulatory compliance. This layer ensures smooth interaction between stakeholders and services, contributing to the system's overall scalability and modularity.

The HEDGE-IoT Monitoring & Computational Orchestration Layer at the top of Figure 1 will be critical for system administration, computational orchestration, and infrastructure planning. This layer will manage and monitor the entire ecosystem, ensuring efficient operation, planning, and scaling of resources. Cybersecurity & Data Privacy considerations will run parallel across the entire architecture, reflecting the importance of maintaining secure operations and regulatory-preserving data sharing.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

TABLE 1 - GLOBAL & EU INITIATIVES, RELATED PROJECTS AND DATA DRIVEN INITIATIVES AND SPECIFICATIONS

GLOBAL & EU INITATIVES	Data Driven Initiatives and Specifications	RELATED PROJECTS
• BRIDGE • SGAM • The European AIAlliance • FIWARE • AIOTI • IoT-EPI	• IDSA • BDVA • GAIA-X	• Attest • Bright • Enershare • I-NERGY • MATRYCS • OneNet • Platone • Resonance • Synergy

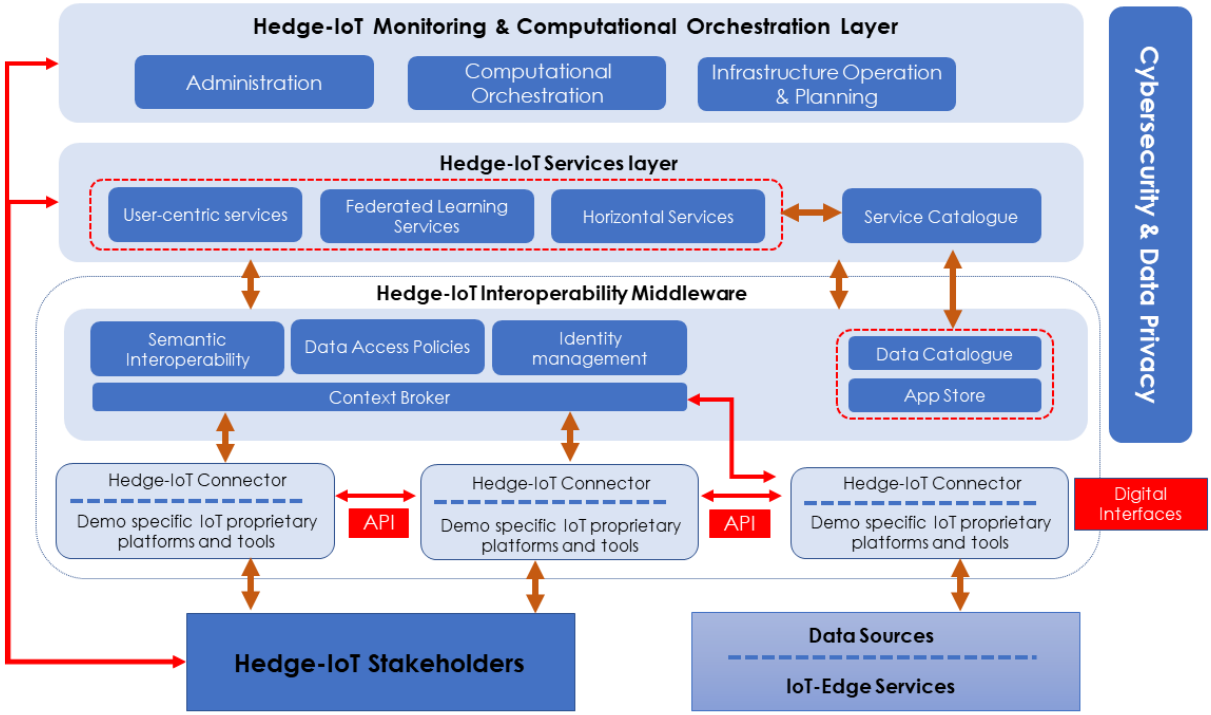

FIGURE 1 - HEDGE-IOT RA INDICATIVE CONCEPT MODEL

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Figure 2 illustrates the key inputs in the methodology used in the design of the HEDGE-IoT RA, highlighting the necessary steps involved. To ensure that the design process aligns with real-world scenarios, the functional specifications derived from business use cases in WP2 must be integrated into the RA to support seamless operation. This alignment ensures that the RA is not only compliant with external regulations but also takes into consideration the semantic ontologies and use cases of the project to maintain interoperability across different technical implementations. The methodology behind the RA will emphasise technical convergence between functional specifications and software architecture. This ensures that the system's technical elements, such as services and system use cases, align with the overarching RA, contributing to overall performance and reliability.

Quality of Service (QoS) is also central to the RA design, ensuring smooth interaction between system components. QoS will monitor system performance to ensure it meets the required standards for service delivery, dictating how actors, services, and technical specifications interact with the broader architecture. This is particularly critical during the alignment and convergence phases, guaranteeing reliable and efficient operation.

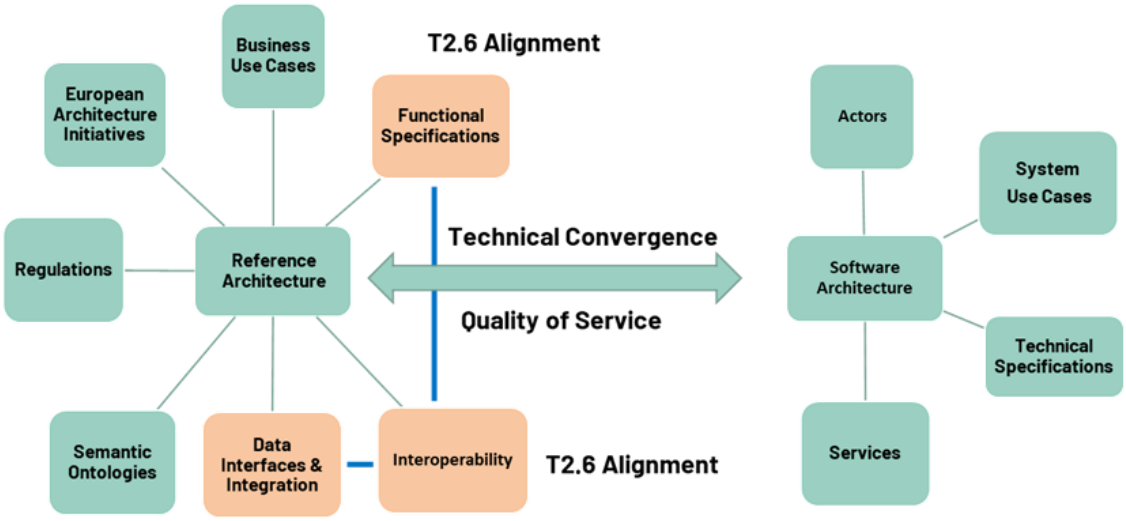

FIGURE 2: HEDGE-IOT RA METHODOLOGY CONSIDERATIONS [74]

The use of ISO 42010 and the 4+1 Architecture Model will structure and describe the RA within the HEDGE-IoT ecosystem. ISO/IEC 42010 provides a standardised approach to describing the architecture of complex systems, addressing stakeholder concerns and viewpoints. The 4+1 Architecture Model will be applied to organise the RA into logical, process, physical, and deployment views, ensuring that all system components are clearly documented and aligned with the RA objectives.

Finally, the development of the RA will follow an iterative approach, ensuring continuous refinement and alignment with stakeholder concerns and project requirements. This will include collecting and analysing system use cases, developing a comprehensive integration plan and gathering feedback, particularly around functional requirements, and refining the architecture to address

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

interoperability. Multiple review cycles will be conducted to validate and adjust the RA, with functional requirements being finalized through this iterative process.

2.2. ISO42010:2022 MODEL

The ISO 42010:2022 [1] is an international standard which provides a standardised framework for creating and managing architecture descriptions of complex systems. It is based upon a conceptual model – or "meta model" – of the terms and concepts affecting architecture descriptions. The standard defines the key elements involved in system architecture and specifies how they relate to the different stakeholder concerns. It distinguishes between the architecture (system fundamental organization) and the architecture description (the documentation for the architecture), by defining its three critical components:

1. **Architecture Description Frameworks (ADFs)**: Structure how the architecture is described.
2. **Architecture Description Languages (ADLs)**: Provide the language for expressing the architecture.
3. **Architecture Viewpoints and Views**: Organise stakeholder concerns during the architecture design process.

The HEDGE-IoT ecosystem is a complex system, which operates within multiple layers of the energy system, and thus introduces complexity that the ISO 42010 standard can manage. The standard's emphasis on stakeholder driven architecture aligns well with the HEDGE-IoT project, which has both diverse actors and a variety of technological systems. The different technologies which are integrated in the project (e.g. IoT devices, edge computing and cloud systems, AI/ML tools, etc.), can be structured through the ISO42010 to address the stakeholder concerns in the architecture of the project. Stakeholder concerns like interoperability and scalability, will be effectively managed through well-defined viewpoints and views, ensuring that the design of the architecture is aligned with the expectations of stakeholders, from grid operators to IoT experts. As such, the architecture description will provide a detailed representation of how the system components interact to ensure coherence across the project's layers.

Within the context of HEDGE-IoT, the ADFs (wherever applicable) will structure the architectural description in a consistent and reusable way, making it easier to manage the complexity of the project. By providing proposed predefined structures like viewpoints, perspective and aspects to manage the design of the HEDGE-IoT system, the standard provides important tools for organizing the different elements in the system involved in the project, like AI/ML tools and cloud-edge integration. This will help address the multi-dimensional nature of the HEDGE-IoT framework by having consistency across various technological pillars. This approach will ensure scalability and adaptability of the system architecture to accommodate the evolving needs across the lifecycle of the project.

It is important to note that the ISO 42010 standard was used not for the actual architecture depiction but rather for the design methodology definition in a form of a series of distinct serial activities.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Correspondence is a concept in the ISO 42010 standard and is useful in the context of the HEDGE-IoT project, because it can help define key relationships between the different elements of an architecture description. They can help ensure that the different components of the architecture are consistent and aligned with each other to promote interoperability. In HEDGE-IoT, correspondences can be used to manage the complex relationships between grid systems and the different technologies that will interact with it, which are crucial for the operation of the HEDGE-IoT system. ISO 42010 specifies the use of ADLs, which provide the formal languages needed to describe complex systems such as HEDGE-IoT. They facilitate clear communication between system components, making it easier to integrate diverse tools, devices and technologies across the architecture. They also help ensure that the architecture's components are described in a way that is unambiguous and standardized. In the context of HEDGE-IoT, ADLs will be used to formalise the interactions between different technologies that exist within the scope of the project.

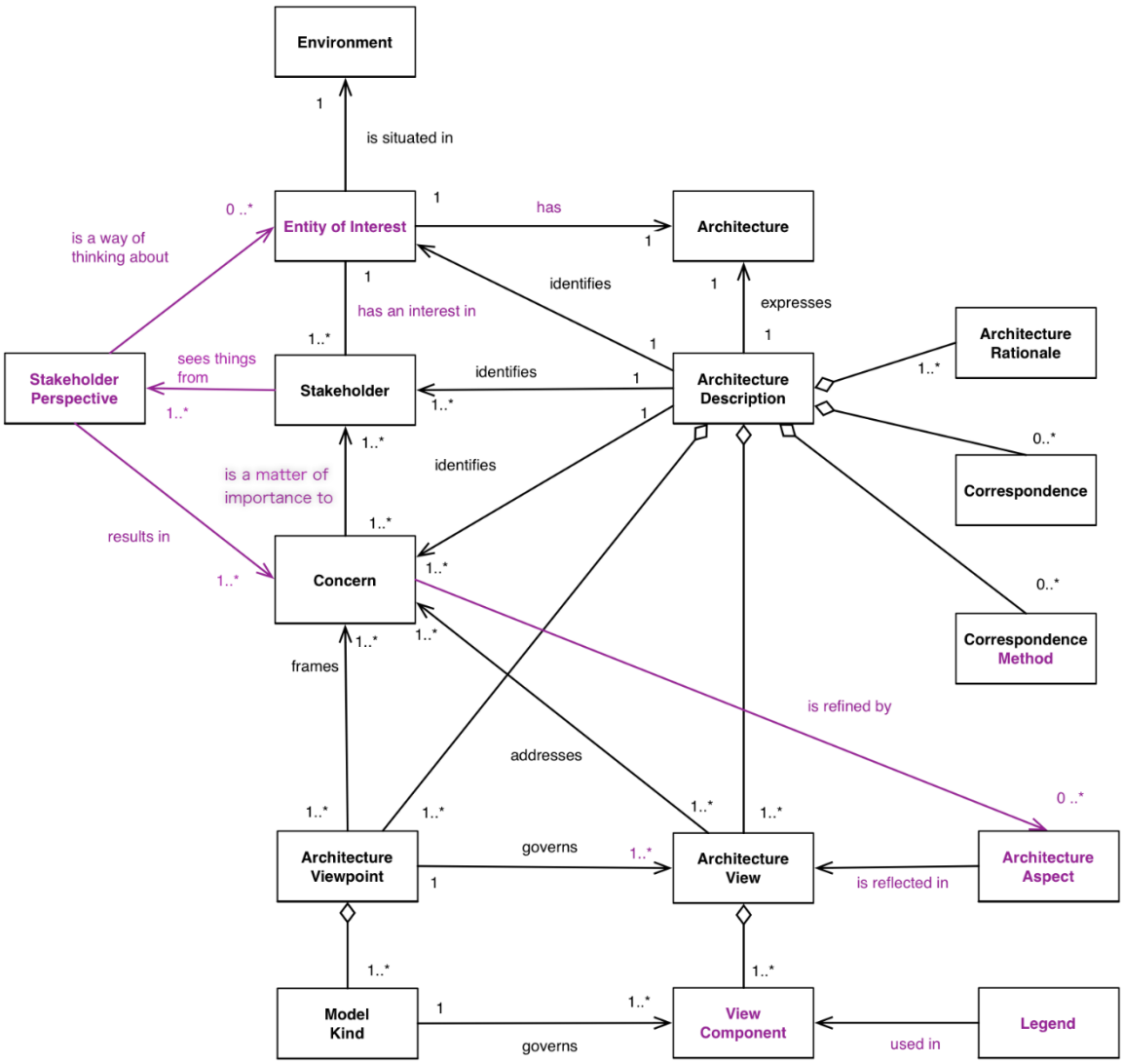

FIGURE 3 - UML CLASS DIAGRAM OF THE ISO 42010:2022 (SECOND EDITION) [1]

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

2.3. 4+1 ARCHITECTURAL VIEW MODEL

The 4+1 Architecture View Model, introduced by Philippe Kruchten [2], proposes a method to describe a system's architecture using five distinct views. These views address different aspects of the system and allow for better communication of design decisions to various stakeholders, such as developers, operators, and users. The model emphasises that no single view can capture all architectural concerns, so multiple views are used to express different parts of the architecture while maintaining a coherent overall structure.

The five views are:

1. **Logical View:** Focuses on the system's functionality, showing how it is decomposed into components or objects. This view captures the system's object model and interactions, often represented through class diagrams and relationships.
2. **Process View:** Handles non-functional requirements, especially those related to concurrency, synchronization, and distribution. This view shows how system processes or threads interact, often with a focus on performance and fault tolerance.
3. **Development View:** Describes the system's organisation in the development environment, including source code organization, modules, libraries, and subsystems. It supports the management of the development process and team collaboration.
4. **Physical View:** Maps the software onto the hardware infrastructure, showing how components are deployed across physical nodes. This view handles concerns like performance, scalability, reliability, and fault tolerance.
5. **Scenarios (Use Case View):** The "plus one" view ties the four other views together by demonstrating how they collaborate to support key use cases or scenarios. This view validates the architecture and ensures it meets the system's requirements.

By combining these five views, the 4+1 model (illustrated in Figure 4) provides a comprehensive description of the system's architecture, allowing different stakeholders to focus on the aspects that are most relevant to them. Within the context of the HEDGE-IoT project, the 4+1 Architecture model can be used to organise the RA into clear and interrelated views, providing a comprehensive understanding of the system's structure and functionality, across logical, process, development, physical, and scenario views. The key objective is to ensure each of these views supports scalability, interoperability of IoT and decentralised services within the HEDGE-IoT ecosystem and being aligned with Dataspace principles.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

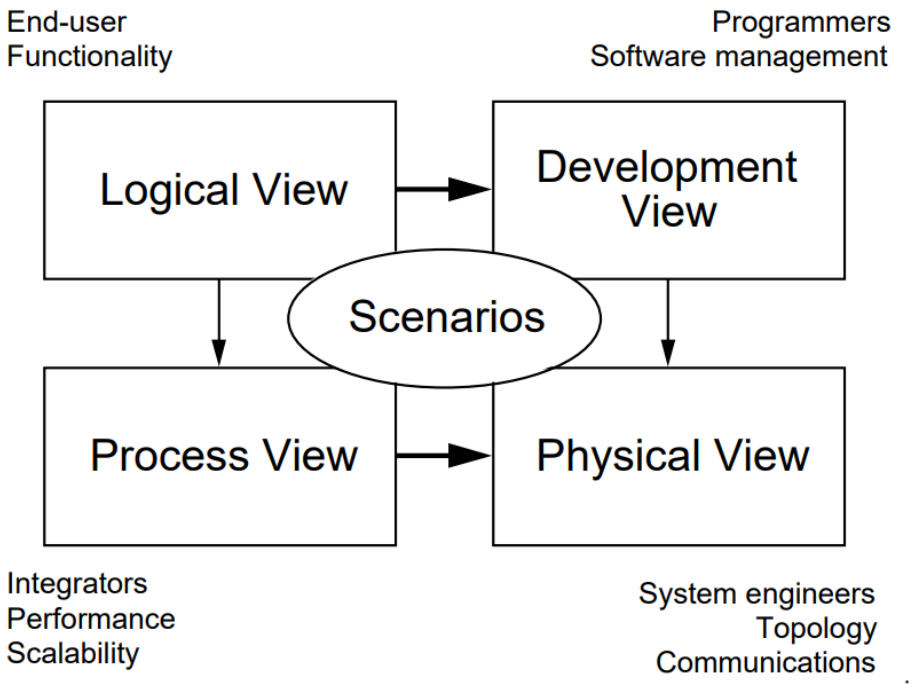

FIGURE 4 - THE 4+1 ARCHITECTURE VIEW MODEL[2]

- **The Logical view** will focus on defining the key HEDGE-IoT system components and their core functionality, which includes the interactions between IoT devices, edge nodes, technical platforms, and the middleware layer. The focus of this view will be on the logical relationship between these components to ensure modularity and flexibility, and to ensure that the concept of interoperability is built in the RA, to enable interconnectivity between layers.
- **The Process View** will address how the system behaves in terms of performance, scalability, and resilience. It will capture the dynamic behaviour of the HEDGE-IoT system during its operation. This means defining the key processes involved in the RA, such as dataflows, decision making protocols and service orchestration. The focus of this view will be on how the operation processes can manage the scalability and have efficient resource use, and to ensure the system can handle high volume data processing in decentralized environments.
- **The Development View** will provide an architectural framework for the design and development of the software systems within HEDGE-IoT, focusing on the middleware, data interfaces, and integration components. The focus of this view will be to guide the development of interoperable building blocks and ensure that software components are aligned with data sovereignty, trust and regulatory compliance.
- **The Physical View** will describe how the HEDGE-IoT system is deployed across physical infrastructure and hardware components. Its focus is to align the physical infrastructure with EU standards and ensure that the physical layout supports efficient data flow and interoperability.
- **The Scenarios View** will focus on extracting stakeholder concerns and validating the RA. This view ensures that the architecture supports real-world operational scenarios which are defined in the scope of this project. The key focus is to verify that the RA meets the

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

functional and non-functional requirements of the system and to address stakeholder concerns.

In the 4+1 Architecture Model, the five views are interrelated, and correspondence between them ensures consistency. In the HEDGE-IoT system, IoT devices represented in the Logical View correspond to processes that manage data collection and processing across cloud and edge layers. The Process View then connects to the Physical View, where these processes are deployed onto physical hardware, ensuring that tasks, like data ingestion and analysis are efficiently distributed across nodes to enhance scalability and performance. The Development View aligns software components with the logical and physical structures, ensuring that the developed modules are modular, scalable, and deployable across the system's physical infrastructure. This view supports the practical organisation of the software and facilitates its deployment. Finally, the Scenarios View ties all other views together, validating the architecture by demonstrating how it supports operational use cases, to satisfy the functional and non-functional requirements of the system.

The 4+1 process was used for the definition of the Transversal Use Cases and in the same manner with the ISO 42010 standard, albeit in a differentiated way. Instead of creating different views we borrow properties from all of them to design the actual Reference Architecture.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

3 EU INITIATIVES AND RELEVANT PROJECTS

3.1. TOWARDS IOT INTEROPERABILITY

3.1.1 Introduction

Interoperability refers to the capacity of IoT systems and their components to effectively communicate and exchange data with one another. This capability is fundamental to fully realising the potential of the IoT paradigm, enabling a wide range of technological, economic, and societal advancements. However, achieving interoperability remains a significant challenge in the IoT landscape, largely due to the absence of universal standards and the broad diversity of existing systems. Interoperability is also critical for big data analytics, as it greatly simplifies data processing and integration. This chapter explores the vital role of IoT interoperability, examining its various forms, associated challenges, practical use cases, and potential solutions. Recognizing its complexity and the multiple facets it encompasses, interoperability is analysed across different layers of IoT architecture. In addition, it is revisited from a global perspective, considering cross-platform and cross-system interactions.

3.1.2 IoT Interoperability Challenges

The Internet of Things (IoT) is expanding rapidly, and one of the most pressing challenges it faces is achieving interoperability. As the number of IoT devices continues to grow, ensuring seamless communication and coordination among them becomes increasingly critical. A lack of interoperability can severely hinder the effectiveness and widespread adoption of IoT technologies. To unlock the full potential of IoT across diverse sectors, systems must be capable of interacting and functioning cohesively. Below are the key interoperability challenges commonly encountered in the IoT landscape.

- **Lack of Standardization:** The diversity in hardware components, communication protocols, and data formats is a primary factor contributing to the lack of interoperability within the IoT ecosystem. IoT devices often rely on different frequencies and utilise distinct protocols—such as Zigbee, Bluetooth, and Wi-Fi—each tailored to specific functions and requirements. This absence of unified standards results in operational inefficiencies and drives up costs, as additional middleware or adapter software is frequently needed to bridge communication gaps. As the total potential value of IoT technologies depends on achieving interoperability, an urgent need for industry-wide standardization is essential to streamline integration and foster a cohesive, efficient IoT environment.

- **Proprietary technologies:** Proprietary technologies represent a major obstacle to achieving interoperability in the IoT space. To differentiate their products, many manufacturers create custom protocols and standards. While this may offer short-term competitive advantages, it often leads to closed ecosystems that are incompatible with other systems, resulting in fragmentation across the IoT landscape. This lack of compatibility fosters vendor lock-in, restricting consumers and businesses to specific providers and limiting their flexibility and options. For enterprises adopting IoT solutions, interoperability among

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

proprietary systems is a major concern, as it hampers scalability and complicates the integration of new technologies.

- **Security challenges:** Integrating diverse IoT systems adds layers of complexity to the network, significantly increasing security risks. Each new device or protocol can introduce potential vulnerabilities, making the overall system more exposed to cyberattacks. As device interconnectivity grows, so does the risk that a single compromised component could trigger a widespread security breach. An industry report revealed that 70% of IoT devices are vulnerable to security threats, highlighting the critical need for strong, standardized security protocols that can be consistently implemented across various devices and platforms to ensure safe and reliable communication.

- **Resource limitations:** IoT devices are often built with a focus on cost-efficiency and low resource consumption, resulting in limited processing power, memory, and battery capacity. These constraints make it difficult to implement advanced interoperability protocols and strong security measures, which typically demand greater computational resources. The challenge becomes even more pronounced in large-scale deployments—such as industrial IoT systems or smart city infrastructures—where thousands or even millions of devices are involved. Striking a balance between maintaining device performance and enabling seamless communication across diverse platforms remains a significant hurdle in scaling and enhancing IoT networks.

- **Data Management and Ownership:** Managing the vast amounts of data produced by IoT devices presents major challenges related to data ownership and governance. Achieving effective interoperability requires not only seamless data exchange but also efficient handling of data storage, analysis, and privacy concerns. When data flows across international borders, it must navigate differing legal and regulatory frameworks regarding privacy and security. As IoT deployments grow in scale, these data management and compliance issues become more complex. For example, regional differences in data regulations can hinder the implementation of global IoT solutions, highlighting the need for a well-considered, flexible approach to data governance and interoperability.

3.1.3 Interoperability solutions

Realising the full potential of the Internet of Things (IoT) depends heavily on achieving interoperability across diverse devices and systems. While the obstacles are considerable, several practical strategies and solutions are available to address them effectively, strategies which are considered in HEDGE-IoT Reference Architecture design:

- **Standardizing Protocols and Frameworks:** One of the most impactful ways to tackle interoperability challenges is through the development and adoption of standardised protocols and frameworks. Standardisation allows devices from different manufacturers to communicate more effectively, reducing complexity and lowering deployment costs. Industry organizations such as the Internet Engineering Task Force (IETF) [77] and the

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Institute of Electrical and Electronics Engineers (IEEE) [78] are leading efforts to establish such common standards. Broad adoption of these standards simplifies integration and fosters innovation by giving developers a common foundation for building interoperable solutions. Notable examples like MQTT[79] demonstrate how standardized protocols can enable efficient device-to-cloud communication, thereby enhancing IoT scalability and performance.

- **Collaboration and Openness:** Fostering interoperability also requires strong collaboration among technology vendors, industry consortia, and government entities. Promoting open standards and embracing transparency can help break down proprietary barriers, leading to more flexible and innovative IoT ecosystems. Collaboration further extends to sharing best practices and unified security approaches, which strengthen overall system resilience. Initiatives like the Open Connectivity Foundation (OCF) illustrate the value of joint efforts in developing universal communication protocols. Additionally, regulatory frameworks that encourage or mandate open standards can help align industry practices, ensuring that products entering the market contribute to a cohesive and interoperable IoT landscape.

- **Testing and Certification:** Robust testing and certification processes are vital for ensuring that IoT devices meet interoperability, security, and reliability standards before deployment. By enforcing standardised testing procedures, stakeholders can verify device compatibility and functionality, building confidence among users and promoting broader adoption. Organisations such as the National Institute of Standards and Technology (NIST) [80] provide important frameworks to validate device compliance with interoperability benchmarks. These practices are essential for maintaining trust and consistency across the rapidly growing IoT ecosystem.

- **Interoperability Platforms and Gateways:** Interoperability platforms and gateways offer practical solutions by enabling communication between devices that use different protocols and standards. Acting as intermediaries, these systems translate between various technologies, facilitating seamless integration without the need for major infrastructure overhauls. These solutions increase system flexibility and significantly ease the deployment of interoperable IoT systems.

- **Edge Computing and Decentralization:** Edge computing introduces a decentralised approach to data processing, allowing data to be handled locally—near the source—rather than relying solely on central servers. This reduces latency, lowers bandwidth usage, and enables faster response times. By processing data on-site, edge computing supports greater interoperability, especially in environments where diverse technologies must function together in real time. This approach is especially valuable in sectors like manufacturing and automotive, where real-time analytics and system responsiveness are critical. By simplifying local integration, edge computing enhances the efficiency and reliability of IoT systems.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Overall, advancing interoperability in IoT requires a multi-faceted strategy that combines technical standardization, collaborative industry practices, rigorous testing, adaptable platforms, and modern computing architectures. Together, these efforts pave the way for a more unified, scalable, and impactful IoT ecosystem.

3.2. GLOBAL & EU INITIATIVES

3.2.1 BRIDGE DERA Reference Architecture

BRIDGE is a European Commission initiative that brings together Horizon 2020 and Horizon Europe projects in smart grids, energy storage, digitalisation, and energy islands. It fosters collaboration, promotes standardisation through frameworks like DERA [83] and HEMRM [42], and supports EU policy alignment. Acting as a central forum, BRIDGE drives interoperability and cross-sector integration by sharing best practices and addressing regulatory and technical barriers.

BRIDGE's structure is articulated through Working Groups (WGs) on:

- **Data Management:** Focused on communication infrastructure, data privacy, cybersecurity, and interoperable data handling.
- **Business Models:** Defines standardised valuation frameworks and explores simulation tools to assess emerging business model viability.
- **Regulation:** Establishes baseline regulatory conditions for smart grids and energy storage, including demand-side response and grid cooperation.
- **Consumer Engagement**: Analyses consumer profiles, motivations, and behavioural triggers to enhance engagement strategies.

These working groups feed into architectural planning, supporting the development of a coherent ecosystem that integrates digital tools and aligns with data space strategies and AI-enabled innovation.

BRIDGE DERA3.0 ARCHITECTURE

The Data Exchange Reference Architecture (DERA) 3.0 [3] developed by the BRIDGE Data Management Working Group, aims to foster cross-sectoral, interoperable, and business process-agnostic data exchange in the European energy domain. It builds upon versions 1.0 and 2.0 by incorporating practical implementation feedback, aligning with EU digitalisation goals (notably DESAP), and integrating with emerging data space frameworks such as Gaia-X, IDSA, and OpenDEI.

DERA 3.0 provides a layered, modular, and federated approach to energy data exchange that bridges local energy platforms (e.g., DSOs, energy communities) with federated data spaces, supporting a scalable and secure EU-wide energy data ecosystem.

ARCHITECTURE PRINCIPLES

DERA 3.0 is structured around the SGAM (Smart Grid Architecture Model) layers (see section 3.2.2), while introducing clear differentiation between:

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- **Local platforms:** e.g., DSOs, data hbs, metering systems.
- **Federated data spaces:** data marketplaces and cross-sector collaboration frameworks.
- **Data Space Connectors**: trusted intermediaries that enable secure, interoperable data flow between local and federated systems.

Key principles include:

- Data sovereignty and role-based access control.
- Protocol and format agnosticism.
- Semantic interoperability via shared vocabularies (e.g., CIM, SAREF).
- Open-source and standard-based integration.
- Cross-sectoral and cross-border reuse of services and data models.

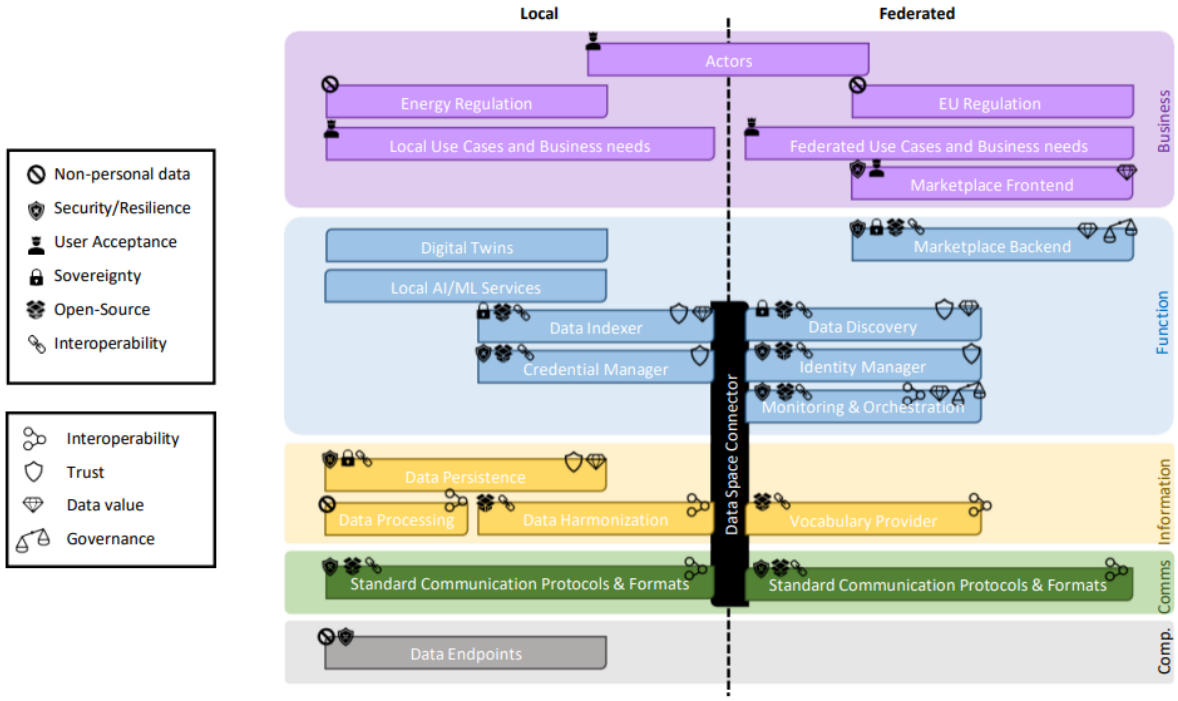

FIGURE 5 - DERA 3.0 LAYERED ARCHITECTURE AND LINK TO THE DESAP AND OPENDEI BUILDING BLOCKS [3]

At the core of DERA 3.0 is the Data Space Connector, a critical software intermediary that enables seamless, secure, and policy-compliant data exchange between local platforms and federated data ecosystems. It acts as a bridge, facilitating the indexing, discovery, and bilateral exchange of data without requiring central replication. By supporting cross-platform and cross-sector interoperability, the connector ensures data flows can occur efficiently across diverse systems and domains. Crucially, it enforces GDPR-compliant mechanisms for consent-driven data sharing, providing a foundation for trustworthy, transparent, and sovereign digital infrastructures.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

ALIGNMENT WITH EU PRIORITIES

DERA 3.0 directly supports the Digitalising the Energy System Action Plan (DESAP) by embedding the following requirements:

TABLE 2 - ARCHITECTURAL ALIGNMENT BETWEEN BRIDGE DERA3.0 AND DESAP REQUIREMENTS

DESAP Requirement	Architectural Alignment
Non-personal Data	Local anonymization, secure endpoints
Security/Resilience	Encrypted communications, identity management
User Acceptance	Simplified marketplace frontend, role models
Sovereignty	Federated governance, local control
Open Source	Open APIs, vocabularies, standards
Interoperability	CIM/SAREF vocabularies, protocol neutrality

DERA 3.0 proposes key steps to boost adoption and cross-sector alignment, including harmonising energy roles via the HEMRM model, developing open-access data models and vocabularies, and creating governance templates and semantic validators. It emphasises collaboration among projects, standard bodies, and regulators, and promotes API-based, business-agnostic Data Exchange Platforms (DEPs) to enable seamless, scalable data sharing across sectors.

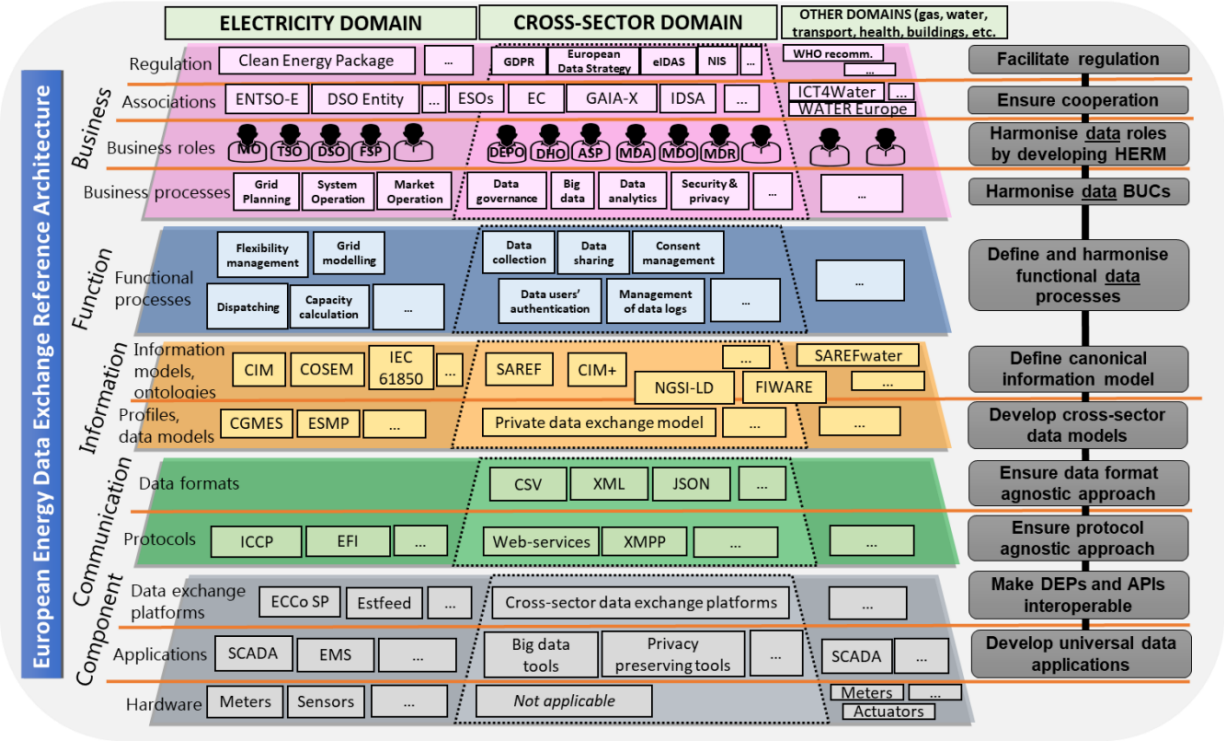

FIGURE 6 - HIGH-LEVEL SGAM BASED REFERENCE ARCHITECTURE FOR EUROPEAN ENERGY DATA EXCHANGE [83]

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

RELEVANCE TO HEDGE-IOT

The architectural vision of the HEDGE-IoT project aligns closely with the principles established in BRIDGE DERA 3.0. Both frameworks emphasise semantic interoperability, leveraging shared vocabularies and ontologies to enable meaningful cross-domain data exchange. HEDGE-IoT integrates federated data spaces using Eclipse Dataspace Connectors (EDC), supporting secure orchestration across edge and cloud infrastructures. Its inclusion of App Stores and Service Catalogues mirrors DERA's marketplace approach, while its embedded commitment to cybersecurity and data sovereignty positions the project to comply with emerging EU standards. As the project evolves, its alignment with DERA 3.0 will ensure greater interoperability, sustainability, and scalability within the broader European digital energy landscape.

3.2.2 SGAM

The Smart Grid Architecture Model (SGAM) is a tool developed to help understand, design, and implement smart grids (SGs). SGs are modernised electrical grids that integrate digital communication technologies, renewable energy sources, and new forms of electricity usage. SGAM was created under the guidance of the European standardisation organisations CEN, CENELEC, and ETSI as part of a European Commission mandate (M/490) [51] to support smart grid development through improved interoperability and standardisation [4]. It is in fact, a structured framework for visualising and organising the many layers and parts of a smart grid. Since smart grid is a complex network that combines electricity infrastructure with modern information technologies, SGAM helps map out this complexity by dividing it into five layers and two dimensions as shown in Figure 7.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

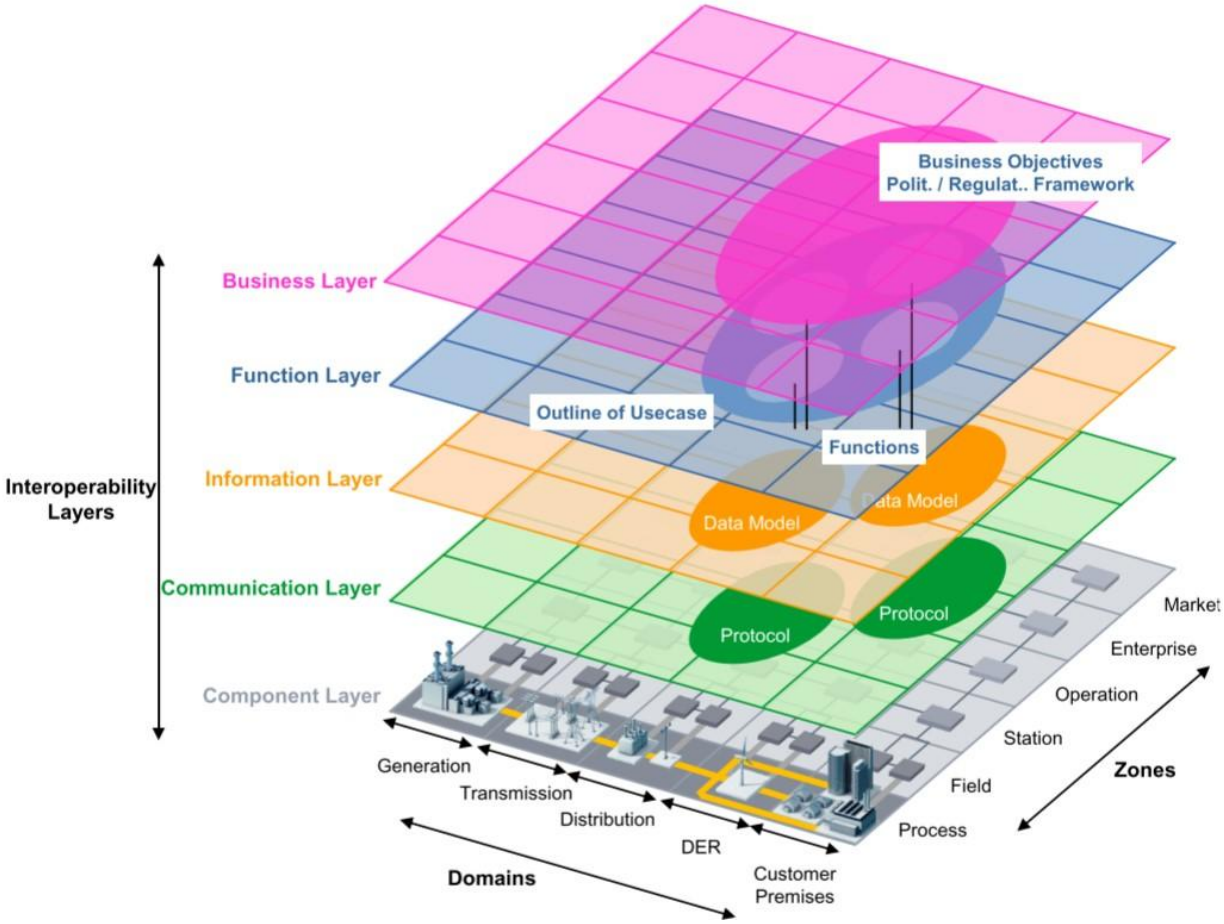

FIGURE 7 – SGAM [4]

LAYERED ARCHITECTURE SUMMARY

A. Component Layer
- Represents data sources and endpoints (e.g., SCADA systems, sensors).
- Supports secure ingestion and pseudonymisation/anonymisation of data.
- Aligned with DESAP goals: non-personal data handling, security, and sovereignty.

B. Communication Layer
- Standardises communication via open protocols and data formats (e.g., MQTT, JSON, CIM, XML).
- Encourages use of interoperable, secure, and open-source technologies.
- Ensures protocol/format neutrality to ease data space integration.

C. Information Layer
- Enables data persistence, harmonisation, and semantic interoperability.
- Divided between:
  - Local: handles data cleaning, quality assurance, vocabulary alignment.
  - Federated: ensures indexing and discovery compliance with shared ontologies.
- Utilises standard vocabularies and metadata schemes (e.g., IEC CIM, SAREF, NGSI).

D. Functional Layer
- Implements data governance and orchestration:

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- Credential & Identity Management (local/federated).
- Data Indexing & Discovery.
- Monitoring & Orchestration.
- Marketplace Backend (billing, contracts, clearing).
- Supports operational trust and traceability aligned with OpenDEI trust and governance building blocks.

E. Business Layer

- Focuses on business use cases, regulatory alignment (e.g., GDPR, eIDAS), and user roles.
- Includes Marketplace Frontend and role modeling (HEMRM).
- Supports Local and Federated business case generation and execution.

The two dimensions represent:

- **Domains** (energy chain stages): Bulk Generation, Transmission, Distribution, Distributed Energy Resources (DER), and Customer Premises.
- **Zones** (hierarchical control levels): Process, Field, Station, Operation, Enterprise, and Market.

By combining these layers and dimensions, SGAM provides a 3D grid-like structure to visualise how different parts of a smart grid system interact, ensuring all players (grid companies, vendors, regulators, etc.) speak the same "architectural language." SGAM serves several purposes as follows:

- It helps stakeholders understand where and how technologies and standards apply.
- It identifies gaps where standardisation is missing.
- It supports the planning and implementation of smart grid projects by aligning technical and business views.
- It ensures interoperability – that is, different devices and systems can work together smoothly.

As the EU moves toward increasingly decentralised energy systems, integrating more Distributed Energy Resources (DERs) into legacy grids significantly raises the complexity of electricity networks. This shift demands close collaboration across multiple disciplines, including information technology (IT), electrical engineering, and business strategy. SGAM plays a crucial role in bridging these domains, providing a unified framework that ensures EU's smart grids remain reliable, interoperable, and adaptable to future needs. It serves as a foundational reference for all stakeholders involved in designing, standardizing, or operating the components of a modern, flexible power grid.

EUROPEAN SMART GRID PROJECTS USING SGAM

SGAM has been adopted and promoted across numerous European research and pilot projects to guide implementation and ensure interoperability. Notable projects include:

- **INTERRFACE** – Aimed to develop an interface between Transmission System Operators (TSOs) and Distribution System Operators (DSOs) for exchanging flexibility services.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- **GRID4EU** – One of the largest smart grid projects in Europe, it explored how smart technologies can be scaled across various national grids.
- **FLEXICIENCY** – Focused on creating a European market for energy services and demonstrated the use of SGAM to support market-oriented use cases.
- **ELECTRA IRP** – Worked on new control architectures for integrating high shares of renewable energy.
- **SmILES** – Addressed the integration of smart grids with local energy storage and optimized energy systems.

3.2.3 European AI Alliance

The European AI Alliance is an initiative of the European Commission to establish an open policy dialogue on Artificial Intelligence (AI) with a broad community of stakeholders [5]. Launched in 2018 as part of the EU's AI strategy, the Alliance has engaged around 6000 members from industry, academia, civil society, and government via online forums and annual assemblies. Its aim is to build an "ecosystem of trust and excellence" for AI in Europe, ensuring that advancements in AI (including those applied to energy systems) align with European values and ethical principles. The Alliance's relevance to digitalisation in energy comes from its role in shaping guidelines and regulations for trustworthy AI – a critical factor as energy systems increasingly relies on AI for optimisation and autonomous control (e.g. in smart grids, demand response, predictive maintenance). By involving experts across domains (health, mobility, energy, environment, etc.), the Alliance helps identify sector-specific AI challenges and solutions, feeding into EU policy recommendations.

One of the Alliance's key contributions is the "Ethics Guidelines for Trustworthy AI" [6], developed by the High-Level Expert Group on AI (AI HLEG) with input from the Alliance. These guidelines define a conceptual reference framework for AI systems, cantered on seven key requirements that AI systems should meet to be deemed trustworthy.

In summary, AI should be:

1. Human-centric – Respecting human agency and oversight (e.g. human-in-the-loop control).
2. Technically robust and safe – Minimising risks of harm or errors.
3. Privacy-preserving and data-governed – Ensuring personal data protection and high data quality.
4. Transparent – Explainable algorithms and traceable decisions.
5. Non-discriminatory and fair – Avoiding biased outcomes and ensuring accessibility.
6. Socially and environmentally beneficial – Supporting societal well-being and sustainability; and
7. Accountable – with mechanisms for auditability and redress

While not a "technical" reference architecture per se, this framework effectively translates into architectural requirements for any AI component within a system: for example, an energy management AI must include modules for logging and explanation (to achieve transparency), data

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

encryption and access control (to ensure privacy and security), and human override controls for critical decisions (to guarantee human agency).

The Alliance complements these high-level principles with operational tools and community guidance. Notably, it released the "Assessment List for Trustworthy AI (ALTAI)" [52] – a checklist-style tool for AI developers to self-assess how well their system meets the above requirements. Through the Alliance's online forum, stakeholders share best practices on implementing such requirements in real-world AI deployments (e.g. techniques for explainable AI in energy forecasting, or frameworks for AI cybersecurity in smart grids). In essence, the Alliance provides an "operational framework" for trustworthy AI: a set of processes, assessment methods, and governance structures that should accompany the technical design of AI systems.

For HEDGE-IoT, which plans to integrate AI/ML at the edge and cloud for energy applications, this means the reference architecture must incorporate features like audit logs, model validation procedures, data governance policies, and user consent management – ensuring alignment with the EU's trustworthiness criteria.

Importantly, the European AI Alliance's work is interoperable with broader EU digital strategies. Its principles dovetail with initiatives such as the European Data Strategy and sector-specific data spaces. For example, the EU's Digitalisation of Energy Action Plan calls for establishing a Common European Energy Data Space for secure data sharing in the energy sector [7]. Trustworthy AI is a key enabler in this context: energy data (from smart meters, IoT sensors, etc.) can be leveraged by AI services only if privacy, security, and interoperability are ensured. The Alliance's guidelines thus inform the architecture of energy data platforms and AI-enabled services to be compliant with forthcoming regulations like the EU AI Act (which will impose requirements on high-risk AI systems including those managing critical energy infrastructure). In summary, the European AI Alliance contributes a value-centric layer to reference architectures – it does not define concrete software modules or protocols, but it sets the requirements and constraints that any AI-enabled architecture (such as HEDGE-IoT's) must satisfy. By following these guidelines, the HEDGE-IoT Reference Architecture can achieve trustworthy AI integration, building public acceptance and robustness into the digitalized energy ecosystem.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

3.2.4 FIWARE Smart Energy Reference Architecture

FIWARE [53] 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.

This high-level model, as illustrated in Figure 8, shows a layered, context-broker-centric IoT architecture for energy solutions. At the foundation, diverse IoT devices and networks feed data upward – their native protocols (MQTT, CoAP, oneM2M, etc.) are translated via IoT agents into a unified format. The core is an Energy Context Information Management layer, built around the FIWARE Orion Context Broker, which aggregates real-time data streams and updates from the field. On top of the context broker, various context processing and analytics components can subscribe to data changes: for example, complex event processing engines or AI/ML modules analyse historical and live data to generate insights or control actions. To the right, an Open Data Portal/Data Marketplace (based on CKAN) allows selected context data to be shared with third-party services or apps under specified terms, with a data monetisation and access control mechanism enforcing usage policies. This architecture emphasises open and modular "Generic Enablers" that can be composed as needed, reflecting interoperability by design.

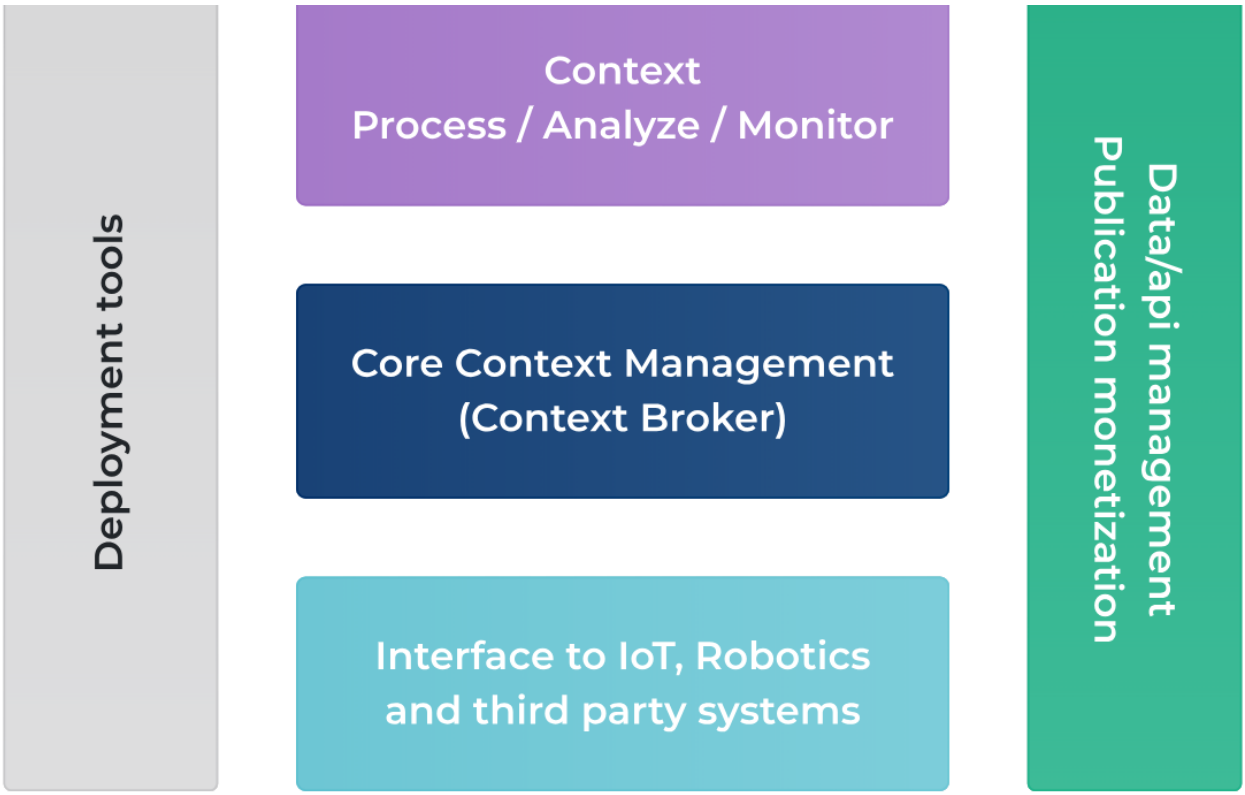

FIGURE 8 - FIWARE COMPONENTS [54]

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

The FIWARE NGSI (Next-Generation Service Interface) API, was initially defined in FIWARE and now standardised as ETSI NGSI-LD, and is the primary interface for creating, retrieving, updating, and subscribing to context information within the system. In a FIWARE-based Smart Energy Reference Architecture, all data from edge devices is modelled as context information. The Context Broker mediates this information: it allows publish/subscribe interactions where producers publish updates and consumers receive notifications. This decoupling via a common data model and API is a key interoperability strategy – new devices or services can plug into the system if they speak NGSI. FIWARE has evolved NGSI from the older v2 to the richer NGSI-LD to support linked data and semantic interoperability, which is highly relevant for energy systems integrating data from many sources.

Figure 9 shows the FIWARE Reference Architecture for Smart Energy Management solutions. 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/OMALWM2M, 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.

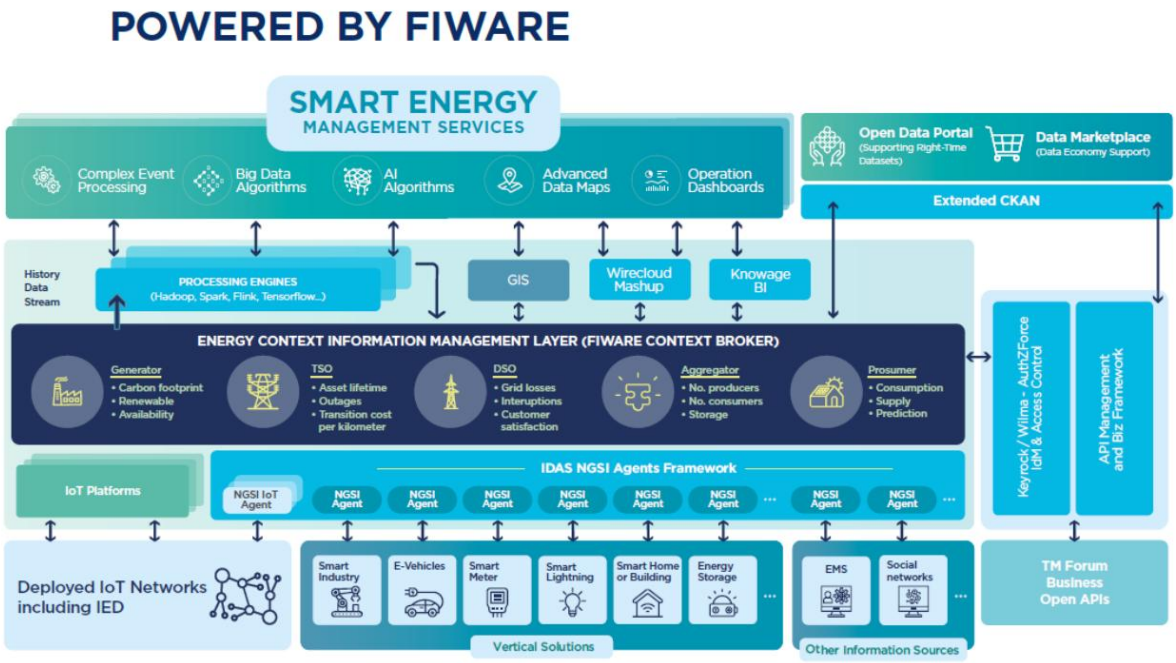

FIGURE 9 - FIWARE ARCHITECTURE MODEL [55]

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

3.2.5 AIOTI

The Alliance for Internet of Things Innovation (AIOTI) is a European forum that plays a pivotal role in IoT standardisation and ecosystem building. Founded in 2015 with support from the European Commission, AIOTI brings together IoT industry players, research institutions, and users to coordinate Europe's IoT innovation and avoid fragmentation. Among its key activities, AIOTI has produced a High-Level Architecture (HLA) for IoT systems – essentially a consolidated reference architecture that integrates best practices from various earlier initiatives. In developing this HLA, AIOTI's Working Group 03 (on IoT Standardisation) followed the ISO/IEC/IEEE 42010 architecture framework, which advocates describing architectures through multiple views and models [9][10]. The result is a vendor-neutral, abstract reference architecture intended to guide IoT deployments across domains (from smart cities to energy, agriculture, manufacturing, etc.), ensuring they share a common vocabulary and structural approach.

AIOTI's reference architecture comprises two main views: a Domain Model and a Functional Model. The Domain Model, derived from the earlier IoT-A project, captures the key entities in an IoT system and their relationships. At a high level, it defines concepts such as "Things", their Virtual Entities, IoT, and IoT Services. For example, in an energy context, an electricity meter is a Thing; its Virtual Entity might be a data object representing the meter's readings and status; the IoT Device is the meter hardware with communication capability; and an IoT Service could be an API to request the latest energy consumption reading of that meter. The Domain Model provides a common lexicon so that different systems can refer to these elements consistently.

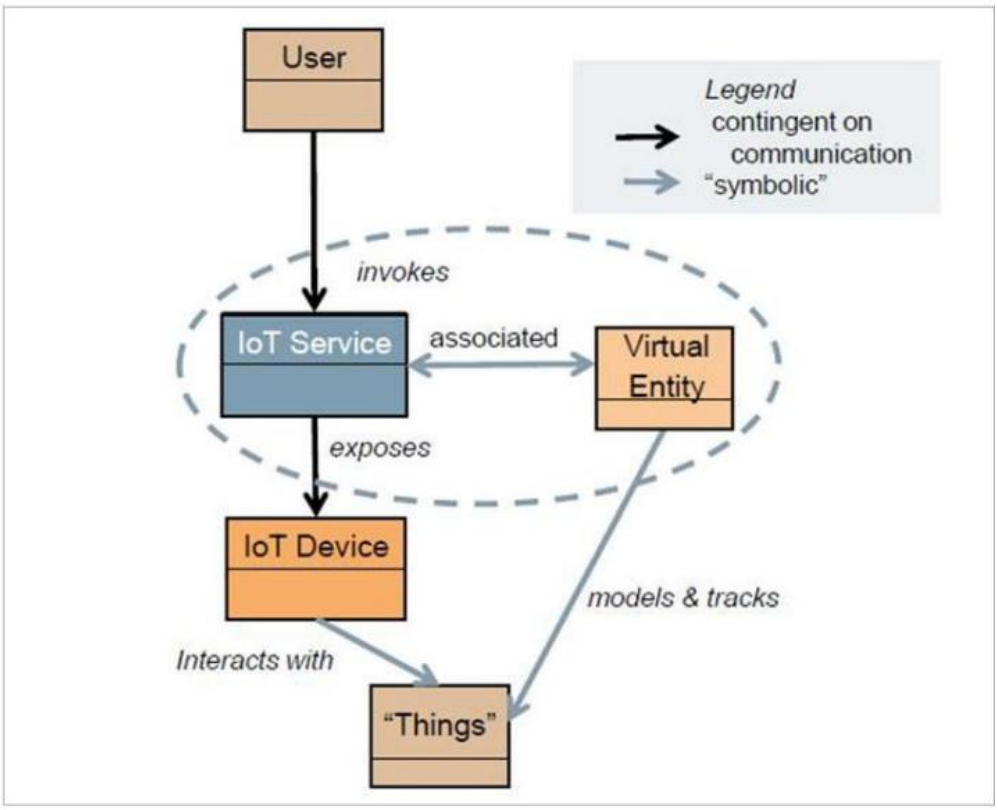

FIGURE 10 – AIOTI HLA DOMAIN MODEL [56]

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

The Functional Model in AIOTI's HLA is presented in Figure 11 describes the logical architecture in terms of layers and functions. AIOTI defines a three-layered IoT architecture:

1. the Network layer,
2. the IoT layer, and
3. the Application layer.

Each layer is a grouping of functional components that provide a cohesive set of services to the layer above. The Network layer corresponds to connectivity and networking services – it encompasses data plane functions for device connectivity and control plane functions such as device addressing, network QoS management, time synchronization, and location services. In essence, this layer ensures that raw data can move from edge devices to the IoT layer reliably and that devices can be reached with commands. The IoT layer sits above and contains the core IoT middleware capabilities. This includes data storage and management, device management, and exposing IoT capabilities via APIs to the applications. The IoT layer essentially transforms raw connectivity into useful services – for instance, translating a stream of readings into higher-level events or coordinating multiple devices' actions. Finally, the Application layer houses the application-specific logic and user interfaces. For an energy system, this could be where a smart home app, a grid monitoring dashboard, or an AI energy optimisation service operates – utilising the IoT layer's services rather than dealing directly with devices. AIOTI's layered model is often depicted with interactions across layers: applications call IoT services through well-defined interfaces; the IoT layer in turn uses network services for communications. Notably, AIOTI specifies interface points (labelled 1 through 5 in their diagrams) between these entities, such as Interface 1 for data formats between Application and IoT layer, Interface 2 for IoT service APIs, Interface 3 for data exchange across networks, etc. – these ensure clarity on how the layers connect and can map to existing standards.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

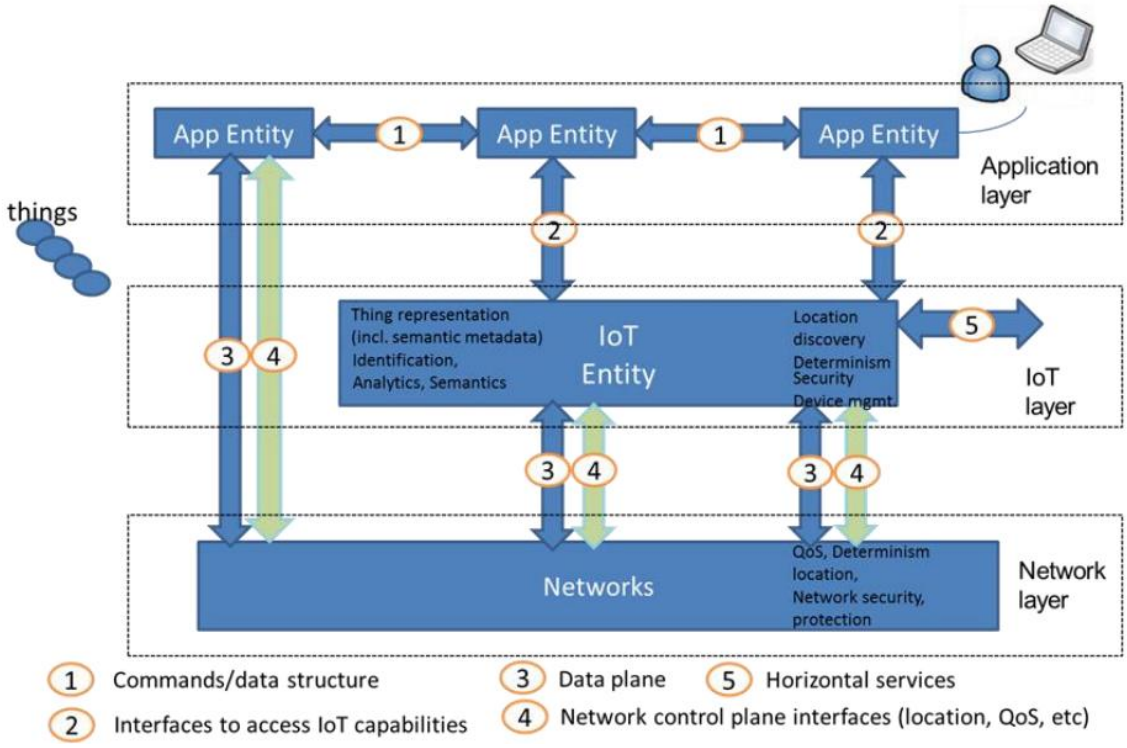

FIGURE 11 - AIOTI HLA FUNCTIONAL MODEL [56]

AIOTI's architecture also stresses cross-cutting functions like security and semantic interoperability rather than treating them as separate layers. In the AIOTI HLA, security mechanisms (authentication, encryption, etc.) are to be applied across all layers (from network up to application) to protect communications and data. Similarly, semantic interoperability is highlighted as a major challenge: the Alliance noted that merely having connectivity (or syntactic interoperability as noted in Figure 12) is not enough if systems don't share meaning. It recommended developing common ontologies and data models for IoT data, and methods to align different domain ontologies and achieve a more advanced interoperability level.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

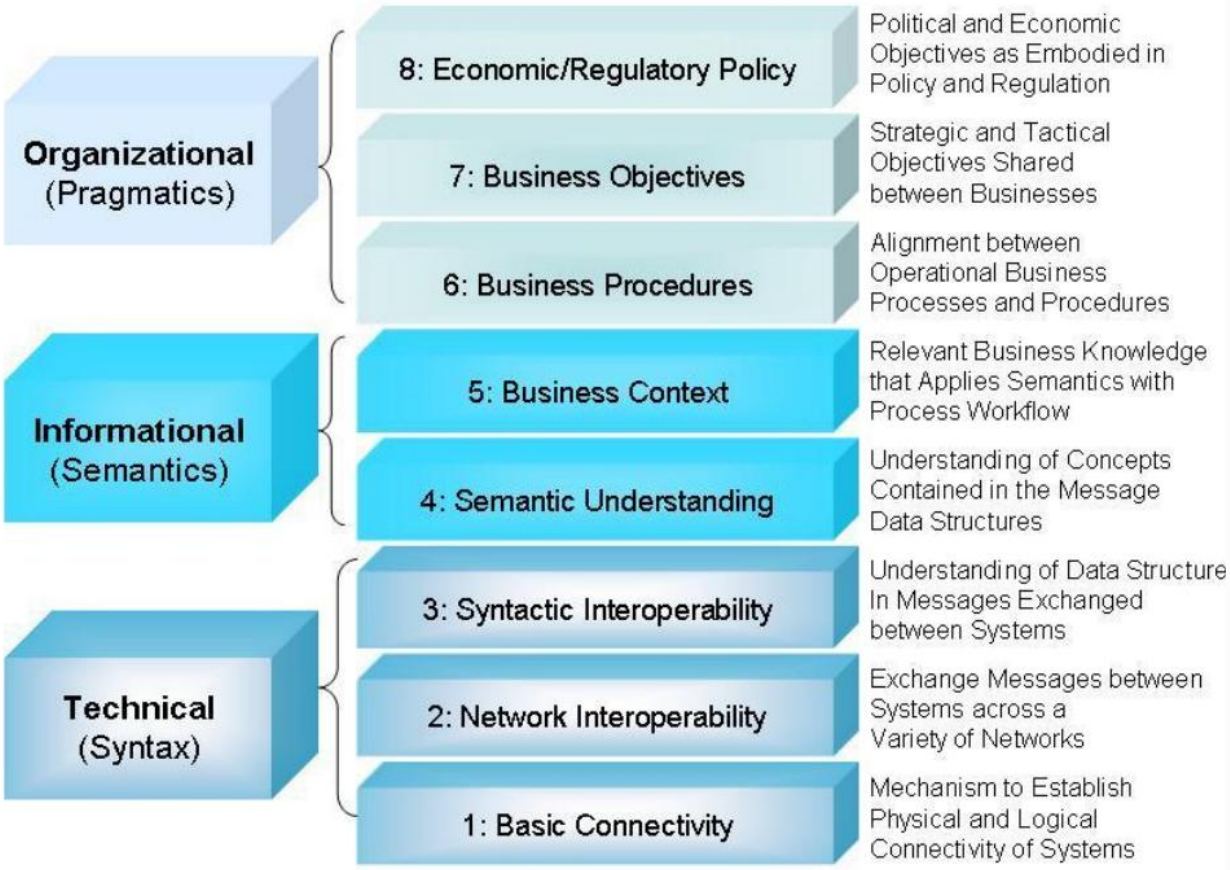

FIGURE 12 - SEMANTIC INTEROPERABILITY LEVELS [57]

RELEVANCE TO HEDGE-IOT

The impact of AIOTI's architecture on HEDGE-IoT is significant, as many European IoT projects have treated AIOTI's RA as a baseline. For instance, the Horizon2020 InterConnect project explicitly based its reference architecture's high-level layers on AIOTI's three-layer model. The HEDGE-IoT project can similarly adopt AIOTI's layered operational framework: this ensures that the system is structured in a clear way, which in turn eases integration with other systems following the same paradigm. By using AIOTI's definitions, HEDGE-IoT can readily map its components to well-understood. Moreover, compliance with AIOTI's architecture means embracing interoperability strategies that are already agreed upon in Europe – like using common API specifications or data formats that AIOTI members promote. This alignment reduces the risk of vendor lock-in and ensures HEDGE-IoT solutions can interoperate with other IoT platforms. Mapping of the HEDGE-IoT RA on the AIOTI RA will be pursued in the final update of this deliverable (D2.4).

3.2.6 IoT-EPI

The IoT European Platforms Initiative (IoT-EPI) was a coordinated effort by the European Commission to foster next-generation IoT platform ecosystems. Under IoT-EPI (2016–2018), seven large research and innovation projects were funded to develop interoperable IoT platforms for

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

"Connected Smart Objects", spanning multiple application domains. The projects – AGILE, BIG IoT, INTER-IoT, VICINITY, SymbIoTe, bIoTope, and TagItSmart – each built different platform components and services but were united by a vision of an IoT landscape where devices and data could flow across platform boundaries. In other words, IoT-EPI's mission was to break the silos of vertical IoT solutions by creating an "IoT web of platforms". This focus on cross-platform interaction makes IoT-EPI highly relevant to HEDGE-IoT, which aims to integrate energy devices and services potentially from different vendors or standards. Digitalisation of energy requires that home IoT, grid IoT, and cloud services interoperate – precisely the kind of scenarios IoT-EPI addressed [11].

Architecturally, IoT-EPI approached the problem on two fronts: common architecture models and common interoperability mechanisms. The initiative recognised that IoT systems involve a stack of technologies from edge to cloud – sensors/actuators, connectivity networks, middleware, data storage, and applications – often provided by different vendors. A key insight was that interoperability must be ensured at each of these layers. IoT-EPI projects collectively covered the full digital value chain of IoT: from devices and gateways to cloud integration and application services. To coordinate efforts, the projects shared results and defined reference interoperability models. For example, the IoT-EPI whitepaper describes a six-level Levels of Conceptual Interoperability Model (LCIM):

1. technical connectivity,
2. syntactic compatibility,
3. semantic understanding,
4. pragmatic alignment,
5. dynamic interoperability, and
6. conceptual alignment.

This model, adapted from simulation theory, provided a vocabulary to discuss where a given solution operates – e.g., a protocol adapter gives technical/syntactic interoperability, whereas a common ontology provides semantic interoperability. IoT-EPI also identified generic patterns of platform interoperability – such as Cross-Platform Access, Platform Federation, Service Brokering, etc. – to classify how platforms can be linked. These conceptual tools informed each project's architecture design.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

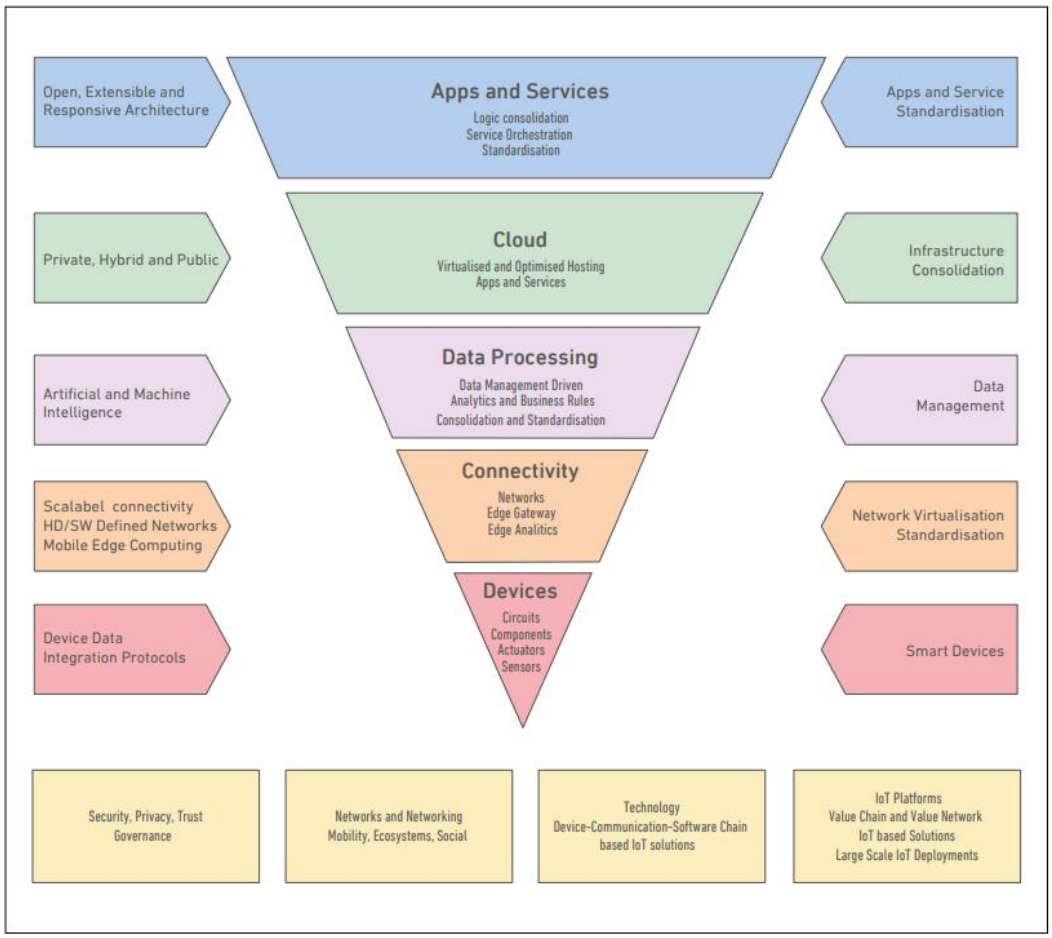

FIGURE 13 - IOT PLATFORMS COVERING THE DATA VALUE CHAIN [11]

Crucially, each IoT-EPI project proposed a reference architecture or framework as part of its solution, and these often-tackled different layers of the IoT stack. A few illustrative examples include:

- **AGILE (Adaptive Gateways for Diverse IoT Environments):** Modular IoT gateway focused on edge computing. Supports multiple device protocols, local processing/storage, and gateway-level security. Relevant for energy scenarios, such as optimising solar and battery data locally before sending aggregated results to the cloud.
- **bIoTope:** Architecture promoting open IoT ecosystems via standardised APIs and data models. Provides interoperability-as-a-service, enabling stakeholders to easily share data with third-party applications through open marketplaces.
- **BIG IoT:** Unified Web API layer facilitating cross-platform IoT interoperability using REST/JSON and semantic descriptors. Enables easy discovery, access, and secure exchange of IoT data/services. Highly relevant to HEDGE-IoT for establishing a unified API for energy data integration.
- **INTER-IoT:** Open cross-layer interoperability framework utilising "Inter-layer mediators." Provides systematic tools for bridging device, network, middleware, data, application, and

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

service layers between different IoT platforms. Particularly useful for integrating diverse energy platforms into cohesive systems.

Across IoT-EPI projects, there were common themes like use of microservices, containerisation, and broker-based communication to enhance scalability and flexibility. Many projects leveraged or extended existing standards: for instance, several used oneM2M's architecture as a starting point, or adopted publish/subscribe brokers like FIWARE's. Semantic web technologies were also frequently employed. In summary, IoT-EPI delivered a rich set of reference architectural patterns tested in real-world scenarios. These include: IoT gateways with local intelligence, federated cloud services with unified APIs, mediator architectures for bridging platforms, and marketplace components for IoT data exchange. All these patterns can inform the design of HEDGE-IoT's Reference Architecture.

From a synthesis perspective, the IoT-EPI experience strongly reinforces interoperability, modularity, and openness as guiding principles. For HEDGE-IoT, aimed at empowering digital energy ecosystems, the ability to incorporate data and services from multiple sources is paramount. IoT-EPI showed that adopting a layered architecture and then implementing specific interoperability enablers at each layer is an effective approach. Concretely, HEDGE-IoT can incorporate an integration middleware similar to that proposed by INTER-IoT, to allow its platform to interface with external IoT without heavy re-engineering. It also underscores the importance of standard APIs and data models in the energy sector – much like BIG IoT and bIoTope created generic APIs, HEDGE-IoT could provide a standard API for energy data/access that third parties could adopt, fostering an ecosystem of "plug-and-play" energy services. Additionally, IoT-EPI highlights edge/cloud distribution: AGILE's gateway and others demonstrate how pushing intelligence to the edge can improve latency and resilience, which HEDGE-IoT should consider for operational decisions.

Finally, IoT-EPI's outcomes align with emerging European initiatives such as European Common Reference Architectures and data spaces. The patterns and tools from these projects are feeding into European standards. By leveraging IoT-EPI lessons, HEDGE-IoT ensures its Reference Architecture is future-proof and compatible. It means HEDGE-IoT can more easily integrate into the coming European Energy Data Space – since it will already use the kinds of open interfaces and semantic interoperability that data space connectors require. In essence, IoT-EPI provides HEDGE-IoT a toolbox of architectural blueprints validated by EU pilots, reducing risk and improving compatibility with the broader IoT landscape in Europe.

3.3. DATA DRIVEN INITIATIVES & SPECIFICATIONS

3.3.1 IDSA

INTRODUCTION & OBJECTIVES

The International Data Spaces Association (IDSA) [12], is a non-profit EU initiative founded as a cooperation of businesses, politics, and research organisations with the goal of the establishment, the development, and the use of a common Reference Architecture Model for secure data spaces and sovereign data sharing on a European and International level. IDSA counts more than 180

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

members from different business domains, sizes that aim to form a universal standard for data exchange and make good use of their data.

The objectives of IDSA initiative could be summarised in the following areas:

- Adoption and support of Modern Data Transfer accommodating modern requirements such as streaming and big data.
- Enhancement of Interoperability, facilitating flexible integration of data space components.
- Enhancement of Standardisation, creating and adopting international standards, providing clear instructions and common understanding among users, and maintaining data quality and integrity.
- Generally, IDSA aims to define a new reference architecture for a secure, sovereign, and trusted data space ecosystem that will appoint the value of data and the participation of actors and stakeholders.

IDSA REFERENCE ARCHITECTURE

IDSA Reference Architecture is inspired by a set of principles and technologies that are crucial for the envisioned concept. A core principle of IDSA is Interoperability. Interoperability is not limited to one data space and can extend across multiple data spaces. This includes:

- **Intra-data space interoperability,** between the data space authority, processing, and data sharing building blocks within a single data space instance.
- **Inter-data space interoperability,** between multiple data space instances at each of the functional levels.

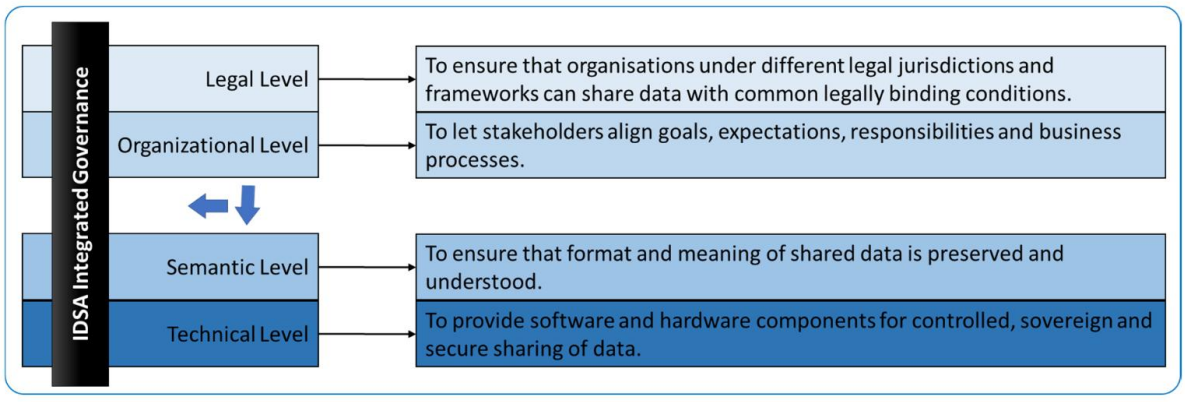

FIGURE 14 - LAYERED FUNCTIONAL MODEL AS ALIGNED WITH THE NEW EUROPEAN INTEROPERABILITY FRAMEWORK [13]

Interoperability within data spaces involves multiple layers and is essential for allowing data sharing across different governing levels. As Figure 14 - Layered functional model as aligned with the New European Interoperability Framework [13]. Figure 14 shows the framework distinguishes four functional levels under an overarching integrated governance approach:

1. Technical level, to provide software and hardware components for controlled, sovereign, and secure sharing of data.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

2. Semantic level, to ensure that format and meaning of shared data is preserved and understood.
3. Organisational level, to let stakeholders align goals, expectations, responsibilities, and business processes.
4. Legal level, to ensure that organisations under different legal jurisdictions and frameworks can share data with common legally binding conditions.

Another core principle of the IDSA initiative is the Data Space Protocol, a set of specifications that enable interoperable data sharing between entities, governed by usage control and based on web technologies. This protocol ensures seamless communication across systems and organisations and consists of two main components, the Control Plane and Data Plane, each playing a crucial role in data management and exchange as it shown in Figure 15.

- **Control Plane:** Ensures interoperability at the dataspace level.
- **Data Plane:** Handles the actual data transfer, implementing various communication protocols like HTTP, to suit specific use cases. This plane manages the practical aspects of data transfer once policies are negotiated.

Key principles and technologies underpinning the IDSA Data Space include: data-driven business ecosystems, data sovereignty, data as an economic good, data exchange and sharing, meaningful data, industrial cloud platforms, big data and AI, IoT and industrial IoT, blockchain, federated frameworks for data sharing agreements, and adherence to regulations like the GDPR. The initiative also contributes to Industry 4.0, the data economy, and ensures privacy in a connected world.

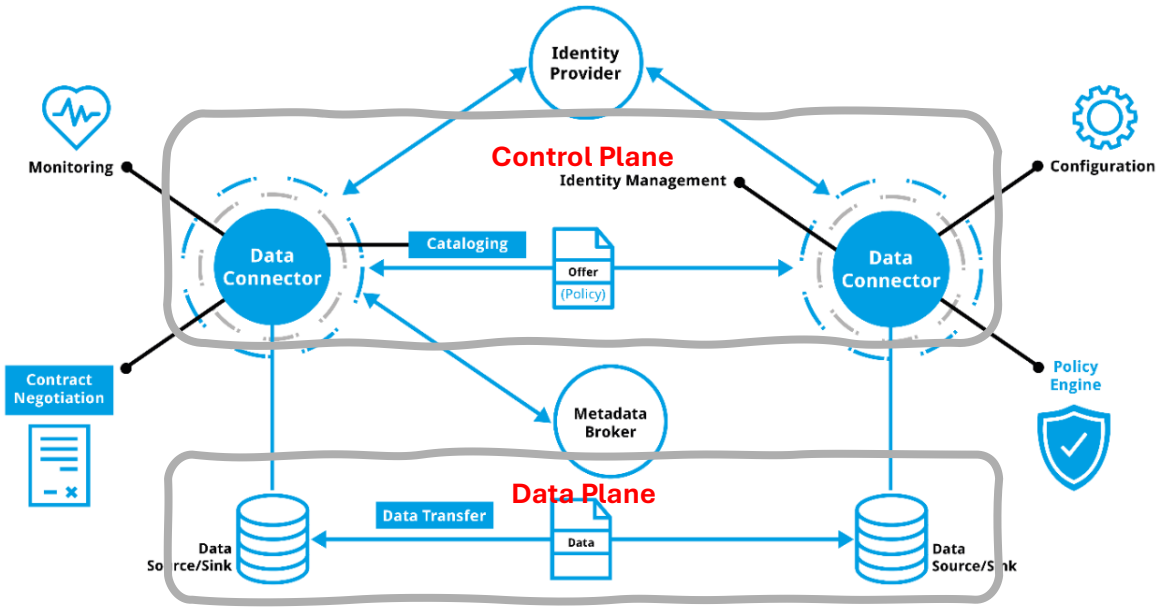

FIGURE 15 - DATA EXCHANGE SERVICES REALIZED BY A DATA CONNECTOR [14]

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

OVERVIEW OF THE IDS RAM

The IDSA defines a framework and governance principles for the Reference Architecture Model (RAM) [15], 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 generalisation of concepts, functionality, and overall processes involved in the creation of a secure "network of trusted data. The Reference Architecture Model uses a five-layer structure that express stakeholder concerns and viewpoints at different levels of granularity as illustrated in Figure 16.

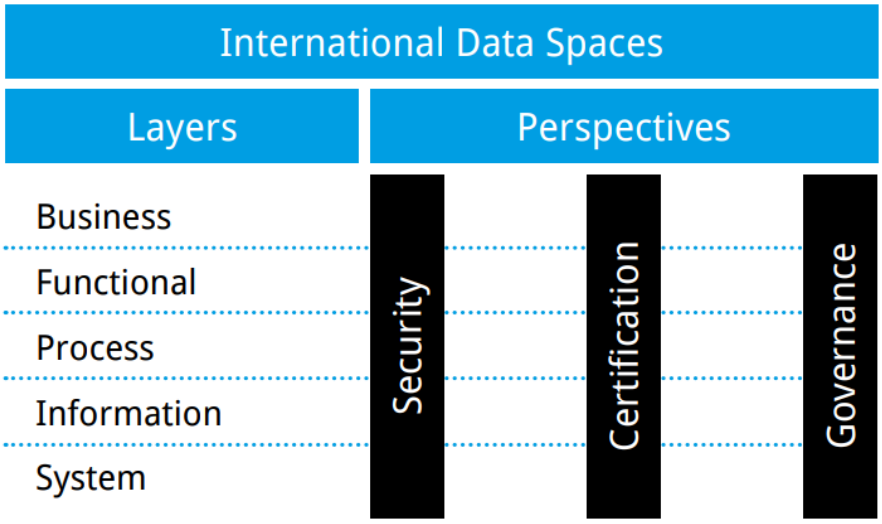

FIGURE 16 - IDSA REFERENCE ARCHITECTURE MODEL [15]

The IDS-RAM introduces a five-layer structure and three perspectives that are the following:

1. **The Business Layer:** Specifies and categorises roles, main activities, and interactions for the IDS participants.
2. **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.
3. **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.
4. **The Process Layer:** Defines the specification of interactions taking place between components by using the BPMN notation, to provide a dynamic view of the RAM.
5. **The System Layer:** Defines the logical software components, considering aspects such as integration, configuration, deployment, and extensibility.

And the three Perspectives:

1. **Security**: Ensures that security measures are integrated across all layers.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

2. **Certification:** Confirms standards and procedures for compliance with IDS-RAM.
3. **Governance:** Provides guidelines for managing data space operations.

BUSINESS LAYER

The Business Layer details the interactions between different roles within data spaces, primarily focusing on how data is shared and utilised among various entities[15]. The key concepts of this structure are Peer-to-Peer Data Exchange without the need of a centralised data approach, a model that supports the formation of a complex value chains and thus sophisticated data service ecosystems, metadata, and transaction management to ensure integrity of data transactions and flexibility in deployment. The overall structure and interactions between the different participants are illustrated in Figure 17 and briefly discussed below.

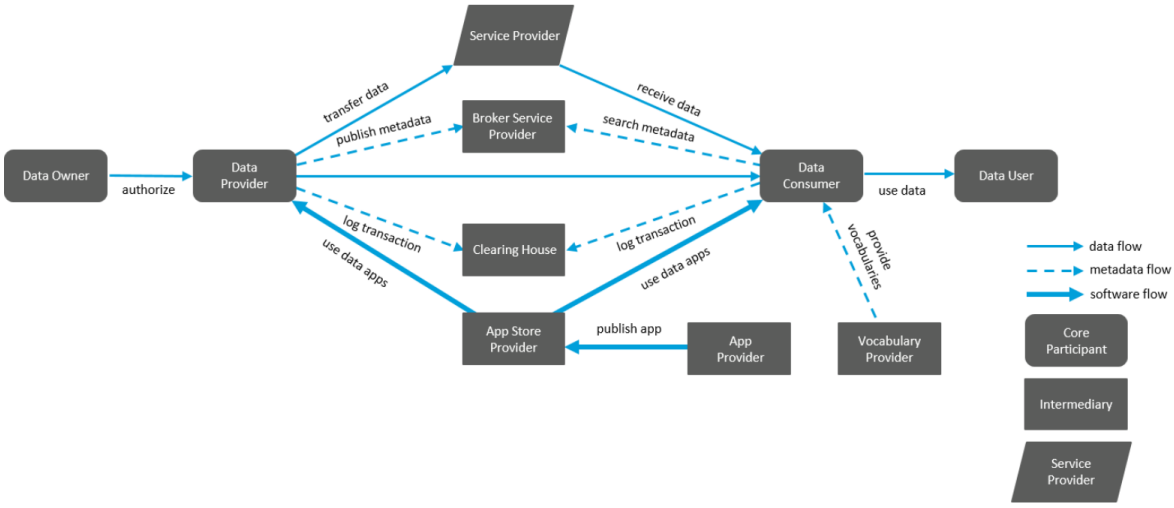

FIGURE 17 - ROLES AND INTERACTIONS IN THE INDUSTRIAL DATA SPACE [15]

The core participants of the Business Layer are:

- **Data Owner:** Holds legal control over data and authorizes its sharing.
- **Data Provider:** Shares data authorized by the Data Owner; often the same entity as the Data Owner.
- **Data Consumer**: Receives data from providers; not necessarily the end user.
- **Data User:** Has the right and permission to use the provided data under agreed conditions.

Supporting Services:

- **Service Providers:** Facilitate data sharing by making data available or processing it for IDS participants.
- **Broker Service Provider [47]:** Helps Data Consumers discover available data sources through metadata management.
- **Clearing House [48]:** Logs data exchange activities, manages billing, and resolves conflicts.
- **App Store Provider [46]:** Publishes compliant data apps facilitating data workflows; built by App Providers.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- **Vocabulary Provider:** Manages ontologies and metadata elements for consistent dataset annotation.
- **Identity Provider:** Validates and authenticates IDS participant identities.
- **Software Provider:** Supplies software components outside the App Store context.
- **Certification Body and Evaluation Facility:** Certify participants and verify technical components' compliance.

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 18 shows the functional architecture of the International Data Spaces, which is divided into six functional groups that must be provided by the IDS.

FIGURE 18 - FUNCTIONAL ARCHITECTURE OF THE INTERNATIONAL DATA SPACES [15]

INFORMATION LAYER

The IDS Information Model is a critical component of the International Data Spaces Association's framework, designed to facilitate effective communication, comprehension, and management of data within an interoperable ecosystem[16]. The primary purpose of this formal model is to enable (semi-)automated exchange of digital resources within a trusted ecosystem of distributed parties, 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".

THE PROCESS LAYER

The Process Layer specifies the interactions taking place between the different components of the International Data Spaces, thereby providing a dynamic view of the Reference Architecture Model.

SYSTEM LAYER

The System Layer maps the roles that are defined in the Business Layer with a concrete data and service architecture to meet the requirements of the Functional Layer. There are three major

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

technical components, which are required to realise an IDS ecosystem: The Connector, the Broker, and the App Store.

RELEVANCE TO HEDGE-IOT

HEDGE-IoT attempts to build a digital framework for the edge-cloud continuum in energy systems using Data Spaces—trusted environments for secure, governed data sharing. The IDS Association, and especially the defined International Data Spaces Reference Architecture, provides the standards and connector frameworks that HEDGE-IoT will adopt.

HEDGE-IoT uses industry standards—like IDS-compliant connectors, semantic models (e.g., SAREF), and Data Spaces governance—that directly map to IDSA's reference architectures and certification programs. This ensures seamless semantic and technical interoperability across devices, systems, and stakeholders.

3.3.2 BDVA

INTRODUCTION & OBJECTIVES

Big Data Value Association (BDVA) is an initiative related research and innovation organisation with the goal of developing an innovation ecosystem that supports AI-enabled and data-driven digital transformation of the economic and social aspects of Europe. BDVA has over 240 participants among Europe and a group of small, medium, and large sized industries cooperating with user and research organisations. Generally, BDVA involves in areas such as data platforms, data spaces, big data services and technologies, data-driven value creation, Industrial AI, standardisation, and skills.

The BDVA initiative focuses on the following main objectives:

- Use data and AI to positively influence business, society, and policymaking with observable outcomes
- Stay up to date with the rapid changes in business and society brought about by AI and data.
- World-class research in AI and data to boost competitiveness.
- Collaborate on novel ventures and capitalise on their potential.
- Make a sustainable future a reality.

The members that participate in the BDVA are enjoying multiple benefits, such as stronger access to the domains of data and AI Research and Innovation policies, standardisation and regulation, broader visibility at EU level, better business opportunities and access to the cutting-edge Research and Innovation environments, and a lot more opportunities to decide, participate and lead.

BDVA ARCHITECTURE

The main centres of activity of BDVA are the Task Forces[17]. The Task Forces are the entities that participate in the planning of the Strategic Research Agendas and in the rest of the initiatives managed by the Association. The BDVA Architecture is composed of three core Task Forces categories, namely Foundational Task Forces, Cross-Sector Task Forces, and the Sectoral Task Forces. Figure 19 presents a schematic instance of the structure of these categories and their content.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

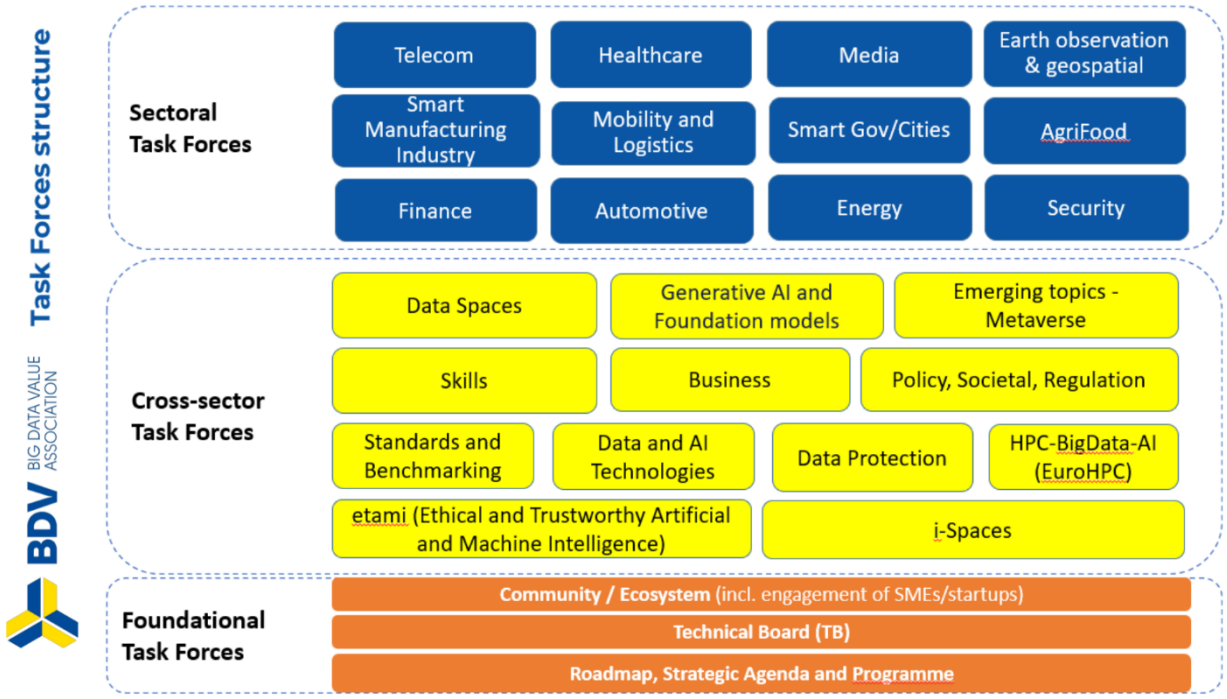

FIGURE 19 - BDVA FOUNDATIONAL TASK FORCES STRUCTURE [17]

The Foundational Task Forces represent the managerial and planning activities, as well as the entities responsible for them. It includes The Roadmap, Strategic Agenda and Programme which coordinated the Strategic Research Agenda and the Strategic Research and Innovation Agenda. The Community and Ecosystem is the Task force that is responsible for developing the engagement activities and tools that will support the BDVA community and attract new members.

The Cross-Sector Task Forces includes concepts and technologies that can be supportive and applied in a wide range of sectors and domains. Analytically, Cross-Sector Task Forces are the following:

- Business.
- Big Data an AI Technologies.
- Data Protection.
- Data Spaces.
- Emerging Topics.
- Ethical and Trustworthy Artificial and Machine Intelligence.
- i-Spaces.
- Policy and Societal.
- Skills.
- Standards and Benchmarking.
- Generative AI / Foundational Models.

Sector Specific Task Forces of BDVA include all the domains of activities that BDVA members become active and operate, namely:

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- Agrifood.
- Automotive.
- Earth Observation and Geospatial.
- Energy.
- Finance.
- Healthcare.
- Media.
- Mobility and Logistics.
- Security.
- Smart Governance and Smart Cities.
- Smart Manufacturing.
- Telecom.

3.3.3 GAIA-X

INTRODUCTION & OBJECTIVES

Gaia-X [58] is an initiative rooted in European values, aimed at establishing an open-source digital governance framework that can be seamlessly integrated into any existing cloud or edge technology stack. This framework is designed to ensure transparency, control, portability, and interoperability of data and services across various platforms. Gaia-X itself is not a market operator, nor does it directly manage or exclusively operate the services that are governed under its framework. The GAIA-X framework [18] embodies the principle of sovereignty by empowering users with the autonomy and self-determination necessary to manage their technology choices independently. It facilitates the development of Data Spaces through trusted platforms that adhere to standardised rules, ensuring that users and providers can establish mutual trust based on objective technological criteria. This foundation enables secure and unrestricted data sharing and exchange among various stakeholders. Rooted in European federalist and democratic traditions, it is based on values including openness, fairness, privacy, security, and transparency. The primary objective is to create a federated and open data infrastructure that aligns with European principles of data and cloud sovereignty. This initiative seeks to develop a data-sharing framework featuring standardised protocols, best practices, and governance structures, all of which are essential to achieving data sovereignty across Europe. Endorsed by all 27 EU member states, the GAIA-X federation is central to Europe's mission of ensuring control over its data landscape, driven by the belief that it will propel the growth of a sustainable and innovative data economy. Key goals of GAIA-X include:

1 **Strengthening Digital Sovereignty**: Empowering European users of cloud services to retain control over their data and make informed choices about their service providers.
2 **Promoting Innovation and Competitiveness**: Facilitating cross-sector data sharing and collaboration among European businesses, thereby enabling the creation of new data-driven services and business models.
3 **Creating an Open and Equitable Digital Ecosystem:** Implementing common standards, requirements, and governance models that ensure transparency, interoperability, security, and robust data protection across the digital landscape.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

GAIA-X AS AN ENABLER FOR ECOSYSTEMS

GAIA-X [58] is crafted to unify Infrastructure and Data Ecosystems through its Operational Model, Conceptual Model, Trust Framework, and Federation Services. The Infrastructure and Data Ecosystems depend on a variety of interconnected services and commodities, each essential for the successful functioning of the other. This integrated approach enables roles such as Providers and Consumers to be interchangeable, with Federators bridging the gaps between different ecosystem components. Governance is ensured through an Architecture of Standards and Policy Rules, which aligns with prevailing standards for infrastructure and data sovereignty, maintaining consistency across the platform. The overall setting is depicted in Figure 20. Federation Services play a key role in enhancing the interoperability of resources across ecosystems, thereby guaranteeing data sovereignty. These services foster trust, make resources consumable and searchable, and support each participant without disrupting their distinct business models, facilitating seamless data and service sharing across ecosystems.

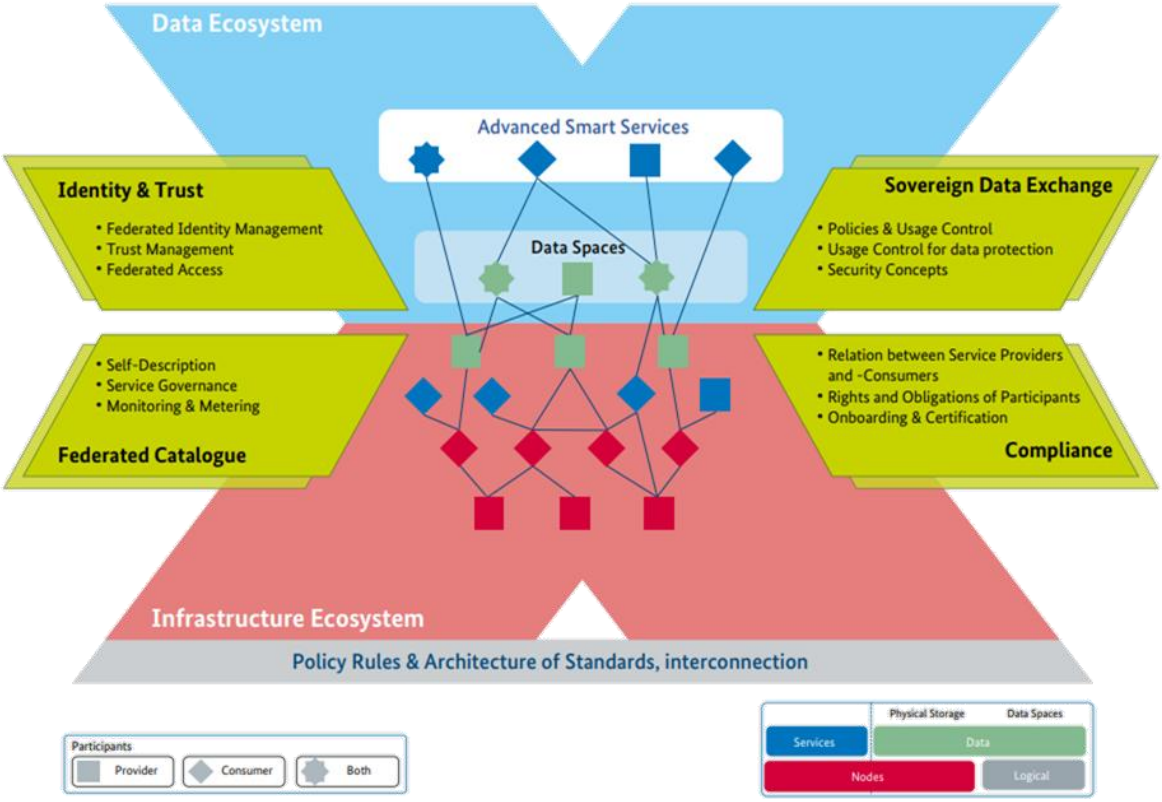

FIGURE 20 - HIGH-LEVEL OVERVIEW OF THE GAIA-X ARCHITECTURE SHOWING THE MAJOR ARCHITECTURE ELEMENTS AND FUNCTIONS ACCOMPANIED BY THE FEDERATION SERVICES [59]

OVERVIEW OF THE GAIA-X ECOSYSTEM

The GAIA-X Ecosystem consists of a federated network of participants, resources, and service offerings, all governed by the GAIA-X Trust Framework and based on NIST's interoperability levels. Below are the descriptions of each plane:

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- **The Trust Plane**: This plane represents the overarching digital governance shared across the entire ecosystem. The common governance rules are defined by the Trust Framework and put into practice through two services:
    - The Gaia-X Registry service, detailed in the Operational Model chapter of this document.
    - The Gaia-X Compliance service, outlined in the Gaia-X Trust Framework.
- **The Usage Plane:** This plane addresses technical interoperability, including interoperability between Service Offerings, ensuring seamless integration within the ecosystem.
- **The Management Plane:** This plane extends the shared digital governance provided by the Federators of the respective ecosystems. It includes potential contract templates tailored to specific vertical markets, such as finance or health, which may have additional governing rules.

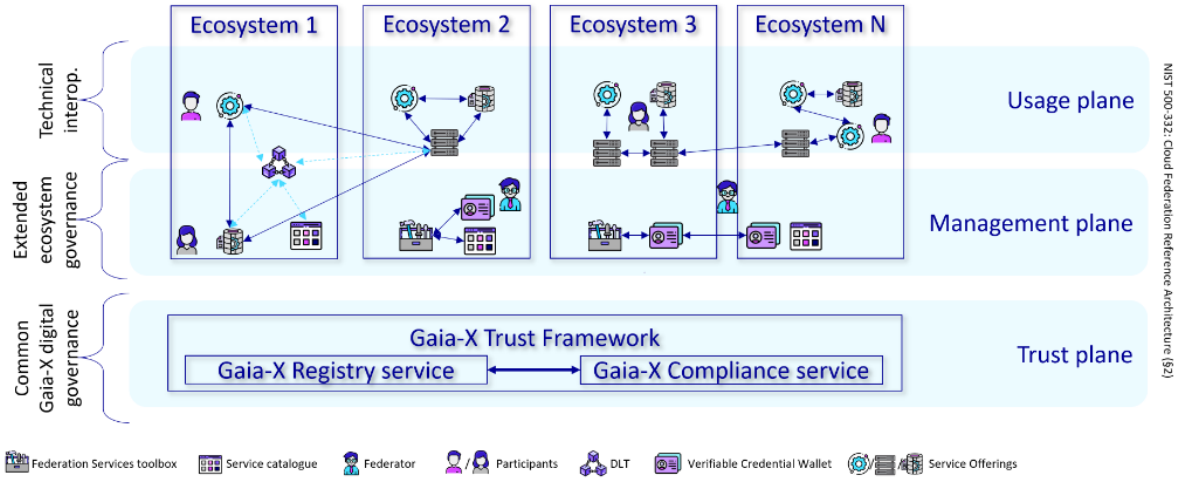

FIGURE 21 - GAIA-X ECOSYSTEM ARCHITECTURE [60]

GAIA-X INITIATIVE ARCHITECTURE

The Gaia-X initiative was launched with the objective of fostering a secure, open, and sovereign approach to data usage. The project is driven by several challenges facing the European digital economy, including:

- Limited transparency and control over data and infrastructure, particularly concerning how data is stored and processed.
- The existence of decentralised processing locations.
- The absence of a unified ontology and sector-specific data spaces.

It is essential to note that the Gaia-X reference architecture [59] is composed of two interlinked ecosystems: the infrastructure ecosystem, which focuses on the provision, connection, and consumption of infrastructure services, and the data ecosystem, where data is treated as the core business asset. These ecosystems are intertwined through federation services and cannot function

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

independently. The federation services encompass Federated Catalogues, Compliance Services, Identity and Trust Services, and Sovereign Data Exchange Services.

GAIA-X CONCEPTUAL MODEL

The Gaia-X Conceptual Model outlines the interactions among various concepts within the Gaia-X framework. It defines key concepts along with essential attributes required for Self-Descriptions, as specified in the Gaia-X Trust Framework. The model is divided into two main sections: the top section focuses on different Gaia-X entities or actors, while the bottom section details elements of commercial transactions and their connections to external parties. This model is visually represented in Figure 22 - Gaia-X Conceptual Model.

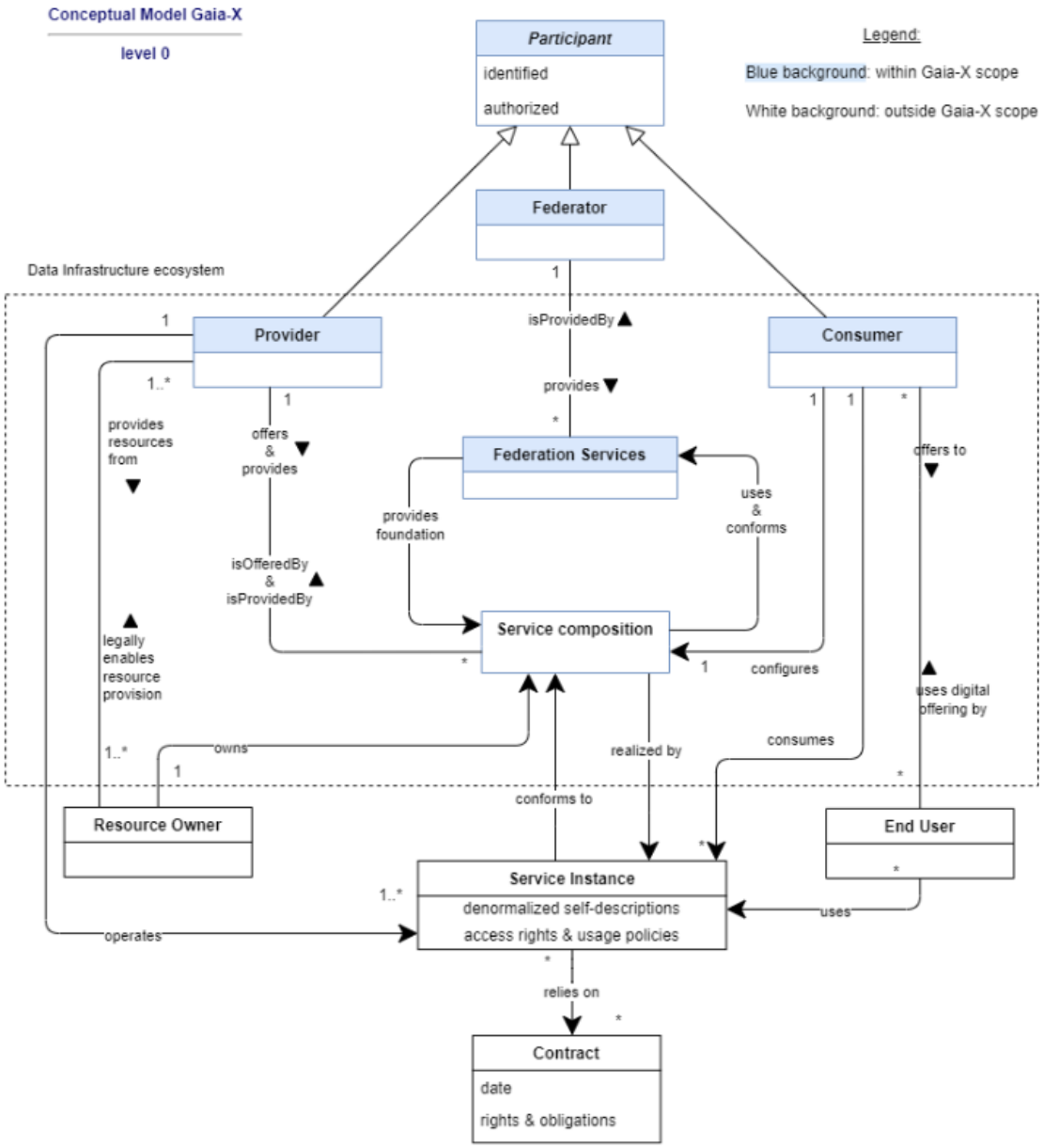

FIGURE 22 - GAIA-X CONCEPTUAL MODEL [60]

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

PARTICIPANTS

Participants in Gaia-X, whether legal entities or individuals, are identified and onboarded through a Gaia-X Self-Description and can assume one of three roles:

- **Federator:** Oversees the management of Federation Services, ensuring the smooth operation of the federation and facilitating interaction among participants.
- **Consumer:** Identifies and leverages service offerings to provide digital services to end-users.
- **Provider:** Offers resources within the ecosystem as services, including associated terms, technical policies, and conditions.

RESOURCES AND POLICIES [19]

In Gaia-X, Policy is a defined set of objectives, rules, practices, or regulations that govern Participant activities. Technically, Policies are assertions, rules, or statements that outline the correct or expected behaviour of an entity. Policies regulate the interaction and usage of the following resources [19]:

- **Consumer Policy/Search Policy:** Lays out the criteria that providers must satisfy to be selected by consumers.
- **Provider Policy/Usage Policy:** Establishes the constraints that consumers must adhere to when using resources.

Resources in Gaia-X are classified into three categories—Virtual, Physical, and Instantiated Virtual Resources [20]. These different types of resources enable various functions within the ecosystem and are defined as:

- **Virtual Resource:** Represents static data, such as a dataset, configuration file, license, key pair, AI model, or neural network weights, along with relevant information.
- **Instantiated Virtual Resource:** Acts as an instance of a Virtual Resource, essentially functioning as a Service Instance with specific endpoints and access rights.
- **Physical Resource:** Represents a tangible entity with weight, space, and location, hosting, controlling, or interacting with other physical entities.

In the Conceptual Model, these resources appear as attributes across all related elements, and their governing policies must align with the general rules outlined in the Policy Rules Document. This relationship is depicted in Figure 23.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

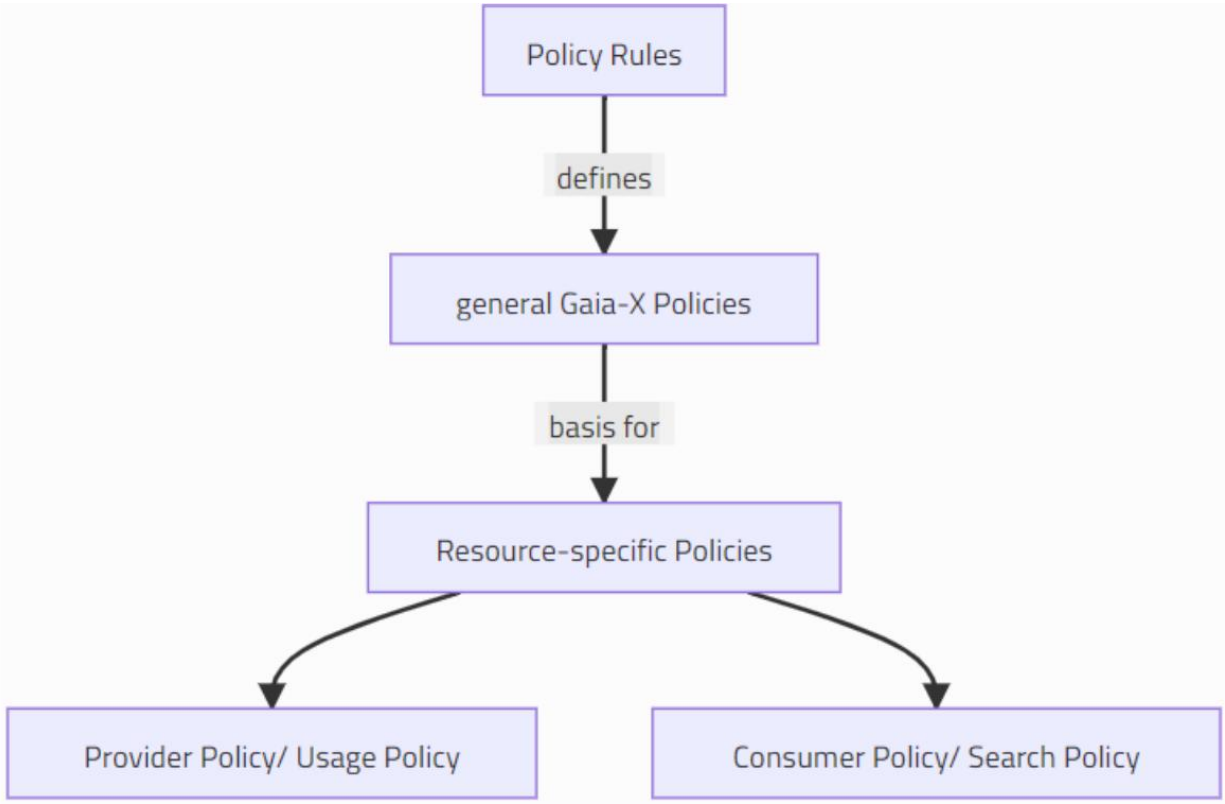

FIGURE 23 - GAIA-X POLICY RULES STRUCTURE [60]

FEDERATION SERVICES

Federation Services are essential for the operational execution of the Gaia-X Ecosystem. These services are organised into four primary categories:

- Federated Catalogue.
- Identity and Trust.
- Compliance.
- Sovereign Data Exchange.

SERVICE OFFERINGS, SERVICE INSTANCES, AND SERVICE CONTRACTS

A Service Offering refers to a collection of Resources that a Provider assembles and publishes as a single entry within a Catalogue. These offerings can be combined to form Service Compositions. A Service Instance represents the real-time instantiation of a Service Offering, directly linked to a specific version of a Self-Description. A Contract is an agreement between a Provider and a Consumer that governs the usage of one or more Service Instances. It is associated with a particular version of a Service, from which it derives the attributes for the Service Instances to be delivered. The Contract has its own lifecycle, independent of the Service Offering, and includes additional attributes and logic that are beyond the scope of the Gaia-X architecture.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SELF-DESCRIPTION DEFINITION

In Gaia-X, Self-Descriptions (SD) provide machine-readable representations of Entities as outlined in the Gaia-X Conceptual Model. These descriptions encompass not only the Participants, but also the Resources and Service Offerings provided by the Providers. To ensure a consistent and standardised portrayal, Self-Description Schemas are carefully defined and can be further customised by Federations to suit their specific domain needs. These schemas play a crucial role in enabling the discovery and comparison of Entities within the Gaia-X ecosystem.

3.4. RELATED PROJECTS

3.4.1. ATTEST

ATTEST PROJECT OVERVIEW

ATTEST (Advanced Tools for the cost-effective decarbonization of future reliable Energy Systems) [21] focuses on researching and developing innovative solutions for the planning and operation of energy transmission and distribution infrastructures. The project seeks to tackle the challenges posed by energy systems in 2030 and beyond, through the creation of a secure, open-source platform. This platform will integrate a suite of optimisation tools aimed at enhancing the operation, planning, and maintenance of power system assets.

The core mission of ATTEST is to assist TSOs and DSOs in optimising and coordinating their systems from technical, economic, and environmental perspectives.

The expected outcomes of the project are:

- To enable accelerated dissemination of the tools among a wide range of research institutions within and outside of the project consortium.
- To help TSO's and DSO's to better manage their networks.
- To provide valuable data for the scientific community and EU energy industry.
- To attest the relevance of the developed solutions.

PROJECT REFERENCE ARCHITECTURE

The ATTEST RA [22] and the key architectural components include the following main aspects:

1. **Modular Open-Source Toolbox:** The project is focused on the creation of a modular, open-source toolbox. It includes three main modules for planning, operation, and asset management. Each of these modules is designed to be flexible and to be used individually in an offline mode, but they will also be integrated into a larger ICT platform.
2. **ICT Platform:** The toolbox will be integrated into a joint ICT platform to enhance collaboration between TSOs (Transmission System Operators) and DSOs (Distribution System Operators). This platform includes several layers:
   - **Data Access Layer:** Enables access to TSO/DSO data and ensures secure data exchange.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- **Visualization Tools:** Provides interfaces for TSO/DSO to visualise data.
- **Converter Layer:** Facilitates conversion between different data formats (e.g., CIM to MATPOWER).
- **Orchestration Layer:** Ensures tools are executed in the correct order for specific tasks.

3. **Data Exchange and Formats:** A variety of formats are used for exchanging data, including MATPOWER, JSON, CSV, and Excel formats. The platform also supports tools for data conversion to handle these different formats.
4. **Design Principles:**
   - **Flexibility:** The system must accommodate future scenarios in energy planning, operation, and management.
   - **Open-Source:** The toolbox and platform will adhere to open-source principles, although some tools might integrate proprietary software.
   - **Optimization:** Tools are developed to support optimised decisions across technical, economic, and environmental considerations.
   - **Secure Collaboration:** Coordination between TSOs and DSOs is a key feature, with mechanisms in place to manage joint technical validation and procurement of ancillary services.

These components reflect the project's aim to support TSO/DSO coordination, enhance system reliability, and promote cost-effective decarbonisation of future energy systems.

RELEVANCE TO HEDGE-IOT

The ATTEST project offers several architectural insights relevant to the development of the HEDGE-IoT Reference Architecture. The modular open-source toolbox developed in ATTEST, with its planning, operation, and asset management modules, highlights a flexible and scalable approach that can inform HEDGE-IoT's objective of enhancing energy system resilience and flexibility. HEDGE-IoT can benefit from ATTEST's ICT platform, which promotes TSO/DSO coordination, secure data exchange, and interoperability across distributed platforms and systems. Additionally, the ATTEST emphasis on optimising both CAPEX and OPEX aligns with HEDGE-IoT's goal of operational efficiency through AI/ML and IoT deployment across edge, fog, and cloud layers.

ATTEST's use of open data formats (e.g., MATPOWER, JSON) and its integration of advanced optimisation tools for real-time operation, planning, and asset management can serve as a foundation for HEDGE-IoT's efforts to develop IoT standards and ensure seamless communication across devices. Moreover, ATTEST's strategy of minimising environmental impacts and increasing network flexibility directly supports HEDGE-IoT's mission of improving renewable energy integration and enabling scalability and replicability in energy systems. Lastly, the collaborative ecosystem approach, involving multiple stakeholders such as TSOs and DSOs, parallels HEDGE-IoT's ambition to drive inclusively and promote trust in ethical IoT practices across the energy sector.

3.4.2. BRIGHT

The BRIGHT project [81], funded by the European Union, aims to significantly enhance demand response capabilities at the residential consumer level by leveraging innovative technologies and

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

collaborative methods. Recognising the transformative potential of increased electrification in heating, transport, and decentralised renewable energy sources, BRIGHT harnesses blockchain technology, digital twins, and advanced artificial intelligence to deliver comprehensive, data-driven energy management solutions. Central to BRIGHT's approach is a participatory co-creation process that elevates individual consumers to an active role, resulting in multi-layered, adaptable, community-centred DR frameworks across diverse domains and timescales. The project's innovative strategies integrate user-centric designs influenced by social science research to effectively motivate user behaviours through both monetary and non-monetary incentives.

BRIGHT Project Objectives:

- Implement a participatory co-creation process, empowering individual consumers to actively engage in demand response activities.
- Develop and deploy multi-layered, community-centred, adaptable, cross-domain demand response solutions.
- Leverage blockchain and smart contract technologies to facilitate secure, semi-decentralised virtual power plants (VPPs) enabling peer-to-peer interactions.
- Utilize digital twin technology for enhanced predictability of consumer energy behaviours and requirements.
- Integrate advanced AI algorithms for managing flexibility, value stacking, and providing both energy and non-energy services.
- Validate the project's methodologies and technologies across four demonstration sites in various EU countries, engaging around 1,000 predominantly residential consumers in diverse community configurations such as Local Energy Communities (LEC), Citizen Energy Communities (CEC), Virtual Energy Communities, and mobile communities.

The BRIGHT architecture for social, technological, and business ecosystems in demand response integrates the following layers (Figure 24):

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

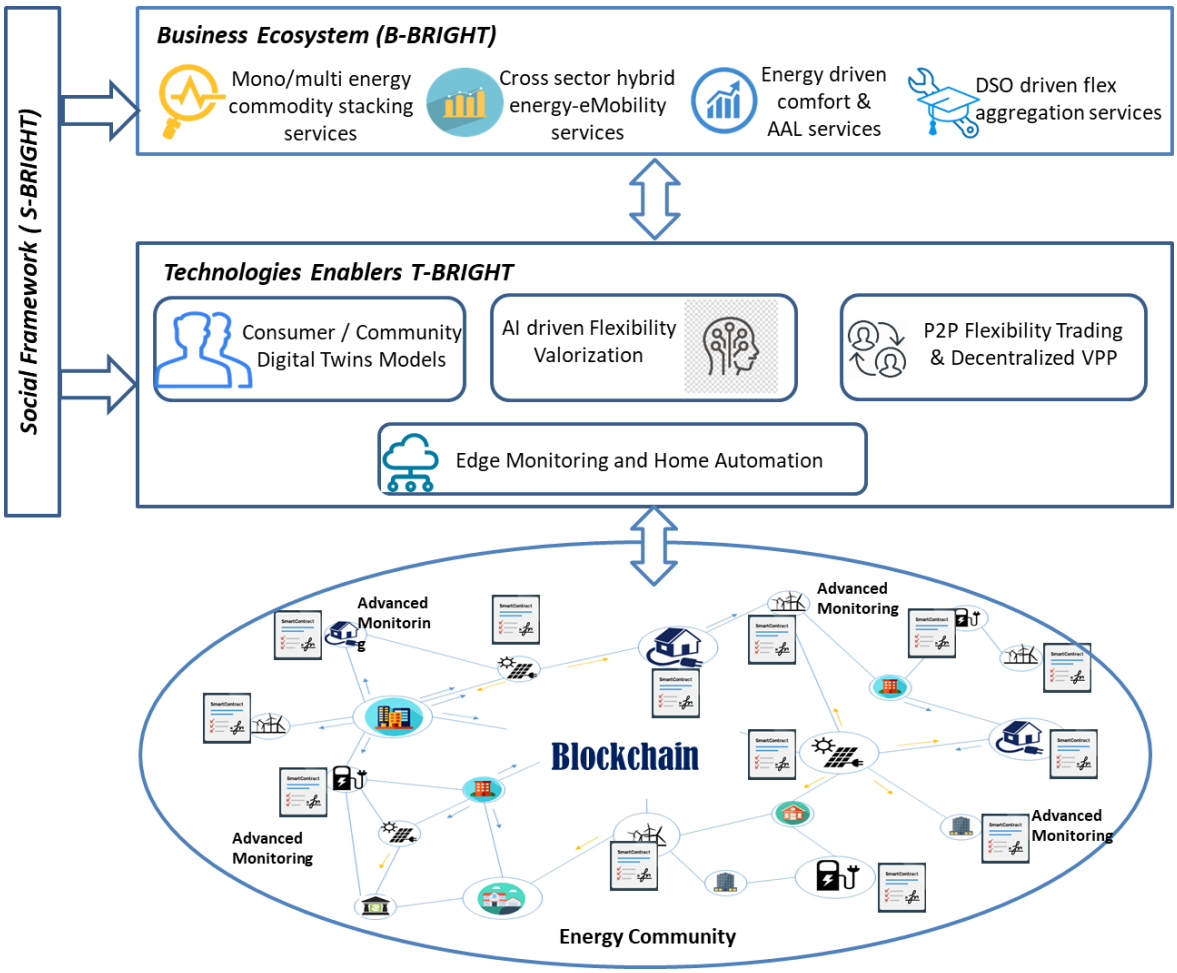

FIGURE 24 - BRIGHT ARCHITECTURE FOR DR SOCIAL, TECHNOLOGICAL AND BUSINESS ECOSYSTEM [81]

S-BRIGHT (BRIGHT Social Science Framework) for soft modelling of end user behaviour when considered as a member of a community-centric organizational configuration. Combines insights from social sciences and behavioural economics to understand the electricity consumer social beyond-economical motivations for participating to DR programs (user experience design) and for appropriate incentive design (e.g. environmental, risk aversion, sense of community belongings, etc.).

T-BRIGHT (BRIGHT Technological Enablers) leverages on latest advancements on IoT, AI, Blockchain and Big Data technologies to build Digital Twins models for individual consumers and for communities aimed to improve consumer behaviour predictability and to support the implementation of novel community-oriented services for increased flexibility mobilization. **T-BRIGHT** includes the following technological tools:

- *B-DT (BRIGHT Digital Twins)* for customers and community and big data enabled accurate prediction. Tools built by integrating data-driven models for citizen and community behaviours, with the respective preferences (e.g., thermal comfort for temperature, reasonable price for flexibility provisioning) and within data-driven models for asset flexibility incentivisation.

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- *B-FLEX (BRIGHT AI Driven Flexibility Valorisation)* consider the Digital Twins models and prediction outcomes to deliver optimal flexibility services at the level of end-user, community and system.
- *B-DLT (BRIGHT Distributed Ledger Technology)* implement a P2P energy flexibility market and decentralised P2P virtual power plant reciprocal complementarities among flexible assets and end users' preferences.
- *B-EMHC (BRIGHT Edge Monitoring and Home Automation)* a stack for electricity metering infrastructure and smart home automated control, with interoperability features. The interoperability is supported using the components presented in Figure 25.

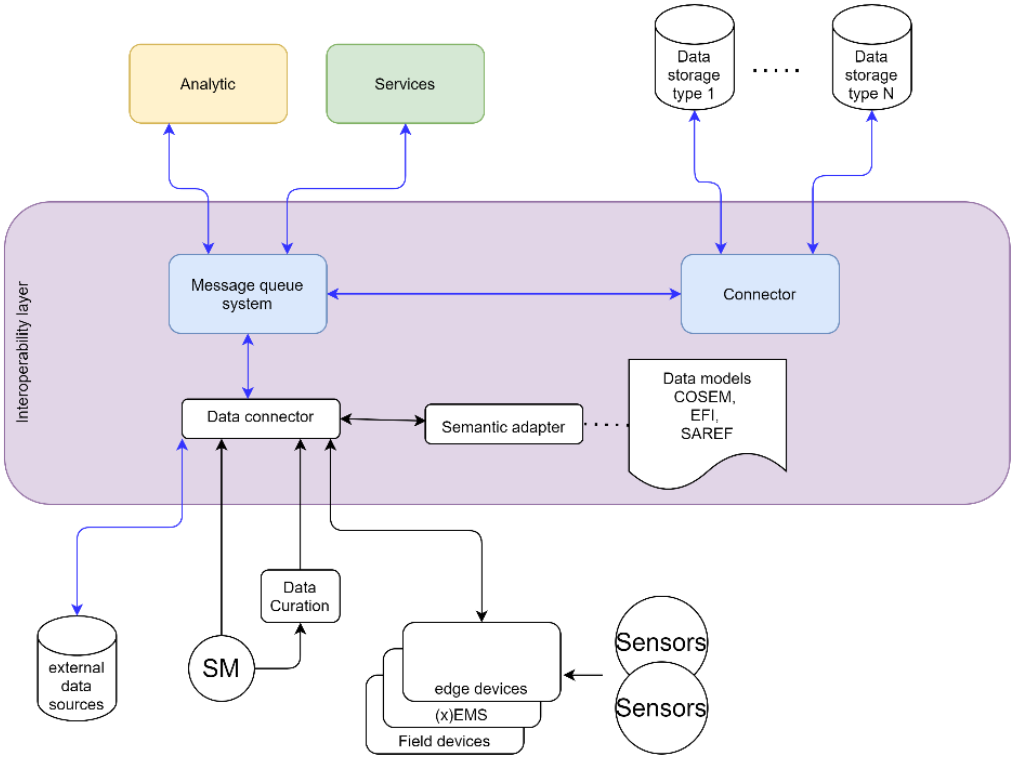

FIGURE 25 – BRIGHT ARCHITECTURE INTEROPERABILITY LAYER WITH THE COMPONENTS [82]

The **B-BRIGHT (BRIGHT Business Ecosystem)** features integrated cross energy sector service offering for both DR operators, consumers and EV mobility managers, personal care operators. Multi-value stacking services such as EVs fleet management to provide DR, comfort-enabled energy management, safety within a smart home context.

3.4.3. Enershare

ENERSHARE PROJECT OVERVIEW

EnerShare [62] (European Common Energy Data Space Framework) is a Horizon Europe project that has as its main goal the development, deployment of a European Data Space which while progressing also towards the governance scheme of data space. The project has a secondary slogan

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

that appeals to the energy domain, namely in exploring the Energy and Non-Energy services that focus on exploring the intrinsic value of data.

The project expects to contribute towards a group of challenges:

- Interoperability & Data Space technological building blocks.
- Data Sharing culture.
- Data Governance Mechanisms and Models.

The project has also specific objectives that navigate around establishing and exploring intrinsic value of data trough intra-energy and cross-sector interoperable services, while maintaining control of data ownership and usage limits by exploring the data space trusted data ecosystem.

ENERSHARE PROJECT REFERENCE ARCHITECTURE

The reference architecture for the project is depicted in the following Figure 26:

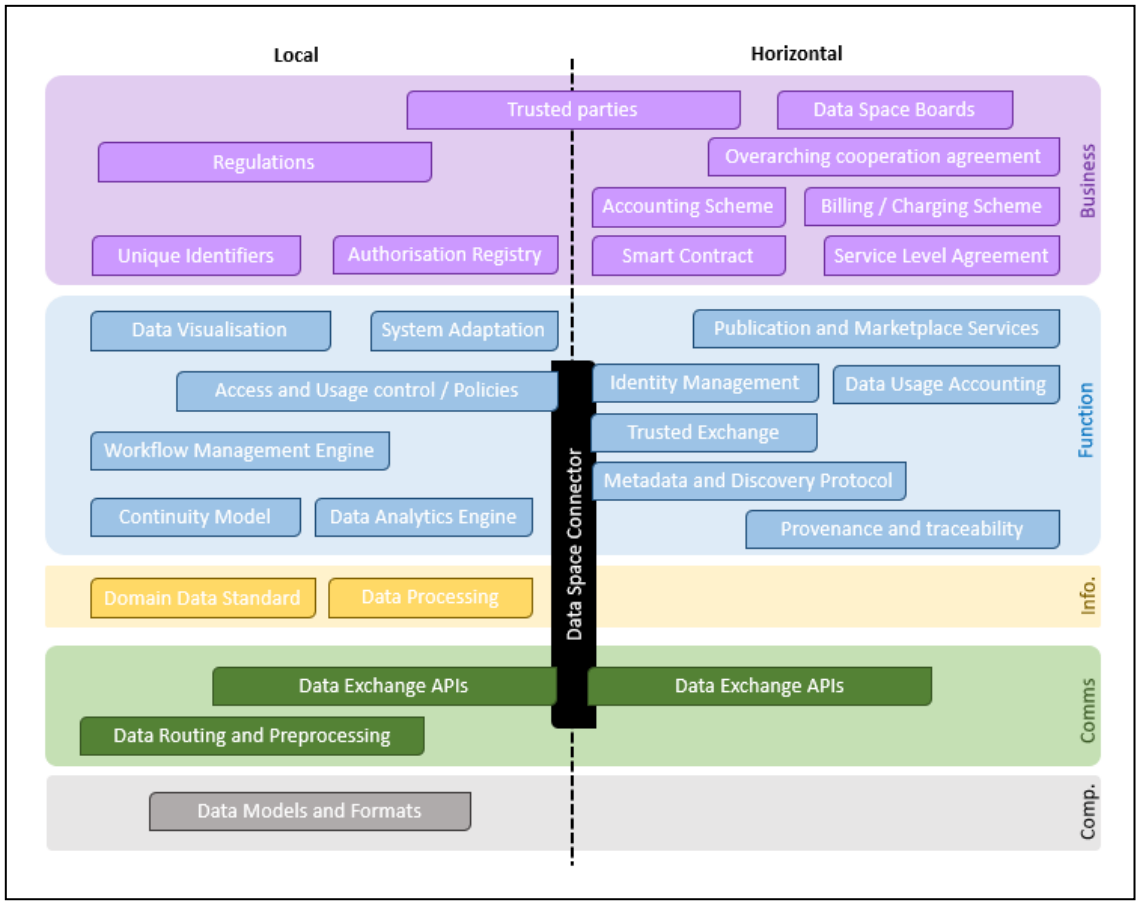

FIGURE 26 - ENERSHARE DATASPACE REFERENCE ARCHITECTURE [61]

The Reference Architecture includes five horizonal layers including the Business, Function, Information, Communication and Component Layers. The vertical split distinguishes between local building blocks that facilitate the functionalities local to a use case, and the horizontal building

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

blocks that allow requirement-abiding participation in the Data Space. The Data Space Connector integrates the local systems with the horizontal domain into the Data Space.

RELEVANCE TO HEDGE-IOT

The discussions held in Enershare's internal forums and most importantly its conclusions are of utmost relevance to HEDGE-IoT. This is reflected in Enershare's reference architecture. As a data spaces' project, the reference architecture for the project departs from the International Data Spaces Association – RAM (Reference Architecture Model) which includes the conceptual, business and technical building blocks. Thus, Enershare departed from RAM, and specialised in the needs of Energy and Non-Energy services. Namely, it included concepts from the last version available of the BRIDGE's SGAM model to reflect the Energy Ecosystem. Special care was devoted to the links between the technical building blocks, namely in the management of independent software components (Apps), the availability and interoperability of available Data Space Connectors within the consortium and the Data Space Governance dimension.

Therefore, HEDGE-IoT should move forward considering the same principles, in this case, departing from the IDSA RAM and available evolutions of the projects, namely those compiled through the INT-NET CSA project, whose initiative includes the collection and collaboration among Data Spaces' sister projects. In HEDGE-IoT case, it should focus in the specialisation of adopting the Edge scenario, enable it with interoperability mechanisms (data space connectors or liaison with service in the vicinity of the edge), exploring the possibilities of edge devices to conduct computation, namely AI inference on Edge Data and; enabling the efficient balance between processing data in the edge for privacy sensitive data/processes with the higher aggregation capabilities of the cloud i.e., the edge-cloud continuum.

Finally, but not less important, HEDGE-IoT should adopt a data space connector that abides by the newly installed data space protocol as to ensure that the services developed in this project are able to be sustained after the project end, via a Data Space connector that should technical and interoperable viability.

3.4.4. I-NERGY

PROJECT OVERVIEW

The I-NERGY project is an innovative initiative aimed at transforming the energy sector through advanced AI and data analytics. It focuses on enhancing energy management, optimising resource allocation, and improving the overall efficiency of energy systems. The project integrates cutting-edge technologies, including ML, DL, and digital twin applications, to address various energy challenges [24].

I-NERGY ARCHITECTURE LAYERS

1. **Interconnection Layer: AIoD-I-NERGY Synergy**

The AI on Demand (AIoD) platform plays a key role in the I-NERGY architecture by enabling two-way sharing of AI resources and supporting innovation in the European AI ecosystem. I-NERGY leverages

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

AIoD to enhance its services—particularly for energy load forecasting—and plans to publish assets on platforms like AI4EU. This integration also fosters community engagement through events and collaborative tools, strengthening ties between I-NERGY and AIoD during solution onboarding and development [25].

2. **Data Service Layer:**

The I-NERGY Data Service Layer acts as a mediator between data providers and consumers, supporting the use of various datasets in AI-trained models and energy analytics applications. The key components are [26]:

- **Data Ingestion** is handled by the Interoperability Service, integrating diverse data types (structured, unstructured, real-time, IoT) across various protocols and actors.
- **Data Harmonization**, via the Homogenisation module, cleanses, curates, anonymises, and models data using shared vocabularies to support a unified data model.
- **Data Storage** organises and stores processed data in suitable systems to support project services and tools.

Application Layer – Energy Analytics Applications: The I-NERGY Application Layer encompasses a range of energy analytics applications and services, including AI/ML models, Digital Twin applications, and user interfaces (UIs), along with the I-NERGY Marketplace. This layer connects to the Data Services Layer for data required in model training and analytics. Key features include [28]:

- Independent Microservices
- Digital Twin Applications
- User Interfaces
- AI Services Categories (e.g. Energy Forecasting, Flexibility Forecasting and Demand Response, Predictive Maintenance, Activity Recognition and Forecasting, as well as Anomalous Behavior Detection)

This layer is integral to the overall architecture, facilitating advanced analytics and real-time decision-making within the energy sector.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

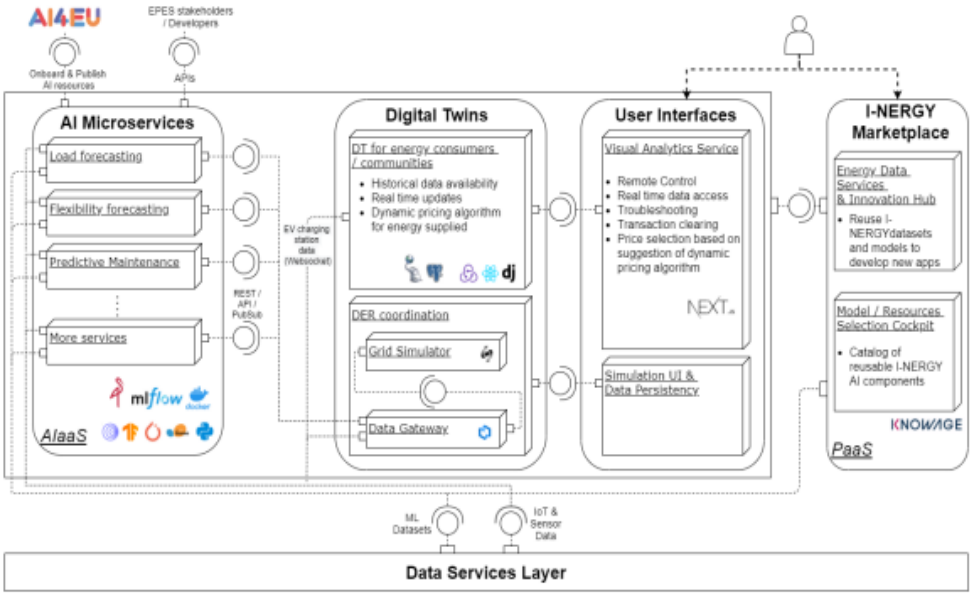

FIGURE 27 - I-NERGY APPLICATION LAYER ARCHITECTURE [28]

I-NERGY Marketplace: The I-NERGY Marketplace is a virtual environment for developing and deploying AI-based energy services. It supports Python and R, offers access to pre-trained models and datasets, and includes two sub-modules: the Innovation Hub for rapid service creation and the Selection Cockpit for browsing ML models. It streamlines model development and accelerates innovation [29].

3.4.5. MATRYCS

PROJECT OVERVIEW

The MATRYCS (Modular Big Data Applications for Holistic Energy Services in Buildings') project is a completed H2020 project, ran from October 2020 to September 2023.

The key technical objectives of the project were:

- To develop a data-driven Reference Architecture for AI-based scalable big data management & analytics in smart energy-efficient buildings, through a secure, scalable and fault-tolerance big data Reference Architecture for smart energy-efficient buildings and underlying set of Open APIs.
- To develop a semantic and business interoperability framework for cross domain analytics applications, cross-context learning and datasets spanning entire buildings value chains.
- To deliver a data governance technology enabler which will facilitate seamless cross-stakeholder data sharing, trusted data exchange and handling, allowing full data sovereignty and control of respective data ownership, access, security and protection.

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- To adapt, evolve, upscale and deploy a technology enabler for a set of trained, high-quality ML and DL models by exploiting existing dataset formats across Europe for advanced classifications, analysis and forecasts related to buildings.
- To upscale and deploy the MATRYCS open, cloud-based data analytics toolbox along different deployment modes (IaaS/SaaS/PaaS).

REFERENCE ARCHITECTURE

Regarding its Reference Architecture, the MATRYCS RA consisted of three independent but interconnected layers:

- The MATRYCS Governance Layer.
- The MATRYCS Processing Layer, and
- The MATRYCS Analytics Layer.

3.4.6. OneNet

PROJECT OVERVIEW

The project OneNet (One Network for Europe) [63] is funded through the EU's eighth Framework Programme Horizon 2020. OneNet provides a seamless integration of all the actors in the electricity network across Europe to create the conditions for a synergistic operation that optimises the overall energy system while creating an open and fair market structure [30].

The key elements of the project are:

- **Definition of a common market design for Europe:** this means standardised products and key parameters for grid services that aim at the coordination of all actors, from grid operators to customers.
- **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
- **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.

REFERENCE ARCHITECTURE APPROACH

Hybrid approach

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.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Following reference architectures and initiatives were given the focus in the OneNet project: BRIDGE, COSMAG, FIWARE (namely the Smart Energy Reference Architecture), ETIP SNET, BDVA, IDSA and GAIA-X.

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.

ONENET REFERENCE ARCHITECTURE:

The Reference Architecture (Figure 28) consists of three logical layers:

- **OneNet Participants Layer** which makes available and accessible data from different Data Sources to the Energy Stakeholders in a secure and trusted way, ensuring data ownership and privacy.
- **OneNet Network of Platforms Layer** which facilitates the platforms integration and cooperation for cross-platform market and network operation services. It includes any demo platform (e.g., DSO platforms, Market platforms, Data Exchange platforms) able to connect with the OneNet Middleware using the OneNet Connector.
- **OneNet Framework Layer** which could be described as a scalable and pluggable solution for facilitating the platform cooperation and integration. It can create a unique ecosystem in which any energy stakeholder can participate. A decentralised middleware is used to ensure different platforms from the Network of Platforms can successfully communicate with the rest of the platform, with FIWARE Context Broker as the unifying component.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

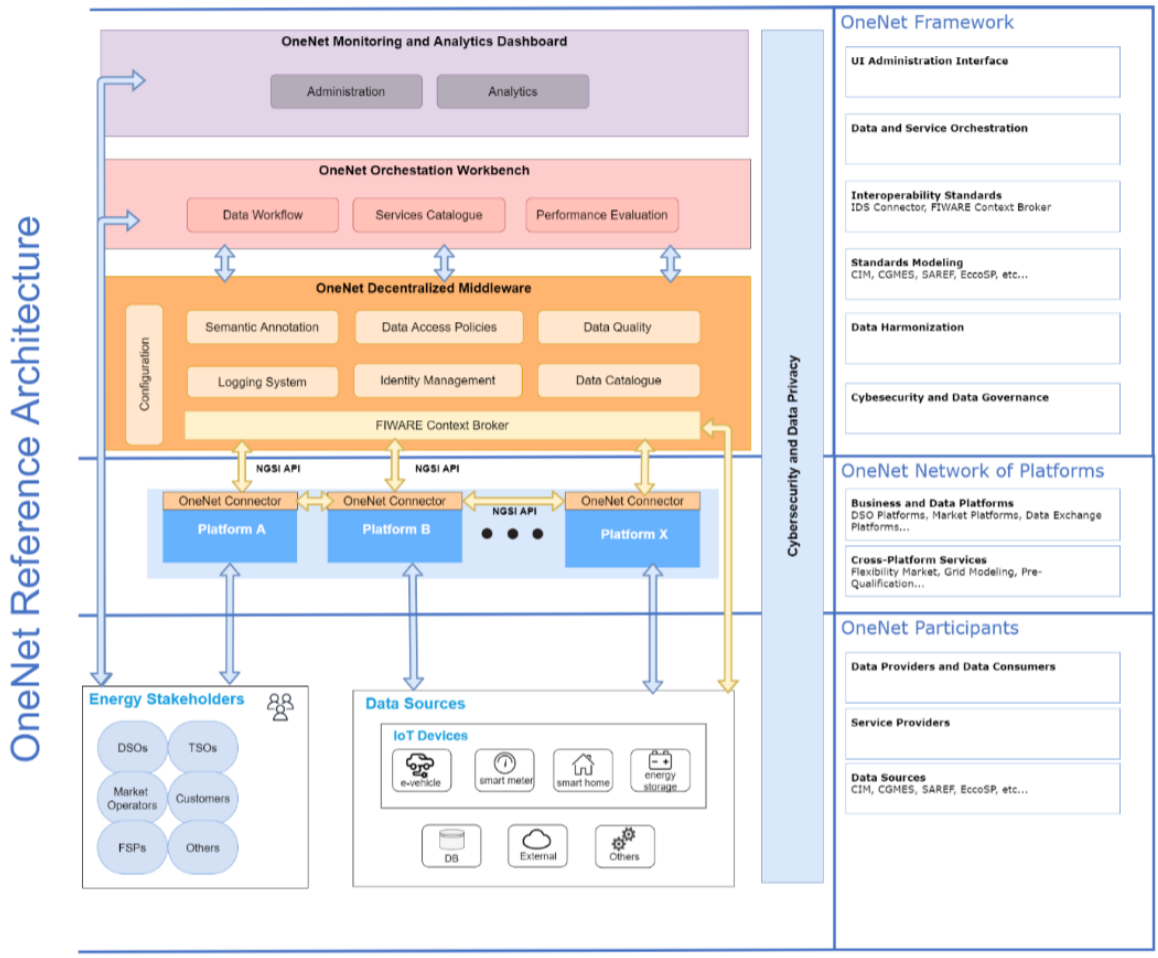

FIGURE 28 - ONENET REFERENCE ARCHITECTURE [30]

FINAL THOUGHTS

Overall, the design of OneNet Reference Architecture considers a comprehensive selection of requirements and aspects of smart grid data, and it uses several international projects and frameworks to establish the groundwork on which OneNet itself is built upon.

FIWARE Context management seems to be the unifying component in connecting different platforms to the OneNet architecture. If Hedge IoT project has these different platforms from different participants of the project, some sort of integration to FIWARE compliant data models/APIs is necessary if OneNet reference architecture is followed to the letter.

3.4.7. PLATONE

PROJECT OVERVIEW

The project "PLATform for Operation of Distribution Networks" (Platone) [64] aimed to develop an architecture for testing and implementing a data acquisition system based on a two-layer Blockchain approach: an "Access Layer" to connect customers to the DSO and a "Service Layer" to link customers and DSO to the Flexibility Market environment. The two layers are linked by a Shared

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Customer Database, containing all the data certified by Blockchain and made available to all the relevant stakeholders of the two layers.

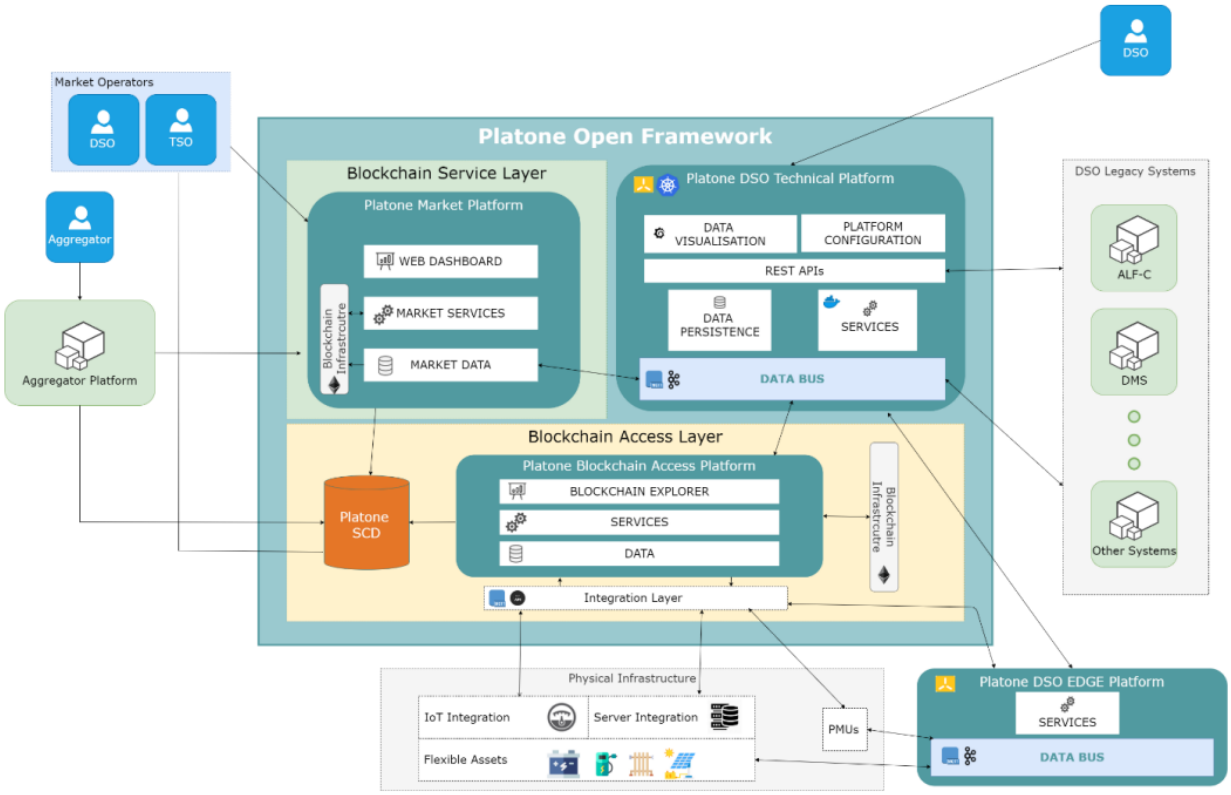

FIGURE 29 - PLATONE REFERENCE ARCHITECTURE [64]

The Platone solution consists of a two-layer architecture named Platone Open Framework. The Platone Open Framework includes the following components [64]:

- ***Blockchain Service Layer and Market Platform*:** this layer enables the deployment of different blockchain-based components, providing a blockchain infrastructure and Smart Contracts services. In the context of Platone, the Platone Market platform allows the support of wide geographical area flexibility requests from TSOs and local flexibility requests from DSOs. These are matched with offers coming from aggregators, resolving conflicts according to pre-defined rules of dispatching priorities. All the market operations are registered and certified within the blockchain service layer, ensuring transparency, security and trustworthiness among all the market participants.
- ***Blockchain Access Layer (BAL)*:** The Blockchain Access Layer and the Light Node form the Access Layer, a data exchange infrastructure among flexible DERs, platforms and stakeholders within the demo architecture. The Light Node is a device, installed at DERs' premises, able to gather metering data from Low Voltage (LV) and Medium Voltage (MV) meters, receives Setpoint from DSO Technical Platform and makes it available to Customers Activation Systems such as Energy Management System (EMS), smart appliance etc. to activate flexibility. The Light Node certifies "from the original source" all data and sends them through the Blockchain Access Layer

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

to the Shared Customer Database. The Blockchain Access Layer then connects the Light Node to the Shared Customer Database ensuring, through timestamping features, the immutability of data along the whole path.

- ***Platone Shared Customer Database (SCD)*:** The Shared Customer Database is a repository system where all data related to flexible resources are stored and made available to platforms and stakeholders. The Database stores data such as PoD general data (connection voltage level, contractual power etc.), Baseline, available flexibility, measurements, setpoint, etc. Some of these data come from the Light Node (e.g. metering data), some others from the Aggregator Platform (e.g. Baseline), others come from the Market Platform (e.g. market outcomes), others from the DSO Technical Platform etc. Data are organised according to predefined schemes and can be read by authorised platforms and stakeholders followed by authentication procedures. Data updating is allowed, after authentication, only for some types of data: for example, the Baseline for the day after can be updated by the Aggregator, while Market Outcomes cannot. Moreover, the Shared Customer Database is a connection point between the two blockchains within the demo, i.e. the Access Layer and the one Market Platform; indeed, data stored in the Database are used by smart-contract and then tokens running on both blockchains.
- ***Platone DSO Technical Platform (DSOTP)*:** The DSO Technical allows the DSOs to improve the DSO reliability and quality of service by exploiting the flexibility made available from DERs connected to the grid. Moreover, the DSOTP interacting with the Market Platform can avoid the activation of flexibility offers requested by the TSO avoiding possible issues on the operated distribution grid. More in detail, the Platform, performing forecasting of state estimation of the distribution grid, can predict grid congestions and voltage violations, define flexibility requests to solve the forecasted issues and verify the market outcomes, including the ones that are related to TSO requests, follow the grid constraints. To perform state estimation forecast and define flexibility requests, the Platform uses several grid data and measurements coming from DSO's Operational Systems, such as Supervisory Control and Data Acquisition (SCADA), Geo-Information System (GIS) and data of flexible DERs from the Shared Customer Database. Once the grid issue is forecasted, the Platform forwards the flexible request to the Market Platform. Finally, the Platform deals with carrying to each PoD the flexibility services activation setpoint defined by the Aggregator Platform
- **Aggregator Platform:** The Aggregator Platform is an operational platform that facilitates aggregators to manage the flexibility assets. It consists of several tools able to analyse data coming from different types of DERs (i.e. generation, consumption and storage), evaluate and aggregate available flexibility from thousands of different PoDs, and provide optimal algorithms to optimise market strategy and flexibility offers. The Aggregator Platform allows the management of the single units/PoDs, the aggregation of the offers, the definition of the baseline, the definition of flexibility services activation setpoint, the market interaction and all the consequent activities, including the economic settlement.

3.4.8. Resonance

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

The RESONANCE project [66] is creating a software framework for plug-and-play development of standard-compliant Customer Energy Manager solutions for demand-side flexibility management of distributed and small-scale assets. The RESONANCE Framework constitutes 3 catalogues of software libraries as well as marketplace services and tools that provide means for rapid, cost-efficient development & customisation of Resource Manager and Customer Energy Manager solutions as well as their aggregation services into different sectors.

The following sections provide an overview of the RESONANCE architecture and framework based on the corresponding deliverable [31]. The RESONANCE project is still ongoing, and updates of the architecture might be done.

RESONANCE FRAMEWORK

The RESONANCE framework [67] is designed to support the creation of demand-side flexibility management (DSFM) systems that meet industry standards. It offers catalogues of software services and tools for three core components: resource managers (RM), customer energy managers (CEM), and aggregation platforms. These catalogues are supplemented by configuration and deployment tools to streamline system implementation. Additionally, the framework includes a marketplace where users can promote and find various services, tools, and data resources within the catalogues.

Figure 30 illustrates the framework, showing the tasks involved in implementing the catalogue modules.

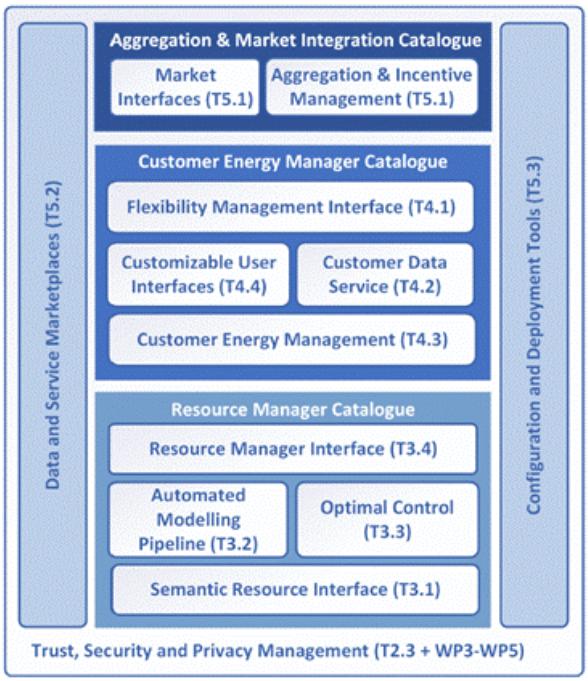

FIGURE 30 – OVERVIEW OF THE RESONANCE FRAMEWORK [67]

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Context view

The context view represents how a system interacts with external systems and stakeholders. In the RESONANCE-based DSFM system, components like RMs, CEMs, and aggregation platforms are shown as a black box, with their interactions outlined.

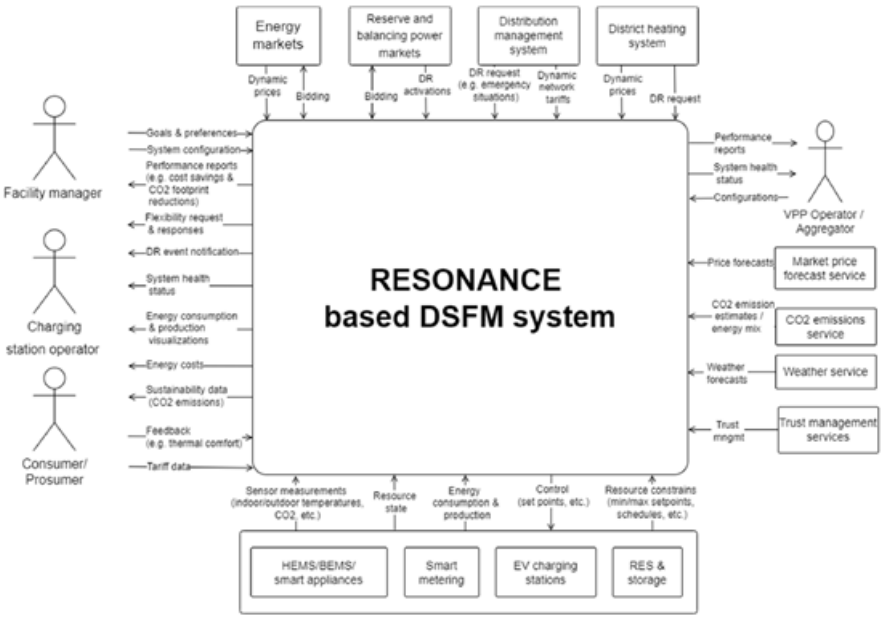

FIGURE 31 – CONTEXT VIEW OF A RESONANCE-BASED DSFM SYSTEM [67]

Functional view

The functional view breaks down the RESONANCE-based DSFM system into logical components, showing how they interact through high-level interfaces. Figure 32 Illustrates the structure.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

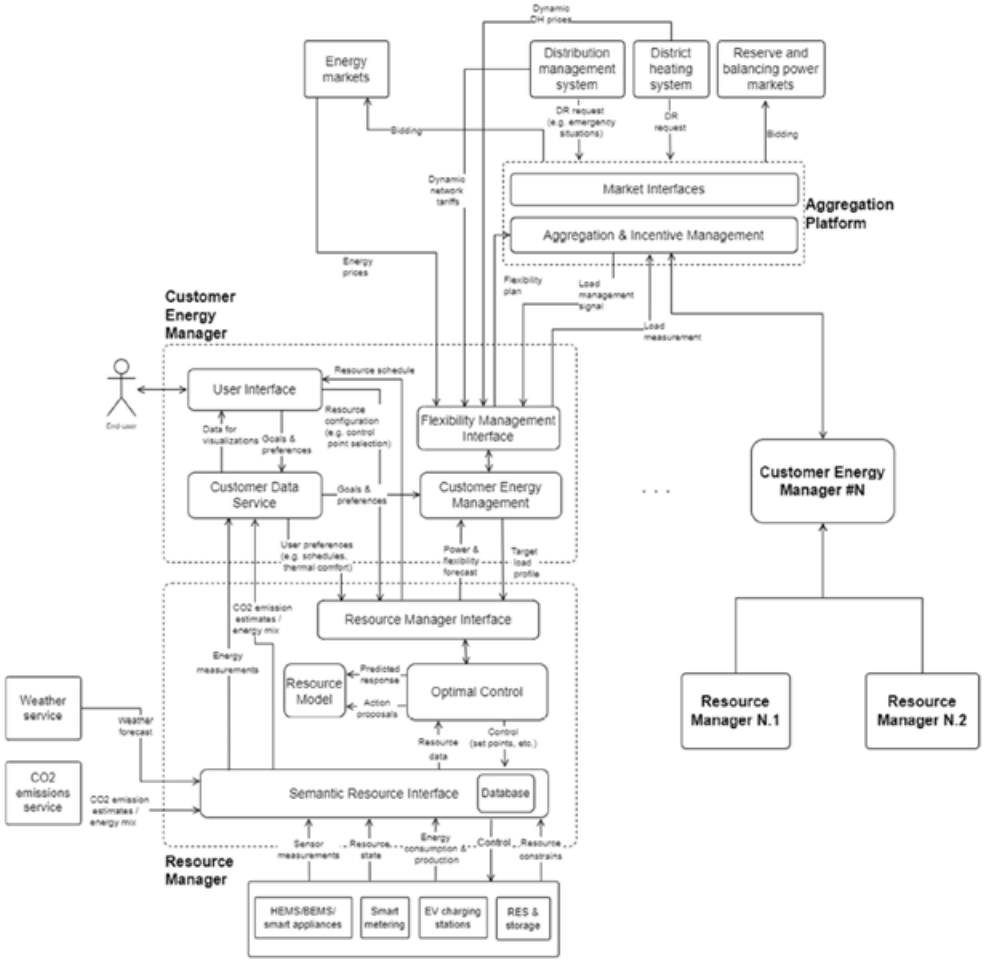

FIGURE 32 – FUNCTIONAL VIEW OF A RESONANCE-BASED DSFM SYSTEM [67]

3.4.9. SYNERGY

The SYNERGY project [68] was an innovative initiative aimed at enhancing coordination among different stakeholders - from electrical power system operators, energy supplier to local public authorities' urban infrastructure providers, with a particular emphasis on improving information exchange. This project focused on utilising electricity-related data from various sources to create new value within the energy sector and beyond. The goal of the Synergy project was to develop and implement an advanced big data platform that addressed the complexities of interactions within the energy sector's value chain. SYNERGY integrated existing technologies, tools, and big data libraries with legacy energy systems, thereby accelerating data management and analysis cycles.

The project also emphasized an innovative and secure framework for data exchange, ensuring the protection of privacy and intellectual property rights, which fostered collaboration between data owners and analytics service providers. The architecture of the SYNERGY platform consisted of three main components:

- the SYNERGY Cloud Infrastructure,
- On-Premise Environments

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- the SYNERGY Energy Apps Portfolio

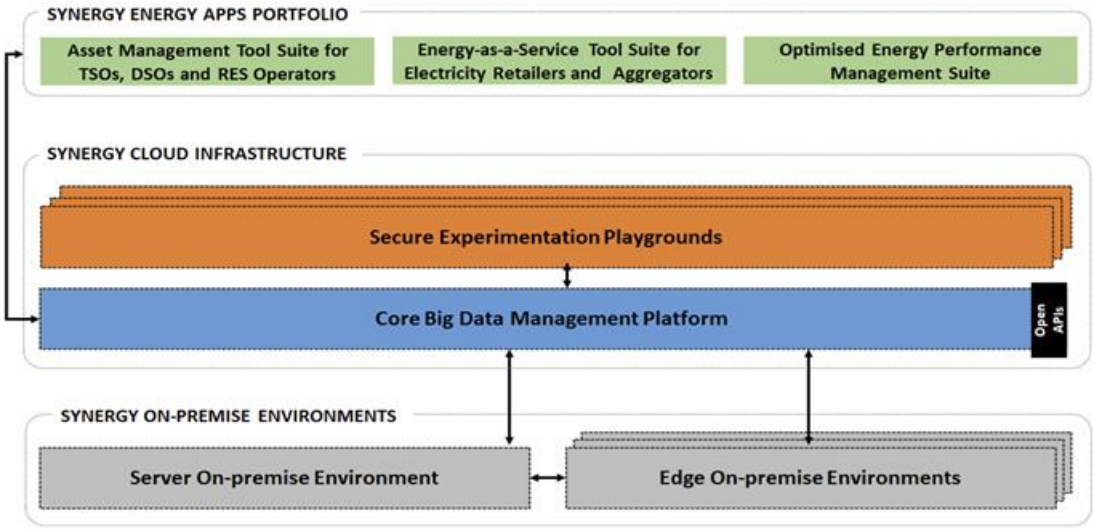

FIGURE 33 - SYNERGY HIGH-LEVEL ARCHITECTURE [69]

The Cloud Infrastructure included the Core Big Data Management Platform, which encompassed the Energy Big Data Platform and the AI Analytics Marketplace. These provided essential functionalities through Secure Experimentation Playgrounds—dedicated virtual machines for various stakeholders to conduct secure and isolated big data analytics.

The SYNERGY Core Big Data Management Platform, or SYNERGY Core Cloud Platform for short, serves as the main entry point for users representing stakeholders in the electricity data value chain. For data transfer, the Data Handling Manager in the SYNERGY Core Cloud Platform allows users to configure and manage data transfer jobs, including uploading batch files, collecting data via third-party APIs or SYNERGY Platform APIs, and ingesting streaming data. Data providers must align their data with the SYNERGY Common Information Model according to the guidelines of the Matching Prediction Engine. They can also set rules for data cleaning, anonymization, and encryption.

The SYNERGY platform offers a comprehensive approach to managing and utilising data within the energy sector, integrating multiple components to address security, data processing, and application needs. At the core of this system is the API Gateway, which facilitates access to both raw data and analytics results for authorized SYNERGY energy applications and third-party applications. This access is granted through the platform's Open APIs, allowing for data retrieval using configured filters. The management of security protocols, organisation and user registration, and authorisation processes is handled by the Security, Authentication & Authorisation Engine, ensuring that only authorised entities can access sensitive data.

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

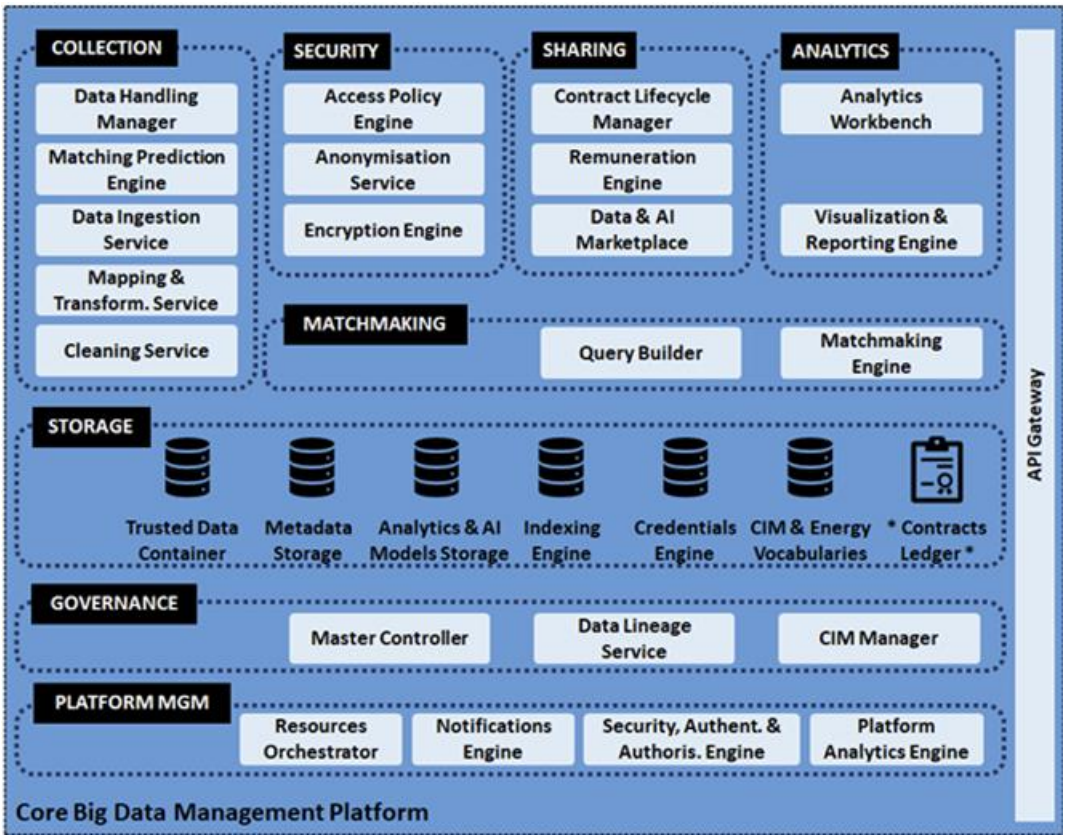

FIGURE 34 - COMPONENT VIEW OF THE SYNERGY CORE CLOUD PLATFORM [69]

Edge On-Premises Environments operate within the physical premises of energy stakeholders. These environments consist of server environments and edge environments installed in gateways. The primary function of this layer is to prepare and store data locally, thereby guaranteeing security and privacy. This capability is crucial for stakeholders who need to process and analyse data on-site, without transmitting it to the cloud. This approach is especially valuable in scenarios where data must remain on the stakeholder's premises or where encryption is necessary to protect sensitive information.

The SYNERGY Apps Portfolio is a suite of applications designed to meet the specific requirements of various users within the energy sector. This includes Distribution System Operators (DSOs), Transmission System Operators (TSOs), and Renewable Energy Source operators, who utilize these applications for grid-level analytics. Furthermore, electricity retailers and aggregators can leverage these applications for Energy-as-a-Service (EaaS) solutions, providing them with the tools needed to deliver innovative and efficient energy services. Through this integrated architecture, the SYNERGY platform effectively supports a wide range of stakeholders, enhancing the management, security, and utilisation of energy data across the sector.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

4. FUNCTIONAL SPECIFICATIONS OF THE HEDGE-IOT SYSTEM

4.1. BUCS & SUCS REFINEMENTS - ALIGNMENT WITH D2.2

Business Use Cases (BUCs) and System Use Cases (SUCs) were defined respectively in deliverables D2.1 [73] and D2.2 [74]. They were defined using the IEC 62559 [41] template, and the methodology is described in these deliverables.

Project pilots take the opportunity of this deliverable to update and refine their BUCs and SUCs when needed. It can be linked to changes in a pilot or the availability of new information.

Given the substantial number of pages and the absence of major changes for the refined BUCs and SUCs of all pilots, these documents are compiled and uploaded to the project website. The compiled document will be publicly available, while the size of this deliverable is not compromised.

The following sections describes the main changes to highlights of the refined BUCs and SUCs.

REMINDERS ON BUSINESS USE CASES (BUCS) AND SYSTEM USE CASES (SUCS)

A use case (UC) describes the interactions of various actors in a system to achieve specific goals. A business use case (BUC) represents a business process, while a system use case (SUC) describes a function that supports one or more business processes.

Both types of UCs are essential for the description of a system and can be used for the system architecture definition. In HEDGE-IoT, the BUCs were the starting point for the pilots to define SUCs and will be also used for the definition of the reference architecture.

The project's functional requirements and non-functional requirements are specified in the form of SUCs.

The BUCs and SUCs were designed following the standardised IEC 62559-2 template and has the following seven main sections:

1. Description of the use case
2. Diagrams of the use case
3. Technical details
4. Step-by-step analysis of the use case
5. Information exchanged
6. Requirements
7. Common terms and definitions

HEDGE-IOT BUCS REMINDER AND REFINEMENTS

14 BUCs were identified and defined by the project pilots. Table 3 - BUCS OVERVIEW provides an overview of all the BUCs of the project.

TABLE 3 - BUCS OVERVIEW

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Pilot	BUC ID	BUC name
1-Finnish	BUC-FI-01	Anomaly detection and fault forecasting to increase Medium Voltage (MV) distribution network resilience
	BUC-FI-02	Predictive and real-time congestion management (CM) to increase network hosting capacity
2-Greek	BUC-GR-01	Flexibility management through active prosumers/consumers engagement
	BUC-GR-02	Leveraging data exchange and AI edge algorithms for energy forecasting and prevention of critical grid events
	BUC-GR-03	Flexibility trading platform for mitigating problems of the T&D networks
3-Italian	BUC-IT-01	Energy flow optimisation with dynamic grid limits
	BUC-IT-02	Flexibility provided by Energy Community to solve a local congestion
4-Dutch	BUC-NL-01	Energy Flexibility at business park
	BUC-NL-02	Enhance local grid resilience through detection & prevention
5-Portuguese	BUC-PT-01	GreenVale: Harnessing the potential of energy communities by leveraging Federated Learning strategies
	BUC-PT-02	Participation of industrial and residential energy communities in ancillary services market for the TSO
	BUC-PT-03	Flexibility aggregation at tertiary buildings
6-Slovenian	BUC-SI-01	Maximizing asset capacity for increased lifetime of DSO and TSO equipment
	BUC-SI-02	Enhanced Network Manageability and Observability

Only one pilot raised the need to update a BUC in this deliverable. This BUC is from the Greek pilot with the title: BUC-GR-01 - Flexibility management through active prosumers/consumers engagement. The update aims to clarify and reflect that the aggregator is the one submitting bids to the Local Flexibility Market (LFM).

HEDGE-IOT SUCS REMINDER AND REFINEMENTS

39 SUCs were identified and defined by the project pilots. Table 4, Table 5, Table 6, Table 7, Table 8 and Table 9 provide an overview of all the SUCs of the project by pilot.

FINNISH PILOT SUCS

The following table links the BUCs and the SUCs of the pilot:

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

TABLE 4 - FINNISH PILOT SUCS

BUC ID & BUC name	SUC ID	SUC name
BUC-FI-01 Anomaly detection and fault forecasting to increase Medium Voltage (MV) distribution network resilience	SUC-FI-01.1	Data collection and anomaly detection
	SUC-FI-01.2	Fault forecasting
BUC-FI-02 Predictive and real-time congestion management (CM) to increase network hosting capacity	SUC-FI-02.1	Congestion prediction in distribution grids
	SUC-FI-02.2	Congestion management planning in distribution grids
	SUC-FI-02.3	State monitoring of the distribution grid
	SUC-FI-02.4	Congestion management decision-making in real-time

The Finnish pilot main SUCs refinements are:

1. Addition of standards and communication protocols used (when relevant) to complete the Information exchanged requirements
2. Reformulation of objectives for a specific SUC
3. Refinement of SUC description
4. Update of scenarios steps

GREEK PILOT SUCS

The following table links the BUCs and the SUCs of the pilot:

TABLE 5 - GREEK PILOT SUCS

BUC ID & BUC name	SUC ID	SUC name
BUC-GR-01 Flexibility management through active prosumers/consumers engagement	SUC-GR-01.01	Optimization of Flexibility Distribution
	SUC-GR-01.02	Demand Forecasting
	SUC-GR-01.03	Production Forecasting
	SUC-GR-01.04	Edge Processing
	SUC-GR-01.05	User Interaction
BUC-GR-02 Leveraging data exchange and AI edge algorithms for energy forecasting and prevention of critical grid events	SUC-GR-02.01	Energy Grid Management using Forecasting Data

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

BUC-GR-03 Flexibility trading platform for mitigating problems of the T&D networks	SUC-GR-03.01	Registration & Prequalification on Local Flexibility Market
	SUC-GR-03.02	Flexibility Trading

The Greek pilot main refinements are:

1. Addition of standards, communication protocols and format used (when relevant) to complete the Information exchanged requirements
2. Update of some diagrams
3. Update document to clarify and reflect that the aggregator is the one submitting bids to the Local Flexibility Market (LFM).
4. Update of actors' lists
5. Refinement of SUC description
6. Update of scenarios steps

ITALIAN PILOT SUCS

The following table links the BUCs and the SUCs of the pilot:

TABLE 6 - ITALIAN PILOT SUCS

BUC ID & BUC name	SUC ID	SUC name
BUC-IT-01 Energy flow optimisation with dynamic grid limits	SUC-IT-01.1	Energy community power management
	SUC-IT-01.2	Energy community performance forecasting
BUC-IT-02 Flexibility provided by Energy Community to solve a local congestion	SUC-IT-02.1	Grid behaviour forecasting
	SUC-IT-02.2	Grid congestion computing
	SUC-IT-02.3	Localized weather forecast

The Italian pilot main refinements are:

1. Addition of standards, communication protocols and format used (when relevant) to complete the Information exchanged requirements
2. Updates of actors' lists

DUTCH PILOT SUCS

The following table links the BUCs and the SUCs of the pilot:

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

TABLE 7 - DUTCH PILOT SUCS

BUC ID & BUC name	SUC ID	SUC name
BUC-NL-01 Energy Flexibility at business park	SUC-NL-01.1	Monitor energy nodes and local grid & dashboard for data insights
	SUC-NL-01.2	Integrate energy nodes and EMS/BMS via semantics for control and explainability
	SUC-NL-01.3	Optimize energy production & consumption
	SUC-NL-01.4	Flexibility alignment
BUC-NL-02 Enhance local grid resilience through detection & prevention	SUC-NL-02.1	Anomaly and fault detection in the local grid
	SUC-NL-02.2	Predictive maintenance

The Dutch pilot main refinements are:

1. Addition of standards and communication protocols used (when relevant)
2. Reformulation of objectives for a specific SUC
3. Refinement of a specific SUC description

PORTUGUESE PILOT SUCS

The following table links the BUCs and the SUCs of the pilot:

TABLE 8 - PORTUGUESE PILOT SUCS

BUC ID & BUC name	SUC ID	SUC name
BUC-PT-01 GreenVale: Harnessing the potential of energy communities by leveraging Federated Learning strategies	SUC-PT-01.1	Connect flexibility providers across the DPP flexibility value chain
	SUC-PT-01.2	Enable Data Exchange via Data Spaces
	SUC-PT-01.3	Mobilizing Energy Flexibility
	SUC-PT-01.4	Activation of Energy Flexibility
BUC-PT-02 Participation of industrial and residential energy communities in ancillary services market for the TSO	SUC-PT-02.1	Bidding & Selection
	SUC-PT-02.2	aFRR/mFRR Activation
	SUC-PT-02.3	aFRR / mFRR Settlement

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

BUC-PT-03 Flexibility aggregation at tertiary buildings	SUC-PT-03.1	Integrate flexible assets from commercial buildings
	SUC-PT-03.2	Default valorisation scenario based on price hedging
	SUC-PT-03.3	TSO valorisation scenario

The Portuguese pilot main SUCs refinements are:

1. Addition of standards and communication protocols used (when relevant) to complete the Information exchanged requirements
2. Addition of non-functional requirements
3. Update of some scenario steps, and information exchanged
4. Update of one diagram

SLOVENIAN PILOT SUCS

The following table links the BUCs and the SUCs of the pilot:

TABLE 9 - SLOVENIAN PILOT SUCS

BUC ID & BUC name	SUC ID	SUC name
BUC-SI-01 Maximizing asset capacity for increased lifetime of DSO and TSO equipment	SUC-SI-01.1	Dynamic Thermal Rating (DTR) edge calculation
	SUC-SI-01.2	Dynamic Line Rating (DLR) edge calculation
BUC-SI-02 Enhanced Network Manageability and Observability	SUC-SI-02.1	Semantic model of the substation
	SUC-SI-02.2	ML algorithm for enhanced network management and planning

The Slovenian pilot main refinements are:

1 Addition of standards, communication protocols and format used (when relevant) to complete the Information exchanged requirements
2 Diagrams updates (use case and sequence diagram)
3 Updates of actors' lists
4 Refinement of SUCs texts

4.2. HEDGE-IOT COMMONALITIES

This chapter presents the results of the BUCs and SUCs analysis to identify high-level commonalities among pilots. The aim was to provide a normalised and synthetic vision at a HEDGE-

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

IoT level to identify potential collaborations and synergies among pilots. This work is based on the project functional specifications defined in the form of BUCs and SUCs.

4.2.1. Commonalities normalisation

This study focuses on:

- roles,
- objectives,
- and beneficiaries.

To find clear commonalities among these three topics, it is necessary to define normalised ones first.

DEFINITION OF NORMALISED ROLES

Normalised roles representing every unique role from every pilot are needed. Those roles are defined in the IEC 62559 documents provided by the pilots (chapter 3.1. Actors). To anticipate, the Harmonised Electricity Market Role Model (HEMRM) document [42] was shared with partners as a reference prior the BUCs and SUCs definition (Section 4.1). Here is the list of the main normalised roles:

1. Consumer and Prosumer
2. Producer
3. Energy Community (EC) and EC manager
4. Flexibility Service Provider (including Balancing Service Provider (BSP))
5. Energy Service Company (ESCO)
6. Energy Trader
7. Meter Operator
8. Market Operator (including Nominated Electricity Market Operator (NEMO))
9. Local Flexibility Market (LFM)Aggregator
10. Resource Aggregator
11. Data Hub Operator
12. Reserve Allocator (RA)
13. Reconciliation Responsible
14. Imbalance Settlement Responsible

DEFINITION OF NORMALISED OBJECTIVES

Normalised objectives representing main objectives from every pilot are needed and were identified based on BUCs and SUCs. Here is the list of the main normalised objectives:

- Anomaly detection
- Fault forecasting – Grid behaviour forecasting - Energy grid management

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- Predictive and real-time congestion management
- Grid load and generation forecasting - energy production and consumption forecasting
- Flexibility optimisation through active prosumer/consumer engagement
- Flexibility trading platform for mitigating problems (of the T&D network)
- Flexibility for energy communities or residential/commercial buildings
- Flexibility potential forecasting
- Optimise energy production and consumption for energy communities or residential/commercial buildings
- Forecast energy production and consumption for energy communities or residential/commercial buildings
- Weather forecast
- Real-time monitoring and analysis (edge) of energy consumption behind the meter
- Energy community or residential/commercial buildings power management
- Energy community or residential/commercial buildings performance forecasting
- Predictive maintenance
- Maximising asset capacity through dynamic thermal rating (DTR) and dynamic line rating (DLR)
- Definition of a semantically unified model for power grid stakeholders.
- Semantic integration of new energy node
- Consumer/Prosumer/Aggregator GUI.

4.2.2. Commonalities analysis

ROLES ANALYSIS

HEDGE-IoT normalised roles popularity

Figure 35 presents the popularity of the normalized roles in the project. This graph shows that the most used roles are "System Operator", "Energy Service Company", and "Flexibility Service Provider".

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

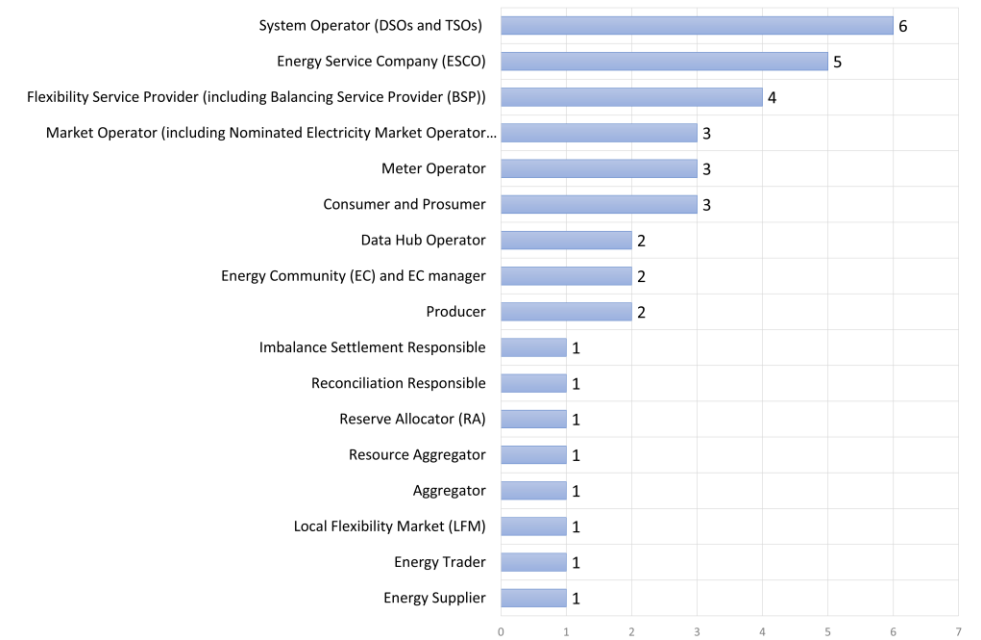

FIGURE 35 COMMONALITIES – ROLES' POPULARITY

HEDGE-IoT normalised roles breakdown by pilot

Table 10 summarises the normalised objectives of each pilot. It allows us to easily identify potential collaboration or synergies among pilots specially for the transversal use cases [Chapter 4.5].

TABLE 10 - COMMONALITIES – NORMALIZED OBJECTIVES PER PILOT

Normalised role	FI	GR	IT	NL	PT	SL
System Operator (DSOs and TSOs)	✓(B)	✓(B)	✓(B)	✓(B)	✓(B)	✓(B)
Energy Supplier		✓				
Consumer and Prosumer		✓(B)		✓	✓(B)	
Producer		✓(B)		✓		
Energy Community (EC) and EC manager			✓		✓(B)	
Flexibility Service Provider (including Balancing Service Provider (BSP))	✓	✓	✓		✓	
Energy Service Company (ESCO)	✓	✓		✓	✓	✓
Energy Trader		✓				
Meter Operator		✓	✓	✓		

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Market Operator (including Nominated Electricity Market Operator (NEMO))	✓		✓(B)		✓	
Local Flexibility Market (LFM)		✓(B)				
Aggregator				✓		
Resource Aggregator					✓(B)	
Data Hub Operator					✓	✓
Reserve Allocator (RA)					✓	
Reconciliation Responsible					✓	
Imbalance Settlement Responsible					✓	

Legend:
✓: Role present in at least one of the pilots' BUCs
(B): Role is the beneficiary in at least one of the pilots' BUCs

HEDGE-IoT main beneficiaries

The study of the main beneficiaries is an important matter, as it shows what is driving the actions. However, it is a delicate line to be drawn, since all actors are in some way beneficiaries from the UCs they are involved in. Here, the main beneficiaries have been the actors to whom the main objectives of the UC are addressed.

The main beneficiaries have been established by pilots considering all their BUCs. This analysis enables us to highlight the drivers of the HEDGE-IoT business model.

The diagram below shows the repartition of the main beneficiaries across the pilots.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

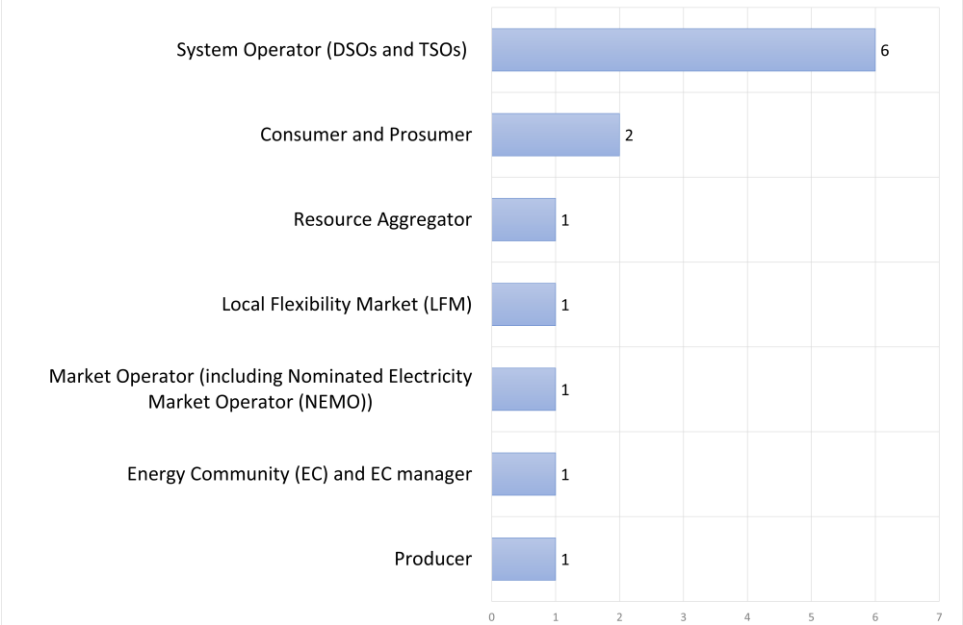

FIGURE 36 - MAIN HEDGE-IOT BUCS BENEFICIARIES

As shown by Figure 36, the main HEDGE-IoT beneficiaries for the pilot is "System Operator (DSO and TSO)". It is then followed by "Consumer and Prosumer", "Resource Aggregator", "Local Flexibility Market", "Market Operator", "Energy community" and "Producer".

OBJECTIVES ANALYSIS

HEDGE-IoT normalised roles popularity

The popularity of each normalised objective was calculated in order to identify the ones most often considered by pilots. The calculation was done by simply counting the number of occurrences of each objective among all BUCs and SUCs and is detailed in Figure 37.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

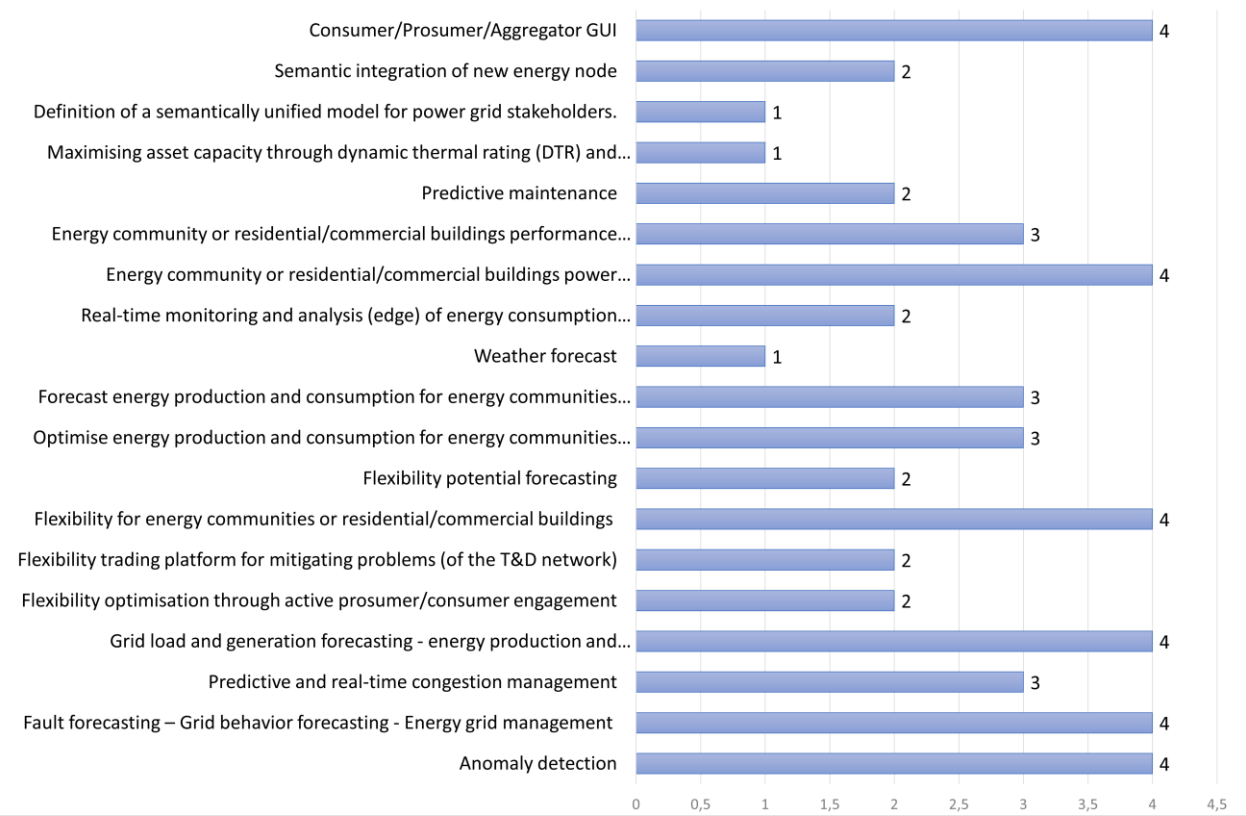

FIGURE 37 - COMMONALITIES - POPULARITY OF OBJECTIVES

The most popular objectives are links to "Anomaly detection", "Energy grid forecasting and management", "Grid load and generation forecasting", "Flexibility for energy communities or residential/commercial buildings", "Energy community or residential/commercial buildings power management" and "Consumer/prosumer/Aggregator GUI".

HEDGE-IoT normalised objectives breakdown by pilot

Table 11 lists he normalised objectives of each pilot. It allows us to identify potential collaborations or synergies among pilots.

TABLE 11 - COMMONALITIES - OBJECTIVES

Normalised objective	FL	GR	IT	NL	PT	SL
Anomaly detection	✓		✓	✓		✓
Fault forecasting – Grid behaviour forecasting - Energy grid management	✓	✓		✓		✓
Predictive and real-time congestion management	✓	✓	✓			
Grid load and generation forecasting - energy production and consumption forecasting	✓	✓		✓		✓

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Flexibility optimisation through active prosumer/consumer engagement		✓			✓	
Flexibility trading platform for mitigating problems (of the T&D network)		✓			✓	
Flexibility for energy communities or residential/commercial buildings		✓	✓	✓	✓	
Flexibility potential forecasting		✓			✓	
Optimise energy production and consumption for energy communities or residential/commercial buildings			✓	✓	✓	
Forecast energy production and consumption for energy communities or residential/commercial buildings		✓	✓		✓	
Weather forecast			✓			
Real-time monitoring and analysis (edge) of energy consumption behind the meter		✓		✓		
Energy community or residential/commercial buildings power management		✓	✓	✓	✓	
Energy community or residential/commercial buildings performance forecasting		✓	✓		✓	
Predictive maintenance	✓			✓		
Maximising asset capacity through dynamic thermal rating (DTR) and dynamic line rating (DLR)						✓
Definition of a semantically unified model for power grid stakeholders.						✓
Semantic integration of new energy node				✓	✓?	
Consumer/Prosumer/Aggregator GUI		✓	✓	✓	✓	

CONCLUSION

This commonalities analysis highlights the most predominant roles, beneficiaries and objectives of HEDGE-IoT pilots. To achieve this, the previously described BUCs and SUCs from each pilot were examined. An effort of harmonisation was done on designations. However, while names could be harmonised, their implementation might not, as it largely depends on the specific components used and the individual approaches of the partners involved.

4.3. INTEROPERABILITY PROFILES

The goals of this subtask of T2.6 are first to support, as a basis, the design of project data integration solutions, ensuring proper data exchange. The second objective is to identify the main interoperability challenges and solutions encountered by HEDGE-IoT and its pilots. This, to support

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

the European Commission's understanding of the interoperability issues encountered in energy innovation projects. These elements will contribute as well to outcomes on policy, roadmap and standardisation. In the long term, the contributions of several European projects to this action, started in the OPEN DEI [84] and Int:net [85] European Coordination and Support Actions (CSA), will give insights into the definition of a smart grid interoperability profile.

4.3.1. Interoperability profile principle

INTEROPERABILITY PROFILE

An interoperability profile gathers information and guidance that can be used to create interoperable systems.

Following ISO/IEC 19941:2017 (Information technology - Cloud computing - Interoperability and portability) and ISO/IEC 21823-1:2019 (Internet of things (IoT) - Interoperability for internet of things systems - Part 1: Framework), the interoperability between two (or more) interacting systems can be described by the 5-facets (or layers) model illustrated on (Figure 38).

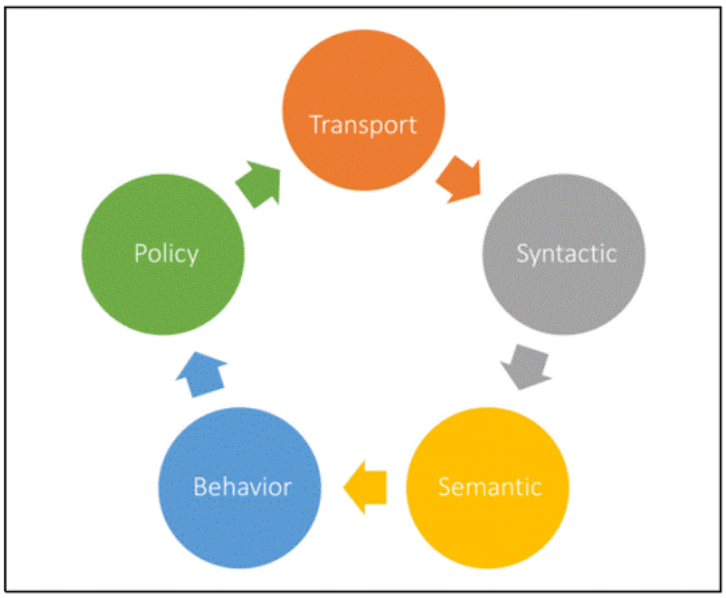

FIGURE 38 - REPRESENTATION OF THE 5-FACETS INTEROPERABILITY MODEL FROM ISO/IEC 19941:2017 AND ISO/IEC 21823-1:2019 [70]

The following table describes these 5 facets and presents a correspondence with the European Interoperability Framework.

TABLE 12 - DESCRIPTION OF THE ISO/IEC 21823-1:2019 INTEROPERABILITY MODEL AND COMPARISON WITH EIF (EUROPEAN INTEROPERABILITY FRAMEWORK), TABLE ADAPTED FROM [70]

Facets from ISO/IEC 21823-1:2019	Description	Correspondence with EIF

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Transport interoperability	Deals with data delivery	Technical interoperability
Syntactic interoperability	Allows reading the data in a known format and grammar	
Semantic interoperability	Responsible for the meaning, enabling the unambiguous interpretation and understanding of data	Semantic interoperability
Behavioural interoperability	Refers to the way in which business processes, responsibilities and expectations are aligned to achieve commonly agreed and mutually beneficial goals	Organizational interoperability
Policy interoperability	Ensures that organizations operating under different legal frameworks, policies and strategies can work together	Legal interoperability

INTEROPERABILITY POINTS AND INTEROPERABILITY CASE

An interoperability profile defines the information and guidance (5-facets) allowing interoperability at a specific interoperability point in each context or system. It supports prerequisites for programmes or projects and enables interoperability implementation and testing.

The European Coordination and Support Action OPEN DEI has defined the terms Interoperability point and interoperability case as follows:

- **An interoperability point,** i.e., a location in the overall system where data is exchanged according to an agreed interoperability specification (e.g., where interoperability takes place in a specific context).
- **An interoperability case,** i.e., a documented justification and agreement on an interoperability point (i.e., why interoperability is needed).

The combination and availability of these two elements lead to the publication of an interoperability profile. As already mentioned, an interoperability profile gathers the information and guidance that can be used to create interoperable systems. It can be considered as the specification for the implementation of the interaction model taking place at an interoperability point.

4.3.2. Methodology and work plan

To address the two previously mentioned objectives, the methodology was divided into two main workflows.

The first objective of the task is to support, as a basis, the design of the project data integration solutions, ensuring proper data exchange. The adopted approach was to complete, when relevant, the pilots' SUCs and more specifically, section 5 - Information Exchange of the IEC 62559 [41] template. The information exchange table of each SUC was enriched with additional available information on standards and communication protocols to be used.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

The second objective of the task is to identify the main interoperability challenges and solutions encountered by HEDGE-IoT and its pilots to contribute to outcomes on policy, roadmap and standardisation. The selected approach was experimented in the Int:net project. This method consists of an interoperability case survey to be completed by pilots, followed by an analysis of the results to understand these interoperability challenges, solutions adopted and determine whether pilots share them. Based on the results, HEDGE-IoT will share the conclusions with the relevant standardisation committees and the European Commission.

4.3.3. Conclusion and next steps

This deliverable provides the first contribution of the subtask, focusing in particular on the first one. D2.3 contribution focuses on enriching the SUCs, by providing more information to design the project data integration solutions. These elements can be found in the refined SUCs in annexes of this document. D2.4 will focus on the second objective, which is the identification and analysis of the main interoperability challenges.

4.4. HEDGE-IOT FUNCTIONAL REQUIREMENTS

A first version of the functional requirements was present in D2.2 of the HEDGE-IoT project, defining the technical capabilities required for HEDGE-IoT. This first version was extracted from the SUCs provided by the pilots using the IEC 62559-2 template. This section aims to update and refine this list based on the progress of the project and pilot.

The HEDGE-IoT technical capabilities section was split into 9 categories:

- Data management
- Interoperability and data exchanges
- Services management
- User interfaces
- Optimisation and forecasting
- Flexibility management
- Grid monitoring and control
- Artificial intelligence
- Main external data.

4.4.1. Data Management

- **IoT data collection:** Collect and monitor real-time data from IoT devices, IEDs, and energy nodes.
- **Data discoverability:** Data customers of the HEDGE-IoT data space should be able to explore the data space catalogue and the possible data from data producers.
- **Computational orchestration:** Coordinating distributed computational tasks for energy services across edge-to-cloud systems, with goals of ensuring responsiveness and cost-effective data exchange, including minimised latency and bandwidth usage.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- **Real-time data processing and aggregation:** Process and aggregate real-time data (e.g., DTR, DLR, DER). The data could be located in the cloud or at the edge level, depending on each pilot.
- **Data storage and access:** Store and access data at different levels of the project architecture (e.g., pilot, orchestrator, service catalogue, app store).
- **Data validation and quality check:** Ensure data accuracy with quality checks.

4.4.2. Interoperability and data exchanges

- **HEDGE-IoT middleware data exchange:** Ensure data exchange through HEDGE-IoT components using Rest API libraries.
- **Interoperability among systems:** Ensure interoperability for communication among systems and grid components with a semantic interoperability layer.
- **Dataspace, dataspace connectors and dataspace protocol:** A shared dataspace infrastructure to facilitate secure, standardised, and scalable data exchange across the various components, stakeholders, and pilot sites involved in the HEDGE-IoT project. Specific connectors will be required for data producers and data customers.
- **Dataspace catalogue:** Provide a catalogue to make available data discoverable for data customers.
- **Pilot data exchanges:** A means of pilot data exchanges, such as a gateway and Rest API.

4.4.3. Services management

- **App store for service:** A centralised repository for services//microservices enabling quick discovery, sharing, and reuse across different pilots and domains. It allows service owners to publish new functionalities, while developers or other system components can access. By ensuring semantic and technical interoperability, the App Store accelerates solution development and deployment, fosters collaboration, and ensures consistent service quality within the HEDGE-IoT framework.

4.4.4. User Interfaces

- **User interfaces:** Provide user interfaces for DSOs, producers, consumers, and aggregators.
- **User interface configuration: Configuration** of user interfaces, such as preferences and parameter settings.
- **Alerting, reporting & visualisation:** Generate security alerts, notifications, reports, and visualise relevant information.
- **Dynamic tariffs interface:** Display dynamic tariffs for customer engagement and flexibility pricing.
- **User registration and contract information:** Implement a user registration system that securely captures and stores user details and contract information, allowing for account creation, verification, and management.

4.4.5. Optimisation and Forecasting

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- **Optimisation**: Manage and optimise consumption, flexibility, congestion and energy management system (EMS) with real-time adjustments.
- **Forecasting:** Predict production, consumption, grid limits, demand, weather, PV production, etc.
- **Anomaly/fault detection and prediction:** Identify and forecast faults or anomalies in the grid.
- **Anomaly/fault assessment and resolution:** Analyse and make decisions to solve or minimise anomaly/fault quickly to maintain operational continuity.
- **Congestion prediction and management planning:** Anticipate and prevent grid congestion.
- **Performance analysis:** Analyse system performance (e.g., photovoltaic (PV) production).
- **Maintenance prediction:** Predict and manage maintenance to ensure grid reliability.

4.4.6. Flexibility Management

- **Registration, prequalification and resources enrolment:** Register and prequalify organisation and flexibility resources for integration.
- **Flexibility offer handling:** Send, receive, accept, or reject flexibility offers; check feasibility and propose incentives.
- **Market price tracking and forecasting:** Track and predict energy and flexibility market prices.
- **Activation & planning:** Execute and plan flexibility actions at both grid and market levels.
- **Flexibility estimation:** Estimate and calculate the required flexibility
- **Real flexibility provided calculation:** Calculation of required/agreed flexibility and provided flexibility.
- **Settlement & payments:** Manage flexibility settlements, payments, and penalties.
- **Vulnerable user identification:** Identify users who have major constraints related to their infrastructures' power supply.

4.4.7. Grid Monitoring and Control

- **Grid state monitoring:** Monitor and estimate grid status in real time.
- **Grid and energy node configuration:** Configure energy nodes and integrate new ones.

4.4.8. Artificial Intelligence

- **AI trustworthiness:** Provide the assurance that AI systems used are trustable, including aspects like security, reliability, safety, ethics, integrity and accuracy.
- **AI explainability:** Provide transparent AI-driven decisions for trust.
- **AI maintenance**: Provide an AI maintenance system that continuously monitors model performance and facilitates updates and further developments.

4.4.9. Main external data

- **Grid historical data:** Access grid historical data as one major input to the system.
- **Weather data:** Incorporate weather forecasts to enhance grid operation decisions.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- **Geographic information system (GIS) model:** Access geographic information systems for environmental data.

4.5. TRANSVERSAL SYSTEM USE CASES

4.5.1. Introduction

Following the definition of pilots' BUCs and SUCs, the project decided to define transversal system use cases to complete the project specifications with the aims to:

- address common needs across use cases,
- enable harmonisation and interoperability,
- and support transversal components specifications, implementation and integration (done by other tasks).

A transversal use case (TUC) is a SUCs that refers to a cross-cutting use case that supports multiple BUCs and SUCs by addressing shared capabilities, services, or requirements that are common across different pilots. Unlike BUCs, which are driven by specific stakeholder goals, and pilots' SUCs, which describe vertical functional interactions, transversal use cases are designed to enable interoperability, reusability, and consistency across the entire ecosystem by specifying horizontal functional interactions.

The following sections provide an overview and a summary of the TUCs' content. Their complete documents can be found in the annex of this deliverable.

4.5.2. Methodology and transversal use cases overview

After the collaborative identification of the TUCs and their scenarios based on the project and pilots' needs, they were defined using the same methodology as BUCs and SUCs, i.e., following the IEC 62559 template. Each TUC is directly linked to a specific task of the project, and the partner in charge of this task has led the specifications phase.

The project pilots were then consulted to estimate a first list of the TUCs and the scenarios that they would implement during the project. This breakdown is a first version and will be updated in the next version of this deliverable, i.e., D2.4.

Table 13 below provides an overview of the selected HEDGE-IoT Transversal Use Cases (TUCs).

TABLE 13 - HEDGE-IOT TRANSVERSAL USE CASES

Transversal use case	Scenario	Description
[Dataspace] Data interoperability Data exchange through HEDGE-IoT Dataspace.	Sc1. Use of the dataspace by a data producer	It describes how a data producer makes its datasets or services available within the dataspace.
	Sc2. Use of the dataspace by a data customer	It describes how a data customer interacts with the dataspace to discover and access data shared by other parties.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

	Sc3. Metadata Discovery and Planning	It describes how an organisation can discover which datasets or services are available, including their conditions of use, data formats, and applied semantic vocabularies.
	Sc4: Federated Service Chaining	It describes how a software component (e.g., an orchestrator or optimization engine) uses the dataspace to access services or modules provided by other partners, in a dynamic and composable way.
[Computational Orchestration] Computational interoperability Automate coordination, management, and execution of HEDGE-IoT computing tasks across the distributed systems/services and cloud environment.	Sc1. Energy services orchestrations at edge geographic redundancy	It describes how the dynamic allocation of computational resources is done for energy services demand across edge, fog, and cloud layers to maintain efficiency and responsiveness.
	Sc2. Federated AI services (hyperparameter tuning)	It describes how the minimisation of data transfer overhead in federated AI services is done by efficiently managing and optimizing the hyperparameters of the learning process.
	Sc3. Energy application rolling-up at Edge	It describes how the efficient update of energy services from cloud to edge avoiding execution disruption is ensured.
[App Store] Functional interoperability Use of the App Store as part of HEDGE-IoT.	Sc1. Publish a service/sub-service in the App Store	It describes how a service provider can publish a new service/sub-service in the HEDGE-IoT environment.
	Sc2. Reuse/Access a service/sub-service in the App Store	It describes how discovery mechanism for developers or users works to find available reusable services.
	Sc3. Interchangeable common services/sub-services (among pilots)	It describes how different providers publishing "functionally equivalent" services following the same data schemas can interchange services.

4.5.3. Transversal Use Cases

TUC-1 - DATA EXCHANGE THROUGH HEDGE-IOT DATASPACE

TABLE 14 TRANSVERSAL USE CASE 1 - DATA EXCHANGE THROUGH HEDGE-IOT DATASPACE

SUC ID	TUC-1
SUC NAME	Data exchange through HEDGE-IoT Dataspace
AREA/DOMAIN	Data interoperability
SCOPE	The scope of this transversal use case is to leverage a shared dataspace infrastructure to facilitate secure, standardized, and scalable data exchange across the various components, stakeholders, and pilot sites involved in the HEDGE-IoT project.
OBJECTIVES	The objectives that the use case is expected to achieve are to: • **Objective 1:** allow data exchange for an edge-cloud continuum

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

	• **Objective 2:** connect data provider and data customer
SHORT DESCRIPTION	This use case describes how partners in the HEDGE-IoT project can exchange data across organizational boundaries using a shared dataspace infrastructure based on the Eclipse Dataspace Connector (EDC). A data provider exposes metadata and access policies for its resources, while a data consumer discovers and retrieves data through secure, policy-compliant mechanisms. The interaction ensures data sovereignty, access control, and interoperability. This pattern can be reused across different pilots and domains to enable secure and standardized data flows.
COMPLETE DESCRIPTION	In the HEDGE-IoT project, several partners collaborate to develop intelligent edge computing solutions for diverse sectors, including energy, mobility, and public services. These partners often need to exchange data across organizational and technical boundaries. However, sharing data between organizations raises concerns about security, control, and compliance with different regulations and usage agreements. To address this, the project uses a shared **dataspace** infrastructure. This allows each organization to remain the owner of its data while making it available to others in a controlled and standardized way. The core of this infrastructure is the **Eclipse Dataspace Connector (EDC)**, a component that enables organizations to publish, find, and exchange data based on clearly defined policies. Here's how it works in practice: a **data provider**, such as a company operating an edge service, wants to make a dataset available to other partners. The provider describes the dataset—what it is, how it can be used, and under which conditions—in a metadata format, and publishes it into a shared catalogue managed by the dataspace. This information does not include the actual data, but tells potential users what is available and how they can request access. A **data consumer**, for example a pilot partner developing a mobility application, browses the catalogue and finds the dataset. If the dataset fits their needs, the consumer initiates a data access request. This triggers a **negotiation phase**, where the consumer's request is matched against the provider's policies (such as usage rights, contract terms, or allowed frequency). If both parties agree, the data is transferred securely using a trusted communication protocol. The actual data never becomes publicly accessible—only those who are authorized through the dataspace infrastructure can retrieve it. Every interaction is logged and monitored to ensure compliance with the agreed rules. This setup ensures **data sovereignty** (each partner controls how their data is used), **interoperability** (partners use common standards), and **security** (data is exchanged securely and only between trusted parties). This kind of interaction is expected to be replicated in multiple use cases within the project—whether it's exchanging energy grid information, mobility patterns, or sensor data—and can also serve as a template for data exchange in future cross-domain projects. **This transversal use case could be split into different scenarios:** Scenario 1: Use of the dataspace by a data producer

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Scenario 2: Use of the dataspace by a data customer
Scenario 3: Metadata Discovery and Planning
Scenario 4: Federated Service Chaining

- **Sc.1 Use of the dataspace by a data producer - Description:**

This scenario describes how a data provider makes its dataset or service available within the dataspace. The provider prepares the asset, defines the associated metadata and access policies, and publishes it through its local EDC connector. The asset becomes discoverable by other parties via the federated catalogue, allowing compliant and secure access negotiations.

Additionally, by exposing curated datasets through the dataspace, data producers contribute to cross-pilot AI training efforts, enabling other partners to discover and evaluate datasets suitable for model development.

- **Sc.2 Use of the dataspace by a data customer - Description:**

In this scenario, a data consumer interacts with the dataspace to discover and access data assets shared by other parties. The consumer queries the catalogue, evaluates metadata and policy terms, and initiates a contract negotiation through its EDC connector. Upon agreement, the data is securely transferred according to the defined usage rules.

- **Sc.3 Metadata Discovery and Planning - Description:**

A partner uses the dataspace not to directly retrieve data, but to discover which datasets or services are available, including their conditions of use, data formats, and applied semantic vocabularies.

This scenario highlights the catalogue and *resource discovery* capabilities of the dataspace, enabling informed planning, semantic mapping, and potential future agreements.

Particularly useful in the design or pre-integration phase.

Reduces effort in bilateral discussions, as the catalogue serves as a shared point of reference.

Reinforces semantic interoperability goals (e.g., Task 4.3).

- **Sc.4 Federated Service Chaining - Description:**

A software component (e.g., an orchestrator or optimization engine) uses the dataspace to access services or modules provided by other partners, in a dynamic and composable way.
For instance, an edge node may call a forecasting module hosted in the cloud by another partner, sending data via the dataspace and receiving a processed result in return.

UML USE CASE DIAGRAM

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

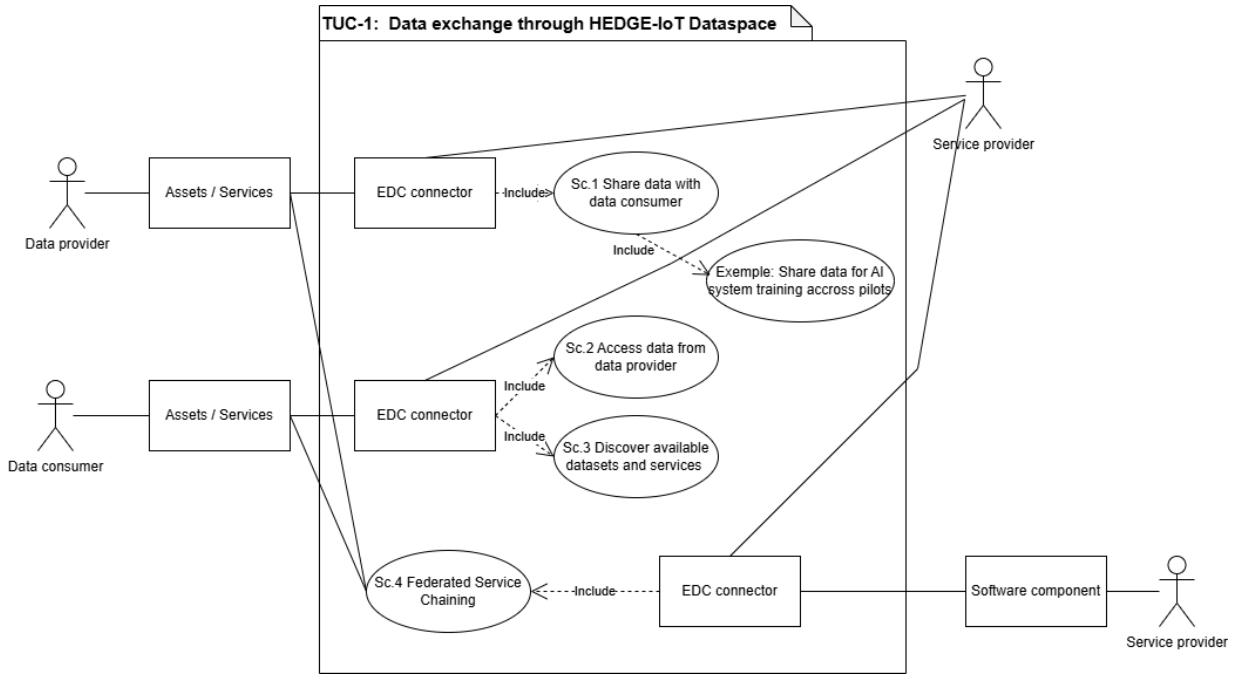

FIGURE 39 - UML USE CASE DIAGRAM

TUC-2 - ORCHESTRATE THE COORDINATION, MANAGEMENT, AND EXECUTION OF ENERGY SERVICES ACROSS THE COMPUTATIONAL CONTINUUM

TABLE 15 - TRANSVERSAL USE CASE 2 - ORCHESTRATE THE COORDINATION, MANAGEMENT, AND EXECUTION OF ENERGY SERVICES ACROSS THE COMPUTATIONAL CONTINUUM

SUC ID	TUC-2
SUC NAME	Orchestrate the coordination, management, and execution of energy services across the computational continuum
AREA/DOMAIN	Computational interoperability
SCOPE	Coordinating distributed computational tasks for energy services across edge-to-cloud systems, with goals of ensuring responsiveness and cost-effective data exchange, including minimized latency and bandwidth usage. We consider containerized energy services that are data space compliant through eclipse data connector.
OBJECTIVES	The goals that the use case is expected to achieve are to: • **Objective 1**: Dynamically allocate computational resources based on energy services demand across edge, fog, and cloud layers to maintain efficiency and responsiveness. • **Objective 2**: Minimize data transfer overhead in federated AI services by efficiently managing and optimizing the hyperparameters of the learning process. • **Objective 3**: Ensure the efficient update of energy services from cloud to edge avoiding execution disruption.

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SHORT DESCRIPTION	The use case focuses on enabling the automated coordination, management, and execution of computational tasks through a computational orchestrator. The orchestrator leverages swarm-based algorithms to optimize resource usage, ensuring both computational and communication efficiency. It integrates with non-AI Energy Services to manage deployment, coordination, and resource allocation, and with AI Federated Services to support hyperparameter tuning and training optimization. Additionally, it enables services roll-up at the edge, allowing automated updates and deployment of new versions. Integration with the Eclipse Data Space Connector ensures compliance with data space standards and secure, interoperable data and service exchange.
COMPLETE DESCRIPTION	This transversal use case could be split into three scenarios: • **Scenario 1: Energy services orchestration at edge for responsiveness and geographic redundancy (Sc.1)** Containerized energy services are deployed across edge-fog-cloud distributed infrastructure overlapping the smart grid. The services and the infrastructure available computing nodes are registered with the computational orchestrator. The orchestrator continuously monitors service locations, resource availability, and task assignments. An integrated Kubernetes component handles the initial task allocation based on current resource availability and predefined configurations. It also supports live monitoring of service status and system resources. When predefined events occur, such as violations of service level agreements or policy conditions, the orchestrator responds by executing a swarm-based optimization algorithm to determine which services should be migrated to other nodes. During service migration, the persistent state and data of each service must also be transferred, and their connectivity via the Eclipse Data Space Connector must be maintained to ensure secure and interoperable data exchange. Therefore, it ensures service responsiveness and geographic redundancy. • **Scenario 2: Federated AI-driven energy services orchestration for cost-effective data exchanges (Sc.2)** The orchestrator manages federated learning processes initiated by AI services deployed across edge, and fog/cloud nodes. The federated architecture may follow either a hierarchical or peer-to-peer model. All participating nodes are registered with the orchestrator, providing metadata on their computational capabilities and availability. Based on service-specific requirements, the orchestrator can cluster nodes to enhance training efficiency. It also performs hyperparameter tuning and training optimization using heuristic-based algorithms, ensuring efficient use of distributed resources at edge and minimizing data exchange overhead among edge and fog/cloud nodes. • **Scenario 3: Energy service rolling out at edge (Sc.3)** The orchestrator can support service providers such as DSO to automatically roll out new versions for energy services for the consumers. The data models (packages or files) are sent through the Eclipse Data Space Connector. It detects available updates for application components, manages versioning and handles service interruption during updates.
UML USE CASE DIAGRAM	

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

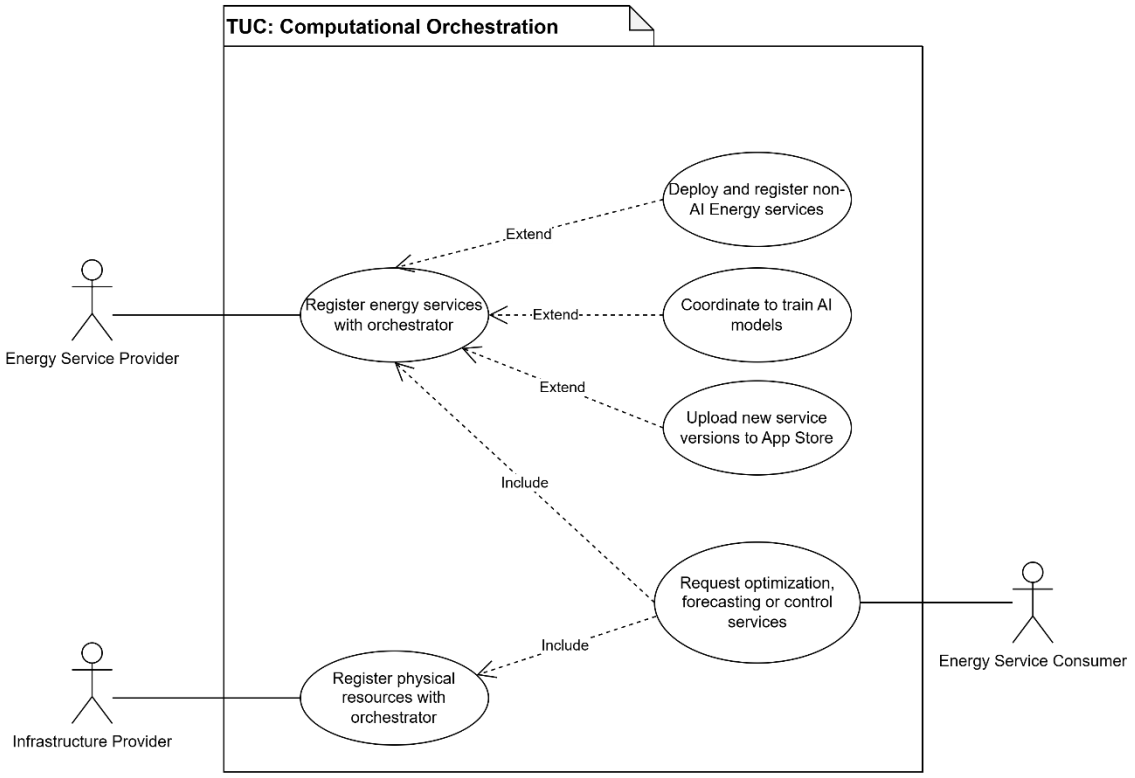

FIGURE 40 - TUC 2 UML USE CASE DIAGRAM

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

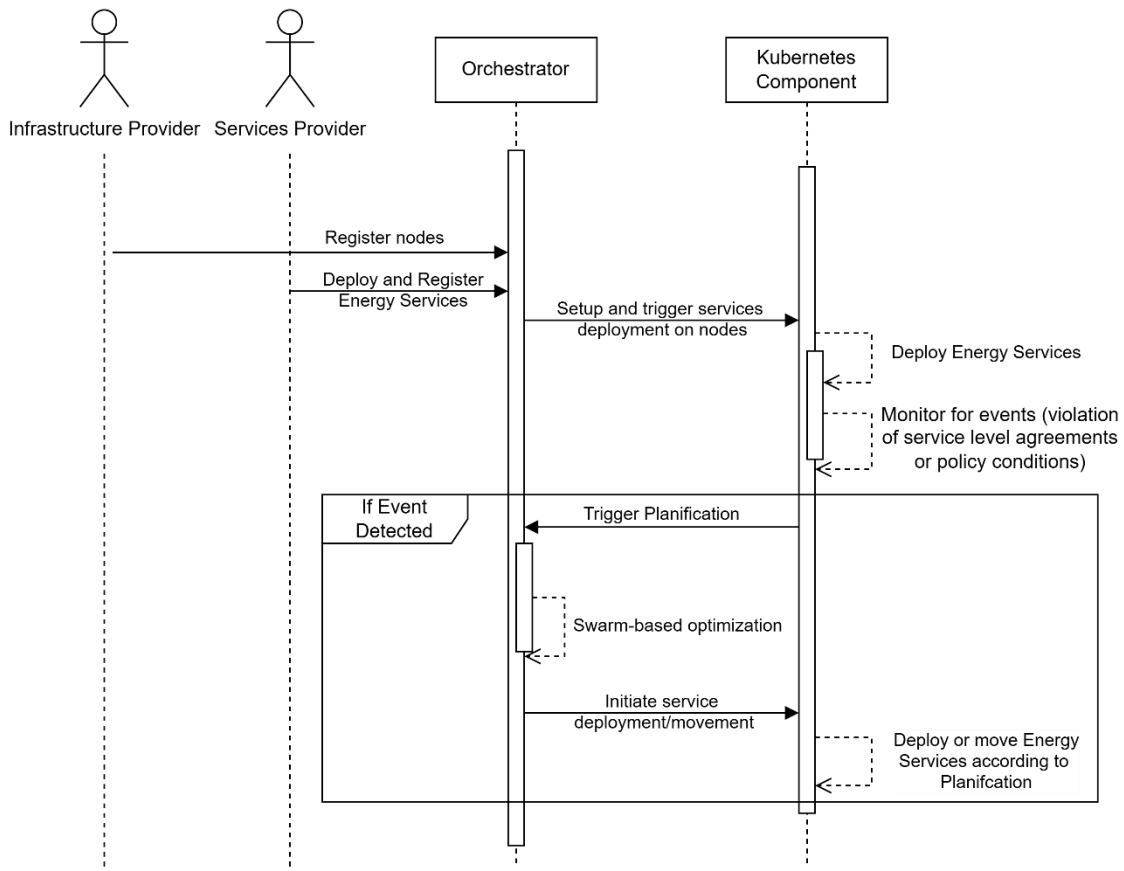

FIGURE 41 - TUC 2 UML SEQUENCE DIAGRAM – SCENARIO 1 NON-AI ENERGY SERVICES

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

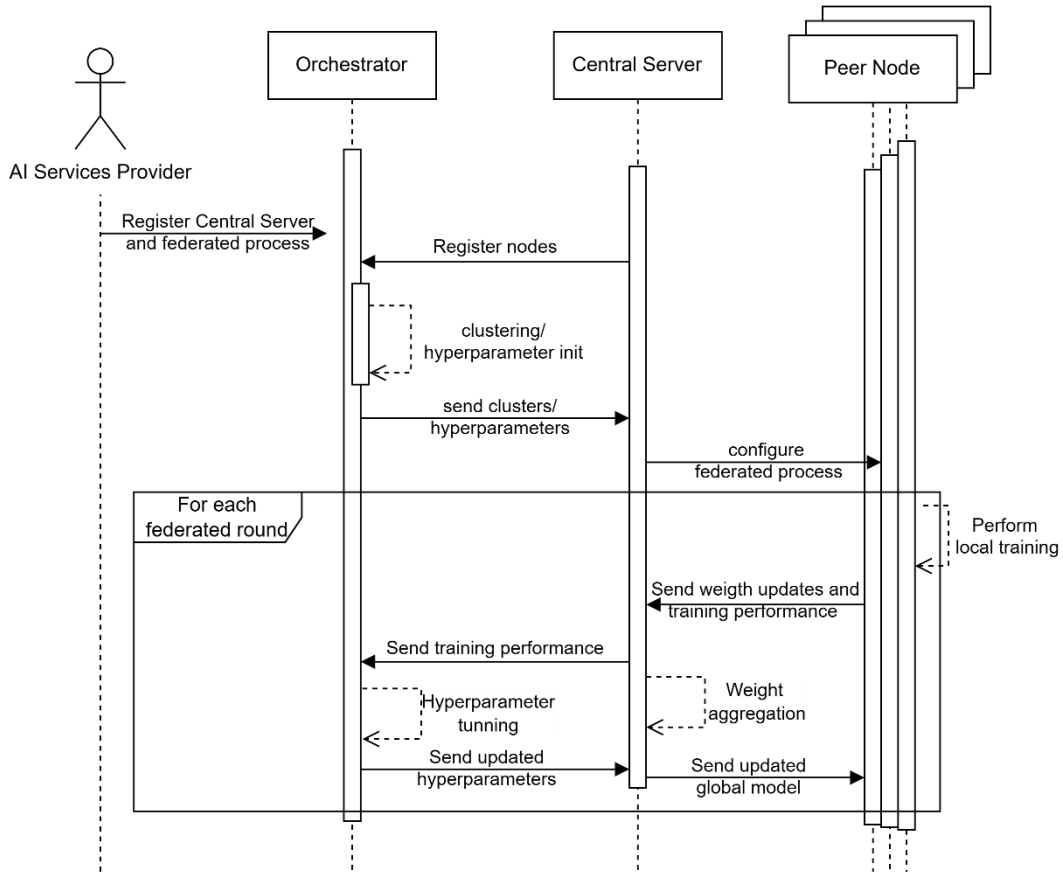

FIGURE 42 - TUC 2 UML SEQUENCE DIAGRAM – SCENARIO 2 AI ENERGY SERVICE

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

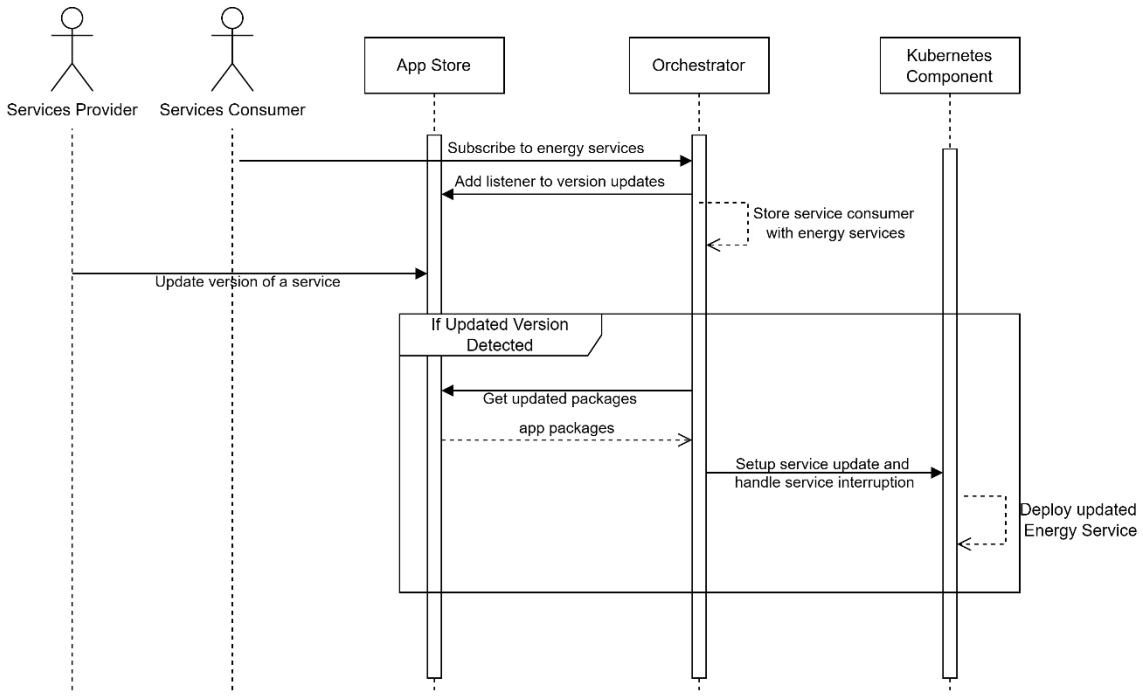

FIGURE 43 - TUC 2 UML SEQUENCE DIAGRAM - SCENARIO 3 ENERGY SERVICES ROLLING OUT AT EDGE

TUC-3 - USE OF THE APP STORE AS PART OF HEDGE-IOT

TABLE 16 - TRANSVERSAL USE CASE 3 - USE OF THE APP STORE AS PART OF HEDGE-IOT

SUC ID	TUC-3
SUC NAME	Use of the App Store as part of HEDGE-IoT
AREA/DOMAIN	Functional interoperability
SCOPE	This use case describes the HEDGE-IoT App Store, a component of the HEDGE-IoT digital middleware, and how it enables publishing, discovering, using and creating new data apps (edge/cloud services) in a trusted, semantically interoperable energy IoT ecosystem. It covers the full lifecycle of data-driven services at the edge or cloud: from App Providers publishing services, to App Users discovering and deploying them, to composing new services from existing ones, and ensuring services are interchangeable in a data space, namely through to semantic standards.
OBJECTIVES	The main objective is to deploy an App Store where third-party developers can publish data apps, certified them, and where energy stakeholders can discover and deploy these apps on their HEDGE-IoT Connectors at the edge or in the cloud. The objectives that the use case is expected to achieve are to: • **Objective 1:** Facilitate publication of new services/sub-services in the HEDGE-IoT environment.

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

	• **Objective 2:** Provide a discovery mechanism so developers or users can find available reusable services. • **Objective 3:** Enable reusability and interoperability among different HEDGE-IoT components, pilot projects or datasets. • **Objective 4:** Promote semantic interoperability (services whose data assets can be used across different pilot contexts).
SHORT DESCRIPTION	The HEDGE-IoT App Store is a repository for Software Applications that operate at least in one data space configuration. Apps include/represent services/microservices enabling quick discovery, sharing, and reuse across different pilots and domains. It allows service owners to publish new service functionalities, while developers or other system components can request and acquire access. By ensuring semantic and technical interoperability, the App Store accelerates solution development and deployment, fosters collaboration, and ensures consistent service quality within the HEDGE-IoT framework. In line with the new data space protocol (version >2), the App Store also promotes the possibility for dataspace compliant connectors to search adopt other versions of control and data planes available.
COMPLETE DESCRIPTION	This transversal use case is therefore split into four scenarios: • **Scenario 1:** Publish a service/sub-service in the App Store A service provider develops or containerizes a new IoT/energy service and registers it within the HEDGE-IoT App Store, supplying descriptive metadata (inputs, outputs, resource requirements, license) along with the container image. An automated certification process checks the connector's compatibility, security, and semantic conformance. Once approved, the service becomes discoverable in the App Store catalogue, ready for other stakeholders to reuse. • **Scenario 2:** Find/Retrieve/Reuse/Access a service/sub-service in the App Store An application developer or system component browses or queries the App Store to locate a suitable service based on functionality or usage terms. After accepting any licensing agreements or data usage policies, the user's edge/cloud environment retrieves the service container from the App Store's registry. The service is then deployed at the selected node(s), where it can securely process data under the HEDGE-IoT dataspace policies. • **Scenario 3:** Interchangeable common services/sub-services *(semantic interoperability across data consumers)* Different providers publish "functionally equivalent" services following the same data schemas. Thanks to uniform semantic definitions, a user can seamlessly swap one service with another without having to modify underlying workflows or data pipelines. This ensures plug-and-play upgrades, vendor-neutral deployments, and consistent service behaviour across diverse HEDGE-IoT environments.
UML USE CASE DIAGRAM	

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

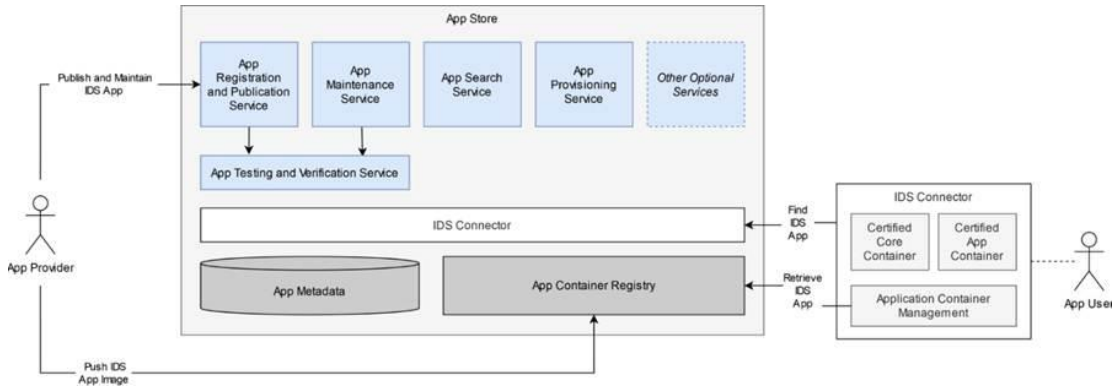

FIGURE 44 - IDS APP STORE REFERENCE ARCHITECTURE

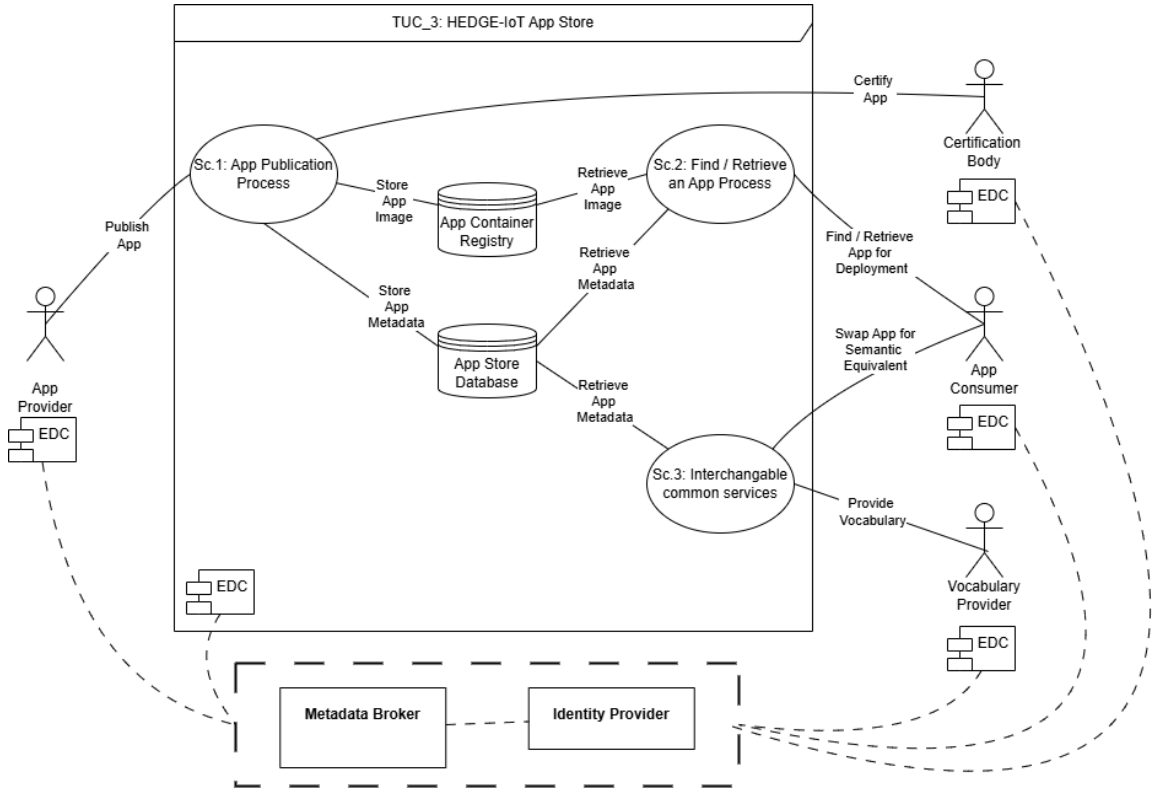

FIGURE 45 - TUC 3 HEDGE-IOT APP STORE UML USE CASE DIAGRAM

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

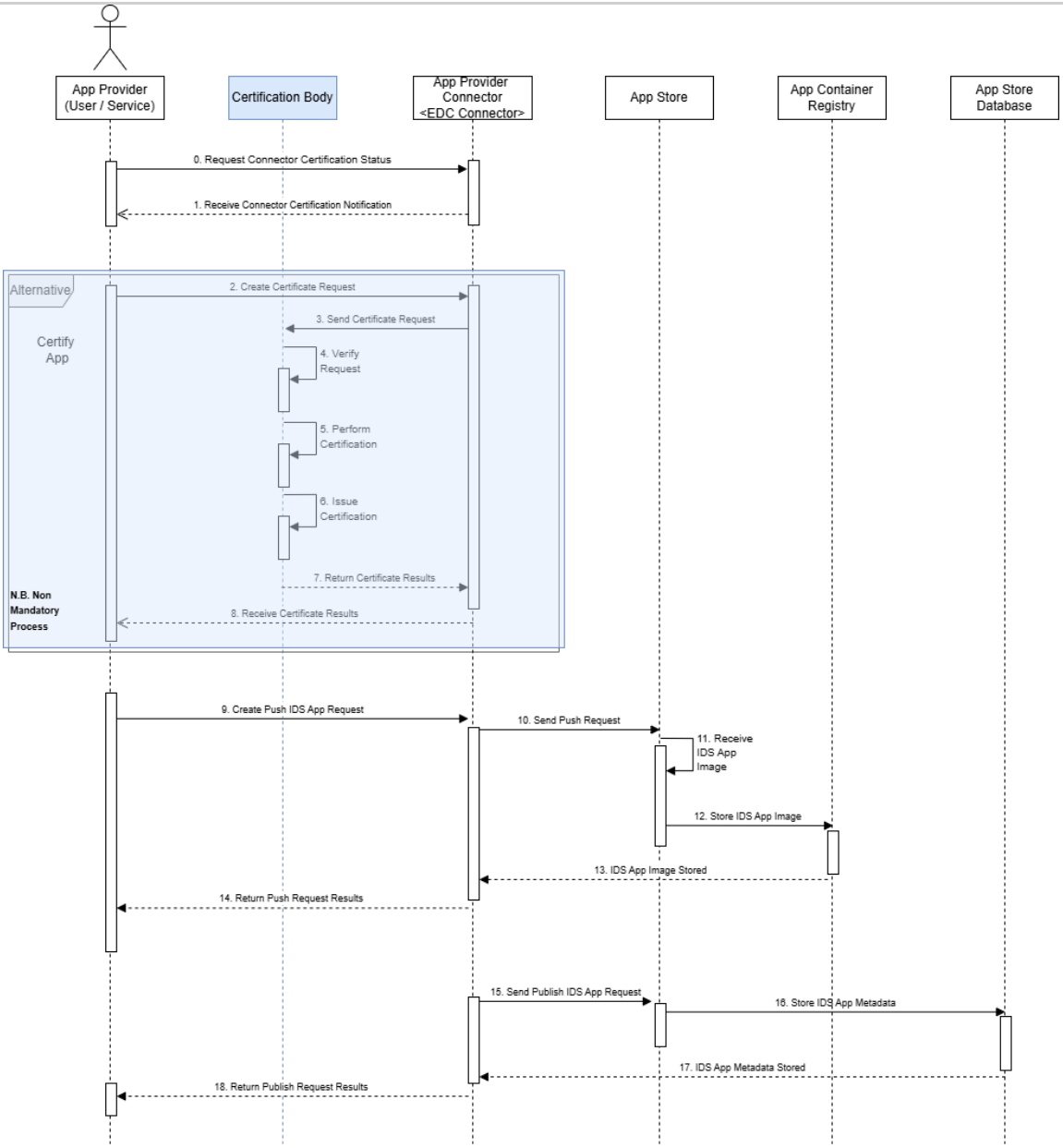

FIGURE 46 - TUC 3 UML SEQUENCE DIAGRAM - SCENARIO 1 "PUBLISH AN APP"

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

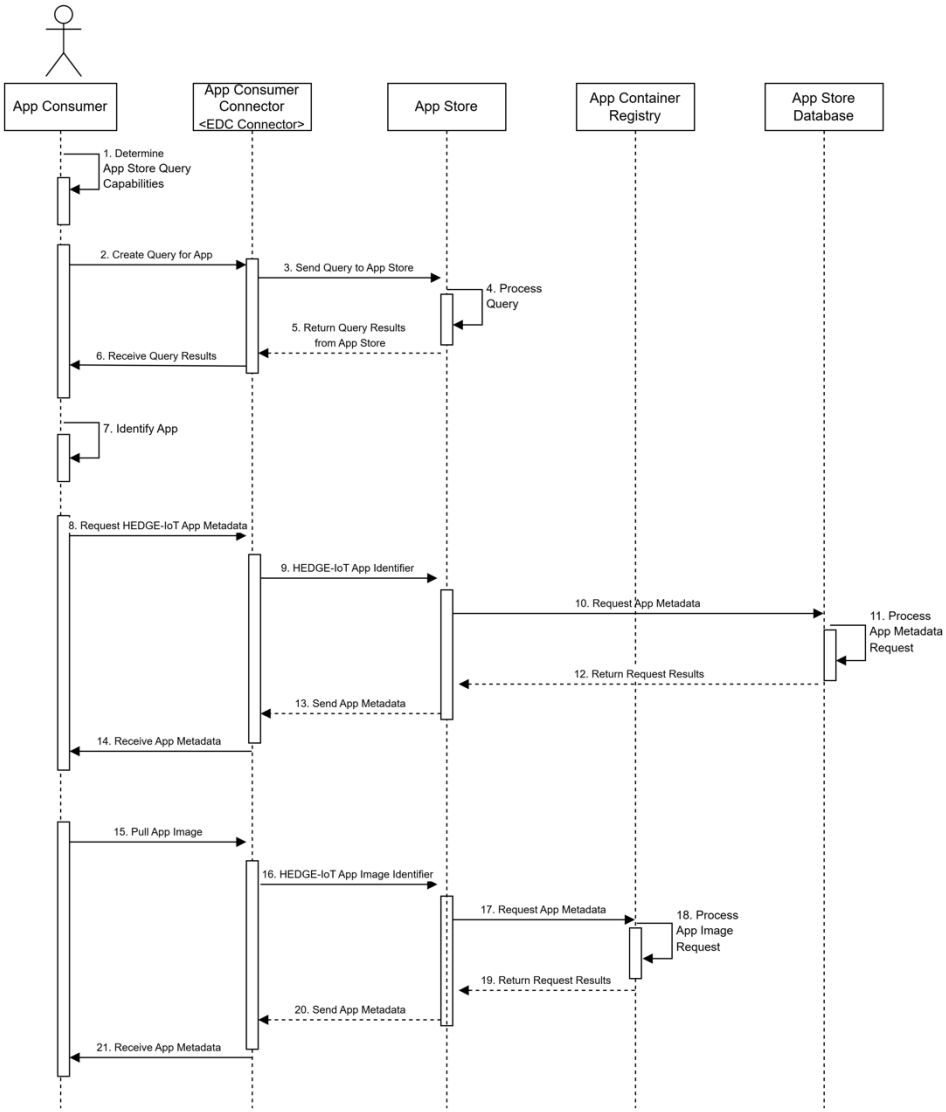

FIGURE 47 - TUC 3 UML SEQUENCE DIAGRAM - SCENARIO 2 "FIND/RETRIEVE/REUSE/ACCESS AN APP"

Note on Scenario 3: Interchangeable common services/sub-services

Scenario 3 illustrates a high level of semantic interoperability within the App-Store workflow: different providers publish functionally equivalent services that are built on the same data models, to allow end-users to swap one service for another without interfering with existing workflows. Because this capability depends on the alignment of ontologies, usage-control policies, and connectors, additional work is required before the sequence diagram can be finalised.

Therefore, the finalized UML sequence diagram for Scenario 3 is not included in this Deliverable D2.3. It will be finalised and included into the next iteration of this report (D2.4) once the necessary interoperability mechanisms have matured appropriately.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

4.5.4. Pilots' implementations of transversal use cases

After the definition of the HEDGE-IoT transversal use cases, a first estimation of their implementation in the pilot was done. Table 17 presents the provisional distribution of TUCs to be implemented and used by pilots. This table is not definitive and will be refined all along the process with the pilots. This is particularly true for scenarios requiring interchangeable common services or data exchanges or reuse of other pilot services.

TABLE 17 - PILOTS' IMPLEMENTATIONS OF TRANSVERSAL USE CASES

Transversal use case	Scenario	FL	GR	IT	NL	PT	SL
[Dataspace] Data interoperability Data exchange through HEDGE-IoT Dataspace.	Sc1. Use of the dataspace by a data producer	✓	✓	✓	✓	✓	✓?
	Sc2. Use of the dataspace by a data customer	✓	✓	✓	✓	✓	✓
	Sc3. Metadata Discovery and Planning		✓	✓	✓	✓	?
	Sc4: Federated Service Chaining		✓	✓	✓		?
[Computational Orchestration] Computational interoperability Automate coordination, management, and execution of HEDGE-IoT computing tasks across the distributed systems/services and cloud environment.	Sc1. Energy services orchestrations at edge geographic redundancy			✓			
	Sc2. Federated AI services (hyperparameter tuning)		✓?			✓	
	Sc3. Energy application rolling-up at Edge	✓					
[App Store] Functional interoperability Use of the App Store as part of HEDGE-IoT.	Sc1. Publish a service/sub-service in the App Store	✓	✓?	✓	✓	✓	✓
	Sc2. Reuse/Access a service/sub-service in the App Store		?	✓	✓	✓	✓?
	(Potential) Sc3. Interchangeable common services/sub-services (among pilots)		?		✓		?

4.5.5. Conclusion and next steps on TUCs

The HEDGE-IoT TUCs were defined as a first version. It will support components' specifications and implementation as well as the pilots' implementations. The TUCs will be revised if needed in D2.4, and a more complete vision of their implementation by the pilots will be provided.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

5. HEDGE-IOT COMPONENTS & SERVICES

5.1. COMPONENT CATALOGUE

TABLE 18 - HEDGE-IOT COMPONENT CATALOGUE

a/a	Provider	Component ID	Component Name	Component Description
1	TUC	COMP-01	Computational Orchestration Platform	An edge computing platform for smart grids will be designed and developed which will allow the discovery and selection of edge nodes for processing workloads offloading and their optimal orchestration for delivery of near real-time AI-driven applications at the edge.
2	INESC	COMP-02	AppStore	The AppStore along with an Open Services Catalogue will enable access to Data Apps for interoperable services. It will consist of a complete functionality for available Data Apps, supporting operations for Services and Data App registration, publication (including metadata), maintenance and query, as well as operations for the provisioning of a Data App to specific service interfaces.
3	ED	COMP-03	Interoperability Middleware	Development of the HEDGE-IoT interoperability middleware, as a basis for the interoperability framework and data sharing in an end-to-end decentralized approach. The middleware will become the basis for the Connector GUI development and the integration API library between stakeholders (local platforms)
4	DST	COMP-04	Open Data Connector	Development of the HEDGE-IoT Data Space connector according to Reference Architecture design and Data Space principles for enabling seamless and secure data exchange.
5	DST/ED	COMP-05	Open Data Connector GUI	Development of the HEDGE-IoT Connector Graphical User interface which will contain access to interoperable Data Space services, allows the creation of Data offerings and basic usage control.
6	TNO	COMP-06	Semantic Interoperability Enablers	A series of Semantic tools dedicated to support HEDGE-IoT semantic ontologies design, harmonisation and validation.
7	WP4	COMP-07	User Management – Identity Provider	A central user authentication and authorisation platform.
8	KONC	COMP-08	PowerCIM	PowerCIM is a platform for storing and exchanging electrical grid models based on IEC CIM standards, enabling unified, semantically aligned models by integrating data from diverse system operator sources.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

5.2. HEDGE-IOT SERVICES

TABLE 19 - HEDGE-IOT OPEN SERVICES INFORMATION

a/a	Provider Name(s)	Service ID	Service Name	Service Description
1	ICCS	SERV-01	Federated Learning for Energy Forecasting & Disaggregation	This solution is designed to enhance energy management by providing accurate predictions of energy consumption and production, coupled with detailed energy disaggregation capabilities. It uses a decentralized horizontal federated learning approach to ensure privacy by keeping raw data localized on local IoT devices, such as smart meters, while enabling centralized model training. The approach leverages advanced time-series models like LSTM and BiLSTM for forecasting and NILM techniques for disaggregating energy consumption at the device level. It aligns seamlessly with the HEDGE-IoT interoperability framework, by adopting the project's open data connectors and semantic interoperability protocols.
2	INESC	SERV-02	Vector Autoregressive Model for Energy Time Series Forecasting	This service employs a vertical federated learning approach to perform short-term energy predictions while preserving data privacy. By keeping data localized on devices and leveraging privacy-preserving encryption, the method allows data owners to collaboratively estimate VAR model coefficients without sharing sensitive information. The approach leverages VAR's multivariate component to extract relevant correlations with non-energy data, such as weather forecasts and humidity. LASSO regularization enables efficient variable selection and model optimization, addressing the high-dimensional nature of energy data. The integration with HEDGE-IoT's interoperability framework will be done via the adoption of the project's open data connector, ensuring secure and interoperable data exchanges.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

3	UNZIG	SERV-03	Enhanced Network Management and Planning	This service utilizes a combination of machine learning techniques to address anomaly detection, distributed energy resource (DER) capacity assessment, and forecasting of electrical quantities in secondary substations. Focused on improving planning and operational efficiency for DSOs, the service operates on edge devices to minimize reliance on centralized data storage and cloud computing. With all calculations performed close to the data source, this approach ensures low-latency decision-making and enhances data privacy. Interoperability is achieved through the PowerCIM tool for data exchange between energy stakeholders and by integrating with the project's interoperability framework.
4	JSI	SERV-04	DTR-DLR on the Edge	is an edge service that utilizes dynamic thermal rating algorithms to optimize the capacity and operational efficiency of overhead lines and transformers by leveraging real-time weather and operational data. Using IoT devices like the Maxx GW-4100 gateway, the service performs localised computations for ampacity, thermal states, and short-term forecasts, providing a contribution to decentralizing the grid. The service integrates the notion of interoperability through the SUMO bus, which uses standardized protocols (e.g., IEC 61850) to enable real-time data exchange with other grid components. This decentralized and interoperable approach reduces latency and ensures secure operation within DSO and TSO infrastructures.
5	VU	SERV-05	Anomaly Detection and Predictive Maintenance on the Grid	This service is designed to identify anomalies and faults in the local grid through real-time analysis of streaming data from IoT devices. The AI algorithm of the service learns the nominal behaviour of energy nodes through online learning, allowing it to adapt to new environments and detect anomalies in both structural and non-structural graph data. The service implements semantic interoperability by using the SAREF ontology combined with TNO's Knowledge Engine as a semantic data broker. By leveraging SAREF-compliant Smart Connectors, the service integrates with the HEDGE-IoT Interoperability Framework, facilitating transparent data exchange and ensuring compatibility with third-party dashboards.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

6	APIO	SERV-06	APIO IoT Platform	This service is a cloud-native, multi-tenant platform designed for managing time-series data and supporting machine learning applications in the energy domain. It integrates edge devices like PGUIs (Power Grid User Interfaces) that aggregate, sign, and securely transmit data from the edge to the cloud, without running any local algorithms themselves. Moreover, the PGUIs power consumption will be estimated by analysing the behavior of the SoC (System on Chip) under several conditions, ensuring that the energy consumption of edge devices stays low. Data privacy is ensured through encryption protocols (CHAIN2 and MQTTS), rotating credentials, and strict access controls, safeguarding the integrity of data throughout its journey. The integration with the HEDGE-IoT Interoperability Framework will be achieved by applying SAREF-based ontologies to the platform's data and by adopting the project's open data connectors.
7	VTT	SERV-07	Anomaly Detection and Fault Forecasting to Increase Distribution Network Resilience	This service enhances grid resilience by analysing high-resolution, real-time data streams from Intelligent Electronic Devices (IEDs) within substations. The service uses advanced deep learning to establish a baseline of the grid's normal status and uses a Convolutional Neural Network (CNN) as a primary anomaly detection model. A Deep Reinforcement Learning (DRL) model is used for fault forecasting, to identify deviations from the grid's normal state and predict the faults before they occur. By processing data locally on the edge devices, the service ensures data privacy and does not rely on central storage. To secure interoperability with grid management systems, the service uses IEC 61850 and open data standards and will also leverage the project's interoperability framework. Currently, the service is at TRL 4 having been validated using historical and synthetic data.
8	TAU	SERV-08	Real-Time Congestion Management	This service is a tool to manage grid congestion by gathering real-time data from primary substation and using edge nodes with significant computational power. Its modular architecture is designed to facilitate the development of algorithms. The system integrates microservices for load and generation estimation, state estimation, and congestion management. By combining active and passive grid management approaches, the service enables grid operators to use flexibility resources effectively while improving grid observability. In terms of flexibility, the service adopts the Eclipse data space connector to ensure secure and interoperable data exchanges between edge nodes and the

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

				cloud. Moreover, its data is based on the IEC61850 standard.
9	INESC	SERV-09	EdgeConnect	This service provides an ecosystem for stakeholders across the flexibility value chain, enabling integration, qualification and market participation, to unlock flexibility potential. The service facilitates onboarding and certification of users, registration and pre-qualification of flexible assets, sharing of flexibility needs, baselines and bids and activation and settlement of flexibility services, allowing consumers to actively participate in energy markets. EdgeConnect ensures data privacy with role-based data access, while having critical information anonymized. Service to service data exchange interoperability is guaranteed via the integration of the project's data space connector. Furthermore, semantic interoperability will be integrated using the approach defined in the project. Currently, the service is at TRL 6, having already been tested in a controlled environment in a different European project.
10	ICCS / HENEX	SERV-10	Flexibility Optimization Service	This service is comprised of four modules that enable consumers to participate and place bids in local flexibility markets: 1) short and long-term forecast for energy demand and production; 2) calculation of incentives optimization and formulation of optimal bid; 3) communication of flexibility requests to consumers and 4) submission of bids in the local flexibility market. The service ensures data privacy by enforcing encryption and access control mechanisms like Attribute-Based and Role-Based Access Control (ABAC and RBAC). Currently, the service is at TRL 3 and the focus is on establishing the foundational architecture.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

11	NESTR	SERV-11	Real-Time Reserve Market Simulator	This service is designed to emulate manual Frequency Restoration Reserve (mFRR) and automatic Frequency Restoration Reserve (aFRR) market operations, providing TSOs and Balancing Service Providers with a platform to test and optimize bidding strategies. The simulator validates bids, performs market simulations, and delivers outputs such as settlement curves and activation setpoints. The main advantage of the tool is enabling real-time market simulations with real consumer and TSO data, but without needing to comply with the full restrictions of the actual market. The tool will integrate HEDGE-IoT's interoperability framework by adopting the project's data space connector and performing data exchanges with the previously mentioned EdgeConnect service. Currently, the application is containerized using Docker and deployed in AWS
12	TAU	SERV-12	Predictive Congestion Management	This service is composed of several micro-services for load, generation and grid state forecasting with the aim of enabling grid operators to procure flexibility. It uses 3 data sources: weather, market, and historical grid data to make predictive analyses and foster market participation. The service will implement the project's data space connector, therefore integrating its interoperability framework. Currently, the service is still at the design stage, as no implementation work has started yet.
13	INESC	SERV-13	Energy Community Management Service for Frequency Restoration Reserve	This service enables Renewable Energy Communities (RECs) to participate in Balancing Service Markets (BSMs) by provisioning mFRR and aFRR, using a set of modules to manage an energy community, including sizing, energy management and settlement. Since they act as natural aggregators, this service can coordinate a REC's members' flexibility while adhering to strict TSO requirements for frequency restoration reserve markets. The service will integrate HEDGE-IoT interoperability framework by adopting the project's data space connector, which will be used for interoperable data exchanges with other frequency restoration reserve market stakeholders. Currently, the frequency restoration reserve service is at TRL 2, while the underlying energy community management platform is at TRL 4, having been tested in a lab environment in the scope of another project.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

14	TUC	SERV-14	Computational Orchestration Framework	This service ensures a streamline, homogenous and efficient cloud-to-edge computational effort, a swarm-based computation orchestration framework is developed in the project and its first specification is provided in this document. This framework has two main goals: 1) edge offloading for low-latency data processing for energy cloud services and 2) to orchestrate federated learning and distributed computing processes across the edge-fog-cloud continuum. Built on KubeEdge, the framework extends Kubernetes capabilities to edge environments, incorporating swarm-based heuristics to optimize resource allocation. Regarding data privacy, it integrates blockchain for secure and transparent service management, taking advantage of smart contracts and tokens for traceability. A monitoring system using Kube Prometheus will be established, supporting real-time infrastructure insights. It integrates HEDGE-IoT's interoperability framework by 1) considering the set of data-driven cloud services available in the project's App Store, 2) by using semantic annotation to expose edge devices computation capabilities and 3) by adopting the project's data space connector to perform interoperable data exchanges with the edge devices that also adopt it.

6. HEDGE-IOT REFERENCE ARCHITECTURE

6.1. VOCABULARY

This section introduces the key terminology associated with the HEDGE-IoT RA. Establishing a shared and precise vocabulary and clearly defined terminology reduces ambiguity and fosters effective collaboration, facilitating a common understanding of the architectural concepts, components, roles, and functionalities described throughout this document.

TABLE 20 - HEDGE-IOT REFERENCE ARCHITECTURE VOCABULARY

Term	Description
Generic Terminology	
Platform	A sophisticated array of integrated systems, interfaces, and processes working together to offer a range of functions and services.
Reference Architecture	A structured template design providing a systematic method for developing system architectures for any domain, ensuring interoperability, scalability, and standardization.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Use Case	A list of actions or event steps typically defining the interactions between a role (known in the Unified Modelling Language (UML) as an actor) and a system to achieve a goal. The actor can be a human or other external system.
Requirement	A documented necessity, either physical or functional, that a particular IoT solution, design, or process aims to fulfil.
Functional Requirement	Specific behaviours, functionalities, and data flows necessary for the proper operation of the IoT platform or application.
Non-Functional Requirement	Quality attributes or constraints under which an IoT solution must operate, such as reliability, maintainability, scalability, performance, and cybersecurity.
Actor	An external entity (human user, external system, or hardware) interacting with the IoT system through data exchanges or service utilization.
Component	A modular and independently deployable unit within the IoT architecture that encapsulates specific functionalities, providing defined interfaces for interacting with other components.
Device	Physical equipment or hardware capable of executing IoT software, storing data, or performing specific operational tasks within the IoT system architecture (e.g., sensors, gateways).
Application Programming Interface (API)	A software interface facilitating interaction, data exchange, and integration between components, services, or tools within the IoT ecosystem.
Semantics [32], [33]	Understanding of the concepts contained in the message data structures. Understanding of the information that needs to be accessed/exchanged. The semantic aspect refers to the meaning of data elements and the relationship between them. It includes developing vocabularies and schemata to describe data exchanges and ensures that data elements are understood in the same way by all communicating parties.
Semantic Model	A structured description of the semantics of a set of information, using some information modelling language (e.g. UML). A semantic model is 'metadata' – 'data about data'. Many different semantic models are possible for the same semantics, even within one modelling language. Semantic modelling only represents information content – it does not include formatting/encoding (syntactical) specifications.
Interoperability [32], [34]	The ability of two or more devices to exchange information and use that information for correct cooperation to perform the required functions. In other words, two or more systems are interoperable, if they can perform cooperatively a specific function by using information that is exchanged.
Ontology	A representation, formal naming and definition of the categories, properties and relations between the concepts, data and entities that substantiate one, many or all domains of discourse.
Reference Architecture	A Reference Architecture describes the structure of a system with its element types and their structures, as well as their interaction types, among each other and with their environment. Describing this, a Reference Architecture defines restrictions for an instantiation (concrete architecture). Through abstraction from individual details, a Reference Architecture is universally valid within a specific domain. Further architectures with the same functional requirements

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

	can be constructed based on the reference architecture. Along with reference architectures comes a recommendation, based on experiences from existing developments as well as from a wide acceptance and recognition by its users or per definition.
HEDGE-IoT Terminology	
HEDGE-IoT Use Case	Use Case derived by following two processes; first, we identify and classify data and used services between actors/platforms for all demos. Second, we include SUCs identified in other H2020 projects, based on the work conducted in the context of WP2 that are relevant to HEDGE-IoT, to have a complete list of General UCs that will be implemented through the HEDGE-IoT digital ecosystem.
HEDGE-IoT Middleware	The central component responsible for core functionalities such as semantic interoperability, user and data management, federated learning, and system administration within the IoT ecosystem.
HEDGE-IoT Dataspace	An integrated data environment enabling secure and standardized exchange of data, encompassing components such as App Store, Orchestrator, and Infrastructure Operations, maintaining data sovereignty and interoperability.
Transversal Use Case	A Use Case applicable across multiple actors and components within the entire HEDGE-IoT Dataspace ecosystem. Unlike pilot-specific or isolated scenarios, transversal use cases demonstrate overarching functionalities and commonalities, highlighting interactions and data exchanges among diverse entities including Data Providers, Data Consumers, and service operators, independent of individual pilots or demonstrations.
Service Catalogue	A structured repository storing metadata about available IoT services, functionalities, and APIs, allowing streamlined discovery, integration, and utilization of services.
Connector GUI	Graphical user interface facilitating the management of connections and interactions among components and actors within the HEDGE-IoT ecosystem.
App Store	Centralized marketplace allowing registration, publishing, discovery, and deployment of applications and services, enabling seamless integration of modular IoT components.
Computational Orchestration	The dynamic management and coordination of computational resources, services, and workloads within the IoT infrastructure to ensure optimal performance and efficiency.
Infrastructure Operation & Planning	Activities and functionalities aimed at managing, planning, and optimizing IoT infrastructure to support scalable deployment and operational efficiency.
Identity Provider	Security component responsible for authentication, authorization, and identity management of users, services, and devices, ensuring secure access within the HEDGE-IoT ecosystem.
Catalogue	Centralized registry within the Dataspace maintaining metadata and descriptions of all available IoT assets, enabling discovery and interoperability.
Energy Stakeholders	Entities directly involved with or utilizing IoT solutions in the energy sector, including Distribution System Operators (DSOs), Transmission System Operators (TSOs), flexibility service providers (FSPs), markets, and consumers.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Pilots	Real-world implementations and testbeds involving IoT technologies to validate the functionalities, interoperability, and effectiveness of the HEDGE-IoT architecture.
IoT-Edge Services	Services specifically designed to operate at the network edge, supporting local data processing, real-time analytics, and interaction with physical sensors and devices.
Data Provider	Actor or entity providing data to the HEDGE-IoT Dataspace, compliant with the reference architecture's specifications.
Data Consumer	Actor or entity consuming data from providers, leveraging IoT services or applications enabled by the architecture.
Fog/Cloud Services	Services operating between cloud and edge layers, enabling hybrid processing capabilities and ensuring efficient data management and analytics.
Eclipse Data Connector (EDC)	A specialized instance of the Eclipse Data Connector framework, employed within the HEDGE-IoT architecture to enable secure, standardized, and policy-driven data exchange among IoT ecosystem components. The EDC facilitates interoperability, preserves data sovereignty, and supports decentralized data sharing in alignment with the architecture's reference specifications.

6.2. ECLIPSE DATA SPACE FRAMEWORK

The concept of data spaces originated several years ago, setting the basis for a domain-agnostic perspective for data handling. The DSSC blueprint defines a data space as "a distributed system defined by a governance framework, that enables trustworthy data transactions among participants, while supporting trust and data sovereignty. A data space is implemented by one or more infrastructures and supports one or more use cases".

This concept sets a move from the web 2.0, where organizations establish silos to acquire and process data, namely through a wide usage of services supported by cloud service providers, where standalone governance rules apply; to the proposed web 3.0 concept where decentralized yet coordinated data governance schemes allow organizations to retain control of their data while promoting data sharing, value extraction and economic growth. This is the basis for a Digital European Single Market, where data spaces are set as the cornerstone for data decentralization and federation, encouraging data sharing among well-established data producers and consumers. This framework envisions data usage to be controlled regarding who, when and for which purpose data can be used, i.e., ensuring data sovereignty, thus supporting a robust and collaborative ecosystem guided by law, regulations, and data usage directives.

This supporting concept leverages three key features, that are embodied in the technologies that support data space deployments, namely: a) security and privacy, b) quality and integrity and c) policy and governance.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

The roll out of a data space is carried out through five main dimensions, extending the previous key features, namely [86]:

- **Business:** studying the business model, particularly the incentives around data exchange of domain-specific data.
- **Legal:** enclosing and evolving the necessary legal frameworks, organizational arrangement, and contractual instruments.
- **Operational:** considering use-cases, requirements, processes, and activities.
- **Functional:** detailing the technical and governance building blocks that embody the needed technical services, their dependencies and ultimately the data standards and interoperability frameworks.
- **Technology:** Offering specifications on adopted standards or required software components, as identified in the energy domain through the SGAM. A primary objective is to ensure interoperability among internal parties and with other data spaces.

Current data space proposals provide an open data concept based on the sparse exchange and copy of data, enabled through syntactic interoperability smart data models, with introductory support for semantic interoperability approaches. Moreover, at most, processes to negotiate digital contracts that unlock access to digital assets (e.g., documents) are automated on data space connectors.

THE ECOSYSTEM

The Eclipse Dataspace ecosystem provides a modular, standards-based framework that enables organizations to securely share, discover, and govern data across various ecosystems. Its architecture is built around interconnected components designed to work together, ensuring data exchanges are trustworthy, compliant, and efficient. The core components of this framework are:

Data Space Connector (DSC): The Data Space Connector is the core component of the ecosystem, acting as the primary interface for both data providers and consumers. It manages secure communication channels, handles data transfer, and enforces access policies. The connector authenticates users and systems through decentralized identifiers and manages interactions via standardized protocols such as REST and MQTT. Its role is to facilitate seamless, policy-driven, and secure exchanges of data assets.

Metadata Catalog / Discovery Service: This component functions as a registry that holds metadata describing available data assets within a data space. It enables data providers to publish descriptions of their data, making it discoverable to potential consumers. By standardizing metadata formats and supporting indexing, it ensures that data assets are easily searchable, well-described, and positioned for seamless integration and reuse.

Policy & Rights Management: In a trustworthy data ecosystem, governance is paramount. This component enforces data usage policies, licensing restrictions, and access rights, embedding these rules directly into data sharing agreements. By leveraging standards like the Object Description Registry Language (ODRL) or IDS policies, it guarantees that data consumers adhere to the conditions specified by data providers, ensuring compliance with legal and organizational policies.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Identity & Credential Management: Trust between parties is established and maintained through this component, which manages decentralized identities using DIDs (Decentralized Identifiers) and issues verifiable credentials. It authenticates entities participating in data sharing, verifying their identities and rights. This setup not only ensures secure access but also fosters a foundation of trust necessary for sensitive or regulated data exchanges.

Data Transfer & Data Plane: The data plane manages the actual transportation of data between systems. It supports various protocols such as HTTPS, MQTT, and FTP, selecting the appropriate method based on the data transfer requirements. This component ensures data is transmitted securely, reliably, and efficiently, often employing encryption and transfer monitoring to provide assurances for data integrity and privacy.

Negotiation & Contract Management: Before data exchange occurs, parties often need to negotiate terms and establish binding agreements. This component manages the negotiation process, allowing data providers and consumers to agree upon access rights and policies. It manages digital contracts, handles signatures, and enforces the conditions stipulated in those agreements throughout the data sharing lifecycle, typically following standards like IDS Contract Negotiation protocols.

Event & Audit Logging: Transparency and accountability are critical in data ecosystems. This component continuously records all relevant events—such as data access, transfer, policy enforcement, and agreement breaches—in comprehensive logs. These audit trails provide traceability, facilitate compliance with regulations, and enable organizations to monitor data usage, detect anomalies, and conduct audits when necessary.

This section will focus primarily on the role of the Data Space connector and how it operates.

ECLIPSE DATA SPACE CONNECTOR

The EDC emerges as a pioneering framework designed to facilitate secure and interoperable data sharing across diverse ecosystems through a standardized architecture.

The EDC aligns with the Data Space paradigm—an emerging framework promoting data sovereignty, interoperability, and controlled data sharing across organizational boundaries. This overview explores the architecture of the EDC, the protocols that underpin its operation, and the essential roles played by the control plane and data plane in enabling efficient and secure data exchange.

The EDC aims to provide an open-source, modular, and extensible platform for connecting data providers and consumers—regardless of geographic or organizational boundaries—while maintaining strict control over data privacy and security. By adhering to standards such as the Trusted Connector and the IDS architecture, the EDC fosters interoperability in heterogeneous environments.

The overarching goal is to foster data sovereignty, enabling data owners to retain control over their datasets while allowing trusted parties to access data securely through well-defined protocols and exchange models.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

The EDC is designed to enable secure, interoperable data sharing within a flexible, modular architecture. Its core architecture distinguishes between two primary planes—the control plane and the data plane—each serving specific roles within the data exchange process. This separation facilitates robust policy enforcement, flexible data transfer mechanisms, and trustable interactions in open and distributed data ecosystems.

EDC CORE ARCHITECTURE

At a high level, the EDC architecture aligns with the International IDS framework [15], which emphasizes trust, interoperability, and sovereignty. EDC acts as a bridge implementing these principles, integrating with existing infrastructure in a plug-and-play fashion, supporting a wide variety of data exchange protocols and policies.

The core architecture is split into two core planes: the control plane and the data place. In a nutshell, the control plane establishes a clear separation in terms of resource advertising, resource discovery and setting clear data usage policies for other connectors and organisations to be able browse and acquire data from fellow data space connectors. The data plane is responsible to act as a data sink and middleware layer, establishing data tunnels with the control planes of other connectors and, with the policy access and smart contract fingerprints mediated by the control plane, allows actual data exchange in the data space.

The architecture emphasizes decoupling both pathways:

- The control plane prepares and authorizes data transfer by establishing contracts, policies, and trust relationships.
- Once negotiations succeed, the data plane executes secure, policy-compliant data transfer, often in parallel or immediately following the control plane's negotiations.

When Data space connectors are set and operating under a common data space, the following exchange flow is expected to occur when resources or data resources are exchanged:

Discovery: Data providers expose catalogues containing metadata about data assets.

- **Negotiation:** Consumers request access, negotiate policies, and establish secure communication channels.
- **Data Transfer:** Once agreements are in place, data is transferred through the data plane securely.
- **Usage & Monitoring:** Usage is tracked, and access can be revoked or modified as needed.

The next sections provide more detail on how the operation is handled at both planes. The main concept for each plane is that it can provide better extensibility when compared with previous technical implementations of data space connector abiding by the former data space protocol. Thus, the current base architecture with both planes favours extensibility, where new control planes can be developed and deployed for new policies and control checkpoints, or new data places can be developed and integrated to allow the link with new data sink technologies, new OSI Layer 2 or OSI layer 3 protocols.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

THE CONTROL PLANE

The control plane orchestrates all activities related to establishing, managing, and terminating data sharing agreements. It manages metadata, policies, participant credentials, and contractual arrangements, acting as the decision-making hub in the data exchange process. It abides by the DS Communication Protocol (IDS CP) [35]: The standard messaging protocol for control-plane actions like negotiation, metadata exchange, and agreement management.

The control plane is composed by several sub-modules, which are listed below:

- **Registry & Discovery Service:** Enables data providers and consumers to find each other, publish, and discover datasets by registering metadata. Additionally, it integrates with catalogues or marketplaces.
- **Contract Negotiation and Management:** Uses protocols (e.g., IDS Contract Negotiation Protocols [36] to manage the lifecycle of agreements, including establishing, updating, and terminating contracts.
- **Credential Management and Trust Establishment**: Verifies identities and manages cryptographic credentials, such as X.509 certificates, ensuring only trusted entities can engage in data exchange.
- **Policy Enforcement:** Ensures that data sharing complies with agreed policies, including access restrictions, usage rights, and audit requirements.

THE DATA PLANE

Upon the establishment of a contract via the control plane, the data plane assumes responsibility for the actual data transfer. This layer is designed to be protocol-agnostic, flexible, and optimized for high-performance data transmission according to the contractual terms. It considers several standards for data exchange, namely RESTful APIs over HTTP(S), MQTT, or other lightweight messaging protocols that facilitate the actual payload transmission in compliance with the control plane agreements.

The data plane is composed of several sub-modules, which are listed below:

- **Data Transfer Protocols**: Supports standard data transfer protocols (e.g., REST over HTTP, MQTT, WebSockets) to transfer datasets, streams, or messages.
- **Data Transformation & Enrichment:** Can include optional data processing steps like transformation, encryption, or compression during transit.
- **Monitoring & Logging:** Tracks data transfer status, performance, and compliance for audit and troubleshooting.

6.3. ARCHITECTURES AND INITIATIVES ALIGNMENT

The integration of Data Spaces and IoT (Internet of Things) in the European Union (EU) is guided by a comprehensive set of initiatives, frameworks, and reference architectures aimed at enabling interoperable, secure, and trustworthy data exchange across sectors and borders. These efforts are crucial for realizing the EU's vision of a digital single market and are tightly aligned with goals for sovereign data sharing, technological independence, and cross-domain innovation.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

6.3.1. EU Initiatives Supporting Data Spaces and IoT Integration

- **The European Data Strategy** is the cornerstone initiative driving the development of common European data spaces across various domains (e.g., health, mobility, manufacturing, energy). It emphasizes interoperability, data sovereignty, and secure access and reuse of industrial and personal data, which directly relates to IoT-generated data.
- **GAIA-X** is a European initiative to build a federated data infrastructure based on principles of openness, transparency, interoperability, and sovereignty. GAIA-X promotes federated services, including IoT data providers and consumers, and introduces a common framework for data exchange, identity, and compliance, making it a key enabler of IoT-data space integration. It aligns with the IDS (International Data Spaces) reference architecture model and supports integration of IoT edge data sources into trusted data sharing environments.
- **Digital Europe Programme & Data Space Support Centre (DSSC):** The Digital Europe Programme (DEP) supports the Data Space Support Centre, which is tasked with developing common building blocks and architectural models for data spaces. DSSC coordinates alignment between IoT data sources, edge/cloud computing, and data space frameworks, ensuring vertical and cross-sector interoperability.
- **Horizon Europe and H2020 Projects**: Numerous EU-funded projects under Horizon 2020 and Horizon Europe (see above related chapter) explore IoT integration in data spaces, focusing on semantic interoperability, standard APIs, and governance frameworks. These projects contribute architectural patterns, middleware components, and data-sharing governance models relevant for integrating IoT into cross-domain data ecosystems.

6.3.2. Architecture Models and Frameworks

- **International Data Spaces Reference Architecture Model (IDS-RAM):** IDS provides a comprehensive **architecture for data sovereignty, trust, and interoperability**, particularly aligned with **IoT integration** through components like:
  - **Connectors**: enabling secure, governed data exchange from IoT devices.
  - **Usage Control**: defining how IoT-generated data can be used for post-sharing.
  - **Metadata and Semantics**: to describe IoT data in a machine-readable, interoperable way.

IDS is widely adopted in GAIA-X, DSSC, and industry-specific data space implementations.

- **FIWARE Framework:** FIWARE is a modular open-source platform offering standardized APIs and **data** models for IoT and smart data integration. It supports context management, NGSI-LD interfaces, and semantic interoperability, allowing IoT data to flow into data spaces efficiently. Many EU initiatives (e.g., Data Space for Smart Cities, Smart AgriFood) use FIWARE to bridge IoT with data ecosystems.
- **Reference Architecture Model Industry 4.0 (RAMI 4.0):** While RAMI 4.0 is primarily industrial, it provides a multi-layered architecture that aligns physical devices (IoT) with digital data ecosystems, relevant to data space architectures. RAMI 4.0 complements IDS and GAIA-X by providing industrial IoT data integration perspectives, including asset administration shells (AAS) for metadata management.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- **Open DEI Reference Architecture:** OPEN DEI aims to harmonize digital platforms in agriculture, energy, manufacturing, and health, aligning with data space and IoT goals. It promotes a federated reference architecture integrating edge, cloud, and data sharing layers, emphasizing standard interfaces and semantic alignment for IoT devices.

6.3.3. Key Alignment Areas

TABLE 21 - EU INITIATIVES ALIGNMENT

Dimension	Description
Interoperability	EU frameworks promote semantic, syntactic, and technical interoperability between IoT platforms and data space services via standardized ontologies, protocols (e.g., NGSI-LD, MQTT), and connectors.
Data Sovereignty	IDS and GAIA-X enable policy-based control over how IoT data is shared, accessed, and used, supporting legal compliance and trust.
Federated Architecture	EU models advocate distributed yet connected infrastructures where IoT devices at the edge integrate into cloud-based data spaces via federated nodes and gateways.
Security and Trust	Architecture models include identity management, data usage policies, and compliance monitoring, all vital for secure IoT data exchange.
Open Standards	EU Initiatives support open APIs and standardized data models, facilitating easy integration of heterogeneous IoT devices into EU data spaces.

6.4. IOT-EDGE NODES

The HEDGE-IoT IoT-edge nodes include the IoT and edge devices from each pilot that interact with the HEDGE-IoT ecosystem. The nodes are mainly where the data is collected from physical assets in the energy grid but also include services that run on the edge. The nodes and their data can be connected with other functionalities and services that are part of other layers of the HEDGE-IoT architecture such as the dataspace and middleware layers. In this section, the node from each pilot is presented, describing the assets deployed at the edge and their connection with the pilot's objectives and main functionalities.

FINNISH PILOT

The IoT-edge node from the Finnish pilot includes the part of the substation infrastructure that will be used in the demonstration, including IEDs and RTUs, as well as smart meters, edge server and data storages. Data from IEDs, other sensors and IoT devices will be processed in the edge server. Using this data, the functionalities of anomaly detection and fault forecasting will be performed in the edge server aiming to increase the network resilience.

GREEK PILOT

The Greek pilot IoT-edge node includes submetering IoT devices and smart meters, LV nodes and DERs, such as residential PVs, batteries, EVs and EV chargers. Real-time data will be gathered from the IoT devices, DERs and databases and sent to the aggregator. Smart building and flexibility modelling AI-based tools will be deployed on both the edge and the cloud. All gathered and

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

aggregated data will be used for demand and production forecasting with the objective of identifying possible grid issues and aid in the grid management and calculation of grid flexibility.

ITALIAN PILOT

The Italian pilot assets and functionalities part of its IoT-edge node include grid measurement assets (IoT sensors and IEDs installed on lines and substations), behind the meter assets and IoT weather stations. The pilot's IoT platform is also related to the node and handles the connection of the IoT resources and makes the data available to other systems. The DERs measurements from the behind the meter assets, metering data, sensor readings and weather data will be used to manage energy communities. The data collected from the edge will be used as an input to forecast the grid behaviour (load and production forecast), which can be used for grid congestion computing.

DUTCH PILOT

The Dutch pilot's assets at the edge that composes its IoT-edge node are metering devices at the DSO infrastructure, submetering IoT devices and DERs (PVs, batteries, heat pumps, EVs and EV chargers). The interoperability layer used to achieve semantic interoperability will also be moved to edge. AI-based tools for smart building and flexibility modelling will be deployed both on the edge and on the cloud. The IoT devices and sensors provide data to be monitored and integrated into the interoperability layer which can then be integrated into EMS and BMS systems to enhance control and explainability. This information will be used to optimize energy consumption and production, and in the flexibility alignment system at the pilot's business park.

PORTUGUESE PILOT

The IoT-edge node from the Portuguese pilot includes smart meters, energy assets, heat pumps, HVAC and batteries. Data from different assets of commercial buildings, such as HVAC, cooling system and batteries, will be integrated via a controller, which also exposes the data to the cloud. This data will be used to feed forecasting models and calculate optimal dispatch. Flexible assets from energy communities will be connected to a digital platform and used for the exploitation of energy flexibility.

SLOVENIAN PILOT

In the Slovenian pilot, edge devices used for Dynamic Thermal Rating (DTR) and Dynamic Line Rating (DLR), power quality meters, weather stations and temperature sensors are part of its IoT-edge node. Data from weather stations and from smart meters will be used to calculate DTR and DLR on the edge devices. The result of the edge calculations will be sent to the cloud and used with the objective to maximise asset capacity and increase the lifetime of DSO and TSO equipment. The gathered IoT data and output from DTR and DLR calculations will also be send to a semantic model of the substation and used in ML solutions to enhance the planning and operation of distribution networks.

6.5. SGAM ADAPTATION OF HEDGE-IOT REFERENCE ARCHITECTURE

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Figure 48 depicts an evolved approach to the HEDGE-IoT reference architecture, taking into consideration the SGAM model based on the specific project needs and expectations. The HEDGE-IoT approach extends the normal SGAM structure with vertical pillars, containing aspects that are relevant across all the horizontal layers. The current deliverable details which other initiatives and architectures will be considered, and how their ideas will be included in the design of this RA, along with the specific needs of the project at the time. In more detail:

- **The Business Layer** includes the Associations, the Business roles (categories of entities involved in the electricity domain, and the Business processes (which represent the high-level activities that these roles might engage in, like service registration, operational data management, etc.)

- **The Function Layer** includes the Functional processes which automate business processes through the HEDGE-IoT software components.

- **The Information Layer** includes Information Models (standards or frameworks for structuring and modelling data) and the Profiles Data models (HEDGE-IoT Semantic Ontologies that fit into the above-mentioned standards).

- **The Communication Layer** includes the Data formats (i.e., the actual formats in which data might be represented) and the Protocols (i.e., communication standards or protocols used for data transfer, such as HTTP/HTTPS, REST, MQTT, etc.).

- Finally, the **Component Layer** includes the Data Exchange Platforms (this likely refers to platforms designed to handle and exchange data, integrating the above layers) the Applications (software or platforms used to control, monitor, and manage the electricity domain processes and data) and the Hardware (physical devices and tools used in the electricity domain, like smart meters, batteries, SCADA systems, sensors, actuators, etc.).

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

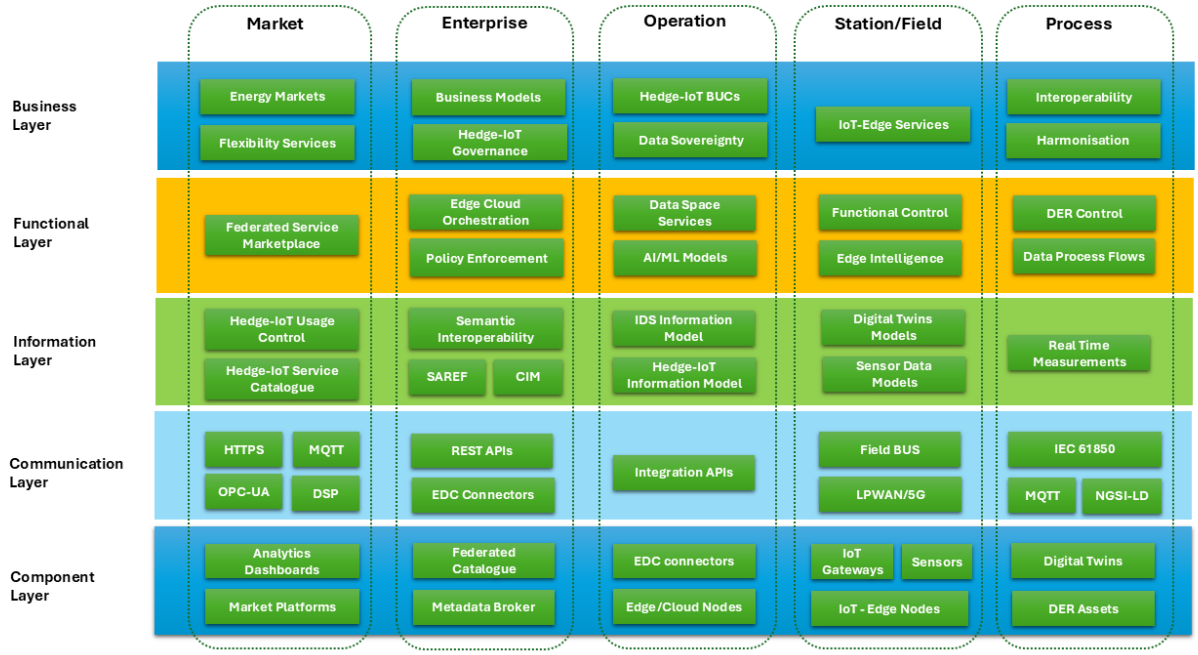

FIGURE 48 - SGAM ADAPTATION OF HEDGE-IOT REFERENCE ARCHITECTURE

6.6. BRIDGE DERA MAPPING OF HEDGE-IOT REFERENCE ARCHITECTURE

The European Energy Data Exchange Reference Architecture (DERA) [49] is a framework developed by the BRIDGE Data Management Working Group to guide the development of interoperable and flexible data exchange systems across the European energy sector. This architecture supports the vision of a common European energy data space, promoting seamless communication, data sharing, and cross-sector collaboration [37]. DERA 3.1 [37] is built on the foundation of earlier DERA versions and aligns with broader European initiatives like Gaia-X and IDSA. It integrates technical structures from the SGAM and adds data governance layer to SGAM's interoperability layers. DERA emphasises data governance, security, interoperability, and user empowerment.

The HEDGE-IoT RA aligns well with DERA's five interoperability layers including component, communication, information, function and business. The following table maps between DERA and HEDGE-IoT RA:

TABLE 22 – DERA MAPPING OF HEDGE-IOT RA WITH RESPECT TO INTEROPERABILITY LAYERS OF SGAM

SGAM Interoperability layers	HEDGE-IoT component	Alignment	Specific notes from DERA
Component	IoT-Edge Services, Sensors	Corresponds to physical data sources and platforms producing data, Data endpoints. DERA clearly separates local	DERA does not include physical components producing data and the ICT infrastructure for enabling its processing

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

		data platforms from federated part. The federated part should just index the local data sets, but never persists them.	and transfer like originally aimed in the SGAM. Local data platforms should take care of data consent and anonymisation or aggregation.
Communication	Rest API, Connector GUI, Cybersecurity layer	Both emphasize protocol and data format agnostic, secure data transfer. REST API aligns with standardised and open protocols in DERA.	The protocol selected should ensure the highest levels of cybersecurity needed for keeping those data sets sovereign and confidential, if applicable.
Information	Data Management, Semantic Interoperability, Context Management	Maps to data harmonisation, vocabulary providers, and semantic interoperability in DERA.	Local data platforms participate by data processing and persistence Establish and maintain a common reference semantic data model and profiles based on existing harmonised data models. Identified open and standardised protocols and data models: IEC CIM, IEC 61850, OCPP, SAREF, OpenADR, COSEM
Function	Orchestrator	Matches DERA's data indexing, discovery, and processing services	
Business	App Store, App Metadata, Service Catalogue, Energy Stakeholders	The app store and service catalogue match the Marketplace frontend/backend in DERA. Stakeholders align with actors and roles.	DERA highlights the Harmonised electricity market role model

DETAILS OF DERA MAPPING TO SGAM INTEROPERABILITY LAYERS

Information layer

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Local data platforms participate by data processing and persistence (local data storage for own and incoming data from dataspace), including functionalities related to data security, data quality, data governance, etc. They make sure to keep data sovereignty and to provide access control to assure confidentiality defined in potential non-disclosure clauses. Therefore, the cybersecurity requirements should be expanded to local data platforms as well. DERA includes also data harmonisation services, which ensure that the sharing format and semantics are appropriate. Data persistence includes also possibilities to control "Data Value", i.e. link it to Data Usage Accounting module at Function layer.

Beyond one project or pilot case, the energy domain should establish and maintain a common reference semantic data model and profiles based on existing harmonized data models. Some harmonised data models already exist like the harmonization of IEC CIM and IEC 61850. However, completely harmonised and ready models do not exist. Models need to be extended, like IEC CIM gets annual modifications. Therefore, ontologies are important. IEC 63417 "Guide and plan to develop smart energy ontologies" is proposing some recommendations to support semantic interoperability. DERA has identified the following open and standardised protocols and data models: IEC CIM, IEC 61850, OCPP, SAREF, OpenADR, and COSEM.

Function layer

DERA highlights to define and harmonise functional data processes. Harmonisation efforts should encompass vocabulary provider, federated catalogue, data quality, data accounting processes, clearing process (audit, logging, etc.), and data tracking and provenance to ensure seamless interoperability and efficient data management across sectors. The utilisation of reference architecture (e.g. HEDGE-IoT interoperability platform) should be described as system use cases.

DERA highlights the duality of data governance between local data platforms and dataspace participants. At the local side the credential manager allows the identification of that data platform as such to open the door for data indexing. The identity manager is located at federated dataspace level to check identities of federated nodes when interacting with federated services. DERA highlights as well that the identification mechanism should be aligned at EU level to progress towards the EU data single market.

Data discovery is organised via data indexer and data discovery modules. Data indexer at local data platform side enables the data to be discoverable. It is based on data harmonisation defined at Information layer to utilise understandable data format and semantics. Data indexing is based on self-descriptive metadata. Data discovery should collect the metadata provided by the local data platforms, incorporate them into data catalogue, and incorporate an engine to discover datasets in the catalogue. All this needs to follow the access policies defined for the data.

Monitoring and orchestration module is utilized to make sure that the system is functioning and performing as expected. Monitoring should provide transparency to the dataspace data and services offered to marketplace and discoverable via discovery module. In addition to security and interoperability requirements, the monitoring should be able to trace all data transactions to record evidence providing the alignment of providers/users and transactions. The orchestration should allow users to instantiate and manage potential infrastructure services.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Marketplace backend module connects users to available data and services. Marketplace includes both the AppStore and the Software-as-a-Service (SaaS). Functionalities needed for the marketplace backend are monetisation engine, contracting module, clearing house and potential additional functionalities.

COMPARISON OF HEDGE-IOT RA AND DERA

Beyond direct layer-to-layer mapping of SGAM, DERA and HEDGE-IoT RA also align through several broader architectural patterns that span multiple layers. These cross-cutting themes highlight shared priorities in enabling interoperable, scalable, and secure energy data ecosystems.

Federated architecture and data sovereignty

Both RAs adopt a federated model, where local platforms maintain control over data while enabling cross-border exchange. DERA uses Data Space Connectors; HEDGE-IoT includes European Data Connectors (e.g., Eclipse data space connector) and decentralised orchestration — supporting sovereignty and secure data sharing.

Semantic interoperability

Both RAs emphasize semantic consistency using shared vocabularies and ontologies (e.g., CIM, SAREF). This ensures that data retains its meaning across systems, enabling harmonized discovery, indexing, and integration.

Cloud-edge integration

Both RAs support hybrid environments, combining edge devices performing local processes, and cloud computing. This flexibility enables efficient, real-time analytics and scalable service deployment across infrastructures.

Marketplace

Each architecture features marketplace components to publish, discover, and manage data and services. DERA has Marketplace Frontend/Backend; HEDGE-IoT includes an App Store and Service Catalogue — both enabling business-driven data exchange and third-party innovation.

Differences between DERA and HEDGE-IoT's RA

While DERA and the HEDGE-IoT RA align structurally across interoperability and governance layers, they differ in focus and design orientation. DERA, developed under the BRIDGE initiative with influence from the OneNet project, reflects a top-down approach, prioritising standardisation, interoperability, and regulatory compliance across the European energy sector. HEDGE-IoT RA has emerged from a technology-driven, pilot-oriented context, where architectural flexibility is essential so that it could be used in different pilots within HEDGE-IoT project. Its emphasis on edge/cloud computing, HPC orchestration, and real-time decision-making supports dynamic applications like congestion management and market participation at the edge. These requirements have led to a more prominent role for local computational intelligence and distributed orchestration in HEDGE-IoT's RA, whereas DERA's architecture is more concerned with ensuring semantic alignment, cross-sector data portability, and compliance with European digital policies.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

This highlights DERA's role as a policy-anchored reference for system-wide interoperability, while HEDGE-IoT serves as blueprint optimized for operational experimentation focused on HEDGE-IoT objectives.

DERA as such start from high-level aims and requirements defined in 2019/944 Electricity Market Directive [38] and European Commission COM(2022)552, Digitalising the energy system – EU action plan [39]. Requirements related to data privacy, security/resilience, and interoperability are therefore highlighted.

6.7. HEDGE-IOT REFERENCE ARCHITECTURE

This section outlines the evolution of the HEDGE-IoT Reference Architecture across three major iterations, reflecting an increasing level of sophistication and alignment with the objectives of WP2. The architectural refinements demonstrate a clear shift toward modularity, interoperability, and secure data sovereignty in federated IoT ecosystems.

HEDGE-IOT RA (1ST RELEASE) - CONCEPTUAL MODEL

The initial conceptual version of the HEDGE-IoT Reference Architecture (Figure 49) was designed around three main layers and a set of horizontal concerns. The goal was to define a foundational blueprint to orchestrate the IoT-Edge services across diverse domains.

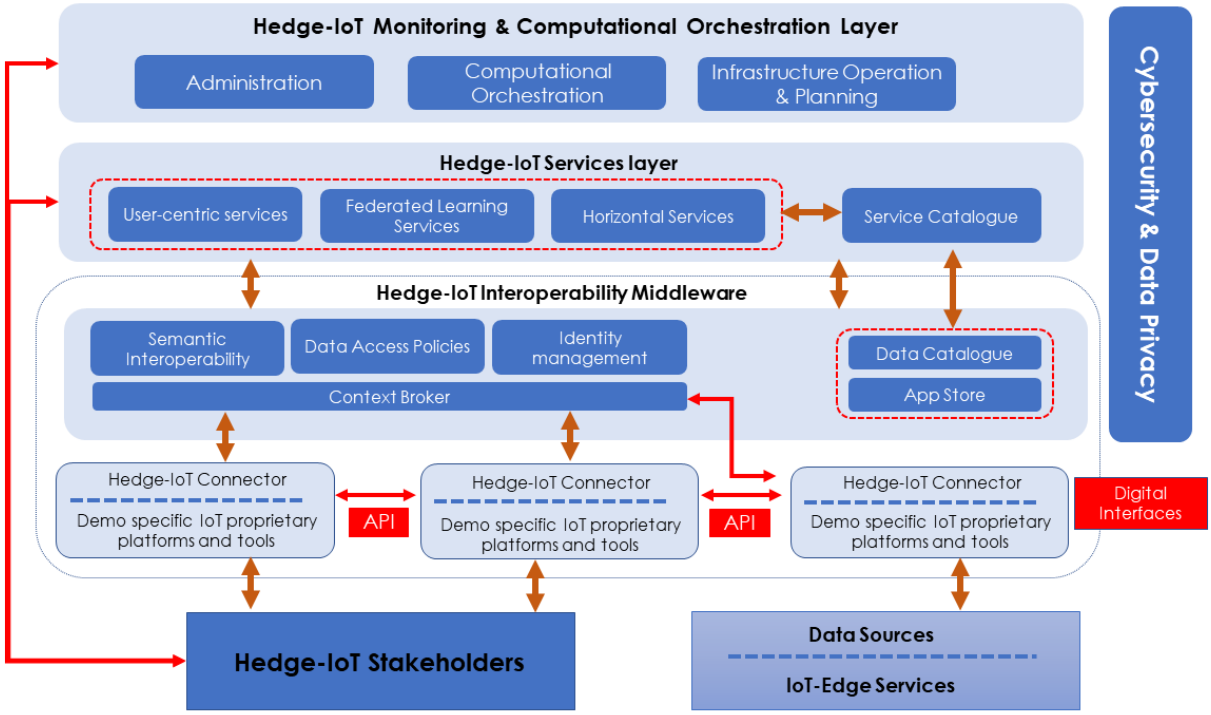

FIGURE 49 - HEDGE-IOT REFERENCE ARCHITECTURE (1ST RELEASE) - CONCEPT MODEL

1. **HEDGE-IoT Monitoring & Computational Orchestration Layer –** This top layer is responsible for system-wide oversight, orchestration, and infrastructure lifecycle management:

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- Included modules for administration, computational orchestration, and infrastructure operation & planning.
- Enabled dynamic workload orchestration across cloud/edge environments.
- Aimed to manage system performance and scalability.

2. **HEDGE-IoT Services Layer –** This layer provides various interoperable services available to stakeholders and applications:
   - Comprised user-centric services, federated learning services, and horizontal services.
   - Centralised in a service catalogue for discoverability.
   - Provided reusable, interoperable functionalities across domains.

3. **HEDGE-IoT Interoperability Middleware –** The core enabling layer for seamless integration and communication between heterogeneous systems and services:
   - Contained essential interoperability tools including:
     - Semantic interoperability, data access policies, and identity management.
     - A context broker for real-time data updates.
     - A data catalogue and app store for data and applications.
   - The initial inclusion of the HEDGE-IoT Connector, bridged the internal HEDGE-IoT architecture with external, proprietary IoT platforms.
     - It provided standardised APIs and digital interfaces to enable seamless integration between the core platform and various demo-specific or vendor-specific systems.
     - These connectors played a key role in facilitating interoperability with real-world deployments, ensuring that external data sources and services could be integrated efficiently and securely.

Additionally, cybersecurity and data privacy were addressed as horizontal concerns across the architecture. The design emphasised compliance, employed role-based access controls, and established secure communication channels to protect sensitive data as it moved through the system.

However, this conceptual version remained high-level and abstract. While it offered clear structural separation and introduced key integration components, it lacked the necessary implementation details required for practical deployment. Notably, it did not yet define the mechanisms for governance, dataspace operations, or integration with EDC Connectors.

HEDGE-IOT RA (1ST RELEASE) - INTERMEDIATE VERSION

The intermediate version (Figure 50) evolved toward a more implementation-oriented model, bridging the conceptual framework with emerging WP3 Services, WP4 Components and WP2 requirements coming from WP5 pilot demonstrations from the project. This version of the HEDGE-IoT RA is structured into four main layers, each with specific functionalities and components. Below is a detailed breakdown of each layer and its key features:

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

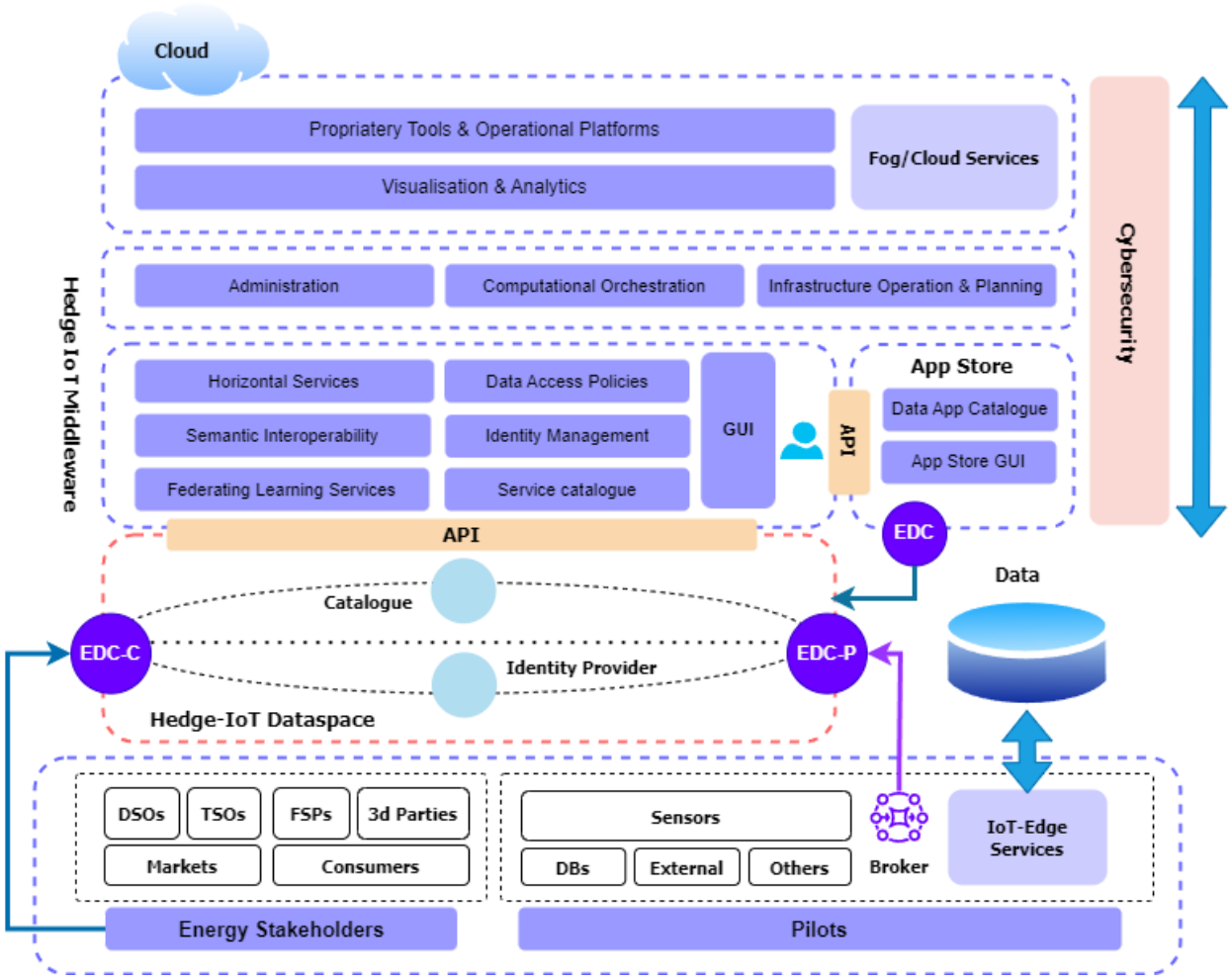

FIGURE 50 – HEDGE-IOT REFERENCE ARCHITECTURE (1ST RELEASE) - INTERMEDIATE VERSION

1. **Middleware Layer -** This is the core integration and orchestration layer that interconnects services, data sources, cloud platforms
   - Centralised integration layer for all interoperability, orchestration, and user access control.
   - App Store was Developed as a modular component with:
     - Catalogue of data-driven applications.
     - API-based integration to both the middleware and dataspace.
     - Introduced App Store GUI interfaces and APIs for improved usability.
     - EDC to support data exchange functions and coordinate with the dataspace.
   - Included Horizontal Services and Federated Learning Services as part of middleware and removed context Broker.
   - Introduced GUI and API for better interactions with Dataspace Layer and App Store.
   - Absorbed The Service Layer from the previous version.

2. **Services Layer**
   - Clearly defined integration points with external tools for visualisation, analytics, and proprietary tools and operational platforms.

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- Introduced Fog/Cloud Services grounded in the actual capabilities and needs identified from pilot implementations.
- Enhanced discoverability and reusability of services through separation and refinement of the Service Catalogue.

3. **HEDGE-IoT Dataspace Layer**
   - Integrated the Eclipse Dataspace Connector (EDC) framework to manage federated data exchange.
     - EDC-P for data providers (e.g., pilot data, external sensors).
     - EDC-C for data consumers (e.g., 3rd party external stakeholders).
   - Defined the Catalogue in the dataspace, responsible for metadata publication and service/data discoverability.
   - Defined the Identity Provider, ensuring secure, policy-compliant access across domains.

4. **Stakeholders / External Interfaces Layer**
   - Recognised and categorised DSOs, TSOs, FSPs, 3rd parties, Markets and Data Consumers and pilot operators as key stakeholders in the HEDGE-IoT ecosystem.
   - Mapped data flows from IoT devices, external databases, and SCADA-like systems through brokers into the dataspace as using an EDC-P.
   - Separated the Service Catalogue and highlighted its interactions with real-time IoT services originating from pilots and other data sources.

The intermediate architecture significantly improved upon the initial conceptual design by operationalising core concepts and bridging them with real-world implementations. It enabled seamless integration of pilot infrastructures and applications, demonstrating how field-deployed systems could interact with the dataspace using standardised connectors. By clearly separating identity management, service and data catalogues, and App Store functions, it illustrated the convergence of discovery, security, and service orchestration.

HEDGE-IOT RA (1ST RELEASE) -FINAL VERSION

The final architecture version is organized into multiple hierarchical layers, each responsible for different functions within an IoT-Edge to Cloud ecosystem. The system ensures secure, interoperable, and flexible orchestration and data handling across stakeholders. Below, we analyse the different aspects (layers) of the proposed architecture.

1. **HEDGE-IoT Application Layer:** Provides interfaces and tools for end-users and operational systems to interact with the platform. It consists of:
   - **Proprietary Tools & Operational Platforms:** Custom tools and operational platforms which are interfacing with the system.
   - **Fog/Cloud Services:** All the hosted services, of the above proprietary tools and operational platforms which have high computational, and storage demands.
   - **REST API:** Gateway for communication between application layer and middleware layer.
   - Visualisation & Analytics: Front-end tools for insights.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- **Data Management:** This module is responsible for any structured storage handling, access and lifecycle data management.

2. **HEDGE-IoT Governance Middleware Layer:** The proposed middleware layer will ensure security, trust, interoperability (governance), policy enforcement, and coordination. It consists of:
   - **Service Catalogue:** This is the central service repository of available services and their associated data (attributes). All data offerings will be aligned with the service catalogue.
   - **Semantic Interoperability:** It consists of all semantic interoperability enablers which will provide standardised meaning (through ontologies and vocabularies) across HEDGE-IoT diverse data sets.
   - **User Management:** The Identity Management and relevant services which will control access, authentication, and authorisation to resources (compliant with role-based access).
   - **Administration:** System-level management (configuration services).
   - **Context Management:** Manages context-aware metadata and will allow for discovery and provide any publishing/subscribe mechanisms if required.
   - **Data Access Policies:** This sub module will be responsible for the definition of data sharing and access control rules (e.g. potential contract definition rules)
   - **Federated Learning:** Supports privacy-preserving distributed learning services.

3. **HEDGE-IoT Dataspace Layer:** The Data Space layer is responsible for all the core data sharing processes and will contain all functionality compliant with IDSA and EDC principles. Key interface of this functionality will be the Connector GUI as an entry point for stakeholders' Data Space operations. It consists of:
   - **App Store:** The HEDGE-IoT App Store is a secure platform responsible for the distribution of data apps. Data apps can be used to process or transform data before or after the actual data exchange takes place. Main sub-modules are i) the specialised GUI for basic interactions, ii) the Container Registry which will holds packaged applications, iii) the App Metadata storage where descriptive app data are registered, and iv) a complete Data App lifecycle management process where we can Register / Publish / Discover Data Apps. The App Store participates in the Data Space through integration with the EDC (Eclipse Data Space connector).
   - **Orchestrator:** This platform will be responsible for the HEDGE-IoT orchestration management with specialised GUI and functions such as workload scheduling, resource and topology management and obviously a persistent service storage data.
   - **Data Exchange Infrastructure:** It contains core Data Space components according to the Eclipse Data Space framework such as i) the Provided Data Catalogue with all registered EDC instances and data offerings, ii) the Identity Provider responsible for authentication & federated identities and iii) the actual EDC (Eclipse Data Space connector) instances, dedicated software components which can be considered secure gateways for HEDGE-IoT data transactions.

4. **Energy Stakeholders & Pilots Layer:** It consists of all Energy Stakeholders such as DSOs, TSOs, FSPs, Markets, Consumers etc. From architecture perspective it also refers to real-world pilot

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

environments (sensors, databases, IoT devices, platforms) which can be considered as data sources and at the same time provide IoT-Edge Services as localized services deployed at the edge for real-time response.

5. **Cybersecurity Layer:** This layer envelops all layers ensuring secure communication, identity, and access control (according to data privacy considerations and the HEDGE-IoT regulation framework)

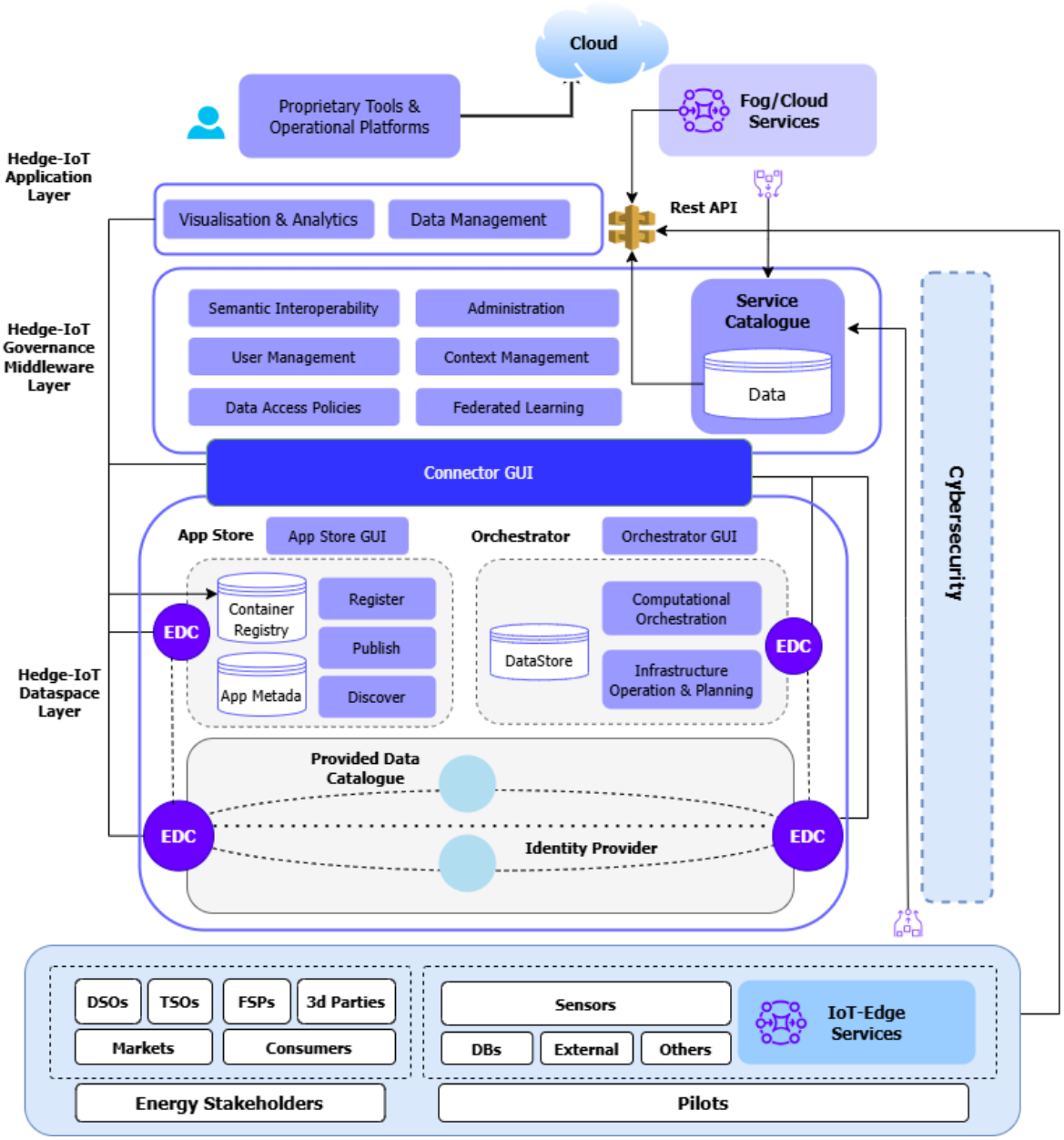

FIGURE 51 - HEDGE-IOT REFERENCE ARCHITECTURE (1ST RELEASE) - FINAL VERSION

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

7. DATASPACES CYBERSECURITY AND PRIVACY CONSIDERATIONS

This chapter aims to provide an overview of the main cybersecurity and privacy concepts and measures for dataspaces. IT is based on the input from Task 4.5 – Cybersecurity considerations and AI safety.

Ensuring robust privacy and security measures is paramount in the development and operation of data spaces. The International Data Spaces Association (IDSA) provides comprehensive guidelines and best practices to address these concerns, as detailed in the IDS-RAM [40].

7.1. SECURITY PERSPECTIVE IN IDS-RAM

Security is one of the three perspectives of IDS-RAM.

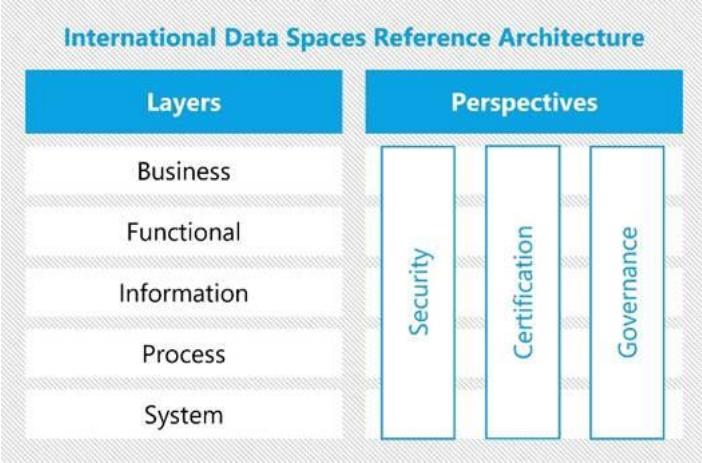

FIGURE 52 - OVERVIEW IDS REFERENCE ARCHITECTURE MODEL[40]

The IDS-RAM outlines a multi-faceted approach to security, emphasizing the following core areas:

IDENTITY AND TRUST MANAGEMENT

Establishing trust among participants is foundational. IDSA recommends implementing robust identity management systems that authenticate and authorize entities within the data space. This includes the use of trusted Identity Providers (IdPs) to issue and verify credentials, ensuring that only authorised participants can access or share data.

SECURING THE PLATFORM

The integrity and security of the data exchange platform are critical. This involves implementing measures such as:

- **TLS / E2E encryption:** Utilising Transport Layer Security (TLS) and end-to-end encryption to protect data in transit. While TLS is effective for data in transit, end-to-end encryption ensures that data remains confidential from the source to the destination, mitigating risks associated with intermediate service providers.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- **Obfuscation Techniques:** Adding random data or noise to existing records to obscure sensitive information, thereby reducing the risk of unauthorised data inference.

SECURING APPLICATIONS

Applications within the data space must adhere to security protocols to prevent vulnerabilities. This includes regular security assessments, implementing secure coding practices, and ensuring that applications do not introduce risks to the overall data space infrastructure.

SECURING INTERACTIONS BETWEEN IDS COMPONENTS

Securing interactions between IDS components is highly important to ensure the integrity, confidentiality, and trustworthiness of data exchanges within the International Data Spaces (IDS). Robust security measures, such as authentication, authorisation, encryption, and secure communication protocols, are implemented to safeguard data flows and prevent unauthorised access, tampering, or breaches. These mechanisms are critical for maintaining data sovereignty and fostering trust in a decentralised, multi-stakeholder environment where sensitive information is shared across diverse participants.

Identity Providers (IdPs) and Trust Anchors play a key role in verifying the identities of participants and components within the IDS ecosystem. Cryptographic techniques, including digital signatures and certificates, are utilised to authenticate data sources and ensure the integrity of transmitted information.

USAGE CONTROL

Securing data usage through usage control is a critical aspect of the International Data Spaces (IDS) framework, ensuring that data is handled in compliance with predefined policies and restrictions. Usage control mechanisms are implemented to enforce how data can be accessed, processed, and shared by authorised participants, thereby preventing misuse or unauthorized exploitation. This is particularly important in a decentralised environment where data sovereignty and compliance with legal or contractual obligations are paramount. By integrating usage control, the IDS framework ensures that data providers retain control over their data even after it has been shared, fostering trust and accountability among all stakeholders.

The IDS framework employs advanced techniques, such as policy enforcement points (PEPs) and policy decision points (PDPs), to dynamically monitor and regulate data usage in real-time. These mechanisms work in tandem with cryptographic methods and secure communication protocols to ensure that data usage adheres to the agreed-upon terms. This approach not only enhances data security but also supports compliance with regulatory requirements, such as GDPR, by providing transparent and auditable data usage trials. By prioritising usage control, the IDS framework enables secure and responsible data sharing, which is essential for building a trustworthy and sustainable data economy.

7.2. PRIVACY PERSPECTIVE IN IDS-RAM

Privacy protection is integral to the IDS framework, with several strategies highlighted:

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

PSEUDONYMIZATION

Replacing identifiable information with pseudonyms to prevent the correlation of data with specific individuals, thereby enhancing privacy.

SECURE MULTIPARTY COMPUTATION

Utilising algorithms that allow computations on data without exposing individual data records, enabling collaborative data analysis while preserving privacy.

ZERO-KNOWLEDGE PROOFS

Implementing cryptographic methods that allow one party to prove knowledge of certain information without revealing the information itself, thus maintaining confidentiality.

8. FUTURE CONSIDERATIONS

The HEGDE-IoT project aims to deliver a scalable, secure, and intelligent architecture for managing heterogeneous IoT systems at the network edge. As IoT ecosystems continue to evolve, the reference architecture must not only address current requirements but also anticipate emerging trends and challenges. Below are key future considerations which will guide the next iterations of the HEDGE-IoT reference architecture:

1) Scalability and Hyper-Connectivity

- IoT device proliferation will continue at increased rates. The architecture (especially the final version) needs to accommodate a plethora of devices with varying communication protocols.
- Adaptive resource allocation in edge and fog layers is essential to maintain performance under dynamic loads.

2) AI-Driven Edge Intelligence

- HEDGE-IoT RA needs to consider the integration of AI and Machine Learning capabilities at the edge for low-latency analytics, anomaly detection, and predictive maintenance.
- The perceived development of standardized interfaces for Federated Learning will allow collaborative model training without compromising data privacy.

3) Human-Centric Design

- The final version of HEDGE-IoT RA needs to anticipate increasing demands for transparency, explainability, and control over how IoT systems behave and make decisions.
- It will also enable user-centric policies for data ownership, consent management, and privacy preservation.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

9. CONCLUSIONS

The objective of this Deliverable is to present the results achieved under Task 2.7 up to the time of writing, culminating in an initial version of the HEDGE-IoT Reference Architecture (RA). The goal was to ensure alignment with the project's defined components and requirements. By applying the '4+1' View Model and incorporating insights from the Business Use Cases, we integrated project-specific scenarios and requirements into a comprehensive RA that reflects the current stage of project development. This version of the RA includes several architectural models, notably integrated IoT-Edge and Data space frameworks, which serve to illustrate the user's entry point into the system and the design of communication interfaces. Additionally, it introduces a streamlined Middleware layer that aligns with the accompanying Interoperability specifications. These specifications provide detailed guidance on both the data interoperability layer and the Sovereignty and Trust layer of the RA. They outline how existing initiatives and frameworks—such as IDSA, GAIA-X, and AIOTI—can be integrated to support the HEDGE-IoT objectives.

One of the ongoing results of this RA is the development of a concrete 'development view', which maps HEDGE-IoT functional specifications to individual components that will be implemented accordingly. This builds directly on earlier outcomes and serves to reinforce the conceptual framework presented in this document, while aligning it with the project's current technical progress.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

REFERENCES

[1] ISO, "ISO/IEC/IEEE 42010:2022 -Software, systems and enterprise — Architecture description," [Online]. Available: https://www.iso.org/standard/74393.html

[2] P. B. Kruchten, "The 4+1 View Model of architecture," in IEEE Software, vol. 12, no. 6, pp. 42-50, Nov. 1995, doi: 10.1109/52.469759.

[3] European Commission: Directorate-General for Energy, "European (energy) data exchange reference architecture 3.0," Publications Office of the European Union, 2023, https://op.europa.eu/en/publication-detail/-/publication/dc073847-4d35-11ee-9220-01aa75ed71a1/language-en.

[4] CEN – CENELEC – ETSI: Smart Grid Coordination Group, Smart Grid Reference Architecture Report V2.0, 2012, https://www.researchgate.net/publication/263264218_CEN_-CENELEC_-_ETSI_Smart_Grid_Coordination_Group_-_Smart_Grid_Reference_Architecture_Report_20

[5] European Commission, "The European AI Alliance," Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance

[6] European Commission, "Ethics guidelines for trustworthy AI," Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai#:~:text=%2A%20Societal%20and%20environmental%20well,Moreover%2C%20adequate%20an%20accessible (accessed Jul. 01, 2025).

[7] European Commission, "Key actions for digitalising energy," Energy. https://energy.ec.europa.eu/topics/eus-energy-system/digitalisation-energy-system/key-actions-digitalising-energy_en#:~:text=,2024 (accessed Jul. 01, 2025).

[8] OneNET D5.2: "OneNet Reference Architecture" [Online] Available: https://onenet-project.eu/wp-content/uploads/2022/12/OneNet_D5.2_v1.0.pdf

[9] AIOTI – Alliance for AI, IoT and Edge Continuum Innovation. https://aioti.eu/

[10] Interconnect "D2.1 - Secure interoperable IoT smart home/building and smart energy system reference architecture," 2020. [Online] Available: https://interconnectproject.eu/wp-content/uploads/2022/03/D2.1-Secure-Interoperable-Smart-Home-Building-and-Smart-Energy-System-Reference-Architecture_FR_v2.pdf

[11] O. Vermesan, "Advancing IoT Platforms Interoperability," June 2018, [Online]. Available: doi: https://doi.org/10.13052/rp-9788770220057

[12] International Data Spaces Association, "Home - International Data Spaces," International Data Spaces, Jun. 21, 2025. https://internationaldataspaces.org/

[13] European Commission, "New European Interoperability Framework: Promoting seamless services and data flows for European public administrations," Luxembourg: Publications Office of the European Union, 2017. doi: 10.2799/78681 E. Union, "New European Interoperability Framework (EIF) – Promoting seamless services and data flows for European public administrations," 2017. [Online]. Available: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf.

[14] Giussani G., Steinbuss S., Data Connector Report, International Data Spaces Association, (6), 2024 https://doi.org/10.5281/zenodo.13838396

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

[15]B. Otto, S. Steinbuß, A. Teuscher, and S. Lohmann, "REFERENCE ARCHITECTURE MODEL: Version 3.0," International Data Spaces Association, Apr. 2019. [Online]. Available: https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf

[16]Bader, S., et. al." The International Data Spaces Information Model – An Ontology for Sovereign Exchange of Digital content", 2020, https://doi.org/10.1007/978-3-030-62466-8_12

[17]"Task forces Archive - BDV Big Data Value Association," BDV Big Data Value Association. https://bdva.eu/task-forces/ "BDVA | Task Forces," [Online]. Available: https://bdva.eu/task-forces/.

[18]Gaia-X European Association for Data and Cloud AISBL, "GAIA-X Framework - GAIA-X: a federated Secure data infrastructure," Gaia-X: A Federated Secure Data Infrastructure -, Mar. 24, 2023. GAIA-X Framework," [Online]. Available: https://gaia-x.eu/gaia-x-framework/.

[19]GAIA-X, "Policy Rules Document," Apr. 2022. [Online]. Available: https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X_Policy-Rules_Document_v22.04_Final.pdf

[20] GAIA-X, "Architecture Document," Apr. 2022. [Online]. Available: https://gaia-x.eu/wp-content/uploads/2022/06/Gaia-x-Architecture-Document-22.04-Release.pdf

[21] ATTEST, "ATTEST - home," Attest Project, Nov. 03, 2023. https://attest-project.eu/

[22] ATTEST "D2.2: Toolbox Specifications," 2020, [Online]. Available: https://attest-project.eu/wp-content/uploads/Attachment_0-4-1.pdf

[23] Enershare "D4.3: ENERSHARE Trust and sovereignty building blocks,", 2022 [Online]. Available: https://enershare.eu/wp-content/deliverables/wp4/Enershare_D4.3_Trust%20and%20sovereignty%20building%20blocks%20%28Final%20version%29%20v1.0.pdf

[24] I-NERGY "D2.5: Section 2.2: I-NERGY Platform: Architecture" 2022, [Onine] Availbale: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f47f03f5&appId=PPGMS

[25] I-NERGY "D2.5: I-NERGY Architecture and I-NERGY–AI4EU Synergies, Section 2.2.1: An I-NERGY – AIoD Interconnection layer which leverages Open APIs. 2022, [Onine] Availbale: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f47f03f5&appId=PPGMS

[26] I-NERGY "D2.5: I-NERGY Architecture and I-NERGY–AI4EU Synergies, Section 2.2.2: Data Services Layer", (p. 19)", 2022, [Online] Available at: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f47f03f5&appId=PPGMS

[27] I-NERGY "D2.5: I-NERGY Architecture and I-NERGY–AI4EU Synergies, Section 2.2.3: AI Trained Models Layer", (p. 19)", 2022, [Online] Available at: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f47f03f5&appId=PPGMS

[28] I-NERGY "D2.5: I-NERGY Architecture and I-NERGY–AI4EU Synergies, Section 2.2.4: Application Layer – Energy Analytics Applications" (p. 22)", 2022, [Onine] Availbale: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f47f03f5&appId=PPGMS

[29] I-NERGY "D2.5: I-NERGY Architecture and I-NERGY–AI4EU Synergies, Section 2.2.5: Marketplace. " (p. 27)" , 2022, [Online] Availbale:

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f47f03f5&appId=PPGMS

[30] OneNET D5.2: "OneNet Reference Architecture" [Online] Available: https://onenet-project.eu/wp-content/uploads/2022/12/OneNet_D5.2_v1.0.pdf

[31]"RESONANCE "D2.1: Initial Requirements and Common System Architecture," 2023, [Online] Available: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5fb270ea8&appId=PPGMS

[32] European Committee for Standardization and European Committee for Electrotechnical Standardization, "Final Report of the Working Group Clean Energy Package (WG-CEP): SEG-CG Report," CENCLCETSI_SEG-CG/Sec/00115/DC, Nov. 2019. [Online]. Available: https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Smart%20Grids%20and%20Meters/Smart%20Grids/finalreportwg-cep_2019.pdf

[33] European Commission, "New European Interoperability Framework: Promoting seamless services and data flows for European public administrations," Luxembourg: Publications Office of the European Union, 2017. doi: 10.2799/78681

[34] International Electrotechnical Commission, "IEC 61850-10: Communication networks and systems for power utility automation – Part 10: Conformance testing," IEC, 2012. [Online]. Available: https://cdn.standards.iteh.ai/samples/19390/3d6fba45956042019454324b4ded03a0/IEC-61850-10-2012.pdf

[35] International Data Spaces Association, "IDS Communication Protocol Version 2 (IDSCP2)," 2024. [Online]. Available: https://docs.internationaldataspaces.org/ids-knowledgebase/ids-g/communication/protocols/idscp2 . [Accessed 25 June 2025].

[36] International Data Spaces Association, "3.4.3 Contract Negotiation | IDS Knowledge base," IDS Knowledge Base. https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3_4_process_layer/3_4_3_contract_negotiation . [Accessed 25 June 2025].

[37] M. Couto, "BRIDGE - European (Energy) Data Exchange Reference Architecture 3.1," European Commission, Data Management Working Group, Oct. 2024. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/6c3b1add-a0a7-11ef-85f0-01aa75ed71a1#

[38] E. Union, "DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU," [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593158348328&uri=CELEX:32019L0944.

[39] European Union, "DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," Official Journal of the European Union, 2019, [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593158348328&uri=CELEX:32019L0944

[40] International Data Spaces Association, "Perspectives of the Reference Architecture Model - Security Perspective," [Online]. Available: https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram-4/perspectives-of-the-reference-architecture-model/4_perspectives/4_1_security_perspective.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

[41] International Electrotechnical Commission, "IEC 62559-2: Use case methodology – Part 2: Definition of the templates for use cases, actor list and requirements list," IEC, Apr. 2015. [Online]. Available: https://cdn.standards.iteh.ai/samples/20300/c3c2f3905fd045cba1b81c615be6d3c3/IEC-62559-2-2015.pdf

[42] European Network of Transmission System Operators for Electricity, "The Harmonised Electricity Market Model," Nov. 2022. [Online]. Available: https://eepublicdownloads.entsoe.eu/clean-documents/EDI/Library/HRM/Harmonised_Role_Model_2022-01.pdf .

[43] INTEGRID, "Generic Non-Functional Requirements".

[44] International Data Spaces Association, "Dataspace Protocol 2024-1," [Online]. Available: https://docs.internationaldataspaces.org/ids-knowledgebase/v/dataspace-protocol.

[45] International Data Spaces Association, "Advancing interoperability: the Dataspace Protocol," [Online]. Available: https://internationaldataspaces.org/offers/dataspace-protocol-overview/.

[46] International Data Spaces Association, "App Store and App Ecosystem," [Online]. Available: https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3_5_0_system_layer/3_5_3_app_store_and_data_apps#app-store-and-ids-apps.

[47] International Data Spaces Association, "Metadata Broker," [Online]. Available: https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3_5_0_system_layer/3_5_4_metadata_broker#metadata-broker.

[48] International Data Spaces Association, ""3.5.5 Clearing House | IDS Knowledge base," IDS Knowledge Base https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3_5_0_system_layer/3_5_5_clearing_house. [Accessed, June 25th, 2025)

[49] European Commission: Directorate-General for Energy, Data Management Working Group, "Directorate-General for Energy, Data Management Working Group," Publications Office of the European Union, 2023. https://bridge-smart-grid-storage-systems-digital-projects.ec.europa.eu/working-groups/data-management

[50] J. Heiles, "AIOTI, AIOTI WG03 IoT Standardisation, Workshop "Platforms for connected Factories of the Future" Brussels, October 5th 2015," Siemens AG, 15 October 2015. [Online]. Available: https://ec.europa.eu/information_society/newsroom/image/document/2015-44/11_heiles_11948.pdf#:~:text=%E2%80%9CThings%E2%80%9D%20IoT%20Device%20User%20invokes,associated%20Virtual%20Entity%20Interacts%20with.

[51]European Commission Directorate-General For Energy, "M/490 - Standardization mandate to European Standardisation Organisations (ESOS) to support European smart grid deployment.", 2021 [Online]. Available: https://energy.ec.europa.eu/publications/mandate-m490-smart-grids-march-2011_en

[52] European Commission, "Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment,"2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

[53] G. De Panfilis, "FIWARE - Open APIs for Open Minds," FIWARE,. https://www.fiware.org/

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

[54] A. Tejado, T. Sapia, and C. Pezuela, "FI-NEXT - D5.2: FIWARE Go-to-Market Y2," 2018. [Online]. Available: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c20897fa&appId=PPGMS
[55] FIWARE, "FIWARE: THE OPEN SOURCE PLATFORM OF CHOICE FOR BUILDING SMART ENERGY SOLUTIONS." Accessed: Jul. 01, 2025. [Online]. Available: https://www.fiware.org/wp-content/directories/marketing-toolbox/material/FIWAREBrochure_SmartEnergy.pdf
[56] Alliance for Internet of Things Innovation "High Level Architecture (HLA), Release 5.0", December 2020, [Online] Available: https://aioti.eu/wp-content/uploads/2020/12/AIOTI_HLA_R5_201221_Published.pdf
[57] The GridWise Architecture Council, "GridWise Interoperability ContextSetting Framework," Mar. 2008. [Online]. Available: https://gridwiseac.org/pdfs/GridWise_Interoperability_Context_Setting_Framework.pdf
[58] "GAIA-X Framework - GAIA-X: A federated Secure data infrastructure," Gaia-X: A Federated Secure Data Infrastructure -. https://gaia-x.eu/gaia-x-framework/
[59] Gaia -X, "GAIA-X: Technical Architecture Release," Federal Ministry for Economic Affairs and Energy (BMWi), Jun. 2020. [Online]. Available: https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Publikationen/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=7
[60] GAIA-X, "Architecture Document," Apr. 2022. [Online]. Available: https://gaia-x.eu/wp-content/uploads/2022/06/Gaia-x-Architecture-Document-22.04-Release.pdf
[61]S. Jiménez, "Interoperability Framework in energy data spaces: Position Paper | Version 2.0," International Data Spaces Association, Mar. 2025. [Online]. Available: https://enershare.eu/wp-content/uploads/IDSA-Position-Paper-Interoperability-Framework-in-Energy-Data-Spaces-v2-2.pdf
[62] "EnerShare | The Energy Data Space for Europe." https://enershare.eu/
[63] OneNET Project: https://www.onenet-project.eu/
[64] Platone "Platform for operation of distribution networks," Platone - Platform for Operation of Distribution Networks. https://www.platone-h2020.eu/
[65] "Platone 'D2.16: Platone Integrated Framework Prototype (V3),'" Aug. 2023. [Online]. Available:https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e500c403fb&appId=PPGMS
[66] RESONANCE Project. https://www.resonance-project.eu/
[67] "RESONANCE 'D2.1: Initial Requirements and Common System Architecture,'" 2023. [Online]. Available: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5fb270ea8&appId=PPGMS
[68] "Synergy for Smart Multi-Objective Optimisation," CORDIS | European Commission, Feb. 26, 2016. https://cordis.europa.eu/project/id/692286
[69] Lampathaki, F., Biliri, E., Tsitsanis, T., Tsatsakis, K., Miltiadou, D., Perakis, K. (2022). Toward an Energy Data Platform Design: Challenges and Perspectives from the SYNERGY Big Data Platform and AI Analytics Marketplace. In: Curry, E., Scerri, S., Tuikka, T. (eds) Data Spaces . Springer, Cham. https://doi.org/10.1007/978-3-030-98636-0_14
[70] International Electrotechnical Commission, "ISO/IEC 21823-1," IEC, Feb. 2019. [Online]. Available:https://cdn.standards.iteh.ai/samples/100715/7e7bb111e4a84829897e7d7b6137714b/ISO-IEC-21823-1-2019.pdf
[71]HEDGE-IoT "D1.1: Project Management Handbook", 2024, [Online] Available: https://hedgeiot.eu/wp-content/uploads/2025/03/D1.1-Management-communication-and-quality-approaches-Data-management-and-IPR-protection-procedures.pdf

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

[72] HEDGE-IoT "D1.4: Data Management Plan", 2024, [Online] Available: https://hedgeiot.eu/wp-content/uploads/2025/03/D1.4-Data-Management-Plan.pdf
[73] HEDGE-IoT "D2.1: Requirements on an IoT Cloud/Edge System for the Energy Ecosystem", 2024, [Online] Available: https://hedgeiot.eu/wp-content/uploads/2025/03/D2.1-Requirements-on-an-IoT-CloudEdge-System-for-the-Energy-Ecosystem.pdf
[74] HEDGE-IoT "D2.2: Functional Specifications of the HEDGE-IoT system", 2024, [Online] Available: https://hedgeiot.eu/wp-content/uploads/2025/03/D2.2-Functional-Specifications-of-the-HEDGE-IoT-system.pdf
[75] HEDGE-IoT "D3.1: HEDGE-IoT Interfaces and Tools for Interoperability", 2025, [Online] Available: https://hedgeiot.eu/wp-content/uploads/2025/03/D3.1-HEDGE-IoT-Interfaces-and-Tools-for-Interoperability.pdf
[76] HEDGE-IoT "D3.3: HEDGE-IoT Technological Enablers (First Release)", 2025, [Online] Available: https://hedgeiot.eu/wp-content/uploads/2025/03/D3.3-HEDGE-IoT-Technological-Enablers-First-Release.pdf
[77] IETF - https://www.ietf.org/
[78] IEEE - https://www.ieee.org/
[79] MQTT - https://mqtt.org/
[80] NIST - https://www.nist.gov/
[81]Cordis. Europa. "Boosting DR through increased communIty-level consumer engaGement by combining Data-driven and blockcHain technology Tools with social science approaches and multi-value service design," CORDIS | European Commission, Sep. 11, 2020. https://cordis.europa.eu/project/id/957816/reporting
[82] Bright "D2.5: Cross-Domain Data & Service Interoperability", 2022, [Online] Available: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f511726d&appId=PPGMS
[83] European Commission, "European Energy Data Exchange Reference Architecture," BRIDGE - Data Management Working Group, 2020. [Online]. Available: https://energy.ec.europa.eu/system/files/2021-06/bridge_wg_data_management_eu_reference_architcture_report_2020-2021_0.pdf
[84] Cordis , "OPEN DEI: Aligning reference architectures, open platforms and large scale pilots in digitising European industry," CORDIS | European Commission, https://cordis.europa.eu/project/id/857065/reporting/es
[85] Cordis, "Int:NET: Interoperability Network for the energy Transition," CORDIS | European Commission, https://cordis.europa.eu/project/id/101070086
[86] Alberto Dognini, "Blueprint of the Common European Energy Data Space," Interoperability Network for the Energy Transition (int:net), Jul. 2024. doi: 10.5281/zenodo.12609569.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

ANNEX 1 – TRANSVERSAL USE CASES

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Transversal Use Case n°1:

Data exchange through HEDGE-IoT Dataspace

[Data interoperability]

1 Description of the use case

This use case describes how partners in the Hedge-IoT project can exchange data across organizational boundaries using a shared dataspace infrastructure based on the Eclipse Dataspace Connector (EDC). A data provider exposes metadata and access policies for its resources, while a data consumer discovers and retrieves data through secure, policy-compliant mechanisms. The interaction ensures data sovereignty, access control, and interoperability. This pattern can be reused across different pilots and domains to enable secure and standardized data flows.

1.1 Name of the use case

ID	*Area / Domain(s) / Zones(s)*	*Name of Use Case*
TUC-1	Data interoperability	Data exchange through HEDGE-IoT Dataspace.

1.2 Version management

Version Management			
Version No.	*Date*	*Name of Author(s)*	*Changes*
0.1	10/04/2025	Trialog	First structure based on project brainstorming.
0.2	07/05/2025	DST	1st Draft version
0.3	20/05/2025	Trialog	Feedback Provided by Trialog
0.4	23/05/2025	DST	Updates provided by DST
0.5	28/05/2025	Trialog	Feedback provided by Trialog
0.6	09/06/2025	DST	1st semi-final version
1.0	12/06/2025	Trialog	1st final version

1.3 Scope and objectives of use case

Scope and Objectives of Use Case	
Scope	The scope of this transversal use case is to leverage a shared dataspace infrastructure to facilitate secure, standardized, and scalable data exchange across the various components, stakeholders, and pilot sites involved in the Hedge-IoT project.
Objective(s)	The objectives that the use case is expected to achieve are to: • **Objective 1:** allow data exchange for an edge-cloud continuum • **Objective 2:** connect data provider and data customer
Related business case(s)	/

1.4 Narrative of use case

Narrative of Use Case
Short description
This use case describes how partners in the Hedge-IoT project can exchange data across organizational boundaries using a shared dataspace infrastructure based on the Eclipse Dataspace Connector (EDC). A data provider exposes metadata and access policies for its resources, while a data consumer discovers and retrieves data through secure, policy-compliant mechanisms. The interaction ensures data sovereignty, access control, and interoperability. This pattern can be reused across different pilots and domains to enable secure and standardized data flows.
Complete description

In the Hedge-IoT project, several partners collaborate to develop intelligent edge computing solutions for diverse sectors, including energy, mobility, and public services. These partners often need to exchange data across organizational and technical boundaries. However, sharing data between organizations raises concerns about security, control, and compliance with different regulations and usage agreements.

To address this, the project uses a shared **dataspace** infrastructure. This allows each organization to remain the owner of its data while making it available to others in a controlled and standardized way. The core of this infrastructure is the **Eclipse Dataspace Connector (EDC)**, a component that enables organizations to publish, find, and exchange data based on clearly defined policies.

Here's how it works in practice: a **data provider**, such as a company operating an edge service, wants to make a dataset available to other partners. The provider describes the dataset—what it is, how it can be used, and under which conditions—in a metadata format, and publishes it into a shared catalog managed by the dataspace. This information does not include the actual data, but tells potential users what is available and how they can request access.

A **data consumer**, for example a pilot partner developing a mobility application, browses the catalog and finds the dataset. If the dataset fits their needs, the consumer initiates a data access request. This triggers a **negotiation phase**, where the consumer's request is matched against the provider's policies (such as usage rights, contract terms, or allowed frequency). If both parties agree, the data is transferred securely using a trusted communication protocol.

The actual data never becomes publicly accessible—only those who are authorized through the dataspace infrastructure can retrieve it. Every interaction is logged and monitored to ensure compliance with the agreed rules.

This setup ensures **data sovereignty** (each partner controls how their data is used), **interoperability** (partners use common standards), and **security** (data is exchanged securely and only between trusted parties).

This kind of interaction is expected to be replicated in multiple use cases within the project—whether it's exchanging energy grid information, mobility patterns, or sensor data—and can also serve as a template for data exchange in future cross-domain projects.

This transversal use case could be split into different scenarios:

- Scenario 1: Use of the dataspace by a data producer
- Scenario 2: Use of the dataspace by a data customer
- Scenario 3: Metadata Discovery and Planning
- Scenario 4: Federated Service Chaining

Sc.1 Use of the dataspace by a data producer - Description:

- This scenario describes how a data provider makes its dataset or service available within the dataspace. The provider prepares the asset, defines the associated metadata and access policies, and publishes it through its local EDC connector. The asset becomes discoverable by other parties via the federated catalog, allowing compliant and secure access negotiations .Additionally, by exposing curated datasets through the dataspace, data producers contribute to cross-pilot AI training efforts, enabling other partners to discover and evaluate datasets suitable for model development.

Sc.2 Use of the dataspace by a data customer - Description:

- In this scenario, a data consumer interacts with the dataspace to discover and access data assets shared by other parties. The consumer queries the catalog, evaluates metadata and policy terms, and initiates a contract negotiation through its EDC connector. Upon agreement, the data is securely transferred according to the defined usage rules.

Sc.3 Metadata Discovery and Planning - Description:

- A partner uses the dataspace not to directly retrieve data, but to discover which datasets or services are available, including their conditions of use, data formats, and applied semantic vocabularies.

This scenario highlights the catalog and *resource discovery* capabilities of the dataspace, enabling informed planning, semantic mapping, and potential future agreements.
- Particularly useful in the design or pre-integration phase.
- Reduces effort in bilateral discussions, as the catalog serves as a shared point of reference.
- Reinforces semantic interoperability goals (e.g., Task 4.3).

Sc.4 Federated Service Chaining - Description:

- A software component (e.g., an orchestrator or optimization engine) uses the dataspace to access services or modules provided by other partners, in a dynamic and composable way. For instance, an edge node may call a forecasting module hosted in the cloud by another partner, sending data via the dataspace and receiving a processed result in return.

1.5 Key performance indicators (KPI)

ID	*Name*	*Description*	*Reference to mentioned use case objectives*
KPI1	Adoption rate of the dataspace	Number of partners successfully integrated with the dataspace infrastructure	Supports the objective of creating a federated, reusable integration layer across pilots
KPI2	Data asset discoverability	Number of data assets made available and searchable via the federated catalog	Enables semantic discovery and contributes to interoperability across work packages
KPI3	Cross-WP or cross-pilot usage patterns	Number of use cases or pilots that rely on the dataspace to communicate and share data	Validates the transversal nature and reusability of the dataspace beyond vertical or isolated implementations

1.6 Use case conditions

Use case conditions
Assumptions
• All relevant partners have or will adopt a compatible version of the Eclipse Dataspace Connector (EDC), or are integrated via proxies. • All participating organizations agree to define and enforce data usage policies according to IDS principles. • Semantic vocabularies used across pilots (e.g., SAREF,IEC CIM) are sufficiently aligned to enable resource discoverability. • A common trust framework will be setup by DST for identity and access control is in place
Prerequisites
• EDC instances are deployed and reachable by partner systems. • Each partner has registered at least one data asset in its local catalog with appropriate metadata. • Policies for access control and data usage are defined and operational. • Communication between connectors is secured and authorized (e.g., via certificates or trusted endpoints). • At least two pilots or services require cross-organizational data exchange.

1.7 Further Information to the use case for classification / mapping

Classification Information
Relation to other use cases
Computational Orchestration
Level of depth
Prioritisation

Generic, regional or national relation
Italian Pilot, Greek Pilot, Dutch Pilot, Portuguese Pilot, Slovenian Pilot, Finnish Pilot
,Nature of the use case
System Use Case, Transversal Use Case
Further keywords for classification
Dataspace, Semantic Interoperability, Connector, Middleware

1.8 General Remarks

General Remarks

2 Diagrams of use case

Diagram(s) of use case

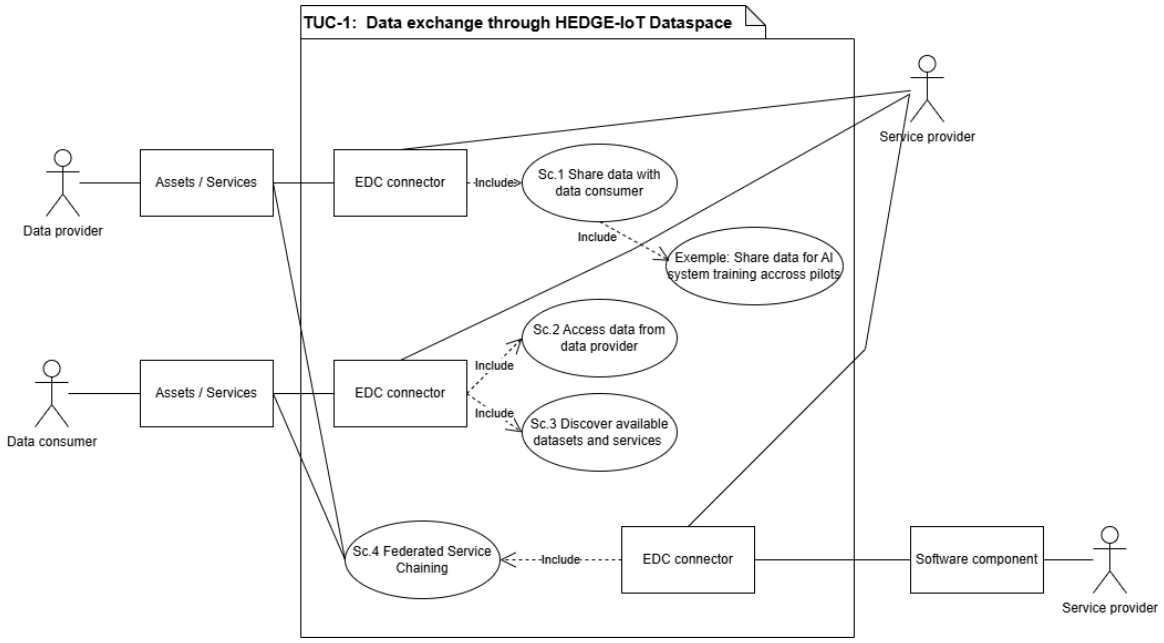

Figure 1: UML use case diagram

3 Technical details

3.1 Actors

Actors			
Actor Name	***Actor Type***	***Actor Description***	***Further information specific to this use case***
Data Provider	Business Actor	Any pilot or service that exposes data (e.g., sensor data, flexibility info, forecasts)	Publishes data assets and defines access policies. Initiates sharing via its EDC connector. {Pilot}
Data Consumer	Business Actor	Any pilot or service that requests data from other partners	Discovers assets, negotiates usage terms, and consumes data via its EDC connector. {Pilot,Service}

EDC Connector	Logical Actor	Eclipse Dataspace Connector instance deployed by each participant	Manages metadata, policies, negotiation, and transfer on behalf of the provider/consumer. {DST}
Dataset Catalog	Logical Actor	Central or distributed catalog for publishing and discovering data assets	Enables data discovery and lookup of published assets in the dataspace. {DST}

3.2 References

References						
No.	***Reference Type***	***Reference***	***Status***	***Impact on use case***	***Originator / organisation***	***Link***
1	GitHub Repository	Eclipse Dataspace Connector (EDC) Documentation	Online	Provides docs for EDC	Eclipse Foundation	https://github.com/eclipse-edc1

4 Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	**Scenario name**	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
1	Use of the dataspace by a Data Provider	A partner exposes a data asset in the dataspace with metadata and access policy	Data Provider	A dataset or service is ready to be shared	EDC connector is deployed, and metadata is defined	Data asset is published and available for discovery
2	Use of the dataspace by a Data Consumer	A partner discovers a data asset, negotiates usage, and retrieves it securely	Data Consumer	A need for external data arises	Catalog is populated and connectors are trusted	Data is transferred securely to the consumer
3	AI Training across Pilots	Data from one pilot is shared with another to support training of AI models	Data Consumer	A training pipeline needs external data	Relevant dataset is available, and policy permits reuse	AI component has access to shared training data
4	Federated Service Chaining	A service (e.g., orchestrator) triggers execution of remote services hosted by other partners via the dataspace	Orchestrator / Service	A workflow requires a remote component's output	Remote service is available and can be invoked via EDC	Result is returned to the orchestrating service
5	Metadata Discovery and Capability Advertising	A partner explores available assets to identify future collaboration or integration opportunities	Data Consumer	Integration planning or exploratory phase begins	Metadata has been published in the catalog	Consumer identifies useful assets or services

4.2 Steps – Scenarios

Scenario								
Scenario name:	Use of the Dataspace by a Data Provider							
Step No.	**Event**	**Name of process/ activity**	**Description of process/ activity**	**Service**	**Information producer (actor)**	**Information receiver (actor)**	**Information Exchanged (IDs)**	**Requirement, R-IDs**
1	New data available	Create data asset	The data provider creates or selects a dataset or service output intended for external sharing.	CREATE	Data Provider	Data Provider	Inf.01	DE.3
2	Asset identified	Define metadata	The provider defines metadata describing the asset (format, structure, purpose, etc.).	CREATE	Data Provider	Data Provider	Inf.02	MD.5
3	Access control needed	Configure access policy	The provider defines access policies such as allowed consumers, usage rights, and expiration terms.	CREATE	Data Provider	Data Provider	Inf.03	MD.1
4	Asset ready to publish	Register asset in connector	The data asset and metadata are registered in the local EDC connector catalog.	REPORT	Data Provider	EDC Connector	Inf.04	MD.6
5	Publication triggered	Publish asset to dataspace	The asset becomes discoverable in the federated dataspace via the connector's catalog endpoint.	REPORT	EDC Connector	Federation Catalog	Inf.05	MD.3
6	Idle	Await request from consumer	No further action until another actor (consumer) discovers and requests the asset.	TIMER	Data Provider	Data Provider	--	--

Scenario								
Scenario name:	Use of the Dataspace by a Data Consumer							
Step	**Event**	**Name of**	**Description of process/**	**Service**	**Information**	**Information**	**Information**	**Requirement, R-IDs**

No.		process/ activity	activity		producer (actor)	receiver (actor)	Exchanged (IDs)	
1	Need for external data arises	Discover data asset	The consumer searches the dataspace catalog for relevant data assets.	GET	Catalog	Data Consumer	Inf.06	MD.6
2	Matching asset found	Request asset access	The consumer selects a dataset and initiates a data usage request through its EDC connector.	EXECUTE	Data Consumer	Data Provider	Inf.07	DE.3
3	Negotiation starts	Negotiate contract	The EDC connectors negotiate a usage agreement (contract offer, response, confirmation).	EXECUTE	EDC Connector	EDC Connector	Inf.08	DE.1
4	Contract accepted	Authorize access	Access is granted according to policy and contract terms.	REPORT	EDC Connector	Data Consumer	Inf.09	CR.3
5	Transfer initialized	Retrieve data	The data is securely transferred from the provider to the consumer.	GET	Data Provider	Data Consumer	Inf.10	DE.3
6	Data received	Confirm transaction	The consumer confirms successful receipt and logs the transaction outcome.	REPORT	Data Consumer	EDC Connector	Inf.11	CR.2

Scenario								
Scenario name:	AI Training Across Pilots							
Step No.	Event	Name of process/ activity	Description of process/ activity	Service	Information producer (actor)	Information receiver (actor)	Information Exchanged (IDs)	Requirement, R-IDs
1	Training data needed	Discover training dataset	The consumer explores the dataspace catalog to find datasets suitable for model training.	GET	Catalog	Data Consumer	Inf.12	MD.6
2	Dataset selected	Request data access	The consumer requests access to the selected training dataset.	EXECUTE	Data Consumer	Data Provider	Inf.13	DE.2
3	Policy evaluation triggered	Negotiate usage agreement	The connectors negotiate the contract terms specific to AI training usage (e.g., retention, reuse).	EXECUTE	EDC Connector	EDC Connector	Inf.14	DE.1

4	Access granted	Transfer training data	Upon contract approval, the training data is transferred securely from provider to consumer.	GET	Data Provider	Data Consumer	Inf.15	DE.3
5	AI model development ongoing	Use data for model training	The consumer uses the dataset locally or in cloud environment to train its AI models.	EXECUTE	Data Consumer	Data Consumer	Inf.16	—
6	Optional feedback	Share model or metadata	Optionally, trained model metadata or feedback can be shared back with the provider or the platform.	REPORT	Data Consumer	Data Provider / Dataset Catalog	Inf.17	MD.4

Scenario								
Scenario name:	Federated Service Chaining							
Step No.	***Event***	***Name of process/ activity***	***Description of process/ activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information Exchanged (IDs)***	***Requirement, R-IDs***
1	Execution plan initialized	Discover available services	The orchestrator queries the dataspace to find remote services (e.g., optimizers, simulators).	GET	Dataset Catalog	Orchestrator	Inf.18	MD.6
2	Suitable service found	Request remote service execution	The orchestrator selects the target service and initiates execution via the dataspace.	EXECUTE	Orchestrator	Service Provider	Inf.19	—
3	Request received	Validate access and execute	The provider verifies the request and executes the requested computation or process.	EXECUTE	Service Provider	Service Provider	Inf.20	CR.1
4	Processing completed	Return execution result	The result of the remote computation is returned via the dataspace to the orchestrator.	REPORT	Service Provider	Orchestrator	Inf.21	—
5	Log transaction	Confirm transaction and record trace	Both parties log the operation for traceability and potential auditing.	REPORT	EDC Connectors	EDC Connectors	Inf.22	CR.2

Scenario								
Scenario name:		Metadata Discovery and Capability Advertising						
Step No.	**Event**	**Name of process/ activity**	**Description of process/ activity**	**Service**	**Information producer (actor)**	**Information receiver (actor)**	**Information Exchanged (IDs)**	**Requirement, R-IDs**
1	Integration or planning initiated	Explore available metadata	A partner accesses the dataspace catalog to explore available data assets and services.	GET	Dataset Catalog	Data Consumer / Planner	Inf.23	MD.6
2	Discovery of potential match	Analyze metadata	The consumer examines information such as data format, access policy, vocabularies used, etc.	GET	Dataset Catalog	Data Consumer	Inf.24	MD.5
3	Need for clarification	Request additional metadata	If necessary, the consumer contacts the provider (via connector) to clarify or retrieve extended info	EXECUTE	Data Consumer	Data Provider	Inf.25	—
4	Info provided	Share additional details	The provider responds with additional documentation or technical specifications	REPORT	Data Provider	Data Consumer	Inf.26	MD.4
5	Decision phase	Log discovery / plan integration	The consumer logs relevant metadata for planning future data usage or service integration	REPORT	Data Consumer	Data Consumer	Inf.27	—

(*) Available options are:

- CREATE means that an information object is to be created at the Producer.
- GET (this is the default value if none is populated) means that the Receiver requests information from the Producer (default).
- CHANGE means that information is to be updated. Producer updates the Receiver's information.
- DELETE means that information is to be deleted. Producer deletes information from the Receiver.
- CANCEL, CLOSE imply actions related to processes, such as the closure of a work order or the cancellation of a control request.
- EXECUTE is used when a complex transaction is being conveyed using a service, which potentially contains more than one verb.
- REPORT is used to represent transferral of unsolicited information or asynchronous information flows. Producer provides information to the Receiver.
- TIMER is used to represent a waiting period. When using the TIMER service, the Information Producer and Information Receiver fields shall refer to the same actor.
- REPEAT is used to indicate that a series of steps is repeated until a condition or trigger event. The condition is specified as the text in the "Event" column for this row or step. Following the word REPEAT, shall appear, in parenthesis, the first and last step numbers of the series to be repeated in the following form REPEAT(X-Y) where X is the first step and Y is the last step.

5 Information exchanged

Information exchanged			
Information exchanged (ID)	***Name of information***	***Description of information exchanged***	***Requirement, R-IDs***
inf.01	Raw or processed dataset	Dataset created by a provider, may include time series, measurements, or computed results.	DE.3
inf.02	Asset metadata	Descriptive information about the data asset: type, format, update frequency, unit, etc.	MD.5
inf.03	Usage policy	Rules defined by the provider about who can access the data, under what conditions and purposes	MD.1
inf.04	Metadata + policy	The combination of asset metadata and usage policy used for registration in the local catalog.	MD.6
inf.05	Federated metadata	Metadata exposed to the federated dataspace catalog, discoverable by external consumers.	MD.1
inf.06	Asset list, metadata	List of available data assets retrieved by a consumer during discovery phase.	MD.6
inf.07	Access request, usage intent	A formal request to access a specific dataset, with declared purpose of use.	DE.3
inf.08	Contract offer, policy details	The contract terms proposed between provider and consumer, including allowed actions, pricing, duration, etc.	DE.1
inf.09	Contract confirmation, access token	Signed agreement and authentication material allowing access to the requested asset.	CR.3
inf.10	Dataset (payload)	The actual data transferred from provider to consumer, according to the contract.	DE.3
inf.11	Transfer status, acknowledgment	Confirmation of successful delivery and receipt of the dataset.	CR.2
inf.12	Metadata on training datasets	Information about datasets suitable for AI model training.	MD.6
inf.13	Access request, intended use	Consumer expresses interest in using dataset for AI training and provides justification.	DE.2
inf.14	Contract offer, policy details	Negotiated terms for use of dataset in training context, possibly stricter than general access.	DE.1
inf.15	Training dataset (input data)	Transferred data used for training AI models.	DE.3
inf.16	Internal model development	Not externally transferred, but part of consumer's local processing (e.g., neural network training).	—
inf.17	Trained model info, evaluation metrics	Feedback or metadata on trained models shared optionally with the original data provider.	MD.4
inf.18	Service metadata, capabilities	Catalogued information about available services and their invocation parameters.	MD.6

inf.19	Input parameters, invocation request	The parameters sent from an orchestrator to a remote service provider via the dataspace.	—
inf.20	Execution results	Output data generated by the remote service in response to the request.	CR.1
inf.21	Output data, execution status	Returned result of the invoked service, sent to the orchestrator.	—
inf.22	Transaction log, timestamps	Audit information logged by the connectors on both sides of the interaction.	CR.2
inf.23	Asset descriptions, metadata	High-level discovery information retrieved from the catalog during integration planning.	MD.6
inf.24	Semantic info, usage conditions	Includes ontologies, tags, units of measure, allowed use cases etc.	MD.5
inf.25	Clarification request, metadata query	A message from a consumer asking for more detail or technical info from the provider.	—
inf.26	Dataset schema, ontology references	Additional descriptive material provided by the data provider.	MD.4
inf.27	Internal planning data	Information recorded by the consumer for later analysis or integration planning.	—

6 Requirements

Data Exchange		
Categories ID	**Category name for Requirement**	**Category description**
DE	Data Exchange	Requirements for the exchange of data between connectors via the dataspace.
Requirement ID	**Requirement Name**	**Requirement description**
DE.1	Max negotiation attempt	Connectors must retry negotiation max 3 times before failing.
DE.2	Metadata must be discoverable	Metadata of published data must be indexed and retrievable via the Broker.
DE.3	Push and pull supported	Both push and pull mechanisms must be available for data transfers.

Metadata Requirements		
Categories ID	**Category name for requirements**	**Category description**
MD	Metadata Requirements	Requirements for metadata structure, discoverability, and lifecycle within the dataspace.
Requirement ID	**Requirement name**	**Requirement description**
MD.1	Metadata Publication Mandatory	Every dataset published by a provider must include a metadata description accessible via broker.
MD.4	Metadata Update Trigger	Metadata must be updated if the associated dataset is modified or deprecated.
MD.5	Metadata Minimum Attributes	Metadata must contain at least title, provider ID, data format, licensing, and update date.

MD.6	Metadata Retrieval Availability	Metadata must be queryable at all times through the dataspace discovery component.

Connector Requirements		
Categories ID	**Category name for requirements**	**Category description**
CR	Connector Requirements	Technical capabilities expected from each EDC connector instance.
Requirement ID	**Requirement name**	**Requirement description**
CR.1	DSP Compliance	The connector must implement the IDSA Data Space Protocol (DSP).
CR.2	Logging enabled	Every connector must log events and transactions for traceability.
CR.3	Identity-based auth	The connector must use the dataspace's Identity Provider for authorization.

7 Common Terms and Definitions

Common Terms and Definitions	
Term	**Definition**
EDC (Eclipse Dataspace Connector)	An open-source component that enables secure, policy-based data exchange across organizations in line with IDS and GAIA-X principles.
IDS (International Data Spaces)	A reference architecture model for trusted data exchange between entities, ensuring sovereignty and compliance.
Catalog	A list of available data assets or services, usually including metadata such as format, owner, and access policy.
Data Provider	An actor that owns a data asset and makes it available through the dataspace.
Data Consumer	An actor that requests and uses data assets shared by other parties in the dataspace.
Metadata	Descriptive information about a data asset, including format, purpose, owner, and usage conditions.
Usage Policy	A set of rules defined by the data provider to govern access and use of the shared asset.
Contract Negotiation	The automated process by which a consumer and provider agree on the terms for data access and usage.
Dataspace	A federated infrastructure for controlled data exchange, based on principles like sovereignty, traceability, and interoperability.
Orchestrator	A component that manages workflows or services by invoking remote or local functions based on data availability or triggers.

Transversal Use Case n°2:

Orchestrate the coordination, management, and execution of energy services across the computational continuum

[Computational interoperability]

1 Description of the use case

1.1 Name of the use case

ID	*Area / Domain(s) / Zones(s)*	*Name of Use Case*
TUC-2	Computational interoperability	Orchestrate the coordination, management, and execution of energy services across the computational continuum

1.2 Version management

Version Management			
Version No.	*Date*	*Name of Author(s)*	*Changes*
0.1	10/04/2025	Trialog	The first structure based on project brainstorming.
0.2	5/05/2025	TUC	Phase 1 Transversal Use Case Definition
0.3	26/05/2025	TUC	First complete version
0.4	6/06/2025	TUC	Updated version
1.0	13/06/2025	Trialog	1st final version

1.3 Scope and objectives of use case

Scope and Objectives of Use Case	
Scope	Coordinating distributed computational tasks for energy services across edge-to-cloud systems, with goals of ensuring responsiveness and cost-effective data exchange, including minimized latency and bandwidth usage. We consider containerized energy services that are data space compliant through eclipse data connector
Objective(s)	The goals that the use case is expected to achieve are to: • **Objective 1:** Dynamically allocate computational resources based on energy services demand across edge, fog, and cloud layers to maintain efficiency and responsiveness. • **Objective 2:** Minimize data transfer overhead in federated AI services by efficiently managing and optimizing the hyperparameters of the learning process. • **Objective 3:** Ensure the efficient update of energy services from cloud to edge avoiding execution disruption
Related business case(s)	• Predictive and real-time congestion management (non-AI) • Forecast energy production and consumption for energy communities or residentials or commercial buildings (AI)

1.4 Narrative of use case

Narrative of Use Case
Short description
The use case focuses on enabling the automated coordination, management, and execution of computational tasks through a computational orchestrator. The orchestrator leverages swarm-based algorithms to optimize resource usage, ensuring both computational and communication efficiency. It integrates with non-AI Energy Services to manage deployment, coordination, and resource allocation, and with AI Federated Services to support hyperparameter tuning and training optimization. Additionally, it enables services roll-up at the edge, allowing automated updates and deployment of new versions. Integration with the Eclipse Data Space Connector ensures compliance with data space standards and secure, interoperable data and service exchange.
Complete description

This transversal use case could be split into three scenarios:

- **Scenario 1: Energy services orchestration at edge for responsiveness and geographic redundancy (Sc.1)**

Containerized energy services are deployed across edge-fog-cloud distributed infrastructure overlapping the smart grid. The services and the infrastructure available computing nodes are registered with the computational orchestrator. The orchestrator continuously monitors service locations, resource availability, and task assignments. An integrated Kubernetes component handles the initial task allocation based on current resource availability and predefined configurations. It also supports live monitoring of service status and system resources. When predefined events occur, such as violations of service level agreements or policy conditions, the orchestrator responds by executing a swarm-based optimization algorithm to determine which services should be migrated to other nodes. During service migration, the persistent state and data of each service must also be transferred, and their connectivity via the Eclipse Data Space Connector must be maintained to ensure secure and interoperable data exchange. Therefore, it ensures service responsiveness and geographic redundancy.

- **Scenario 2: Federated AI-driven energy services orchestration for cost-effective data exchanges (Sc.2)**

The orchestrator manages federated learning processes initiated by AI services deployed across edge, and fog/cloud nodes. The federated architecture may follow either a hierarchical or peer-to-peer model. All participating nodes are registered with the orchestrator, providing metadata on their computational capabilities and availability. Based on service-specific requirements, the orchestrator can cluster nodes to enhance training efficiency. It also performs hyperparameter tuning and training optimization using heuristic-based algorithms, ensuring efficient use of distributed resources at edge and minimizing data exchange overhead among edge and fog/cloud nodes.

- **Scenario 3: Energy service rolling out at edge (Sc.3)**

The orchestrator can support service providers such as DSO to automatically roll out new versions for energy services for the consumers. The data models (packages or files) are sent through the Eclipse Data Space Connector. It detects available updates for application components, manages versioning and handles service interruption during updates.

1.5 Key performance indicators (KPI)

ID	*Name*	*Description*	*Reference to mentioned use case objectives*
KPI1	Decrease of data exchange between nodes	Measures the percentage reduction in communication data volume due to orchestrator optimization (%)	Objective 2
KPI2	Savings in network bandwidth and lower latency	Measures the percentage savings in network bandwidth usage and percentage reduction in service response latency through localized processing and optimized resource allocation (%)	Objective 1 and Objective 3

1.6 Use case conditions

Use case conditions
Assumptions
Sc.1 • The services are data space compliant • Edge nodes with sufficient computational resources are available at the deployment sites. **Sc.2** • Federated AI services for the energy sector are assumed to be in place, utilizing either hierarchical or peer-to-peer architectures. • Training nodes are assumed to have access to local datasets that are not shared with other nodes and must remain private due to data sovereignty or regulatory constraints.

• A communication infrastructure exists between nodes, using a data space connector or an equivalent secure communication protocol. • In scenarios involving hyperparameter tuning, each node can perform training using distinct hyperparameter configurations **Sc.3.** • All existing services are assumed to be registered in a federated catalog or app store to support service discovery and orchestration. • Federated models are assumed to be updatable through ongoing training or fine-tuning at participating nodes
Prerequisites

Sc. 1
• All services intended for deployment on edge nodes are assumed to be containerized (e.g., using Docker).
• An existing workload management platformed is assumed to be in place for managing edge nodes and monitoring deployed services (e.g. Kubernetes-based platform with KubeEdge).
Sc.2
• Each service exposes a communication interface and includes a data space connector, enabling the orchestrator to:
  ○ Retrieve metadata and status information about services and edge nodes
  ○ Configure optimization parameters such as hyperparameters, selected training nodes, and other task-specific settings.
Sc. 3
• Edge nodes that deploy applications from the catalog or use federated models are assumed to be registered with the orchestrator
• The orchestrator is assumed to have access to application images and federated models and is notified when updated versions become available.
• The orchestrator is assumed to have the capability and permission to manage updates to federate models.

1.7 Further Information to the use case for classification / mapping

Classification Information
Relation to other use cases
/
Level of depth
/
Prioritisation
/
Generic, regional or national relation
/
Nature of the use case
System Use Case, Transversal (system) Use Case
Further keywords for classification
/

1.8 General Remarks

General Remarks
/

2 Diagrams of use case

Diagram(s) of use case

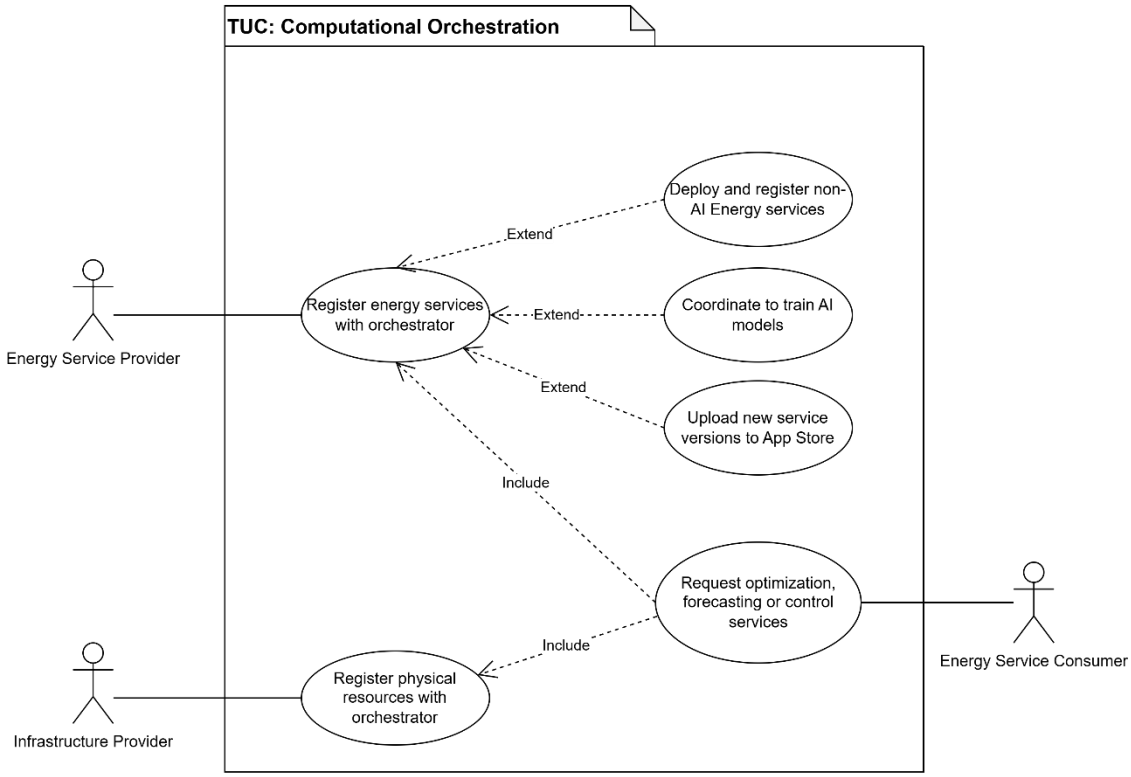

Figure 1: UML use case diagram

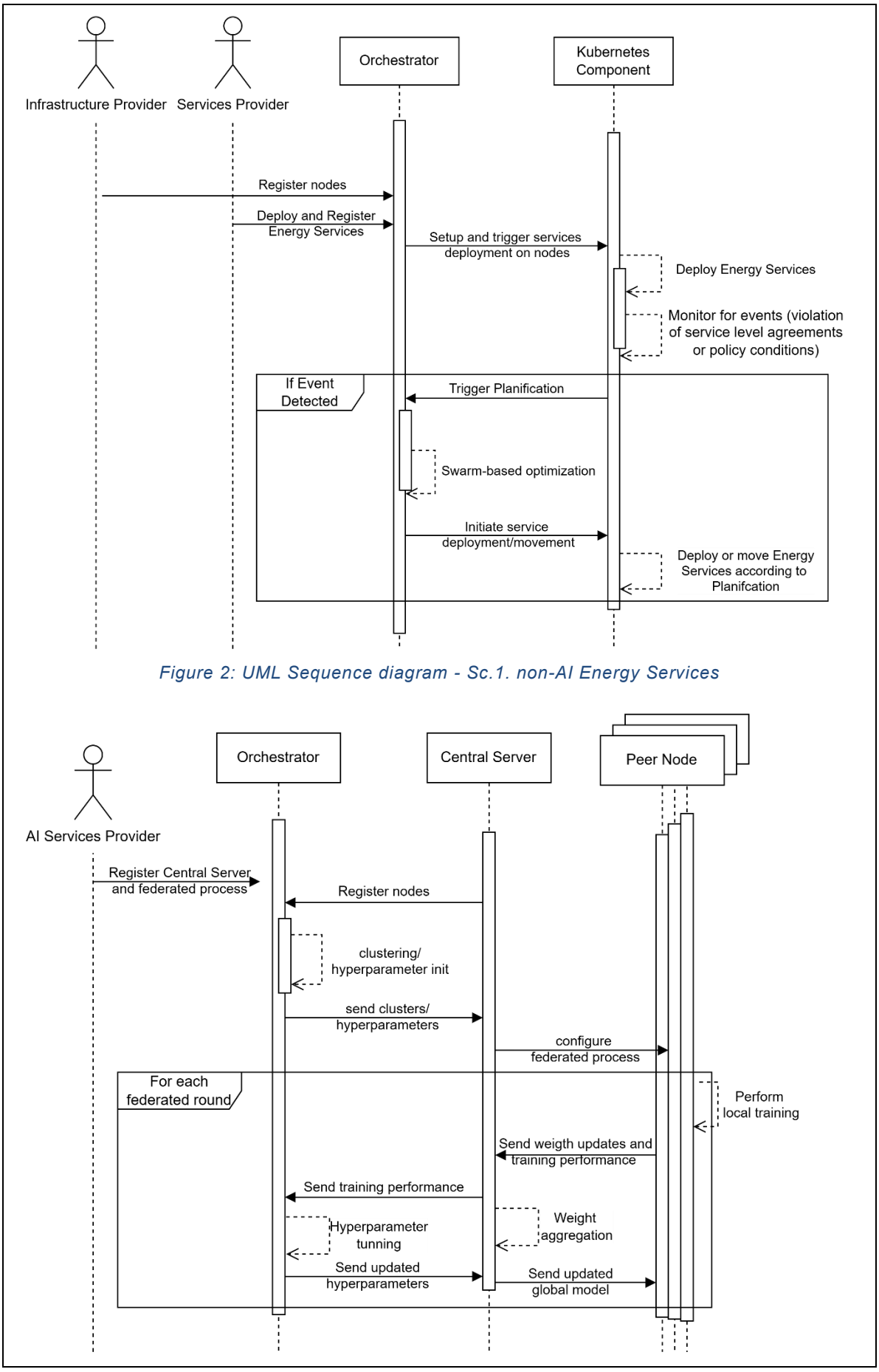

Figure 2: UML Sequence diagram - Sc.1. non-AI Energy Services

Figure 3: UML Sequence diagram - Sc.2. AI Energy Services

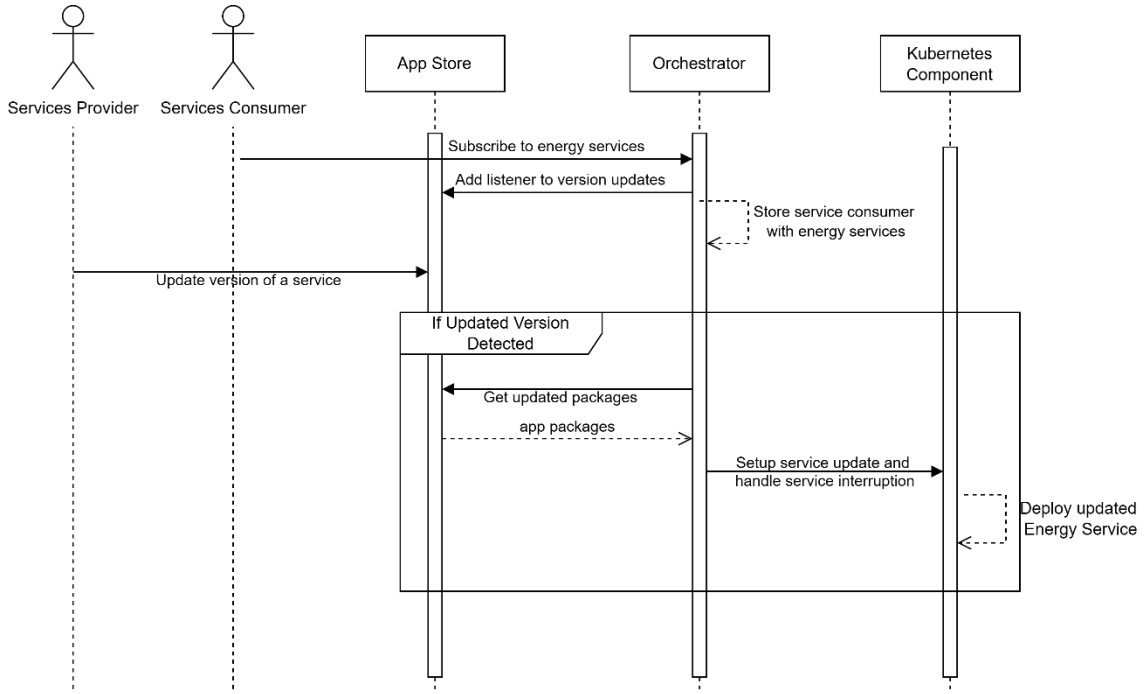

Figure 4: UML Sequence diagram - Sc. 3 Energy Services rolling out at edge

3 Technical details

3.1 Actors

Actors			
Actor Name	***Actor Type***	***Actor Description***	***Further information specific to this use case***
Energy Service Provider	Business actor	Provides energy forecasting, or congestion management services	- ARETI DSO (Italian Pilot – Sc.1) Congestion prediction and optimal power flow service - INESC Energy Community Service Provider (Portuguese Pilot – Sc.2) - TAU (Finland Pilot - Sc.3) Congestion management service
Infrastructure Provider	Business actor	Owns or operates the computational resources and communication network infrastructure	- ARETI & DST (Italian Pilot Sc.1) - TUC & INESC (Portuguese Pilot - Sc. 2) - TUC & TAU (Finland Pilot – Sc. 3)
Energy Service Consumers	Operator	Needs the optimization, forecasting, or control services	Energy communities, prosumers, DSO, customers
Computational Orchestrator	Logical actor	Manages registration, scheduling, and coordination of services and nodes.	Orchestration logic
EDC Connector	Logical actor	Used for communication between services	Ensure connectivity and secure data exchange

3.2 References

References						
No.	*Reference Type*	*Reference*	*Status*	*Impact on use case*	*Originator / organisation*	*Link*

4 Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	**Scenario name**	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
Sc. 1	Energy services orchestration at edge for responsiveness and geographic redundancy	A distributed orchestration system leverages Kubernetes and swarm-based optimization to dynamically allocate and migrate containerized energy services across edge-fog-cloud infrastructure	Energy service provider	An energy services needs to be deployed/relocated due to violations of service level agreements or policy conditions	The service is containerized and data space compliant	SLA compliance, service is successfully relocated, communication links with other services are preserved
Sc. 2	Federated AI-driven energy services orchestration for cost-effective data exchanges	The orchestrator coordinates federated learning across edge, fog, and cloud nodes using hierarchical or peer-to-peer models, optimizing node clustering, hyperparameters, and training efficiency through heuristics while minimizing data exchange overhead.	Energy service provider	Initiate the model training for the federated AI service	The federated service exposes a communication interface, and the training process is configurable	Average data exchange is reduced compared with the baseline
Sc. 3	Energy service rolling out at edge	The orchestrator enables automated rollout of updated energy service versions for consumers on behalf of service providers	Energy service provider	A new version of an energy service is available	Service consumers are registered with the orchestrator; Orchestrator has access to updated versions through EDC	Updated service version is deployed

4.2 Steps – Scenarios

Scenario								
Scenario name:		**Sc. 1**						
Step No.	**Event**	**Name of process/ activity**	**Description of process/ activity**	**Service**	**Information producer (actor)**	**Information receiver (actor)**	**Information Exchanged (IDs)**	**Requirement, R-IDs**
St.1	New energy services available	Register new energy service	Service provider registers a service, including its policies and service level agreements	CREATE	Energy service provider	Orchestrator	Inf.01	D.1
St.2	New infrastructure resource available	Register new nodes	Infrastructure provider registers new available edge nodes	CREATE	Infrastructure provider	Orchestrator	Inf.02	D.2
St.3	New service or constraint violation	Trigger planification	Edge nodes and services are monitored; Orchestrator listens for new events.	REPORT	Kubernetes Component	Orchestrator	Inf.03	QoS.1 QoS.2
St.4	Planification triggered	Run swarm-based optimization	Orchestrator runs optimization algorithm based on monitoring and service information	EXECUTE	Orchestrator	-	-	QoS.1 QoS.2
St.5	Optimization completed	Initiate service deployment/movement	Orchestrator sends the optimization results to Kubernetes platform	CHANGE	Orchestrator	Kubernetes Component	Inf.04	Conf.2
St.6	Kubernetes Component receives new planification	Deploy/relocate services	Kubernetes component handles deployment of the services and preserves the links between services	EXECUTE	Kubernetes Component	Kubernetes Cluster	Inf.05	Conf.1 QoS.2

Scenario								
Scenario name:		**Sc. 2**						
Step No.	**Event**	**Name of process/ activity**	**Description of process/ activity**	**Service**	**Information producer (actor)**	**Information receiver (actor)**	**Information Exchanged (IDs)**	**Requirement, R-IDs**
St.7	New initiated federated process	Register new federated process	Service provider registers a federated process with its configuration and hyperparameters	CREATE	AI Energy service provider	Orchestrator	Inf.06	D.1 Conf.2
St.8	Federated	Register edge	Available training edge nodes	CREATE	Central	Orchestrator	Inf.07	D.2

	process registered	nodes	are registered with orchestrator		Server/Edge Node/ AI Service Provider			
St.9	Federated process triggered	Initialization of the federated process	Orchestrator performs clustering/initialization for optimization algorithm	EXECUTE	Orchestrator	-	-	Conf.2
St.10	Next federated round/ optimization needed	Orchestrator performs optimization	Orchestrator runs optimization algorithm for the configured hyperparameters	REPEAT (5, 6)	Orchestrator	-	-	Conf.2
St.11	Optimizatio n completed	Sends optimization results	Orchestrator sends the optimization results to edge nodes	CHANGE	Orchestrator	Edge nodes	Inf.08	D.2 Conf.2
St.12	New hyperparam eters/config uration available	Perform local training and send training performance	Edge nodes perform training based on the received configuration/hyperparameter s and send performance results back	REPORT	Edge nodes	Orchestrator	Inf.09	D.2 Conf.2

Scenario name:		**Sc. 3**						
Step No.	***Event***	***Name of process/ activity***	***Description of process/ activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information Exchanged (IDs)***	***Requirement, R-IDs***
St.13	New subscriber to energy services	Register energy service consumer	Service consumer requests energy service	CREATE	Energy service consumer	AppStore / Orchestrator	Inf.02	D.1 D.2
St.14	New version of a service / federated model available	Detect new updated version	Orchestrator checks the consumers of the service and gets the updated package through data space connector	GET	App Store / Federated Catalogue	Orchestrator	Inf.10	D.1 D.3 Conf. 2
St.15	New app package / federated model received	Handle version update	Handle possible service interruption and send update command to the Kubernetes component	CHANGE	Orchestrator	Kubernetes Cluster / Edge Nodes	Inf.11	QoS.1 Conf.1 Conf.2
St.16	New update command	Update energy services/federa	Update the service version at edge nodes	CHANGE	Kubernetes Cluster	Edge Nodes	Inf.12	QoS.1 Conf.1

	(if the updates are made through the Kubernetes component)	ted model						

5 Information exchanged

Information exchanged			
Information exchanged (ID)	***Name of information***	***Description of information exchanged***	***Requirement, R-IDs***
Inf.1	Energy service metadata	Computational requirements, links with other services, policies and service level agreements Communication protocol: HTTP Format: Json	*D.1*
Inf.2	Edge node metadata	Computational resources, location Communication protocol: HTTP Format: Json	*D.2*
Inf.3	Service monitored data	Data monitored in real time by Kubernetes component and alerts for policy/agreement violations - Kubernetes API	*Conf. 1*
Inf.4	Service planification	The results of the swarm-based optimization run by orchestrator Communication protocol: HTTP Format: Json	*QoS.1* *QoS.2* *Conf.1* *Conf.2*
Inf.5	Deployment information	Container image, deployment description, configuration - JSON or YMAL format for specification, docker image	*Conf.1*
Inf.6	Federated process hyperparameters	Training nodes, number of rounds Communication protocol: HTTP Format: Json	*D.1*
Inf.7	Descriptive Data Profile	Statistics on energy data stored on the edge nodes Communication protocol: HTTP Format: Json	*D.1* *D.2*
Inf.8	Federated process configuration	Optimization/clustering result computed by the orchestrator Communication protocol: HTTP Format: Json	*D.2* *Conf.2*
Inf.9	Training performance data	Training performance of the edge nodes for the configuration given in the current round Communication protocol: HTTP Format: Json	*D.2*
Inf.10	New version notification	Produced when a new version is available for a service Communication protocol: HTTP or MQTT	*D.1*
Inf.11	App package / federated model parameters	Updated version of the app package or federated model Binary package or Docker image or JSON	*Conf.1*
Inf.12	Deployment update information	Updated image, configuration, rollout strategy - Kubernetes API in JSON or YMAL format	*QoS.1* *Conf.1*

6 Requirements

Quality of Service Requirements		
Categories ID	***Category name for requirements***	***Category description***
QoS	Quality of Service	Generic properties that service/SUC should provide – quality attributes.
Requirement ID	***Requirement name***	***Requirement description***
QoS.1	Service availability	The system must ensure availability of the services after relocation or updating
QoS.2	Services inter-connection	The connections between services are maintained after relocation

Security Requirements		
Categories ID	***Category name for requirements***	***Category description***
Sec	Security	Authentication of user, confidentiality, integrity, prevention of denial of service, non-repudiation or accountability, error management.
Requirement ID	***Requirement name***	***Requirement description***
Sec.1	Secure data exchange	Data exchange between services and orchestrator is secured (provided by Dataspace Connector)
Sec.2	Controlled access	Provided by the Dataspace Connector that ensures authorized access to data

Data Management Requirements		
Categories ID	***Category name for requirements***	***Category description***
D	Data Management	Type of source of data, correctness or validity of data, timeliness or time stamping of data, volume of data, synchronization, or consistency of data across systems, timely access to data, validation of data across organizational boundaries, transaction management, data naming, identification, formats across disparate systems, maintenance of data and databases.
Requirement ID	***Requirement name***	***Requirement description***
D.1	Management of service data exchange between provider and orchestrator	The orchestrator must access, store, and manage metadata and deployment information about energy services provided by the service provider
D.2	Management of data between orchestrator and edge nodes	The orchestrator must receive and store information about edge node computational resources, location and it sends configurations, updated app packages
D.3	Compliance with Eclipse Data Space Connector	Data exchanges between services should be made using Eclipse Data Space Connector

Discovery and Configuration Requirements		
Categories ID	***Category name for requirements***	***Category description***
Conf	Configuration	Locations, distances, communication layout, commonly used communication protocol media, network bandwidth, existing protocols, number of devices, systems, volume of data items, expected growth, etc.
Requirement ID	***Requirement name***	***Requirement description***
Conf.1	Deployment automation using Kubernetes	The services deployment should be automated using Kubernetes component
Conf.2	Service configurability	Services should support external configuration, and the orchestrator generates and manages these configuration

7 Common Terms and Definitions

Common Terms and Definitions	
Term	**Definition**
EDC	Eclipse Dataspace Component
API	Application programming interface
JSON	JavaScript Object Notation
YMAL	“YAML Ain’t Markup Language” or “Yet Another Markup Language”
MQTT	Message Queuing Telemetry Transport
HTTP	Hypertext Transfer Protocol

Transversal Use Case n°3:

Use of the App Store as part of HEDGE-IoT

[Functional interoperability]

1 Description of the use case

1.1 Name of the use case

ID	*Area / Domain(s) / Zones(s)*	*Name of Use Case*
TUC-3	Functional interoperability	Use of the App Store as part of HEDGE-IoT.

1.2 Version management

Version Management			
Version No.	*Date*	*Name of Author(s)*	*Changes*
0.1	10/04/2025	Trialog	First structure based on project brainstorming.
0.2	05/05/2025	ED	1st Draft: Sections 1-3
0.3	26/05/2025	ED	Sequence Diagrams and corrections on comments
0.4	30/05/2025	ED	Completed Scenario Tables
0.5	11/06/2025	ED	Updated Sequence Diagrams
0.6	18/06/2025	INESC	Updated Scenario Descriptions
0.7	19/06/2025	ED	Updates based on partner feedback
0.8	20/06/2025	ED	Finalised 1st Draft Version
1.0	27/06/2025	Trialog	1st final version

1.3 Scope and objectives of use case

Scope and Objectives of Use Case	
Scope	This use case describes the HEDGE-IoT App Store, a component of the HEDGE-IoT digital middleware, and how it enables publishing, discovering, using and creating new data apps (edge/cloud services) in a trusted, semantically interoperable energy IoT ecosystem. It covers the full lifecycle of data-driven services at the edge or cloud: from App Providers publishing services, to App Users discovering and deploying them, to composing new services from existing ones, and ensuring services are interchangeable in a data space, namely through to semantic standards.
Objective(s)	The main objective is to deploy an App Store where third-party developers can publish data apps, certified them, and where energy stakeholders can discover and deploy these apps on their HEDGE-IoT Connectors at the edge or in the cloud. The objectives that the use case is expected to achieve are to: • **Objective 1:** Facilitate publication of new services/sub-services in the HEDGE-IoT environment. • **Objective 2:** Provide a discovery mechanism so developers or users can find available reusable services. • **Objective 3:** Enable reusability and interoperability among different HEDGE-IoT components, pilot projects or datasets. • **Objective 4:** Promote semantic interoperability (services whose data assets can be used across different pilot contexts).
Related business case(s)	/

1.4 Narrative of use case

Narrative of Use Case
Short description
The HEDGE-IoT App Store is a repository for Software Applications that operate at least in one data space configuration. Apps include/represent services/microservices enabling quick discovery, sharing, and reuse across different pilots and domains. It allows service owners to publish new service functionalities, while developers or other system components can request and acquire access. By ensuring semantic and technical interoperability, the App Store accelerates solution development and deployment, fosters collaboration, and ensures consistent service quality within the HEDGE-IoT framework. In line with the new data space protocol (version >2), the App Store also promotes the possibility for dataspace compliant connectors to search adopt other versions of control and data planes available.
Complete description
This transversal use case is therefore split into four scenarios: • **Scenario 1:** Publish a service/sub-service in the App Store A service provider develops or containerizes a new IoT/energy service and registers it within the HEDGE-IoT App Store, supplying descriptive metadata (inputs, outputs, resource requirements, license) along with the container image. An automated certification process checks the connector's compatibility, security, and semantic conformance. Once approved, the service becomes discoverable in the App Store catalogue, ready for other stakeholders to reuse. • **Scenario 2:** Find/Retrieve/Reuse/Access a service/sub-service in the App Store An application developer or system component browses or queries the App Store to locate a suitable service based on functionality or usage terms. After accepting any licensing agreements or data usage policies, the user's edge/cloud environment retrieves the service container from the App Store's registry. The service is then deployed at the selected node(s), where it can securely process data under the HEDGE-IoT dataspace policies. • **Scenario 3:** Interchangeable common services/sub-services *(semantic interoperability across data consumers)* Different providers publish "functionally equivalent" services following the same data schemas. Thanks to uniform semantic definitions, a user can seamlessly swap one service with another without having to modify underlying workflows or data pipelines. This ensures plug-and-play upgrades, vendor-neutral deployments, and consistent service behaviour across diverse HEDGE-IoT environments.

1.5 Key performance indicators (KPI)

ID	Name	Description	Reference to mentioned use case objectives
KPI1	Open source released developments related to data connector implementation	Target: > 2 Y1, > 3 Y2, > 5 Y3 This KPI provides a counter of the number of Apps/services available in the App Store. It expects more than 2 services in year 1 of the project, more than 3 in year 2 and more than 5 in year 3. The counter is cumulative with past years. (*KPI5*).	Objective 1

1.6 Use case conditions

Use case conditions
Assumptions
1. The App Store must be part of the HEDGE-IoT Dataspace and operating via a functioning, compatible Connector. 2. There is a functioning HEDGE-IoT Connector environment for both App Providers and App Consumers (including identity management etc.). 3. Each participants Connector must be configured with valid identities and certificates, and in some cases equipped with an App Execution Environment to run the downloaded apps. 4. There is an established semantic model, ontology or set of ontologies so that published services can be semantically described. 5. The certification process is established for connector's that require it. 6. The HEDGE-IoT dataspace is operational 7. Apps are packaged as container images and include metadata according to the IDS Information Model and project-specific schemas. 8. The App Store has the necessary container registry and metadata database in place.
Prerequisites
• App Provider has corrected access rights and credentials to access the dataspace and to publish container images. • App Consumer is onboarded to the HEDGE-IoT environment, with a certified connector that can pull and deploy container images.

1.7 Further Information to the use case for classification / mapping

Classification Information
Relation to other use cases
Ties in with all pilot-specific SUCs/BUCs that need data processing or specialized analytics.
Level of depth
Prioritisation
High priority (since the App Store is a fundamental piece for the entire HEDGE-IoT solution).
Generic, regional or national relation

Generic
Nature of the use case
System use case, Transversal use case Technical/system *use case* that supports business processes across different pilot use cases.
Further keywords for classification
App Store, Services, Interoperability, Data App, Connector

1.8 General Remarks

General Remarks
• HEDGE-IoT App Store design is based on the IDSA guidelines (RAM v4.0) • HEDGE-IoT Connector design is based on EDC Framework

2 Diagrams of use case

Diagram(s) of use case

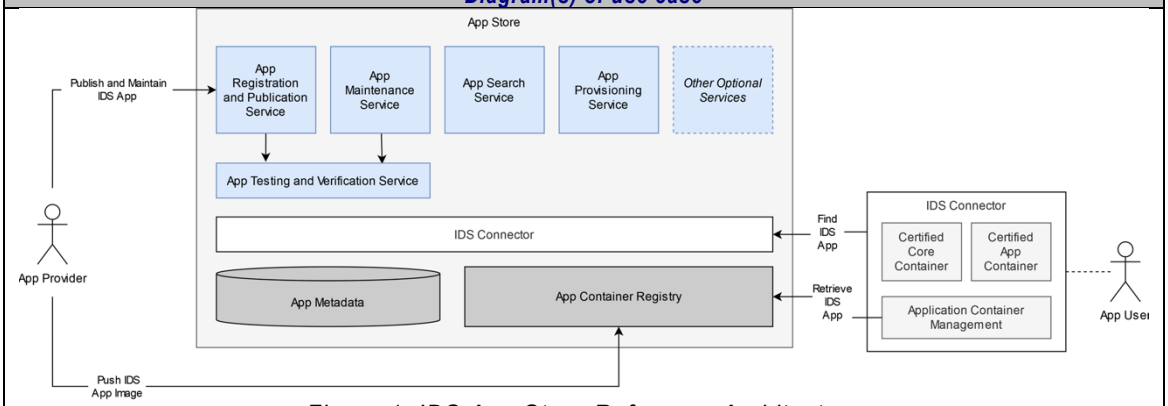

Figure 1: IDS App Store Reference Architecture

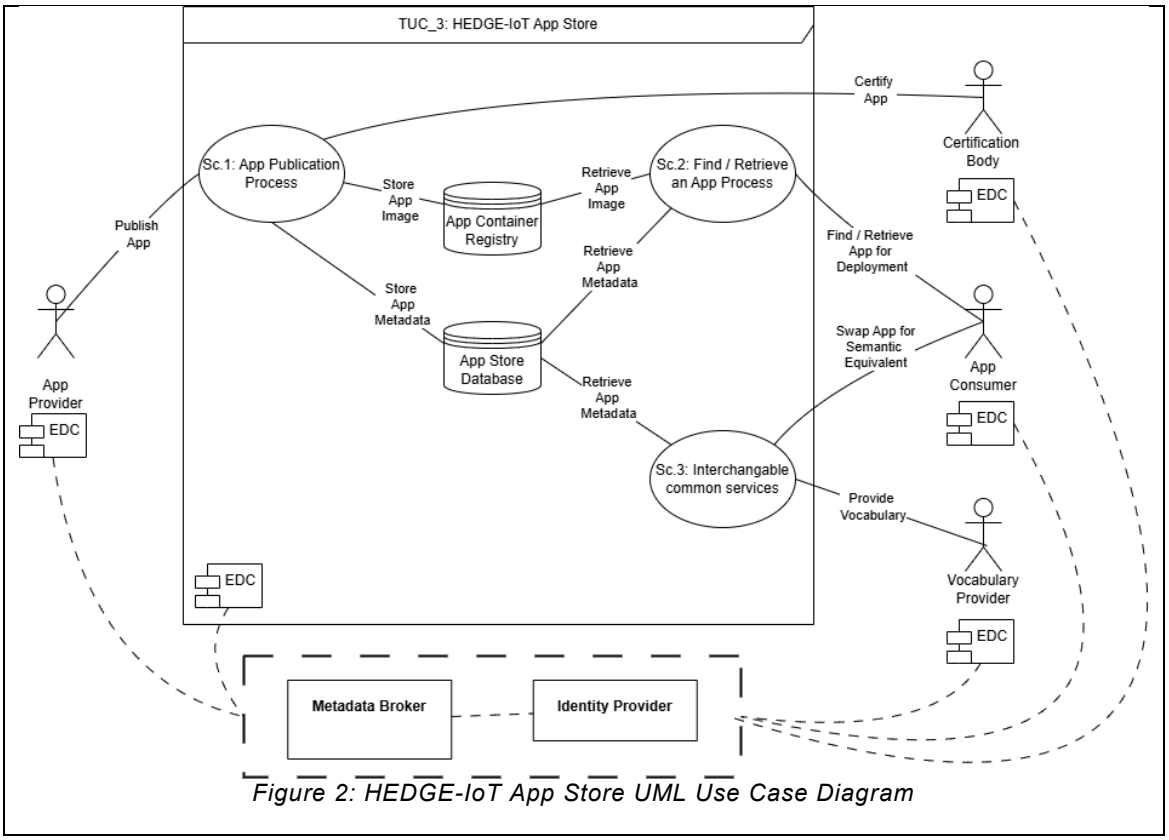

Figure 2: HEDGE-IoT App Store UML Use Case Diagram

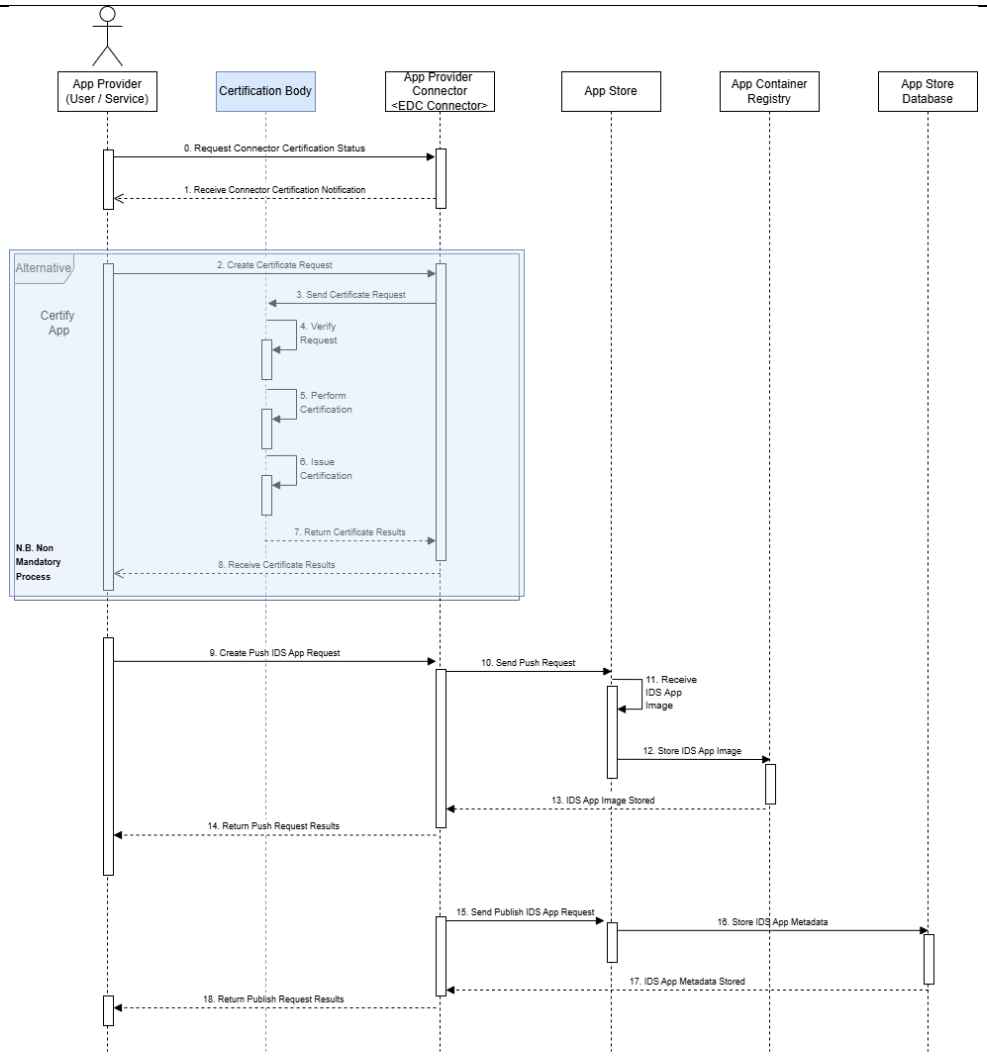

Figure 3: Scenario 1 - 'Publish an App Process'' UML Sequence Diagram

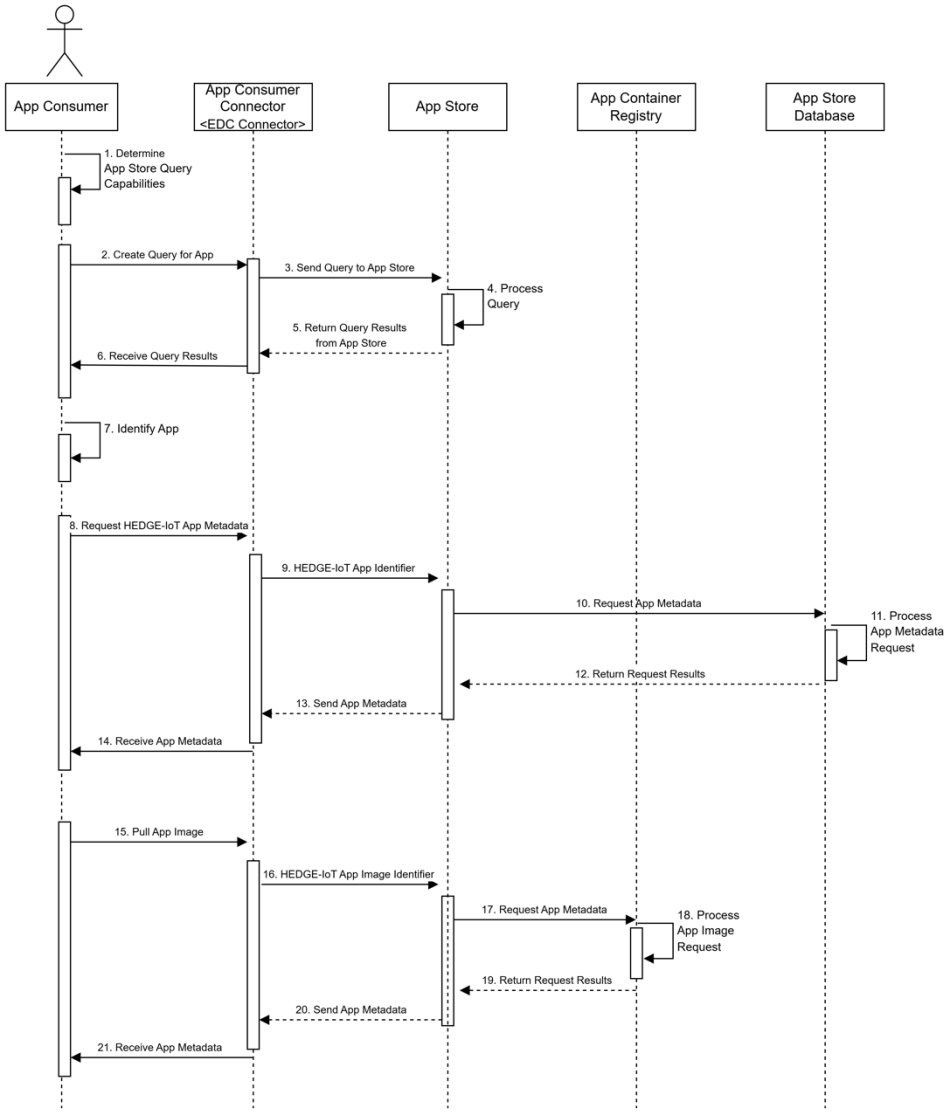

Figure 4: Scenario 2 - "Find/Retrieve/Reuse/Access an App Process" UML Sequence Diagram

3 Technical details

3.1 Actors

Actors			
Actor Name	***Actor Type***	***Actor Description***	***Further information specific to this use case***
Data App Provider	Logical Actor	An entity that publishes an IDS App to the App Store. The App Provider is responsible for creating or owning the app and for supplying its metadata and container image.	HEDGE-IoT Data App Developers (Demos / 3rd Parties from Open Calls)
App Store	Logical Actor	The platform (software component) that manages the lifecycle of data apps. It provides interfaces for: App Registration & Publication: accepting new app submissions, including metadata. App Maintenance: updating or removing apps, managing versions. App Search/Query: allowing users to find apps by various criteria. App Provisioning: delivering the app (metadata and container) to the requesting user's connector. Other Optional services	TBD
Data App User / Data App Consumer	Logical Actor	An entity that discovers and uses apps from the App Store. The role involves searching the castep-by-stepping an app, possibly negotiating usage terms and deploying the app in their environment. The App User operates a HEDGE-IoT Connector that can receive and run the app.	TBD
Certification Body	Logical Actor	A Certification Body can issue a Certificate for a connector for compliance with security, safety, or interoperability standards	TBD
Vocabulary Provider	Logical Actor	Semantic Interoperability Technological Enablers Providers	TBD
App Store Container Registry	Logical Actors	Holds and manages software containers representing Apps in the data space or any required components.	TBD
App Store Metadata Registry	Logical Actors	App Store sub-module	TBD
App Provider Connector <EDC Connector>	Logical Actor	Eclipse Dataspace Connector instance deployed by each participant	Manages metadata, policies, negotiation, and transfer on behalf of the provider/consumer. {DST}
Metadata Broker	Logical Actor	Federated catalogue service that stores and exposes only descriptive metadata (no data or binaries). Enables search and discovery of data assets and services across the dataspace.	• IDS-compliant Broker implementation
Identity Provider	Logical Actor	Issues, validates, and revokes identities for all HEDGE-IoT ecosystem participants.	• Manages identities at two levels: (1) Organisation level – each company/platform receives a certified IDS Participant ID;

			(2) Individual/user level – personal certificates

3.2 References

References						
No.	**Reference Type**	**Reference**	**Status**	**Impact on use case**	**Originator / organisation**	**Link**
1	IDSA Specification	IDSA 3.5.3: App Store and App Ecosystem	Online	Defines app store ops, app types, endpoints	IDSA	IDS Knowledge Base 3.5.3
2	IDSA Processes	IDSA 3.4.5: Publishing & Using Data Apps		Lays out the Publish/Find/Retrieve/Use processes	IDSA	IDS Knowledge Base 3.4.5
3	IDSA Usage Control	IDSA 4.1.6: Usage Control	Online		IDSA	IDS Knowledge Base 4.1.6
4	GitHub Repository	Eclipse Dataspace Connector (EDC) Documentation	Online	Provides docs for EDC	Eclipse Foundation	https://github.com/eclipse-edc1
5	International Data Spaces Information Model	**Revision:** 4.2.0	Online	The Information Model primarily aims at describing, publishing and detecting data products (Data Assets) and reusable data processing software (Data Apps) in the International Data Space. Data Assets and Data Apps are the core resources of the International Data Space and are hereinafter referred to as resources.	IDSA	https://w3id.org/idsa/core
6.	IDS Message Types	Aligned to v4.1.0	Online	Descriptions for each message, information about the payload as well as changes in the properties, i.e., new properties and additional mandatory properties. "Message Class" and "Message Subclass" are just for structural / hierarchial description. The "Message Name" contains the actual Message which is used. New properties, which are mandatory are		IDS MessageTypes

				marked with an (*). Existing properties, which are mandatory for a specific message are listed in the corresponding column.		
7.	Dataspace Protocol		Online	The Dataspace Protocol is a set of specifications designed to facilitate interoperable data sharing between entities governed by usage control and based on Web technologies. These specifications define the schemas and protocols required for entities to publish data, negotiate Agreements, and access data as part of a federation of technical systems termed a Dataspace.		Dataspace Protocol 2025-1-RC1
8.	3.5.4. IDS Metadata Broker					IDS Knowledge Base

4 Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	**Scenario name**	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
Sc.1	Publish a Service/ Sub-service	A service provider develops or containerizes a new IoT/energy service and registers it in the HEDGE-IoT App Store, providing metadata (inputs, outputs, license) and container image. After automated checks (testing/certification) the connector is compliant.	App Provider	The provider deploys a new service or updates an existing one.	1) The service is containerized and meets basic compliance requirements (semantic metadata, security, etc.). 2) App Store is operational and accepting submissions. 3) (Optional) Connector Certification is completed if the store/policies require it.	The new service appears in the App Store catalogue, ready for others to discover and deploy (if certification is active, only after passing this process).
Sc. 2	Find/Retrieve/Reuse/Access a service/sub-service in the App Store	A developer or system component searches the App Store for suitable services. After selecting and accepting licensing/usage terms, the app	App Consumers	A need arises for a specific functionality that could be fulfilled by a published service.	1) The user is onboarded with the App Store (valid IDS Connector). 2) The user has the required permissions or license to deploy services. 3) At least one suitable service is	The service is successfully deployed on the user's node(s) and becomes operational, processing data according to data usage

		container is retrieved and deployed at the user's edge/cloud. The service can then process data under HEDGE-IoT policies.			published in the catalogue.	policies and providing the intended functionality.
Sc.3	Interchangeable Common Services/ Sub-services	Multiple providers publish functionally equivalent services using the same data schema/APIs. Users can seamlessly swap one for another without re-engineering data flows—promoting plug-and-play upgrades and vendor-neutral deployments.	App Consumers	The App consumer needs to replace or upgrade an existing service with a new one of similar functionality.	1) Common interface/data schemas are defined (semantic interoperability). 2) Multiple equivalent services are available in the App Store. 3) User's existing workflows and connectors are already configured to consume these standardized services.	The user replaces one service with another having the same interface, maintaining data flows and workflows with minimal reconfiguration. The new service takes over under the same usage policies.

4.2 Steps – Scenarios

Scenario								
Scenario name:		**Sc. 1 – Publishing an App Process**						
Step No.	**Event**	**Name of process/ activity**	**Description of process/ activity**	**Service**	**Information producer (actor**	**Information receiver (actor)**	**Information Exchanged (IDs)**	**Requirement, R-IDs**
St.0	Determine if Connector requires Certification	0. Request Connector Certification Status	Data App Provider verifies if its connector is certified to publish a Data App on the HEDGE-IoT App Store.	CREATE	App Provider	App Provider Connector	Inf.00	SEC.2, SEC.4, O.X
St.1	Receive Connector Certification Status	1.Recieve Connector Notification Information	Data App Provider Receives the connector notification message with the up to date the Connector Certification status.	GET	App Provider Connector	App Provider	Inf. 01	SEC.2, SEC.4, D.2,, O.X
St.2	Determination that Certification is Required	2.Create Certification Requests	As certification is required, the provider instructs its local EDC Connector to assemble a certification request.	CREATE	App Provider	App Provider Connector	Inf. 02	SEC.2, SEC.4,, O.X
St.3	Connector Receives Instruction from App Provider	3. Send Certificate Request	Connector creates and sends a new request to the Certification Body.	CREATE	App Provider Connector	Certification Body	Inf. 03	SEC.2, SEC.4,, O.X
St.4	Certification Body receives certification request	4.Verify Request	The Certification Body checks the request and verifies the completeness and schedules the connector for security & interoperability testing.	EXECUTE	Certification Body	Certification Body	Inf. 04	SEC.2, SEC.4, D.2, O.X
St.5	Verification Request Approved	5.Perform Certification	Compliance tests are executed by the Certification Body in an isolated testbed; results are recorded	EXECUTE	Certification Body	Certification Body	Inf. 05	SEC.2, SEC.4, D.2, O.X
St.6	Certification Completed	6.Issue Certification	Upon successful tests, the Certification Body creates a signed digital certificate that attests the Connector's	CREATE	Certification Body	Certification Body	Inf. 06	SEC.2, SEC.4, D.2, O.X

			compliance level and returns it to the requester.					
St.7	Certificate Issued from Certification Body	7. Return Certificate Results	The Certification Body transmits the signed certificate back to the EDC Connector using IDS Response messages.	GET	Certification Body	App Provider Connector	Inf. 07	SEC.2, SEC.4, D.2, O.X
St.8	Certification Results Issued and Sent to Data App Producer	8. Received Certificate Results	The EDC Connector forwards the received certificate and report to the Data-App Provider	GET	App Provider Connector	App Provider	Inf. 08	SEC.2, SEC.4, D.2, O.X
St.9	Certification Results Successful	9.Create Push IDS App Image Request	The provider now commands the EDC Connector to push the container image to the designated App-Store registry, referencing the certificate ID in the request header.	CREATE	App Provider	App Provider Connector	Inf. 09	SEC.2, SEC.4, O.X
St.10	EDC Received Push Request from Daya App Producer	10.Send Push Request	The EDC Connector creates a Push-Request message that announces the forthcoming upload.	CREATE	App Provider Connector	App Store	Inf.10	SEC.2, SEC.4, O.X
St.11	EDC Pushes the App Image to App store	11.Receive IDS App Image	The App Store receives the container image stream from the connector, performs integrity checks.	CREATE	App Store	App Store	Inf.11	SEC.2, SEC.4, D.2, O.X
St.12	App Store Reives Valid App Image	12.Store IDS App Image	After validation, the App Store creates a new registry image in the App Container Registry.	CREATE	App Store	App Container Registry	Inf.12	SEC.2, SEC.4, O.X
St.13	App image received and stored	13. IDS App Image Stored	The registry reports successful storage by sending an acknowledgement.	REPORT	App Container Registry	App Provider Connector	Inf.13	SEC.2, SEC.4, O.X
St.14	Push Request Results Available and Routed via EDC Connector	14.Return Push Request Message	The EDC Connector relays the positive push result back to the Data-App Provider, completing the binary-upload phase.	GET	App Provider Connector	App Producer	Inf .14	SEC.2, SEC.4, D.2, O.X

St.15	Push Request Successful	15.Publish IDS App Request	The provider instructs the connector to publish the app's metadata to the App-Store catalogue.	CREATE	App Provider	App Provider Connector	Inf.15	SEC.2, SEC.4, D.5, O.X
St.16	EDC Received Publish Request from Daya App Producer	16.Send Publish Request	The EDC Connector sends a Publish-Request message with the metadata to the App Store.	CREATE	App Provider Connector	App Store	Inf.16	SEC.2, SEC.4, O.X
St.17	App Store Reives Valid App Metadata	17.Store IDS App Metadata	The App Store validates semantic fields, checks certificate references, then creates the metadata record into the App Store Database.	CREATE	App Store	App Store Database	Inf.17	SEC.2, SEC.4, O.X
St.18	App Metadata stored	18.IDS App Metadata Stored	The database returns a success message and the new App-ID; the App Store registers this ID in its self-description and notifies the connector that the entry is active.	REPORT	App Store Database	App Provider Connector	Inf.18	SEC.2, SEC.4, O.X
St.19	Publish Request Results Available and Routed via EDC Connector	19. Return Publish Request Results	The EDC Connector forwards the publish-result to the Data-App Provider. The app is now visible in the catalogue and ready for discovery by consumers.	GET	App Provider Connector	App Provider	Inf .19	SEC.2, SEC.4, D.2, O.X

Scenario								
Scenario name:		***Sc. 2 – Find/Retrieve/Reuse/Access a service/sub-service in the App Store***						
Step No.	***Event***	***Name of process/ activity***	***Description of process/ activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information Exchanged (IDs)***	***Requirement, R-IDs***
St.1	Data App needed by App Consumer	Determine App Store Query Capabilities	App Consumer identifies how to query the App Store	EXECUTE	App Consumer	App Consumer	Inf.20	SEC.2, SEC.4, O.X

St.2	Query capabilities determined	Create Query for App	App Consumer creates a query request to find a specific App in the App Store	CREATE	App Consumer	EDC Connector	Inf.21	SEC.2, SEC.4, O.X
St.3	App query received by EDC	Send Query to App Store	App Provider Connector creates a new query-message and pushes it to the App Store	CREATE	App Provider Connector	App Store	Inf.22	SEC.2, SEC.4, D.2, O.X
St.4	App query received by App Store	Process Query	App Store processes the received app query	EXECUTE	App Store	App Store	Inf.23	SEC.2, SEC.4, O.X
St.5	App Store processed query	Return Query Results	App Store returns query results back to the App Provider Connector	GET	App Store	App Provider Connector	Inf.24	SEC.2, SEC.4, D.2, O.X
St.6	App Provider Connector received query results	Receive Query Results	EDC forwards the query results to the App Consumer	GET	App Provider Connector	App Consumer	Inf.25	SEC.2, SEC.4, D.2, O.X
St.7	App Consumer received results	Identify App	App Consumer identifies desired app from query results	EXECUTE	App Consumer	App Consumer	Inf.26	SEC.2, SEC.4, O.X
St.8	Desired app identified	Request HEDGE-IoT App Metadata	App Consumer requests detailed metadata for the identified app from EDC	CREATE	App Consumer	App Provider Connector	Inf.27	SEC.2, SEC.4, O.X
St.9	Metadata request received by EDC	HEDGE-IoT App Identifier	EDC creates an App-metadata request and sends it to the App Store.	CREATE	App Provider Connector	App Store	Inf.28	SEC.2, SEC.4, O.X
St.10	Metadata request received by App Store	Request App Metadata	The App Store creates a metadata-lookup request for its Database	CREATE	App Store	App Store Database	Inf.29	SEC.2, SEC.4, O.X
St.11	Metadata request received by Database	Process App Metadata Request	Database processes and retrieves app metadata	EXECUTE	App Store Database	App Store Database	Inf.29	SEC.2, SEC.4, D.2, O.X
St.12	Database completed processing	Return Request Results	Database returns app metadata to App Store	GET	App Store Database	App Store	Inf.31	SEC.2, SEC.4, O.X

St.13	App metadata available at App Store	Send App Metadata	App Store sends retrieved app metadata to App Provider Connector	GET	App Store	App Provider Connector	Inf.27	SEC.2, SEC.4, O.X
St.14	EDC received metadata	Receive App Metadata	EDC sends app metadata to App Consumer	GET	App Provider Connector	App Consumer	Inf.27	SEC.2, SEC.4, D.2, O.X
St.15	App Consumer received metadata	Pull App Image	App Consumer requests app image downloads from App Provider Connector	CREATE	App Consumer	App Provider Connector	Inf.34	SEC.2, SEC.4, O.X
St.16	Image request received by EDC	HEDGE-IoT App Image Identifier	EDC creates and forwards an image-download request to the App Store	CREATE	App Provider Connector	App Store	Inf.29	SEC.2, SEC.4, O.X
St.17	App Store received app image request	Request App Metadata	The App Store creates a fetch-request message for the Container Registry	CREATE	App Store	App Container Registry	Inf.33	SEC.2, SEC.4, D.2, O.X
St.18	Image request received by Registry	Process App Image Request	App Container Registry processes request and prepares app image	EXECUTE	App Container Registry	App Container Registry	Inf.37	SEC.2, SEC.4, O.X
St.19	Registry processed app image request	Return Request Results	App Container Registry returns app image details to App Store	GET	App Container Registry	App Store	Inf.38	SEC.2, SEC.4, D.2, O.X
St.20	App Store received app image details	Send App Metadata	App Store sends app image details to App Provider Connector	GET	App Store	App Provider Connector	Inf.39	SEC.2, SEC.4, O.X
St.21	EDC received app image details	Receive App Metadata	EDC sends app image details to App Consumer	GET	App Provider Connector	App Consumer	Inf. 40	SEC.2, SEC.4, D.2, O.X

5 Information exchanged

Information exchanged			
Information exchanged (ID)	***Name of information***	***Description of information exchanged***	***Requirement, IDs***
Inf.00	Request Connector Certification Status	[HTTP] Request to query the status of a connector specified by its ID	O.X
Inf. 01	Receive Connector Notification Information	[HTTP] Status of a connector certification identified by its ID	O.X
Inf. 02	Create Certification Requests	[HTTP] Issue a certification request targeting the one instance of a connector	O.X
Inf. 03	Send Certificate Request	[HTTP] Summary of the certification request, including reference to the app with the data space identifier and app store registry internal identifier.	O.X
Inf. 04	Verify Request	[HTTP] Process Trigger	O.X
Inf. 05	Perform Certification	[HTTP] Certification process trigger	O.X
Inf. 06	Issue Certification	[HTTP] Trigger to issue a new certificate	O.X
Inf. 07	Return Certificate Results	[HTTP] Digital certificate, including the signature hashcode.	O.X
Inf. 08	Received Certificate Results	[HTTP] Result status of the certificate issue process. (can include the certificate as detailed in Inf.08)	O.X
Inf. 09	Create Push IDS App Image Request	[HTTP] Request to create a new App image, including the App internal identification, including name and version.	O.X
Inf.10	Send Push Request	[HTTP] Push OIC compliant App image	O.X
Inf.11	Receive IDS App Image	[HTTP] App image details and processing repository details.	O.X
Inf.12	Store IDS App Image	[HTTP] App binary content is received, processed, stored.	O.X
Inf.13	IDS App Image Stored	[HTTP] Confirmation and digest for OIC image stored.	O.X
Inf .14	Return Push Request Message	[HTTP] Confirmation of success of failure of process.	O.X
Inf.15	Publish IDS App Request	[HTTP] Request for visibility change and publication of the App.	O.X
Inf.16	Send Publish Request	[HTTP] Request for visibility change and publication of the App.	O.X
Inf.17	Store IDS App Metadata	[HTTP] App details and linked software images and version details.	O.X
Inf.18	IDS App Metadata Stored	[HTTP] Confirmation that App details and linked software images and version details where stored.	O.X
Inf .19	Return Publish Request Results	[HTTP] Confirmation that App details and linked software images and version details where stored.	O.X
Inf.20	Determine App Store Query Capabilities	[HTTP] Poll query mechanism for App store users.	O.X
Inf.21	Create Query for App	[HTTP] Create an app catalogue request targeting the App Store instance in the dataspace.	O.X
Inf.22	Send Query to App Store	[HTTP] Query of Apps in the dataspace catalogue, targeting the App store instance.	O.X

Inf.23	Process Query	[HTTP] List with App metadata available in the catalogue.	O.X
Inf.24	Return Query Results	[HTTP] List with App metadata available in the catalogue.	O.X
Inf.25	Receive Query Results	[HTTP] List with App metadata available in the catalogue.	O.X
Inf.27	App Metadata	App metadata available in the catalogue	O.X
Inf.28	HEDGE-IoT App Identifier	App identifier in the catalogue.	O.X
Inf.29	Request App Metadata	Issue request for App metadata.	O.X
Inf.31	Return Request Results	App metadata details	O.X
Inf.34	Pull App Image	Binary data of the App image together with the digest confirmation	O.X

ids:Message	Core ids:Message class with it's properties, which are equal for all messages. For communication in the IDS, the specific message types (second table, below) are used.		
Property	**Always mandatory property**	**Can have multiple values at the same time**	**Description**
modelVersion	✓		Information Model version, against which the Message should be interpreted
issued	✓		Date of issuing the message
correlationMessage			Correlated message. Usually needed, if a messages responds to a previous message. A Connector may, e.g., send a MessageProcessedNotification as a response to an incoming message and therefore needs this property to refer to the incoming message.
issuerConnector	✓		Origin Connector of the message
recipientConnector		✓	Target Connector
senderAgent	✓		Agent, which initiated the message
recipientAgent		✓	Agent, for which the message is intended
securityToken	✓		Token representing a claim, that the sender supports a certain security profile
authorizationToken			Authorization token
transferContract			Contract which is (or will be) the legal basis of the data transfer
contentVersion			Version of the content in the payload

IDS Message Types	The table contains descriptions for each message, information about the payload as well as changes in the properties, i.e., new properties and additional mandatory properties. "Message Class" and "Message Subclass" are just for structural / hierarchical description. The "Message Name" contains the actual Message which is used. New properties, which are mandatory are marked with an (*). Existing properties, which are mandatory for a specific message are listed in the corresponding column. **All mandatory property declarations of the core ids:Message above still hold**.

Message Class	Message Subclass (Abstract)	Message Name	Description
Request Messages		**RequestMessage**	Client-generated message initiating a communication, motivated by a certain reason and with an answer expected. May be used for messages, which are not covered by the core IDS messages.
		CommandMessage	Command messages are usually sent when a response is expected by the sender. Changes state on the recipient side. Therefore, commands are not 'safe' in the sense of REST.
		InvokeOperationMessage	Message requesting the recipient to invoke a specific operation.
		ContractRequestMessage	Message containing a suggested content contract (as offered by the data consumer to the data provider) in the associated payload (which is an instance of ids:ContractRequest).
		ArtifactRequestMessage	Message asking for retrieving the specified Artifact as the payload of an ArtifactResponse message.
		AccessTokenRequestMessage	Message requesting an access token. This is intended for point-to-point communication with, e.g., Brokers.
		QueryMessage	Query message intended to be consumed by specific components.
		DescriptionRequestMessage	Message requesting metadata. If no URI is supplied via the ids:requestedElement field, this message is treated like a self-description request and the recipient should return its self-description via an ids:DescriptionResponseMessage. However, if a URI is supplied, the Connector should either return metadata about the requested element via an ids:DescriptionResponseMessage, or send an ids:RejectionMessage, e.g. because the element was not found
		ParticipantRequestMessage	This class is deprecated. Use ids:DescriptionRequestMessage instead. Message asking for retrieving the specified Participants information as the payload of an ids:ParticipantResponse message.
		UploadMessage	Message used to upload a data to a recipient. Payload contains data

		AppRegistrationRequestMessage	Message that asks for registration or update of a data app to the App Store. Payload contains app-related metadata (instance of class ids:AppResource). Message header may contain an app identifier parameter of a prior registered data app. If the app identifier is supplied, the message should be interpreted as a registration for an app update. Otherwise, this message is used to register a new app.
		AppUploadMessage	Message that usually follows a AppRegistrationResponseMessage and is used to upload a data app to the app store. Payload contains data app. Note that the message must refer to the prior sent, corresponding AppResource instance. The IRI of the ids:appArtifactReference must must match the IRI of the artifact which is the value for the ids:instance property. The ids:instance is specific for each representation. Therefore, if someone wants to upload multiple representations for an app, he has to state them using multiple ids:instance properties inside the AppRepresentation (and therefore inside the AppResource). Otherwise, no mapping between payload and app metadata can be achieved.
ResponseMessage		**ResponseMessage**	Response messages hold information about the reaction of a recipient to a formerly sent command or event. They must be correlated to this message. May be used for messages, which are not covered by the core IDS messages.
		ArtifactResponseMessage	Message that follows up a ArtifactRequestMessage and contains the Artifact's data in the payload section.
		AccessTokenResponseMessage	Response to an access token request, intended for point-to-point communication.
		ContractAgreementMessage	Message containing a contract, as an instance of ids:ContractAgreement, with resource access modalities on which two parties have agreed in the payload.
		ContractResponseMessage	Message containing a response to a contract request (of a data consumer) in form of a counter-proposal of a contract in the associated payload (which is an instance of ContractOffcer).
		ResultMessage	Result messages are intended to annotate the results of a query command.
		RejectionMessage	Rejection messages are specialized response messages that notify the sender of a message that processing of this message has failed.
		OperationResultMessage	Message indicating that the result of a former InvokeOperation message is available. May transfer the result data in its associated payload section
		ParticipantResponseMessage	This class is deprecated. Use ids:DescriptionResponseMessage instead.

			ParticipantResponseMessage follows up a ParticipantRequestMessage and contains the Participant's information in the payload section.
		ContractRejectionMessage	Message indicating rejection of a contract.
		DescriptionResponseMessage	Message containing the metadata, which a Connector previously requested via the ids:DescriptionRequestMessage, in its payload.
		UploadResponseMessage	Message that follows up a UploadMessage and contains the upload confirmation.
		AppUploadResponseMessage	Message that follows up an AppUploadMessage and contains the app upload confimation.
		AppRegistrationResponseMessage	Message that follows up an AppRegistrationRequestMessage and contains the app registration confimation.
NotificationMessage		**NotificationMessage**	Notification messages are informative, and no response is expected by the sender. May be used for scenarios, which are not covered by the core IDS messages.
		LogMessage	Log Message which can be used to transfer logs e.g. to the clearing house.
		ContractOfferMessage	Message containing a offered content contract (as offered by a data provider to the data consumer) in the associated payload (which is an instance of ContractOffer). In contrast to the ids:ContractResponseMessage, the ids:ContractOfferMessage is not related to a previous contract request.
		ContractSupplementMessage	Message containing supplemental information to access resources of a contract.
		MessageProcessedNotificationMessage	Notification that a message has been successfully processed (i.e., not ignored or rejected).
		OperationResultMessage	Message indicating that the result of a former InvokeOperation message is available. May transfer the result data in its associated payload section.
		RequestInProcessMessage	Notification that a request has been accepted and is being processed.
	ConnectorNotificationMessage	**ConnectorInactiveMessage**	Event notifying the recipient(s) that a connector will be unavailable. The same connector may be available again in the future
		ConnectorUpdateMessage	Event notifying the recipient(s) about the availability and current configuration of a connector. The payload of the message must

			contain the updated connector's self-description
		ConnectorCertificateGrantedMessage	Whenever a Connector has been successfully certified by the Certification Body, the Identity Provider can use this message to notify Infrastructure Components.
		ConnectorCertificateRevokedMessage	Indicates that a (previously certified) Connector is no more certified. This could happen, for instance, if the Certification Body revokes a granted certificate or if the certificate has just expired.
	ResourceNotification Message	**ResourceUnavailableMessage**	Message indicating that a specific resource is unavailable. The same resource may be available again in the future.
		ResourceUpdateMessage	Message indicating the availability and current description of a specific resource. The resource must be present in the payload of this message.
	AppNotification Message	**AppAvailableMessage**	Message indicating that a specific App should be available (again) in the AppStore.
		AppUnavailableMessage	Message indicating that a specific App should be unavailable in the AppStore.
		AppDeleteMessage	Message indicating that an App should be deleted from the AppStore.
	ParticipantNotification Message	**ParticipantUnavailableMessage**	Event notifying the recipient(s) that a participant will be unavailable. The same participant may be available again in the future.
		ParticipantUpdateMessage	Event notifying the recipient(s) about the availability and current description of a participant. The payload of the message must contain the participant's self-description
		ParticipantCertificateGrantedMessage	Whenever a Participant has been successfully certified by the Certification Body, the Identity Provider can use this message to notify Infrastructure Components
		ParticipantCertificateUnavailableMessage	Indicates that a (previously certified) Participant is no more certified. This could happen, for instance, if the Certification Body revokes a granted certificate or if the certificate has just expired.

6 Requirements

Quality of Service Requirements		
Categories ID	***Category name for requirements***	***Category description***
QoS	Quality of Service	Generic properties that service/SUC should provide – quality attributes.
Requirement ID	***Requirement name***	***Requirement description***
QoS.1	Elapsed time response requirements for exchanging data	More than 10 seconds
QoS.2	Availability of information flows	Continuous availability not required but must be available at specific times or under specific conditions
QoS.3	Accuracy of data requirements	Adequate accuracy can be assumed
QoS.4	Frequency of data exchanges	Upon event

Security Requirements		
Categories ID	***Category name for requirements***	***Category description***
Sec	Security	Authentication of user, confidentiality, integrity, prevention of denial of service, non-repudiation or accountability, error management.
Requirement ID	***Requirement name***	***Requirement description***
Sec.2	Eavesdropping	Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is: Quite important
Sec.4	Authentication and Access Control mechanisms commonly used with this data exchange	Public key encryption (e.g. SSL/TLS)

Data Management Requirements		
Categories ID	***Category name for requirements***	***Category description***
D	Data Management	Type of source of data, correctness or validity of data, timeliness or time stamping of data, volume of data, synchronization, or consistency of data across systems, timely access to data, validation of data across organizational boundaries, transaction management, data naming, identification, formats across disparate systems, maintenance of data and databases.
Requirement ID	***Requirement name***	***Requirement description***
D.2	Correctness of source data	Source data is always correct (e.g. by definition)
D.5	Management of data across organizational boundaries	Data exchanges go across organizational boundaries

D.6	Data maintenance effort: human versus automation	Data maintenance is mostly automated but requires occasional intervention

Discovery and Configuration Requirements		
Categories ID	***Category name for requirements***	***Category description***
Conf	Configuration	Locations, distances, communication layout, commonly used communication protocol media, network bandwidth, existing protocols, number of devices, systems, volume of data items, expected growth, etc.
Requirement ID	***Requirement name***	***Requirement description***
Conf.2	Distance between entities	Varies and/or is not relevant
Conf.3	Number of Information Producers	Few to a hundred
Conf.4	Number of Information Receivers	Two to a few
Conf.6	Data exchange methods	Other: REST API (client-server)
Conf.7	Communication access services requirements	Request-response
Conf.8	Commonly used communication protocol	Natively REST, other protocols (e.g., MODBUS, MQTT) supported via semantic adapters.

Other Requirements		
Categories ID	***Category name for requirements***	***Category description***
O	Regulatory obligation related to privacy	2016/679 GDPR (General Data Protection Regulation)
Requirement R-ID	***Requirement name***	***Requirement description***
O.2	Personal data use	Personal data may not be processed unless there is at least one legal basis to do so.
O.3	Right to access, rectify, erasure, restriction	Data retention policy outlines the specific sensitive time period data can be retained, plus how it will be disposed of when the time to do so comes.
O.4	Data transfer consent	The data subject shall have the right to obtain from the controller without undue delay the access/rectification/erasure/restriction of inaccurate personal data concerning him or her.
O.5	Data retention policy	Personal data may not be transferred to a third-party if the data subject did not agree and the third party provide appropriate safeguard.
O.X	All constraints also apply.	All requirements in this category.

7 Common Terms and Definitions

Common Terms and Definitions	
Term	**Definition**
App Container Registry	A secure repository that stores and serves container images (e.g., Docker/OCI images) for download by authorised connectors.
App Metadata	The JSON-LD (or equivalent) description of an app: name, version, licence, required inputs/outputs, semantic tags, certification status, etc.
App Store	The marketplace component of the dataspace that lets participants publish, discover, and download certified data-apps and related services.
App Store Database	The internal catalogue that holds all published app-metadata records, making them searchable for users and connectors.
Certification Body	An independent organisation that tests and certifies apps or connectors for security, interoperability and compliance with IDS rules.
Container Image	A packaged, runnable file system (e.g., OCI/Docker image) that contains all binaries and dependencies required to execute an app.
Data Consumer	A participant that retrieves data or services from the dataspace under agreed usage policies.
Data Provider	A participant that offers data assets or services to other parties through an IDS-compliant connector and usage policies.
Dataspace	A federated, governed data-exchange ecosystem where sovereign data sharing occurs via certified IDS connectors and common policies.
EDC (Eclipse Dataspace Connector)	An open-source implementation of an IDS Connector used to connect participants, enforce usage control and host apps.
IDS (International Data Spaces)	A reference architecture, specification and governance model enabling secure, sovereign and interoperable data sharing.
Metadata	Descriptive information about a resource (data asset or app) that enables catalogue search, discovery and correct technical use.
Semantic Interoperability	The ability of systems to exchange data/app interfaces with unambiguous, shared meaning, enabled by common vocabularies and ontologies.
Usage Policy	A machine-readable rule set (e.g., ODRL profile) that defines how, by whom, and under what conditions data or apps may be used.
Vocabulary Provider	A service that curates and exposes controlled vocabularies or ontologies so that all participants use consistent terms.

HEDGE-IoT