HEDGE-IoT

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

D4.2

HEDGE-IoT Interoperability Framework and Integrated Solution (Intermediate 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.	D4.2							
Deliverable Title	Digital Interoperability Framework and Integrated Solution							
Work-Package No.	WP4							
Work-Package Title	HEDGE-IoT Interoperability Framework and Integrated Solution (Intermediate release)							
Lead Beneficiary	DST							
Main Author	DST							
Other Authors	ED, TNO, TRIALOG, INESC							
Due date	30/09/2025							
Deliverable Type		Document, Report (R)		Data management plan (DMP)		Websites, press & media action (DEC)	X	Other
Dissemination Level	X	Public (PU)		Sensitive (SEN)		Classified		
	PU: Public, fully open SEN: Sensitive, limited under the conditions of the Grant Agreement							

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.

	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	25/06/2025	First ToC	Antonella Cadeddu (DST) DST
0,2	02/07/2025	ToC revisions	All WP4 partners
0.3	10/07/2025	Final ToC, structure and guidelines	Antonella Cadeddu (DST) Giovanni Natale (DST)
0.4	30/07/2025	First partners' contribution	Antonella Cadeddu (DST) Giovanni Natale TNO ED TRIALOG
005	27/08/2025	Consolidation	Antonella Cadeddu (DST) Giovanni Natale (DST)
0.6	30/09/2025	Second partner's contributions	Apostolos Kapetanios (ED) Lenos Peratitis (ED) Cornelis Bouter (TNO) Laura Daniele (TNO) Léo Cornec (TRIALOG) Fábio Coelho (INESC)
0.7	03/10/2025	Consolidation	Antonella Cadeddu (DST) Giovanni Natale (DST)
0.8	06/01/2025	Third partner's contributions	Apostolos Kapetanios (ED) Lenos Peratitis (ED) Cornelis Bouter (TNO) Laura Daniele (TNO) Léo Cornec (TRIALOG) Fábio Coelho (INESC)
0.9	08/10/2025	Consolidation and final touches	Antonella Cadeddu (DST) Giovanni Natale (DST)
0.10	15/10/2025	Review by VVT	Muhammad Faheem (VVT)
0.11	20/10/2025	Review by QUE	Thanos Kalamaris (QUE)
0.12	23/10/2025	Review by ED	Lenos Peratitis (ED) Nikos Bilidis (ED)
1.0	30/10/2025	Processing of reviewers' comments and Full complete version	Antonella Cadeddu (DST) Giovanni Natale (DST)

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

EXECUTIVE SUMMARY

HEDGE-IoT (Holistic Approach towards Empowerment of the Digitalization of the Energy Ecosystem through adoption of IoT solutions) is a flagship project funded under the European Union's Horizon Europe research and innovation program. The initiative aims to deliver a state-of-the-art, interoperable digital framework for the energy sector, enabling the seamless deployment of Internet of Things (IoT) assets across the entire energy ecosystem — from Transmission System Operators (TSOs) to behind-the-meter applications.

This document provides a clear and comprehensive overview of the progress and key achievements of Work Package 4 (WP4) within the HEDGE-IoT project, covering the period from Month 15 to Month 21.

It reports on the Second Technology Release, which builds upon the initial prototype described in Deliverable D4.1 and presents an updated set of interoperability enablers, architectural refinements, and functional extensions.

In particular, this deliverable describes:

- The enhancement of the Interoperability Middleware, including the evolution of the Eclipse Dataspace Connector (EDC)-based architecture and its integration with the Federated Catalogue and Knowledge Engine;
- The expansion of the Open Services Catalogue, providing new APIs, data exchange workflows, and early validation feedback from pilot sites;
- The advancements in Semantic Interoperability, detailing the consolidation of common ontologies and semantic tools (e.g., TKE, SEF, ODCT);
- The updated Cloud-Edge orchestration layer, supporting multi-node deployments and secure data transfers;
- The reinforcement of Security and Privacy mechanisms, aligned with the project's Cross-Cutting Characteristics Plan (X-CCP).

Overall, D4.2 marks a significant step forward from the first release, providing a more mature, integrated, and deployable technical framework for the HEDGE-IoT dataspace 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.

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.

ABBREVIATIONS

Abbreviation	Full description
AI	Artificial Intelligence
AIOTI	Alliance for Internet of Things Innovation
API	Application Programming Interface
BDD	Behavior-Driven Development
BiLSTM	Bidirectional Long Short-Term Memory
BPMN	Business Process Model and Notation
BSM	Behavioral State Manager
BSP	Balancing Service Provider
CAI	Conformity Aspect of Interest
CD	Committee Draft (ISO stage)
CEEDS	Clean Energy Ecosystem Data Spaces
CGMES	Common Grid Model Exchange Standard
CIM	Common Information Model
COC	Code Of Conduct
DLR	Dynamic Line Rating
DSO	Distribution System Operator
DTR	Dynamic Thermal Rating
EDC	Eclipse Dataspace Connector
EEBUS	European Energy Bus
EMS	Energy Management System
ESA	Energy Smart Appliance
ETSI	European Telecommunications Standards Institute

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.

HEDGE-IoT	Holistic Energy Decentralised Grid for Enhanced IoT
ICSC	International Conference on Semantic Computing
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
JRC	Joint Research Centre
JTC	Joint Technical Committee
KE	Knowledge Engine
LSTM	Long Short-Term Memory
MQTT	Message Queuing Telemetry Transport
MVD	Multi-View Data (Dashboard)
NILM	Non-Intrusive Load Monitoring
OCPP	Open Charge Point Protocol
ODC	Ontology-Driven Constraint
ODCT	Ontology-Driven Constraint Tester
OWL	Web Ontology Language
RA	Reference Architecture
RDF	Resource Description Framework
SAREF	Smart Applications REFerence ontology
SEF	Semantic Enabler Framework
SGAM	Smart Grid Architecture Model
SHACL	Shapes Constraint Language
SIF	Semantic Interoperability Framework
SPARQL	SPARQL Protocol and RDF Query Language
SPINE	Smart Premises Interoperable Neutral-message 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.

STH	Semantic Treehouse
TKE	The Knowledge Engine
TLS	Transport Layer Security
TSO	Transmission System Operator
UI	User Interface
UML	Unified Modeling Language
URL	Uniform Resource Locator
V2G	Vehicle-to-Grid
WP	Work Package
X-CCP	Cross-Cutting Characteristics Plan

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

The HEDGE-IoT project continues to advance its mission of transforming the interaction between data and digital services in distributed environments, with a strong emphasis on the energy sector. Building upon the foundations laid in the previous phase, the project is now entering a stage of consolidation and validation of its interoperability framework. By leveraging Artificial Intelligence (AI), Internet of Things (IoT), and cloud/edge computing, HEDGE-IoT is progressively shaping an interoperable and intelligent data-sharing ecosystem that enhances data-driven decision-making and optimizes energy management across stakeholders.

Within this framework, Work Package 4 (WP4) plays a central role in designing, implementing, and validating the digital enablers required for seamless integration. The previous deliverable introduced the first operational version of these enablers, including the Eclipse Dataspace Connector (EDC)-based middleware, the Open Services Catalogue and App Store, and the semantic interoperability layer based on standardized ontologies such as ETSI SAREF and IEC CIM.

This new deliverable extends those results by presenting further developments, refinements, and integrations. Specifically, WP4 has focused on:

- Consolidating the EDC-based architecture, ensuring compliance with European Data Spaces requirements and strengthening scalability and security.
- Expanding the Open Services Catalogue and App Store with additional functionalities for service discovery, registration, and deployment.
- Validating the semantic interoperability mechanisms with practical use cases and cross-sector data alignment.
- Enhancing cybersecurity and privacy measures, with particular emphasis on risk assessment and mitigation in distributed IoT contexts.

The outcome of these activities is a more mature interoperability framework, validated through initial deployments and pilot scenarios. This represents a significant step forward in ensuring that HEDGE-IoT not only provides technical solutions but also delivers an operational and replicable model for cross-domain data spaces in the energy sector and beyond.

1.1 PURPOSE OF THE DOCUMENT

This document, Deliverable D4.2, represents the continuation of the HEDGE-IoT project's effort to create a robust, scalable, and interoperable framework for the IoT energy ecosystem. Building on the foundations established in Deliverable D4.1, this report focuses on consolidating the interoperability framework and validating its core components through enhanced implementations and initial pilot integrations.

The main objectives of this document are to:

- Present the refined design and implementation of the interoperability framework, highlighting improvements in the Interoperability Middleware, Semantic Interoperability Framework, and Open Services Catalogue.
- Provide updated architecture specifications, including technical enhancements that

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.

strengthen scalability, security, and compliance with European Data Spaces principles.

- Report on the integration and validation activities carried out with selected pilots, demonstrating the operational maturity of the framework in realistic scenarios.
- Detail the advancements in methodologies, standards, and tools adopted to reinforce data sovereignty, privacy, and interoperability across heterogeneous IoT platforms and AI-driven services.
- Serve as a reference for the next project phase, which will concentrate on large-scale validation, broader integration of services, and preparation for cross-sector replication.

1.2 Document structure

The deliverable is organised into seven main sections, each focusing on a distinct yet complementary aspect of the project's technical and architectural evolution. Together, these sections provide a coherent narrative of how the interoperability framework has matured since the previous release, linking design choices with practical validation in pilots and preparing the ground for large-scale deployment.

- **Section 1 – Introduction-**This deliverable provides the second release of the HEDGE-IoT interoperability framework, capturing the evolution of technical components, semantic enablers, and validation activities across pilots. The document highlights both the architectural refinements and the functional progress achieved, while also outlining the alignment with European standards and dataspace initiatives.
- **Section 2 – Interoperability Middleware** introduces the updated middleware architecture and the prototype of the MVD Data Dashboard, including its core components: assets, contracts, policies, catalogues, and transfers.
- **Section 3 – Open Services Catalogue and App Store** presents service-layer improvements, such as upgrades to the API gateway, new deployment features, and early feedback from pilot use.
- **Section 4 – Semantic Interoperability** reviews the evolution of semantic models across the project pilots and the role of enablers and tools such as Semantic Treehouse, ODCT, TKE/SIF/SEF, and PowerCIM.
- **Section 5 – IoT Cloud/Edge System Integration** outlines the refined methodology, validated through pilots, and provides a roadmap towards full interoperability.
- **Section 6 – Security and Privacy** reports on the Cross-Cutting Characteristics Plan (X-CCP), including workshops on AI trustworthiness, pilot results, and the development of trustworthiness profiles.
- **Section 7 Conclusions** - The results achieved in this deliverable demonstrate the project's tangible progress from a conceptual framework (D4.1) to a set of validated prototypes and integration flows (D4.2). The document concludes with a synthesis of achievements, an outlook on forthcoming activities, and annexes containing supplementary technical material.

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. INTEROPERABILITY MIDDLEWARE – UPDATED ARCHITECTURE

2.1 Introduction to the App Integration Flow within the Dataspace Connector

The integration of an application within the HEDGE-IoT Dataspace Connector represents a fundamental step towards enabling a seamless, secure, and standardised interaction between external services and the core dataspace infrastructure. This process ensures that applications can publish, discover, and consume data assets while remaining fully compliant with the governance, policy, and interoperability principles defined in the project.

The integration flow starts with the preparation of the application environment, which must be deployed in an OCI-compliant container format (e.g., Docker image) to guarantee portability and compatibility with the connector runtime. The connector itself operates on a dual-plane architecture — control plane for contract negotiation and policy enforcement, and data plane for actual data exchange — ensuring both legal and technical compliance of all interactions.

Once deployed, the application communicates with the dataspace connector through its internal API, leveraging programmatic clients to initiate secure data sharing operations.

This includes:

- Publication of data assets with standardized metadata.
- Application of usage policies and contractual terms for data governance.
- Discovery and negotiation with other dataspace participants.
- Execution of transfers using secure and auditable communication channels.

The integration flow therefore guarantees that applications are not only functionally connected but also aligned with interoperability and trust requirements. This methodology promotes scalability, reusability, and cross-domain adoption of services within the HEDGE-IoT ecosystem.

The source code related to the developments described in this section is available in the public repository at the following link:
https://github.com/HEDGE-IoT/mvd

A detailed, step-by-step description of the integration process, including configuration guidelines, client libraries, and deployment examples, is provided in Annex B EDC Integration Playbook

2.2 MVD Data Dashboard

As part of the development of the Minimum Viable Dataspace (MVD), a dedicated data dashboard has been implemented to provide a clear and immediate overview of the connector's status and activities. The dashboard consolidates essential system metrics, contract information, and transfer statistics into a unified visual environment, thereby facilitating both operational monitoring and technical validation during pilot testing.

The current version of the MVD Data Dashboard represents a prototype still under active

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.

development. At this stage, the dashboard is not yet integrated with the operational Minimum Viable Dataspace (MVD); instead, all values and records displayed are mock data, serving as illustrative examples for the interface and functionality.

It is important to note that the features presented in this release are subject to change: certain functionalities may be simplified or removed in future iterations, while others will be refined or expanded based on project requirements and stakeholder feedback. The dashboard therefore provides a preview of the intended capabilities, offering insights into how data assets, contracts, policies, and transfers could be monitored and managed through a unified interface.

The following subsections present the different pages of the dashboard, highlighting their role within the broader dataspace lifecycle and illustrating the current design direction.

Figure 1 presents the main landing page of the dashboard. It enables stakeholders to quickly assess the health and usage of the connector through the following key sections:

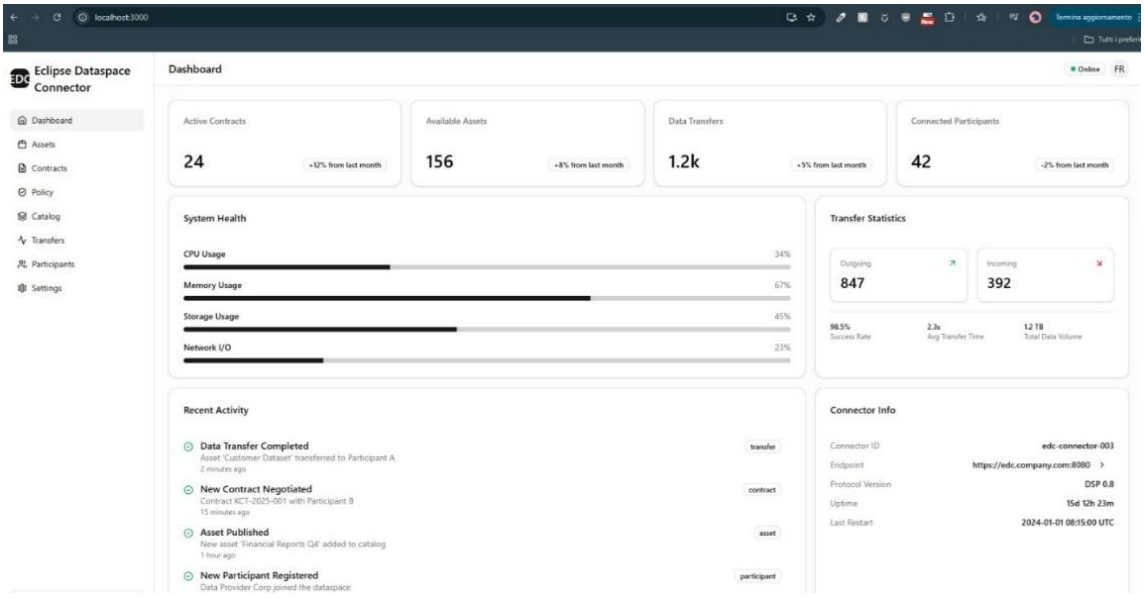


FIGURE 1:MVD DASHBOARD LENDING PAGE

- **Summary Indicators**: A set of top-level metrics shows the current number of active contracts, available assets, completed data transfers, and connected participants. Each indicator also provides a comparison with the previous month, highlighting trends
- **System Health**: Resource utilisation is continuously monitored, with visual bars reporting CPU usage, memory usage, storage usage, and network I/O. These indicators allow early detection of potential bottlenecks and provide transparency on connector performance.
- **Transfer Statistics**: Outgoing and incoming data flows are displayed, together with performance metrics such as success rate, average transfer time, and cumulative data volume exchanged.
- **Recent Activity**: A chronological feed lists the most recent actions performed by the connector, such as data transfers, contract negotiations, asset publications, and new participant registrations. This feature ensures full traceability of connector operations.

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.

- **Connector Information**: Technical details are included, such as the connector ID, endpoint URL, protocol version, uptime, and last restart timestamp.

2.3 Data Assets

The Data Assets section of the MVD dashboard allows users to manage datasets and resources that are made available within the dataspace. A data asset represents the fundamental digital entity that can be shared, discovered, and consumed across participants. Each asset is described through metadata such as its name, content type, version, status, and keywords, ensuring that information is structured and easily searchable.

Figure 2 shows the Asset Catalog interface, where all registered assets are listed. The dashboard provides summary indicators on the total number of assets, the variety of content types (e.g., JSON, CSV, Parquet, YAML), and the most recent version available.

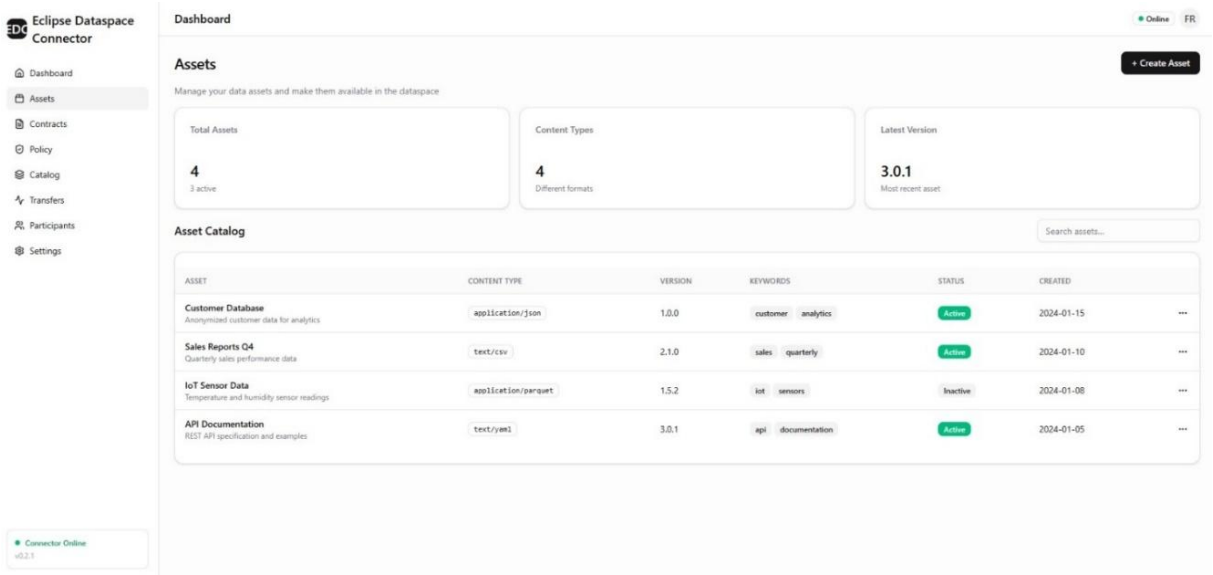


FIGURE 2:MVD DASHBOARD DATA ASSET

For each asset, the catalog details include:

1. **Name and Description:** e.g., Customer Database (anonymized customer data), IoT Sensor Data (temperature and humidity readings).
2. **Content Type:** Specifies the data format, supporting interoperability with multiple systems.
3. **Versioning:** Each dataset can evolve, with version numbers ensuring traceability and reproducibility.
4. **Keywords:** Metadata tags (e.g., analytics, sales, IoT) support discoverability.
5. **Status:** Assets can be active or inactive, enabling selective availability within the dataspace.
6. **Creation Date:** Timestamp of when the asset was published.

This structured approach ensures that data assets are well-described, discoverable, and controllable, reinforcing both usability and governance within the Minimum Viable Dataspace. By

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.

combining metadata-driven descriptions with policy-based governance, the MVD enables transparent and secure data sharing across all participants.

2.4 Contracts

Within a Minimum Viable Dataspace (MVD), a contract represents the formal agreement that governs how a specific data asset can be accessed and used by a participant. While policies define the conditions and constraints (e.g., access, usage, retention), the contract is the operational instance that binds a data provider and a consumer under those rules, making data exchange both technically enforceable and legally compliant.

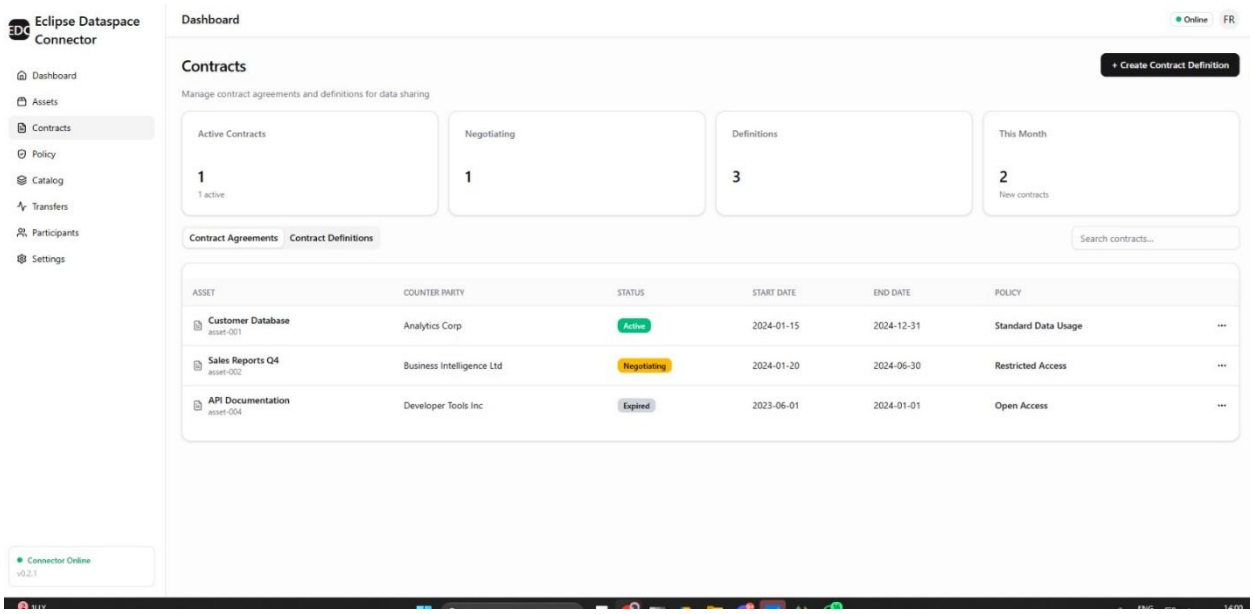


FIGURE 3:MVD DASHBOARD CONTRACTS

Figure 3 shows the Contracts dashboard, which allows users to manage all ongoing and past agreements. The interface provides:

- **Summary indicators** on active contracts, ongoing negotiations, and contract definitions.
- **Contract list** detailing each agreement, including the linked asset, the counterparty, current status (*active*, *negotiating*, or *expired*), start and end dates, and the policy applied.
- **Lifecycle visibility**, enabling users to track the entire contract process, from definition to activation and eventual expiration.

From this page, users can therefore initiate, monitor, and manage data sharing agreements. This ensures that all transactions within the MVD are transparent, auditable, and aligned with the dataspace's trust framework.

2.5 Policies

In the context of a dataspace, policies define the rules and constraints governing how data assets can be accessed, shared, and used by participants. They represent the enforcement layer that ensures trust, compliance, and contractual validity in all data transactions. While assets describe

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.

what data is available, policies describe *how* that data can be consumed.

There are different categories of policies, such as:

- **Access Policies** – rules specifying authentication or authorisation requirements for accessing an asset.
- **Usage Policies** – conditions that determine the scope and limitations of use, such as retention periods, anonymisation requirements, or jurisdictional constraints.
- **Contract Policies** – binding terms that link policies to contractual agreements between parties.

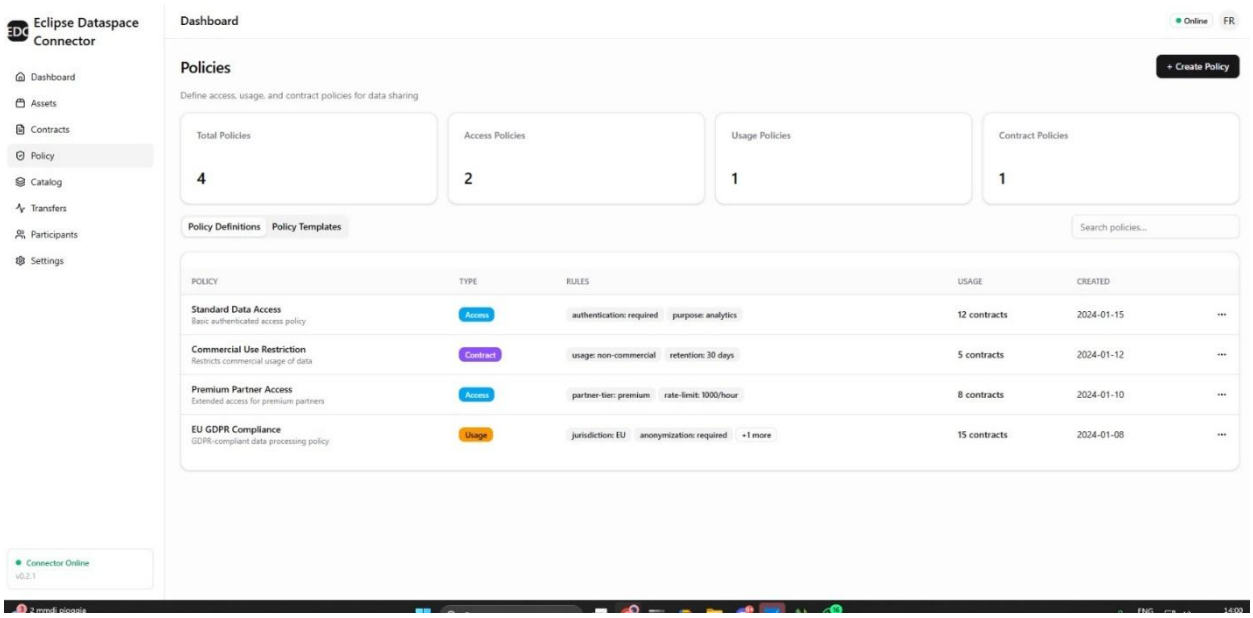


FIGURE 4:MVD DATADASHBOARD POLICIES

Figure 4 shows the Policies dashboard, which provides an overview of all configured policies, their type, rules, usage, and creation date. From this page, users can:

- Create and manage new policies.
- Associate policies with specific data assets.
- Define constraints such as authentication requirements, usage limitations (e.g., non-commercial), or compliance with GDPR.
- Monitor policy usage across existing contracts, ensuring transparency and enforceability.

By managing policies through this interface, the MVD guarantees that data sharing is not only technically feasible but also secure, compliant, and aligned with the agreed governance framework.

2.6 Dataset Catalog

The Catalog page provides a federated view of all available data assets within the dataspace, allowing users to browse and discover datasets published by different providers. Unlike the 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.

Assets page—which is dedicated to managing one's *own* data assets (creation, editing, activation/deactivation)—the Catalog is designed exclusively for exploration and discovery.

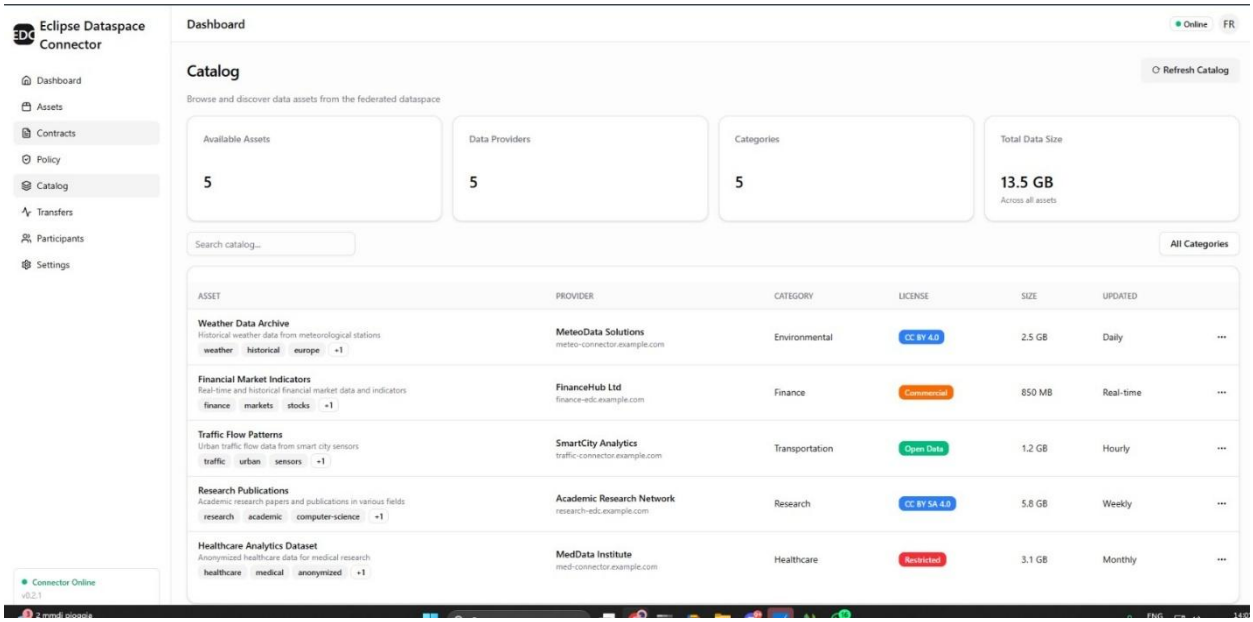


FIGURE 5:MVD DATADASHBOARD CATALOG

As shown in Figure 5, the dashboard summarises the number of available assets, data providers, categories, and the total volume of data currently accessible in the dataspace. Each listed asset includes detailed metadata such as:

- **Provider** – the organisation making the asset available.
- **Category** – thematic grouping (e.g., Finance, Transportation, Healthcare).
- **License type** – ranging from open data (e.g., *CC BY 4.0*) to restricted or commercial licenses.
- **Data size and update frequency** – indicating how large the dataset is and how often it is refreshed (e.g., real-time, hourly, weekly).
- **Keywords** – descriptive tags to facilitate search and filtering.

The Catalog therefore acts as the marketplace of the dataspace, enabling participants to discover data relevant to their use cases and assess its availability, licensing, and quality before initiating contracts or transfers.

2.7 Transfers

The Transfers page provides an overview of all ongoing and past data exchange operations within the Minimum Viable Dataspace (MVD). From here, users can monitor the lifecycle of each transfer, gaining visibility on both technical progress and contractual compliance.

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.

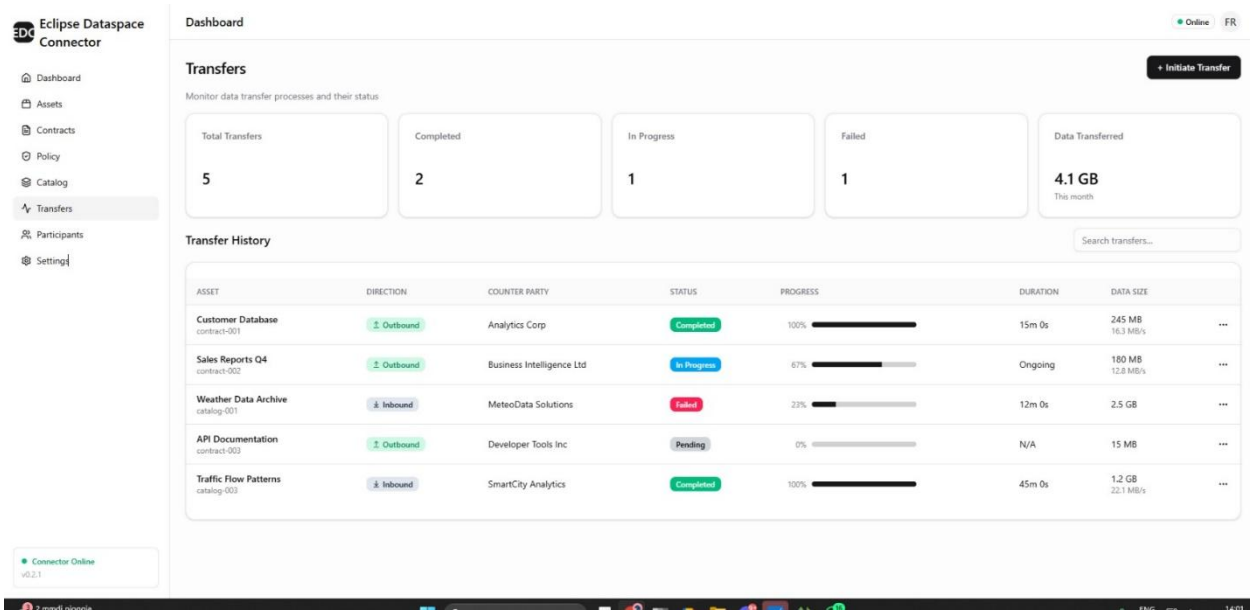


FIGURE 6:MVD DASHBOARD TRANSFER

As shown in Figure 6, the dashboard summarises the number of:

- **Total Transfers** initiated.
- **Completed** transfers successfully finalised.
- **In Progress** transfers still ongoing.
- **Failed** transfers where issues have occurred.
- **Total Data Volume** exchanged during the current period.

The Transfer History table lists each transaction with detailed metadata, including:

1. **Asset name** – the dataset being transferred.
2. **Direction** – inbound (received from another participant) or outbound (sent to another participant).
3. **Counterparty** – the partner organisation involved in the transaction.
4. **Status and Progress** – with real-time indicators (e.g., *Completed*, *In Progress*, *Failed*, *Pending*).
5. **Duration and Data Size** – showing how long the transfer took and the volume of data exchanged.

This functionality ensures traceability and transparency across the entire data exchange process, enabling users to quickly identify bottlenecks, verify contract execution, and monitor the health of data flows. By centralising transfer monitoring in a single interface, the MVD dashboard provides not only operational oversight but also a foundation for auditing and trust-building within the dataspace, ensuring that data exchanges remain secure, reliable, and compliant with defined policies and contracts.

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.

All the source code related to the technical developments described in this section is available in the public repository at the following link:

https://github.com/HEDGE-IoT/mvd-data-dashboard

3. OPEN SERVICES CATALOGUE AND APP STORE – SECOND ITERATION

In this deliverable (D4.2), the Open Services Catalogue and the App Store are presented as a single application, allowing the registration, search, download and integration with the EDC-based data space connector. This section presents the architectural enhancements introduced since D4.1, including conceptual integration with the satellite components required to support the App Store running capacity. Moreover, the section characterizes the details that support one *App* and showcases the available user interface mocks available. As part of the integration with the EDC connector, we undergo a review of the ongoing options to propose the concept of App in the scope of the new Data Space Protocol (DSP). Finally, we introduce an EDC compliant applicational client, which provides the possibility to programmatically interface with the EDC connector. Table 1 overviews the deployment roadmap, including the simplified functionality backlog.

TABLE 1 - APP STORE FUNCTIONALITY ROADMAP

Component	App Store
Alpha Version Functionalities	Register Apps Remove Apps Preliminary Integration with EDC Connector Publish App Publish App Metadata Search Apps
Beta Version Functionalities	Integration with code repository for integrated build view Consolidated App metadata encoded through the DSP Deployable applications are available in the App Store. Fully Operational Setup

Currently the App Store has an operational alpha version, which provides essential functionalities. The integration required to make it fully operational within the dataspace will be released in the coming months and will be reported in D4.3.

3.1 Architecture Enhancements

The architecture for the App Store evolved mainly on the side of the integration with the EDC connector, particularly in the core consideration of what a Data Space App is under the new DSP version. The current version of the DSP installs two new and relevant layers in the architecture of the dataspace connector, namely: the control and data plane. They establish a logical separation between the control and operation flow cycle for all data exchanges. The control plane establishes

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 sharing contracts among dataspace participants and their data assets or applying data usage policies to those data assets to impose usage limits in terms of time and purpose among others. This plane ultimately provides cryptographical signatures as tokens, that are used onwards in the actual data exchange. The data plane is responsible for handling all the data exchange process, considering the exchange permission tokens maintained in the control plane. The sole focus of this latter plan is to support specific transport layer level (as per the OSI applicational representation) operations, allowing for specialization of these operations depending on the option of the underlying protocol. This means that specific data planes will exist for HTTP communication, S3 object-storage, MQTT-based, among others. This architectural decision provides flexibility in the way the integration with legacy applications is handled but also serves as the basis to support future data exchange protocols.

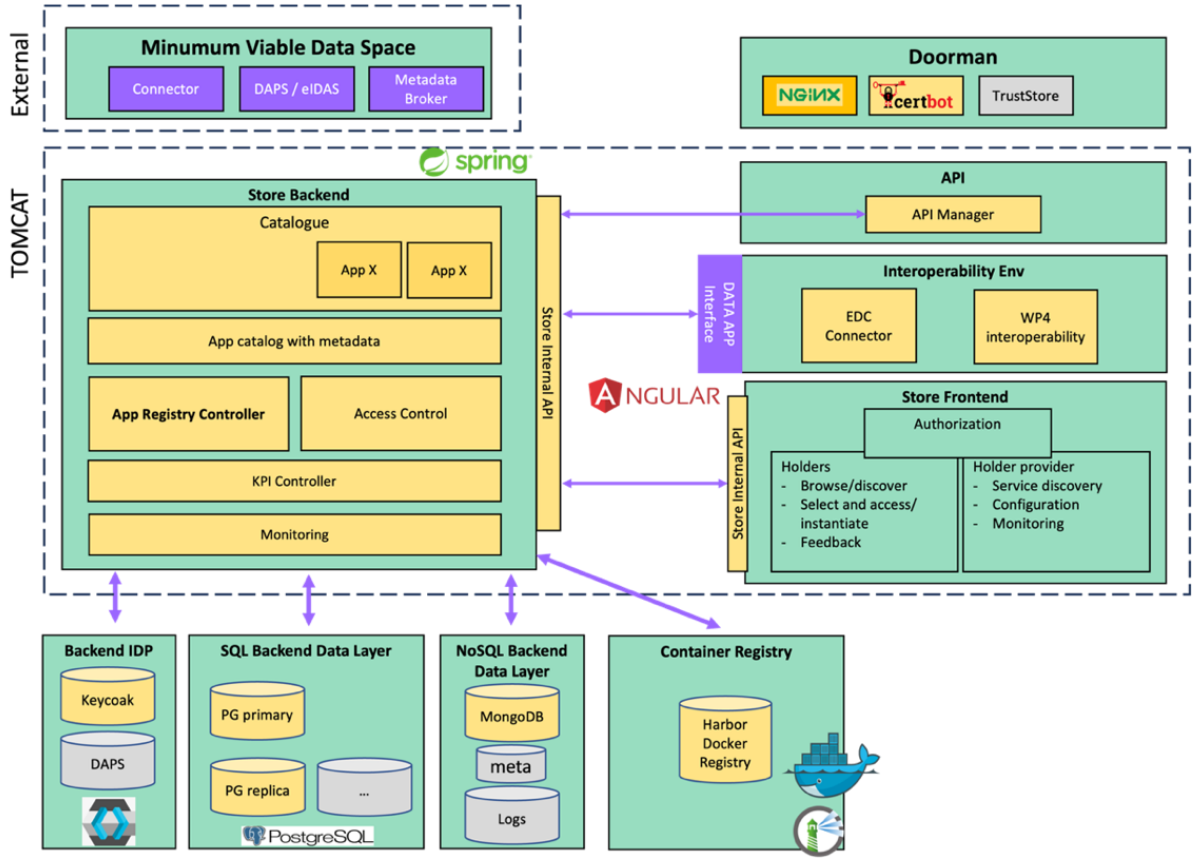


FIGURE 7 - REVISED APP STORE ARCHITECTURE

We provide an updated architecture diagram, that specifically addresses the options to generate usable applications in the context of the dataspace, which is depicted in Figure 7.

In this context an App is composed of an applicational environment, with architectural independence from the actual dataspace connector. This is depicted in Figure 8.

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.

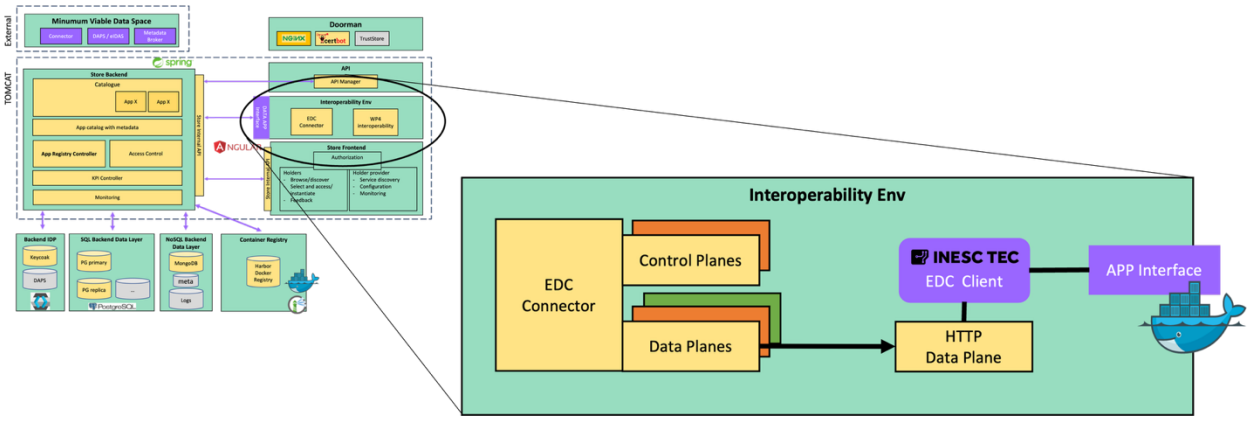


FIGURE 8 EDC DATA AND CONTROL PLANE INTERFACE

This applicational environment is integrated with the dataspace connector, by using its internal API, which is mediated through INESCTEC's dataspace connector client. This applicational environment should be bundled in an OCI compliant format such as docker. For the dataspace connector to establish a link with an App, the connector should be deployed under a compatible control plane and, most importantly, with a compatible data plane. The data plane is responsible for allowing the dataspace connector to operate a common transport protocol. Two widely used data plans offer the possibility to consider HTTP-based exchanges. i.e., those such as the ones available for RESTFull interfaces, or S3 object storage capabilities. Thus, the configuration and capability to deploy a given App requires a bundle of the App container image, and the requirements on the side of the connector to deploy the appropriate data planes. Afterwards, the App should be built to include the key stages for dataspace operation, namely, the publication of data assets, the discoverability and characterization of the data assets through meaningful metadata characteristics, and the control loops to push or receive data to and from the remaining dataspace connectors in the configured dataspace. The EDC programmatic client allows its inclusion as a library in an application consuming and pushing data assets to the dataspace. It is provided as a tool that can also assist the creation of Apps.

The current client allows for direct integration with python applications, and is compatible with the EDC connector, as long as the HTTP data plane is present. Moreover, this client implementation serves as a base for other distributions, namely in JAVA or other widely used application development frameworks.

3.2 New Functionalities and User Flows

We introduce in this deliverable the user interface overview for the App Store, showcasing a demonstration environment with Apps registered and the overview of dataspace connectors available. This is introduced in Figure 9 and Figure 10.

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.

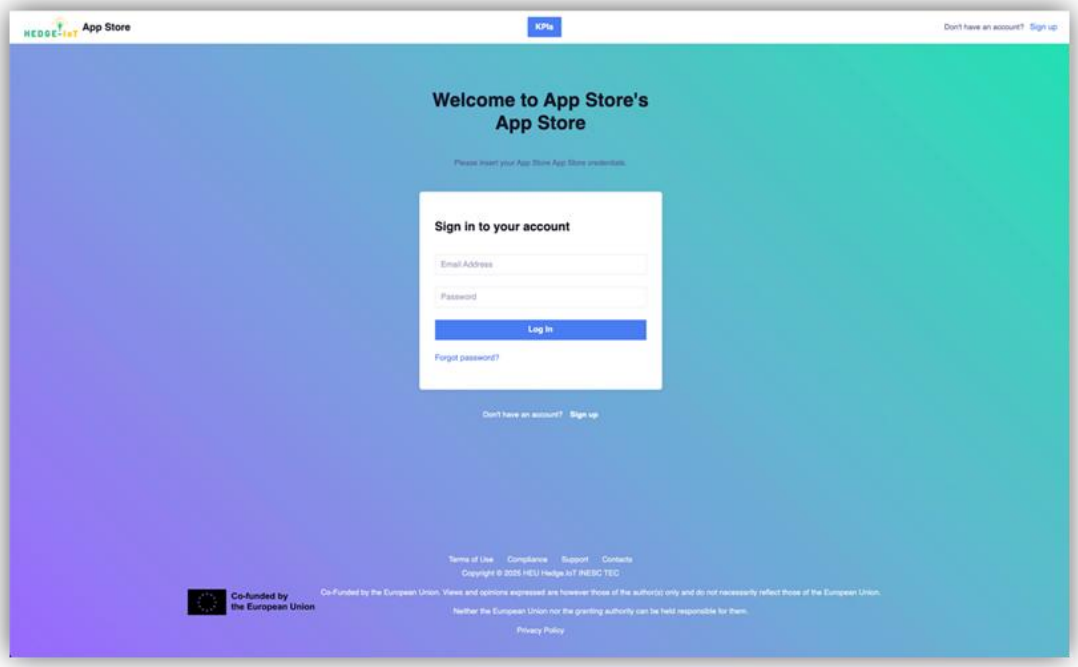


FIGURE 9 APP STORE LOGIN WELCOME PAGE

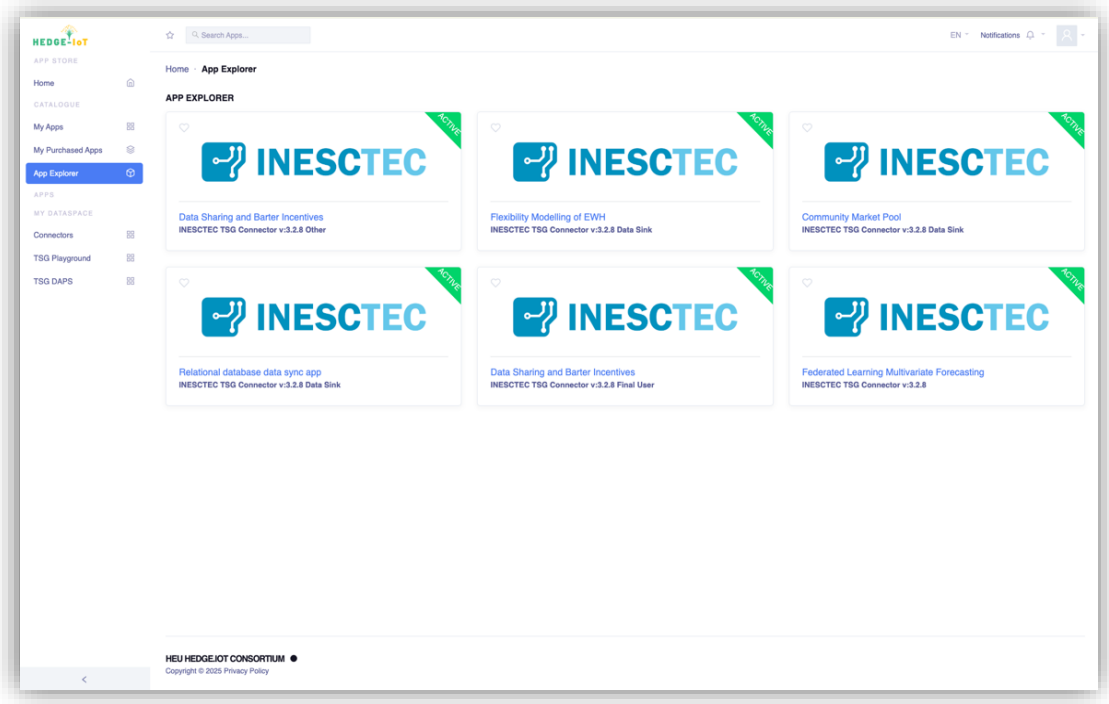


FIGURE 10 APP STORE APP CATALOGUE

Other options allow the user to navigate in the App available in this instance, and to search through them by provider, capabilities or type.

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.

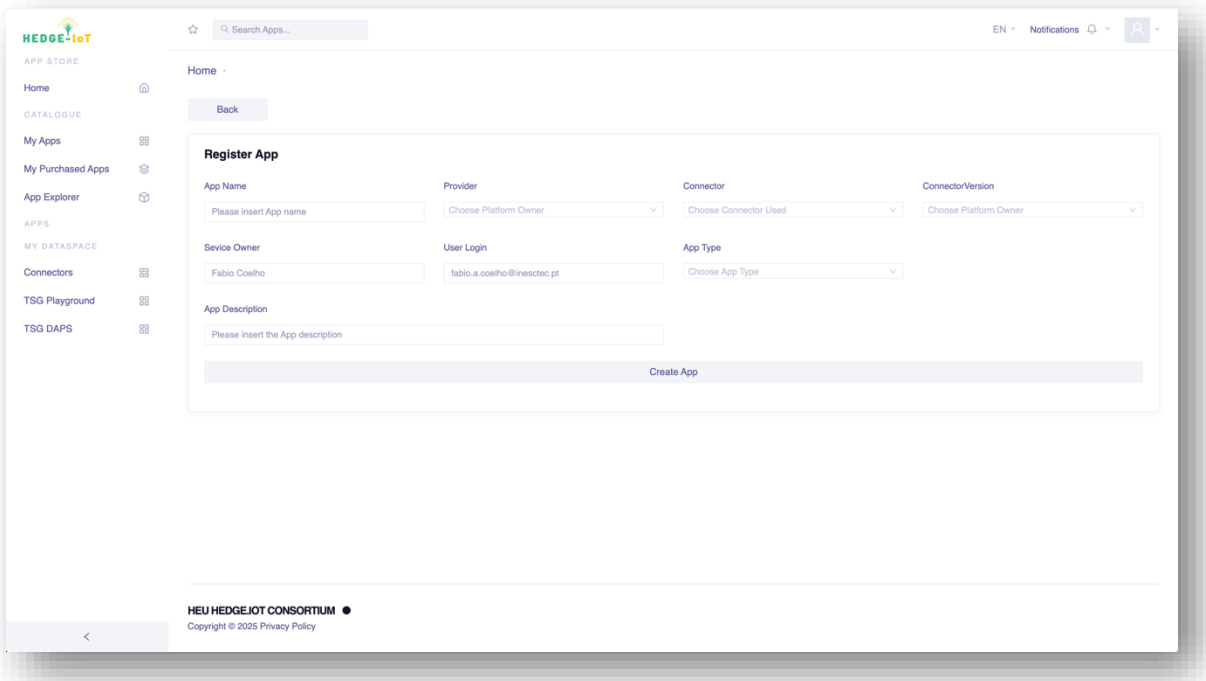


Figure 11 APP STORE APP REGISTRATION FORM

As a data owner, the App store allows the publication of new Apps. A dedicated user interface allows one user to fill a form with the most important information about an app and afterwards, proceed to upload the corresponding container image for that App. This is depicted in Figure 11.

The App registry component in the App Store, allows for several app versions to be uploaded, enabling version control and keeping track of the evolution of one App through its lifecycle, as depicted by Figure 12.

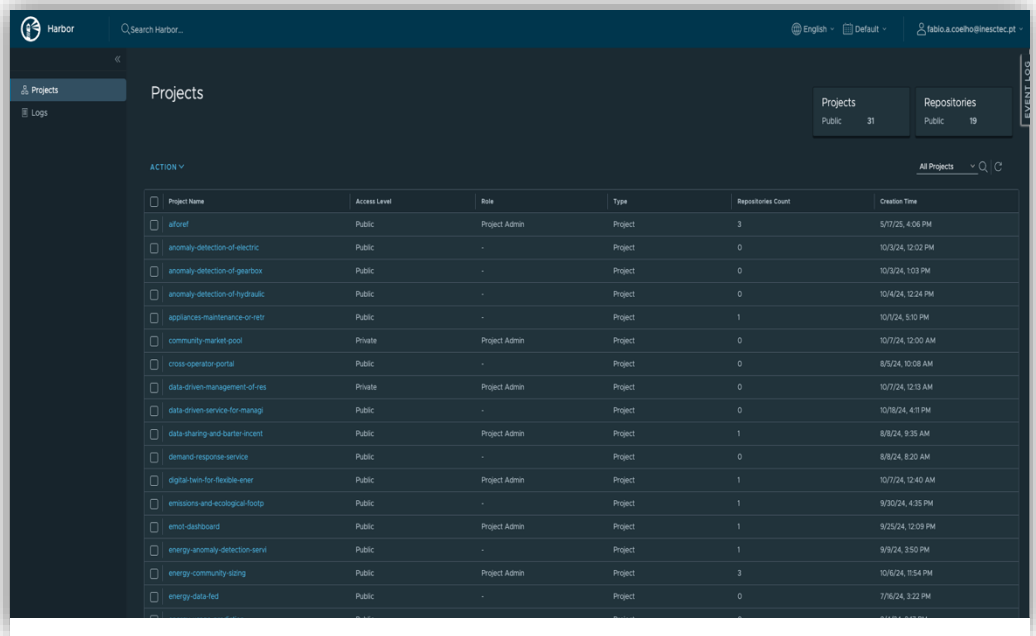


FIGURE 12 APP STORE APP REGISTRY

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. SEMANTIC INTEROPERABILITY – TOOLS AND MODELS

4.1 Evolution of the Semantic Models

4.1.1 Dutch Pilot

The Dutch pilot site of Arnhem's Buiten consists of a multitude of Internet of Things devices situated throughout a business park. The BUCs and SUCs of the pilot mainly concern sharing data among these devices for energy flexibility and anomaly detection. Therefore, the SAREF suite of ontologies, including its extensions of SAREF4ENER on energy flexibility and SAREF4BLDG on building topologies, cover most of its needs. A use-case specific extension with some classes and properties specific to Arnhem's Buiten is being developed, but it is not yet decided whether these are generic enough to be proposed for standardisation or to be shared with other pilots. Additionally, we consider including semantic models coming from the BIM (Building Information Management) communities, such as the Building Topology Ontology (BOT) and the buildingSMART Data Dictionary (bSDD).

4.1.2 Greek Pilot

The Greek pilot acts primarily as a consumer of home appliance interoperability, leveraging existing APIs, IoT devices, and communication protocols to access, collect, and process energy-related data from residential environments. The main objective is not to design new interoperability standards, but rather to effectively utilise and integrate existing ones within a scalable, standards-compliant energy management framework. Through this approach, the pilot demonstrates how residential flexibility and demand-side participation can be achieved by orchestrating data and control signals from multiple devices and vendors under a unified system.

To overcome the heterogeneity of home appliances, sensor types, and manufacturers, interoperability across devices is achieved through a gateway-based architecture combined with a unified data harmonisation layer, implemented within the Energy Home System (EHS) framework developed by ICCS. This framework constitutes the central technological backbone of the Greek pilot, integrating both edge and cloud components. Specifically, the EHS edge gateway performs real-time data collection, filtering, and preprocessing from smart meters, IoT sensors, and submetering devices using lightweight protocols such as MQTT. These edge devices handle communication and control locally, ensuring low-latency responses and continuity of operation even during temporary connectivity issues.

At the cloud level, advanced analytics, forecasting and disaggregation services such as the Non-Intrusive Load Monitoring (NILM) engine process aggregated measurements to infer appliance-level behaviour, while RESTful APIs facilitate interaction between cloud-based forecasting, optimisation, and flexibility management modules. This modular, service-oriented architecture ensures that energy data, forecasts, and control signals can flow securely and efficiently between all actors involved in the energy value chain, including consumers, aggregators, DSOs, TSOs, and market operators.

From a semantic perspective, while the initial data models were custom-built to satisfy the specific requirements and data structures of the Greek demonstration, all relevant datasets have since been

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.

mapped to SAREF (Smart Appliances REFerence Ontology) to ensure semantic alignment and machine-readability across all partners. This mapping enables the data produced by the pilot to be shared, interpreted, and reused by other systems and pilots within the HEDGE-IoT ecosystem, promoting a high degree of semantic interoperability and standard compliance.

To further strengthen interoperability, the Greek demo integrates multiple internationally recognised standards, including SAREF for ontology-based modelling, IEC 61850 for communication networks and system automation in energy environments, OpenADR 2.0b for demand-response coordination, MQTT for IoT data streaming, and OpenAPI 3.0 for the standardisation of web service interfaces. The combination of these standards ensures that all data exchanges, whether between the edge, cloud, or external actors, follow well-established conventions for reliability, transparency, and compatibility.

Beyond data-level interoperability, the Greek demo also supports functional and service-level interoperability through the HEDGE-IoT Data Space Connector. This secure infrastructure enables the sharing of trained AI models, forecasting engines, flexibility optimisation algorithms, and related energy management services with other pilots and consortium partners. By adopting a federated and privacy-preserving data exchange mechanism, it ensures that sensitive data remain protected while promoting collaborative innovation and reuse of digital assets across the HEDGE-IoT project. The combination of open data models, common protocols, and a scalable architectural design guarantees the smooth integration of heterogeneous systems, facilitates replication in other pilot sites, and ensures long-term scalability and maintainability. With this approach the Greek demo also contributes to the broader vision of interoperability and digitalisation within the European smart energy ecosystem.

4.1.3 Italian Pilot

In the Italian pilot, the analysis focused on identifying interfaces where interoperability would provide the highest value. Three main data exchange flows were considered:

1) The flow of measurement data from the power grid user interface to the IoT platform.
2) The exchange of requests and offers between the energy community management platform and the market
3) The communication of measurements and setpoints (uplink/downlink) between edge devices and the energy community management platform to support interoperability, the SAREF semantic model was adopted as the reference framework. During this phase, the focus was on modelling Flow-7, using the Semantic Treehouse platform to define a mapping between an existing JSON-based data structure and its corresponding SAREF representation. This approach enabled the semantic extension of already deployed interfaces without requiring changes in their implementation. Future steps foresee the alignment of additional data flows with SAREF-based specifications, ensuring consistency and interoperability across the different layers of the pilot's 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.

4.1.4 Finnish Pilot

The implementation of algorithms and interfaces between systems in Finnish pilot, are on the levels, 3, 4 and 5 of the Hedge-IoT interoperability levels framework, as defined in Deliverable 3.2 "HEDGE-IoT Interfaces and Tools for Interoperability". Level 3, corresponds to "Technical interoperability via data space connector" which is beyond the classic technical interoperability (e.g. communication and network, syntax) by utilizing data space connector for a secure and trustworthy data exchange. Level 4, corresponds to "Entry point semantic interoperability" and it is the first level that considers semantics on top of the syntax. Level 5, corresponds to "Basic semantic interoperability", and is not only informally defined like in level 4, but it is explicitly mapped or annotated syntactical data structure. Based on that, in the Finnish pilot, the data exchange between edge and cloud for congestion management is in level 3, because of using Eclipse data space connector to enhance security and trustworthiness. For the interfaces between ABB, TAU and JSE systems, interoperability level 4 is realized through custom interface documentation that leads to mutual understanding of syntaxes and semantics of message payloads, standard communication protocols (such as MQTT and JSON). For the measurement data from the primary substation, level 5 of interoperability is realized through utilizing IEC 61850 standard. In summary, interoperability levels 3, 4 and 5 are realized in the Finnish pilot.

4.1.5 Slovenian Pilot

Within the Slovenian pilot, a semantic model based on the CIM standard was developed using the PowerCIM tool. The model provides a structured description of substations and their components, thereby ensuring a standardized representation of the power network infrastructure.

The PowerCIM platform enables grid model data persistence and exchange by leveraging the widely adopted IEC Common Information Model (CIM) standards and data formats. This allows for efficient management of versioned model data, as well as the semantic enrichment of telemetry time-series data, ensuring alignment between static grid models and real-time operational information. In this way, PowerCIM serves as a unifying layer that supports interoperability, consistency, and scalability across heterogeneous data sources and applications.

The architecture implemented in the Elektro Gorenjska network includes IoT sensors at the network edge, a GIS system, weather data, a central DTR service, and a centralized PowerCIM system with a unified telemetry database. Static models are transferred from the GIS to PowerCIM by means of IEC 61970-552 CIM/XML files, while the DTR service integrates telemetry, meteorological, and measurement data. All data are standardized in compliance with the CIM model and associated with measurement points defined in the static model.

4.1.6 Portugese Pilot

The Portuguese pilot considers three axes of interoperability contributions, namely in the provision of data to and from the metering equipment in the tertiary buildings (supermarket stores); in the interplay between the EdgeConnect platform and the market simulator; and the availability of flexibility information from the whole pilot to the dataspaces initiative. The shape for interoperable

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 exchange occurs abiding by several interoperability levels, whose description is provided afterwards.

In the tertiary buildings, data concerning the metering information of the whole buildings and from the individual metering devices are attached to the energy assets (e.g., cold freezer unit, cold storage units, HVAC, lighting, etc). The data is exchanged with the EdgeConnect platform through H2020 Interconnect's Semantic Interoperability Framework, through SAREF compliant graph pattern representations. These exchanges abide by the highest-level of semantic data representations, allowing also to reasoning capabilities to operate directly on top of the graph data representation.

The EdgeConnect platform, operating as a value-chain enabler, makes flexibility data available to a connected dataspace, providing market activation information and flexibility volumes that are operated in the pilot. This information is provided to the dataspace according to a mix of JSON-LD data schemas, but also through RDF data.

The data exchanges that occur between the EdgeConnect platform and the market simulator platform are established according to the IEC 62325 standard, which provides XML-based standard representations of Balancing Service Provider (BSP) upstream market bids and downstream flexibility bid activations. Finally, metering information from the community manger to the EdgeConnect platform is provided through the CIM standard.

4.2 SEMANTIC INTEROPERABILITY ENABLERS IN THE RA

Semantic enablers are foundational components of the Reference Architecture (RA) that support interoperability by providing a common understanding of data exchanged across systems. Semantic interoperability ensures that information shared between diverse systems maintains its meaning and context, thus avoiding ambiguity and misinterpretation. To achieve this, harmonization frameworks are employed, which define shared vocabularies, data models, and ontologies. These frameworks support consistent and standardized data exchange, enabling systems and stakeholders to integrate and interpret data seamlessly. Within the CEEDS ecosystem, standards such as SAREF, IEC 61970, IEC 62325, IEC 62746, IEC 61850-7, OCPP, and the Common Information Model (CIM) are key enablers, helping to ensure alignment with established industry practices and improving compatibility across the smart grid landscape.

In data-sharing environments, especially within federated data spaces, semantic enablers help prevent the formation of data silos by emphasizing machine-readable ontologies that reveal relationships among data instances. Technologies such as RDF (Resource Description Framework) allow data to be linked and exchanged without losing semantic clarity, using structured triples to represent facts. This approach supports richer data integration and discoverability, particularly when paired with Vocabulary Hubs and standardized protocols. Through the use of shared ontologies and syntactic standards, semantic enablers in the RA promote seamless data fusion, service interoperability, and more effective collaboration across heterogeneous systems and applications.

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.

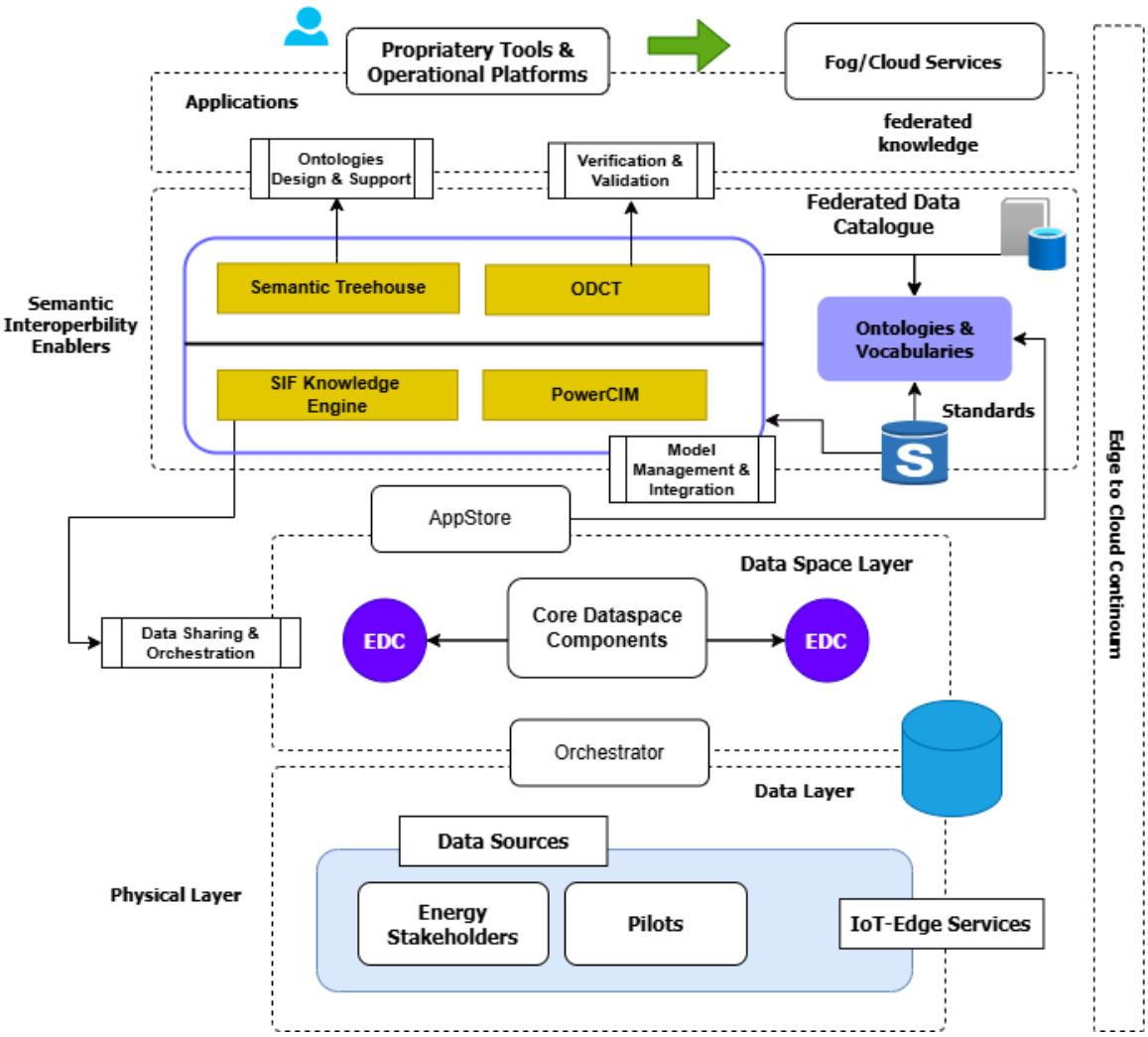


FIGURE 13 SEMANTIC INTEROPERABILITY ENABLERS

Figure 13 Semantic interoperability enablers depicts a structured data pipeline extending from physical assets to applications, ensuring interoperability across distinct layers. At the bottom, the Physical Layer comprises Data Sources, including Energy Stakeholders, Pilots, and IoT-Edge Services, which generate and consume operational data. This data is then managed by the Data Layer, incorporating an Orchestrator and persistent storage, facilitating secure data handling and lifecycle management. Above this, the Data Space Layer hosts the Core Dataspace Components, connected via IDS-compliant EDC connectors, which guarantee sovereign data exchange through policy enforcement and secure transactions. The Data Sharing & Orchestration function coordinates these flows, establishing repeatable and compliant transfers. Finally, at the top of the architecture, the Applications layer provides Proprietary Tools & Operational Platforms and Fog/Cloud Services that ingest semantically consistent data and federated knowledge along the full Edge-to-Cloud continuum, supported by the intermediary AppStore, which publishes and provisions Data Apps leveraging harmonized semantic outputs.

Central to the architecture is the Semantic Interoperability Enablers zone, outlined in blue within the middleware, consisting of specialized components that manage semantics across the 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 ecosystem. The Semantic Treehouse functions as a central vocabulary hub for ontology publishing, mapping, and collaborative ontology lifecycle management, directly supporting the Ontologies Design & Support activity. In parallel, the Ontolog ODCT ensures that semantic structures and behaviors align with agreed-upon ontologies and test scenarios through rigorous verification and validation processes. Meanwhile, the SIF KE conducts distributed semantic reasoning, knowledge federation, and matchmaking based on ETSI SAREF-centric ontologies, effectively translating raw data streams into actionable federated knowledge. Complementing this, PowerCIM maintains persistent IEC CIM-compliant models for grid infrastructure, ensuring the integrity and semantic alignment of telemetry data against static grid topologies. Additionally, the Model Management & Integration function orchestrates semantic adapters, ontology mappings, and facilitates runtime deployment, ensuring continuous semantic consistency across the data flow.

Semantics are systematically propagated through the dataspace following a clearly defined sequence from standardization to service delivery. Data originating from physical assets and platforms first enter the dataspace via the EDC connectors, undergoing rigorous contract- and policy-based governance within the Core Dataspace Components. Once ingested, data streams are semantically enriched by aligning them with shared conceptual definitions curated within the Ontologies & Vocabularies repository, itself directly informed by recognized Standards such as ETSI SAREF and IEC CIM[10]. This semantic enrichment is operationalized by the Model Management & Integration function, drawing upon the capabilities of Semantic Treehouse and PowerCIM. The enriched data is then processed by the Knowledge Engine, transforming it into federated knowledge through semantic reasoning and matchmaking. Prior to broad dissemination, the ODCT ensures semantic and behavioral compliance. Finally, the Federated Data Catalogue indexes and exposes semantically annotated assets, datasets, and services, enabling their discovery and reuse by the AppStore and higher-level applications, thereby closing the semantic propagation loop with rigorous traceability from standards through to deployed knowledge.

4.3 Update on semantic Interoperability enablers

4.3.1 SEMANTIC TREEHOUSE

Semantic Treehouse (STH) is an open-source platform that helps data sharing communities to define, agree on, and improve shared data models. It serves as the vocabulary hub in the Hedge-IoT data space; it makes semantic specifications findable and accessible while providing services to facilitate their adoption by data owners and data consumers.

In Hedge-IoT, we leverage STH's functionalities to improve data interoperability between pilots and improve STH itself based on lessons learned from this experience. This update only covers the former; report of how the platform has been improved will be included in deliverable 4.3.

4.3.2 Ontology-Driven Constraints Tester

In the context of HEDGE-IoT, TRIALOG is exploring behavioral testing throughout the development of a new testing flow for the ODC-Tester proof of concept.

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.

Behavioral interoperability is defined in ISO/IEC JTC 1/SC41 21823-5 as follows: "interoperability so that the actual result achieves the expected outcome". Behavioral testing relates to functional testing as follows: it is the part of interoperability that one wants to test.

With this semantic enabler, Trialog wants to define a methodology for behavioral testing based on ontologies and demonstrate it with first simulated data, then (if available) real data coming from a pilot. The ODCT long-term value propositions identified at this stage are the following (and may change):

- Interoperability compliance validation (semantic)
- Engineering support for interoperability (semantic)
- Interoperability compliance validation (behavior)
- Engineering support for interoperability (behavior)
- Compliance extension
- Engineering support extension

The Ontology-Driven Constraint Tester (ODC-Tester) focuses on ensuring technology-neutral ontology-based interoperability. It aims to support engineers to verify, ensure and validate the interoperability compliance of data exchange between various systems with ontologies (e.g., SAREF at the moment). The testing methodology is based on the Joint Research Center (JRC) initiative for a Code of Conduct (CoC) for Energy Smart Appliance (ESA) interoperability test method.

This exploratory work aims to support JRC CoC ESA as well as ISO/IEC 21823-5 behavioral and policy interoperability. TRIALOG is actively contributing to this standard.[9]

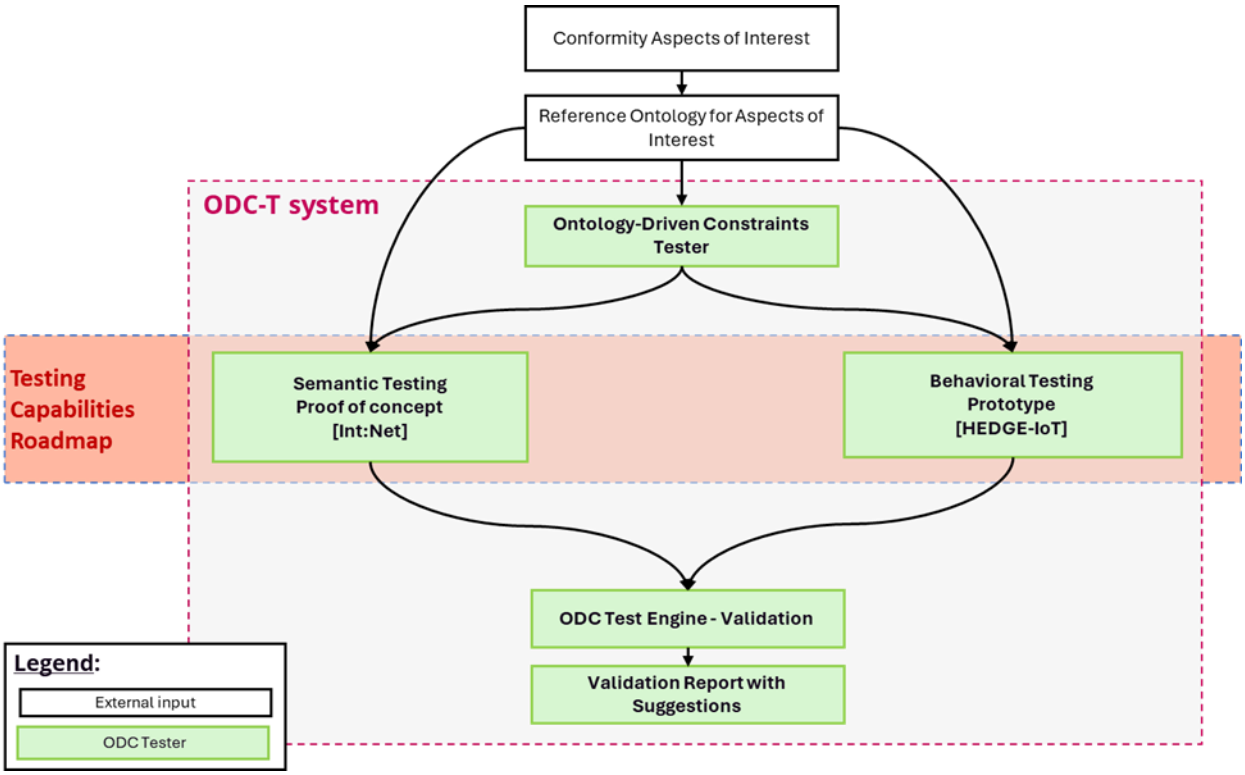


FIGURE 14 TRIALOG ODC-TESTER OVERALL TESTING CAPABILITIES

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.

4.3.3 ODC-T activities in HEDGE-IoT

The following list provides an overview of the TRIALOG's activities on ODC-Tester in HEDGE-IoT:

- Literature review on behavioral testing methods
- Definition of a first testing architecture for behavioral testing based on BPMN
- Creation of a simulated dataset to enable behavioral testing
- Creation of industry collaborations (Miele, Beko) to support ODC-Tester development with real-dataset and identify their needs
- Active contributions to the relative standards:
  - ISO/IEC 21823-5 Behavioral & Policy interoperability
  - EN 50631-3-1 Household appliances network & grid connectivity-Specific Data Model mapping: SPINE & SPINE-IoT
- Participation and contributions to the ecosystem:
  - JRC CoC ESA [8]
  - EEBUS Spine IoT WG
- Academic & Research Collaboration
  - Joint publications in preparations
  - Behavioral testing methodology review by TNO

Most of these subjects are detailed in Annex A:

4.3.4 ODC-Tester next steps

For the next steps, TRIALOG will continue working on behavioral architecture. The collection of real data and generation of simulated data will continue, as well as the active contribution to JRC CoC ESA, ISO/IEC JTC 1/SC41 21823-5 and EEBUS SPINE IoT working group [12]. A review of the approach will be done inside the consortium (TNO).

4.3.5 Knowledge Engine / Semantic Interoperability Framework

The Knowledge Engine, also known as the Semantic Interoperability Framework, is an open-source distributed middleware that helps to exchange data based on their semantics, i.e. the meaning of the data. It facilitates making an open data sharing ecosystem.
We've released several new versions of the software during HEDGE-IoT so far. The most important changes include:

- Improving the robustness of the software, especially for distributed settings
- Improved performance through a new algorithm that has improved handling of large amounts of data
- Added a new documentation website to enable developers to easily find relevant information for the software
- Improved the developer experience through improved configuration and documentation
- Implemented a new reasoning algorithm. This algorithm has more levels, making it better adjustable to various use cases depending on the desired semantic interoperability level.
- New feature that allows users to include domain knowledge in the reasoning process

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.

Future developments within HEDGE-IoT will focus on improving robustness and performance in operational settings.

4.3.6 PowerCIM

PowerCIM is an advanced software solution designed for managing data models in electric power systems based on the CIM (Common Information Model) standard. Developed to meet the needs of modern transmission and distribution system operators, PowerCIM enables efficient integration, validation, and exchange of technical data across various systems and applications within the power system ecosystem. Within the HEDGE-IoT project, PowerCIM consolidates data from different systems used by the distribution system operator, enabling interoperability in the context of the pilot implementation.

In the Slovenian pilot, the Power CIM platform has been extended to act as the central integration layer for subsystems across the distribution grid, including GIS, smart metering, Dynamic Thermal Rating (DTR), and environmental data. By applying IEC 61968 and 61970 CIM standards, Power CIM enables standardized data exchange, reduces redundancy, and overcomes the traditional isolation of these systems.

DTR calculations are performed locally on IoT devices installed at secondary transformer substations. This edge-based approach provides real-time insights into transformer loading capacity, allowing safe operation above rated limits in favorable weather while protecting asset lifetime.

Through this integration, Power CIM demonstrates its value as a unifying tool, ensuring interoperability and supporting smarter, more flexible grid operation within the pilot.

4.3.7 Semantic Interoperability in Data Spaces

Semantic interoperability is a key enabler for communication and coordination in complex systems such as smart grids [3]. It ensures that information exchanged between heterogeneous devices and applications is consistently understood and interpreted, regardless of differing formats or protocols. This capability supports accurate data interpretation, seamless integration across diverse components, informed decision-making, and adaptability to evolving technologies. Furthermore, semantic interoperability fosters innovation by enabling collaboration among vendors, researchers, and stakeholders who rely on standardized semantic models and open formats to build interoperable solutions.
Despite its benefits, achieving semantic interoperability presents significant challenges due to the high heterogeneity of devices, applications, and data models within energy systems. Current standards, such as the IEC Common Information Model (CIM) and frameworks like SGAM, provide a foundation for shared semantics but often remain limited to core concepts or high-level abstractions. More comprehensive models, such as those developed in the H2020 SYNERGY project, extend these efforts by harmonizing prominent energy data models into detailed semantic representations. However, the decentralized and dynamic nature of energy systems requires continuous alignment, lifecycle management of semantic models, and cross-sector harmonization to effectively capture emerging concepts such as distributed energy resources (DERs).

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 address these challenges, harmonization frameworks, system adaptation mechanisms, and established standards play a central role in enabling interoperability. Frameworks support consistent data exchange through shared vocabularies and ontologies, while lifecycle management ensures models evolve with system needs. Linked data approaches, such as RDF, allow relationships between data to be expressed in machine-readable formats, avoiding silos and supporting automated interpretation. Meanwhile, standards like CIM, IEC 61850, and DLMS/COSEM provide common ground for defining data models, message formats, and communication protocols. Together, these building blocks establish a reliable foundation for semantic interoperability, enhancing communication, collaboration, and operational efficiency across the smart grid ecosystem.

4.3.8 Interoperability levels in the project

In Deliverable 3.2 "HEDGE-IoT Interfaces and Tools for Interoperability" we have defined an interoperability framework consisting of seven interoperability levels, based on the existing frameworks defined by the European Interoperability Framework Toolbox (EIF) by the EC and the Interoperability Context-Setting Framework by the Gridwise Architecture Council (GWAC). We didn't want to introduce yet another interoperability framework, but instead echo the call that the current EIF gets outdated with the increased adoption of SHACL and the introduction of artificial intelligence technologies.[4] Therefore, we have shared the Next Generation EIF survey with the Task 4.3 participants: Next Generation EIF - Survey | Interoperable Europe Portal The project pilots will at least achieve interoperability level 3 of technical interoperability via a data space connector, which distinguishes HEDGE-IoT.

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. IOT CLOUD/EDGE SYSTEM INTEGRATION – PILOT-DRIVEN UPDATE

This section consolidates the pilot-driven evolution of the HEDGE-IoT cloud/edge stack, describing how service orchestration and a Dataspace framework realise the reference implementation across stakeholders. It tracks progress from the first to the current technological release, highlighting interoperability, trust, sovereignty, and end-to-end data-flow compliance. It also frames how these integrations feed demonstrator scenarios and prepare the final release.

5.1 Introduction

The primary goal of Task 4.4 "IoT Cloud/Edge System integration" is to integrate the technology components that enable interoperability, trust and data sovereignty, as well as the data process flows as specified in the functional requirements. By providing the necessary service orchestration and a Dataspace technological framework, these components will form the reference implementation for HEDGE-IoT.

The outcome will include processes, services, communication channels, and interfaces aligned with the demonstrator scenarios. The integrated Data Space will manage data access for various stakeholders within the energy ecosystem, as well as external services/platforms, in an interoperable way. As defined in D4.1 "Interoperability Framework and Integrated Solution (First Release)", the HEDGE-IoT integration methodology process comprises the following key areas:

- **Integration Guidelines:** Established integration guidelines for middleware components, defining processes, responsibilities, and an activity plan with clear objectives, milestones, and interdependencies to ensure successful alignment and realization of the HEDGE-IoT technical framework.
- **Contingency Plan:** Described a detailed methodology with mitigation strategies designed to address integration risks, scheduling delays, or other potential issues.
- **Service Orchestration:** Described how service orchestration would manage software and service configuration, unifying stand-alone subsystems into a consistent system while ensuring compliance with Data Space guidelines and Eclipse MVD implementation.
- **Actual integration and deployment of the HEDGE-IoT Data Space:** Described the necessary activities for integrating and deploying the HEDGE-IoT Data Space, using communication channels and APIs to enable seamless, interoperable, and decentralized data access for all stakeholders.
- **A comprehensive testing process:** Defined a release testing process aimed at resolving integration issues, build a fully functional platform and deliver a prototype for validation.

Continuous Activities for Moving from First to Intermediate Technological Release

Task 4.4, in alignment with WP3 and WP4 has performed the following 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.

1. **Refining Integration Guidelines**
    - Continuously update integration guidelines based on lessons learned from the first release.
    - Adjust objectives, milestones, and interdependencies to reflect evolving requirements and new component/service maturity.
2. **Iterative Risk & Contingency Management**
    - Monitor integration risks, scheduling challenges, and technical dependencies.
    - Apply mitigation strategies and refine the contingency plan as issues are identified and resolved.
3. **Progressive Service Orchestration**
    - Incrementally expand the orchestration process to include newly developed components and services based on the delivered technological enablers.
    - Ensure ongoing compliance with Data Space integration guidelines and Eclipse MVD standards.
4. **Incremental System Integration & Deployment**
    - Continuously support the integration of additional processes, services, APIs, and communication channels.
    - Coordinated the expansion of the HEDGE-IoT Data Space step by step towards a complete and interoperable ecosystem.
5. **Ongoing Testing & Validation**
    - Supported the iterative testing on each integrated version to identify and resolve technical issues.
    - Through the **Technical Board** activities, validated interoperability, trust, sovereignty, and data flow requirements at each stage.
6. **Stakeholder Feedback & Alignment**
    - Engage stakeholders (energy ecosystem actors and external platforms) in early testing cycles.
    - Incorporate feedback to improve usability, interoperability, and compliance with real-world needs.
7. **Documentation & Knowledge Transfer**
    - Continuously document integration steps, orchestration configurations, testing outcomes, and component/service tracking.

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.

- Share updates with technical teams and stakeholders to ensure alignment and consistent progress.

Finally, one of the most important aspects of the T4.4 activities is the "**Component & Service Development Tracking".** In short, we maintain a living register of all components and services, capturing i) Current development status (planned, in-progress, completed, tested, integrated), ii) Dependencies between services and components and iii) Alignment with functional requirements and demonstrator needs. The goal behind this activity is prioritize integration order, monitor gaps, and forecast readiness for the next (and final) release.

5.1.1 Main Technological Enablers register: Interoperability Framework & Integrated Solution

This subsection introduces the core interoperability assets and explains how they underpin secure, policy-driven data exchange. It positions Table 2 as a status snapshot from first to current release with a forward view.

TABLE 2 MAIN TECHNOLOGICAL ENABLERS

Interoperability Middleware			
Eclipse Data space connector 1. Connector core runtime (control & data plane, service extensions) 2. Backend services (federated catalogue, identity management) 3. Graphical User Interface	**Description**	**First Release**	**Current release**
	EDC is the central middleware Data Space component responsible for handling secure data transfers between a provider and a consumer.	First release implementation focuses on establishing the fundamental capabilities of the connector, including policy negotiation, contract enforcement, and secure data exchange.	EDC further extended to include more complex integrations with additional partners and services, further strengthening the HEDGE-IoT interoperability framework.
Backend Service: EDC Data Catalogue	The main Data register in a Data Space	Implemented in first release as built in functionality	Continuous updates
GUI: EDC Data Dashboard	The main user interface for EDC aims to improve user experience and easy	n/a	Core functionalities implemented such as asset & contract 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.

	access to EDC framework functionality.		policies definition and basic data sharing and transfer.
Open Service Catalogue and App Store 1. App Store 2. App Store Front End 3. IDS Connector 4. IDM 5. Container Registry	The App Store integrates into the IDSA ecosystem as one of its main building blocks. It interfaces with the IDS Connector and enables Data Apps to be distributed within the data space. Data Apps are reusable applications that are used to process or transform data before or after the data is exchanged.	• Users can access the App Store through a friendly user interface. • Capability to browse the available Apps and verify their requirements/ functionalities before downloading them. • Instantiation in the user's IDS Connector instance after download. • Capability to publish Data Apps so they can be used by other users. • Users use the App Store to fast prototype new Data Apps, focusing on the business-related data acquisition or data transformations, while ensuring key data acquisition and integration with the IDS connector environment is taken care of.	Several service-layer improvements have been implemented, such as upgrades to the API gateway, new deployment features, based on feedback from pilot users.

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.

Semantic Interoperability Enablers	See chapter Semantic Interoperability – Tools and models

5.1.2 Main Technological Enablers register: Federated learning technology enablers targeting residential end-users

This subsection summarises the federated learning stack and how pilot data and tooling mature from the 1st Tech release to real-world pilot demonstrations. Table 3 captures first-release baselines, current integrations, and next-step pilots at scale.

TABLE 3 FEDERATED LEARNING TECHNOLOGY ENABLERS

Technology Enabler	1st Tech Release [1]	Current Tech Release [2]	Future Development
Federated Learning for Energy Forecasting (ICCS)	Decentralized federated learning architecture using LSTM/BiLSTM models for forecasting energy demand and production. Initial training conducted using open datasets such as StoreNet. Model updates exchanged via MQTT secured by TLS.	BiLSTM models, trained with pilot data from residential apartments. Models converted to TensorFlow Lite for deployment on Shelly 3EM meters. MinIO used for model storage and secure model distribution. Integrated secure MQTT-based communication.	Pilot deployment and real-world testing in 100 Greek apartments. Validation of real-time performance on edge devices. Iterative model refinement based on pilot results. Energy footprint monitoring for edge model inference.
Vector Autoregressive Model for Energy Time Series Forecasting (INESC)	Proof of concept algorithm observed with synthetic data. Data processing pipeline developed and connected to real pilot data, for a selected group of users.	First lab concept solution in a fully functioning demo environment with 4 different simulated edge agents. Design an initial development of integration of pilot users' data pipeline for each agent.	Integrate the lab prototype into a larger scale environment according to the number of users participating in the pilot at the given date. Integrate the edge nodes with the computational orchestrator tool being developed in WP3.

5.1.3 Main Technological Enablers register: HEDGE-IoT's Data-Driven Edge-to-Cloud Technology Enablers

This subsection lists grid-facing analytics and control enablers, mapping their path from synthetic to realistic/pilot data. Table 4 provides a concise maturity view and planned robust improvements.

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 HEDGE-IOT'S DATA-DRIVEN EDGE-TO-CLOUD TECHNOLOGY ENABLERS

Technology Enabler	1st Tech Release [1]	Current Tech Release [2]	Future Development
Enhanced Network Management and Planning (UNIZG)	Investigation of techniques used in anomaly detection, demand forecast and initial development and testing of algorithms.	Testing anomaly detection and demand forecast algorithms on synthetic data. Research on techniques to detect PVs in secondary distribution networks from limited measurements.	Testing anomaly detection and demand forecast algorithms on realistic data and PV detection algorithm on synthetic data.
DTR-DLR on the Edge (JSI)	Initial overview of the DLR/DTR and weather forecast algorithms.	DLR/DTR algorithms adapted to IoT use case, improved interoperability plan.	Improved overall robustness of DLR/DTR algorithms, weather forecast algorithms deployed and updated, improved interoperability.
Anomaly Detection and Predictive Maintenance on the Grid (VU)	Learn patterns of nominal device behaviour from SAREFised data streams.	Recognize and report unnatural deviations from learned patterns (via SIF).	Improve overall robustness and minimize false error rate; add admin UI and export function.
Anomaly Detection and Fault Forecasting to Increase Distribution Network Resilience (VTT)	Deep Learning Model to Analyze data patterns, correlations, and identify anomalies.	HLSTM model to analyze data patterns, correlations, identify anomalies, and forecast future anomalies.	Improved identification of data patterns and anomaly detection with high accuracy and forecasting of future anomalies.
Real-Time Congestion Management (TAU)	Breaking down the service into micro services to enhance modularity of algorithms and to facilitate coordination and cooperation of developers. Specifying the steps in which the implementations could be realized. Those steps are data preparation	Micro services and the hardware where they are going to be executed have been decided. Initial agreement on the timeline of microservice developments done by different organizations aimed at piloting the whole solution. Harmonizing Input data has been completed. (validating the input data is expected to be completed by the end of	Real-time CM is also developed. State estimation and real-time CM micro services are integrated for the full-service testing in Lab with real-world input data (grid and load data). The tested setup is piloted in the pilot site and some results are already achievable.

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.

	and harmonization, work related to edge server (engineering the hardware, establishing virtual machines, networking), component development and testing, integration testing of developed components, and finally, piloting the solutions.	April). It is expected to have the first version of state estimation micro service necessary for real-time congestion management ready for this deliverable. The first version of the test environment where the developed micro services will be tested is also expected to be ready.	
HEMS (INESC)	TE not described in D3.3 [1]	Integrations with PT pilot DERs: Heat pump, EV charger and inverter. Core functionalities developed and initiated deployment.	Improvement of the integration between DER and Cloud service. New functionalities developed: flexibility actions, user notifications and incentives.
Digital platform capabilities for distribution automation (ABB)	TE not described in D3.3 [1]	Implemented virtualized protection solution and pre-processing modules to calculate Fast Fourier Transforms.	Modules to provide communication capabilities to the solution, namely to SCADA, to the congestion management and anomaly detection solution. Data storage for the results of the application.

5.1.4 Main Technological Enablers register: HEDGE-IoT's Cloud Technology Enablers

This subsection covers cloud services enabling flexibility and markets—platforms, simulators, predictive CM, energy community services, and local market tooling—aligned with standards and dataspace integration. Table 5 reports current deployments, integrations, and upcoming functionality.

TABLE 5 HEDGE-IOT'S CLOUD TECHNOLOGY ENABLERS

Technology Enabler	1st Tech Release [1]	Current Tech Release [2]	Future Development
EdgeConnect (INESC)	Design presentation of the existing platform to	This platform established an ecosystem for stakeholders across the flexibility value chain, enabling integration,	Bilateral agreement functionalities and full communication over standard protocols such as IEC 62325.

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.

	HEDGE-IoT configuration and System Operator types.	qualification and market participation, to unlock flexibility potential from LV and MV grids. The platform unlocks a multi-stakeholder environment where all relevant roles coexist.	Deployment complete and operational with integration with partner's platforms and services completed or tested.
Flexibility Optimization Service (ICCS)	Initial Overview of the algorithms of bidding strategies and flexibility dispatch.	IoT data cleaning and processing to fit into the decision-making algorithms and an initial implementation of specific algorithm to one defined scenario.	Define more scenarios and identify more decision-making algorithms.
Real-Time Reserve Market Simulator (NESTER)	Initial internal release allowing basic single bid submission, clearing and response.	Integration of IEC 62325 standard for energy market communication and file exchange. Multiple bid submission and analysis implementation. Release for pilot's initial integration testing. Improvements in bid validation, clearing and activation signal.	Full deployment of both services mFRR and aFRR with complete data stream tested and implemented among the pilot's members.
Predictive Congestion Management (TAU)	Breaking down the service into micro services to enhance modularity of algorithms and to facilitate coordination and cooperation of developers. However, this service has been in the design stage and implementation work has not yet started.	Define the data exchange's payload between cloud and edge to be able to develop adaptors (cloud-edge data exchange adaptor). The progress in real-time congestion management on edge will have an over-lapping benefit for this service for example in the areas of input data because the same grid and load data could be used in the cloud during the simulations. For the state forecast algorithm, the state estimation algorithm on the edge could be already a good starting point. The first version of the test environment (virtual machine running on the cloud) is ready.	The simulated predictive CM is tested and then executed on the cloud and the results are already available for analysis.
Energy Community Management	Platform's main functionalities developed and being tested in a	Incorporate new functionality for flexibility provision to the	Integrate the functionality in the platform and with 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.

Service for Frequency Restoration Reserve (INESC)	relevant environment (another European project pilot).	reserve market and test it with mock data provided by the TSO.	market platform using data spaces. Test the prototype with the new functionalities and integrations in the relevant environment (PT pilot).
Local Flexibility Market Platform (HENEX)	TE not described in D3.3 [1]	Developed an algorithm for daily generation and configuration of MTUs and for the automated operation of trading gates according to market schedule. Implemented algorithm for the execution of the market clearing.	Implement asset registration and pre-qualification and portfolio management. Deployment of settlement and clearing mechanisms.
Energy Community Platform (APIO)	TE not described in D3.3 [1]	Development and implementation of core functionalities, like baseline computation, flexibility offer optimization and energy community power management.	Connection to local flexibility market platform. Integration with the interoperability framework of the project.
TurnGreen – OptiFlex (ELERG)	TE not described in D3.3 [1]	Integrated new EnergyBox solutions into supermarkets and into the OptiFlex platform.	Asset integration. Develop optimization algorithm for each asset. Create automated responses for flexibility requests.
PowerCIM tool (KONČAR)	TE not described in D3.3 [1]	Imported preliminary data and created appropriate measurements for the time series for DTR calculations.	Updates to the CIM models to reflect measurement points of the substation and for DTR integration.

5.1.5 Main Technological Enablers register: HEDGE-IoT's Computational Orchestration Framework

This subsection introduces the orchestration framework for edge offloading and federated learning roll-out, detailing its integration points with HEDGE-IoT services and the dataspace. Table 6 outlines design, current implementation status, and next steps toward pilot integration.

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 6 HEDGE-IOT'S COMPUTATIONAL ORCHESTRATION FRAMEWORK

Technology Enabler	1st Tech Release [1]	Current Tech Release [2]	Future Development
Computational Orchestration Framework (TUC)	High level design of the orchestration framework architecture and first specifications for two use cases: edge offloading for low-latency data processing and federated learning orchestration.	Detailed design of orchestration framework along with current implementation for each of the two use cases, and for an additional use-case that was identified: application/federated learning models rolling out at edge. Orchestrator integration with the HEDGE IoT framework focusing on available services, and data space connector.	Integration of orchestration framework with services available in pilots. Complete the integration with blockchain platform. Dashboard for real-time metric monitoring and performance 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.

6. SECURITY AND PRIVACY – SECOND PHASE IMPLEMENTATION

6.1 Update on Cross-Cutting Characteristics Plan

This section presents the status of the Cross-Cutting Characteristics Plan (X-CCP) defined in D4.1 and in progress within HEDGE-IoT T4.5. This task aims to ensure robust cybersecurity, data privacy, and AI trustworthiness throughout the project and its pilots..

As a reminder, the X-CCP covers the following trustworthiness characteristics:

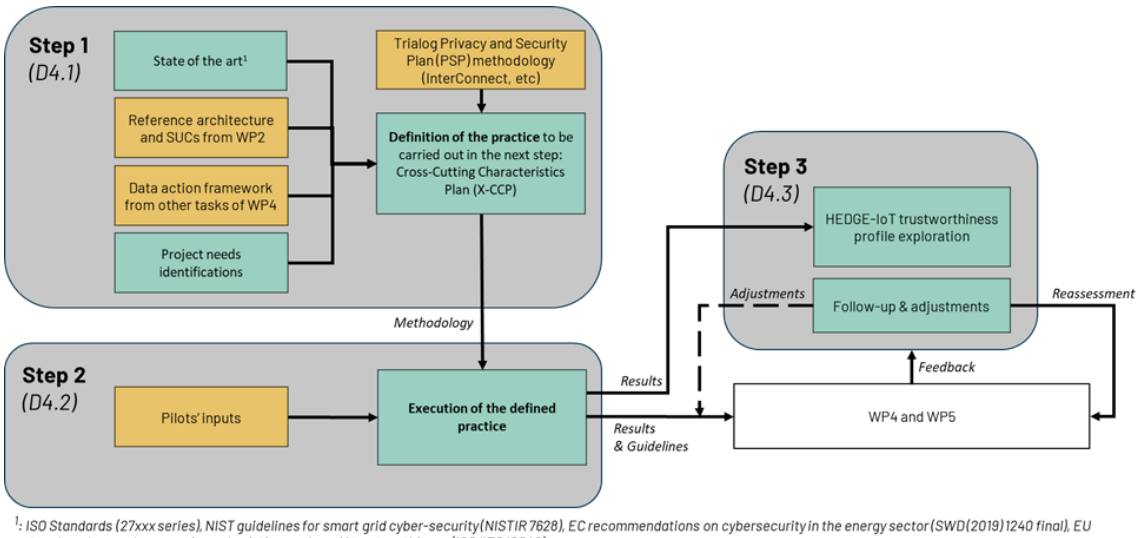
- AI Trustworthiness,
- Data privacy,
- Cybersecurity,
- Key Performance Indicators definition and
- a plan progress assessment.

X-CCP methodology objective reminder:

Ensure that cybersecurity, data privacy and AI safety is adequately managed in HEGDE-IoT demonstrators, system-of-interest and its associated ecosystem.

As presented in D4.1, this task is divided into 3 main steps, as described by Figure 15:

- **Step 1,** refers to the preparation and definition of the practice based on a state of the art, previous work in the project, pilots' answers to a questionnaire and the TRIALOG Privacy and Security (PSP) methodology.
- **Step 2 (Ongoing),** refers to the execution of the defined practice, also named Cross-Cutting Characteristics (X-CCP) in the project. For this step, the inputs of the pilots will be necessary to ensure relevant analysis.
- **Step 3**, refers to the HEDGE-IoT trustworthiness profile exploration, and the adjustment of the action plan based on pilots' feedback and progress.



[1]: ISO Standards (27xxx series), NIST guidelines for smart grid cyber-security (NISTIR 7628), EC recommendations on cybersecurity in the energy sector (SWD(2019)1240 final), EU network code on cyber security and existing work on AI trustworthiness (ISO/IEC/SC42).

FIGURE 15 TASK STRATEGY

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 X-CCP is ongoing (Step 2). This practice comprises 5 activities, and includes one training and one workshop per pilot.

These activities are:

- Prepare a X-CCP,
- AI Trustworthiness,
- Data privacy,
- Cybersecurity,
- Definition of Key Performance Indicators (KPIs)

6.2 First results of X-CCP

The following sections present a brief summary of the reports describing the outcomes of the X-CCP for each pilot.

6.2.1 Workshop 1 - Prepare an X-CCP

To prepare the X-CCP practice and ensure success on this task, the first workshop "prepare a X-CCP" was held to gather a complete vision on the following subjects:

- Brief description of the pilots
- Identification of potential sub-pilots
- Pilot's environment description
- Organisation list and role(s)
- Use-case(s) of the pilot/sub-pilots
- Governance participants and roles for the pilots
- First concerns for privacy
- First concerns for Cybersecurity in your pilot
- Pilot architecture schema
- Get documentation from pilot

The HEDGE-IoT project includes six pilots. In some cases, a pilot could be split into several sub-pilots (e.g., different architectures, not the same use cases). A very brief reminder of each pilot information is available below.

6.2.1.1 Finnish Pilot

Brief description: The pilot demonstrates next-generation grid automation with IoT and edge/cloud data to improve distribution grid resiliency. The developed solutions aim to (i) enable the DSO to improve efficiency and reliability of its supply service through congestion management and fault forecasting, (ii) provide an automation platform on which different functionalities (including third-party ones) can operate and (iii) enhance the utilization of small-scale distributed energy resources (DERs) for different flexibility needs.

- Two use cases to be piloted:
    - Anomaly detection and fault forecasting to increase Medium Voltage (MV) distribution network resilience

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 (CM) to increase network hosting capacity
- Two pilot sites, where both use cases will be tested:
  - Anttola HV/MV substation
  - Hirvensalmi HV/MV substation
- No sub-pilot identified
- Initial privacy concerns:
  - Presence of PII in the collected data
  - Compliance with regulation (GDPR) is essential
  - Anonymisation and aggregation techniques are required
- Initial cybersecurity concerns:
  - Securing data transmission channels
  - Protecting critical infrastructure components from unauthorised access or cyberattacks
  - Ensuring the integrity and availability of monitoring data to maintain operational reliability.

For the Finnish pilot, the X-CCP will be performed through a unique analysis.

6.2.1.2 Greek Pilot

Brief description: The Greek pilot focuses on leveraging IoT and Edge Computing technologies to foster Local Flexibility Markets (LFMs). It aims to facilitate real-time monitoring and control of flexible assets, allowing the DSO, TSO, Market Operator, and Energy Service Providers to optimize grid operation, particularly under conditions of increasing DERs and electricity demand. The pilot demonstrates different Scientific Use Cases.

- Two use cases to be piloted:
  - GR 01 - Flexibility management through active prosumers/consumers engagement
  - GR 02 - Leveraging data exchange and AI edge algorithms for energy forecasting and prevention of critical grid events.
  - GR 03 - Flexibility trading platform for mitigating problems of the T&D networks.
- No sub-pilot identified
- Initial privacy concerns:
  - Ensuring GDPR compliance during data collection, processing, and storage.
  - Secure handling of Personally Identifiable Information (PII), including names, emails, and electricity usage.
  - Anonymisation of electricity usage data stored on edge/cloud systems
  - Avoiding unauthorised access to sensitive network and consumer data.
- Initial cybersecurity concerns:
  - Secure communication between edge, cloud and market components.
  - Threats such as unauthorised access, data breaches, and network attacks.
  - Ensuring secure APIs and authentication mechanisms.
  - Maintaining cybersecurity while supporting federated learning and real-time 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.

For the Greek pilot, the X-CCP will be performed through a unique analysis.

6.2.1.3 Italian Pilot

Brief description: The Pilot focuses on the DSO provisioning Flexibility from Energy Communities through the optimization of the Flexibility Service Provider. This is implemented, first, through a market approach, where the local flexibility market is used as primary method to interact with DERs, then through a non-market approach, where the DSO can dispatch grid limits to DERs for grid health purposes (2 BUCs). We leverage the ecosystem implemented first in PlatOne (European Project previous to RomeFlex), then in RomeFlex but all the data flows belong to the same architecture / use case. The pilots builds on previous projects results (PlatOne and RomeFlex).

- Context: The MV and LV distribution network in the Rome area. Different areas of Rome, not the whole city. At least one Energy Community will use the HEDGE-IoT platform and only one flexibility provider (Aggregator).
- Use cases:
  - Energy flow optimisation with dynamic grid limits
  - Flexibility provided by Energy Community to solve a local congestion
- No sub-pilot identified
- Initial privacy concerns:
  - None, as all the data in the Italian Pilot will be anonymised and de-georeferenced
- Initial cybersecurity concerns:
  - No specific cybersecurity concerns for the pilot, as the project is being developed on top of an existing infrastructure (RomeFlex) that already adheres to cybersecurity requirements

For the Italian pilot, the X-CCP will be performed through a unique analysis.

6.2.1.4 Dutch Pilot

Brief description: The pilot aims to build a flexible, decentralized smart grid system that not only optimizes energy usage and costs but also provides robust monitoring and control features, paving the way for sustainable and scalable energy management at Arnhems Buiten. The goal is that the implemented solutions are scalable to other business parks.

- Use cases:
  - Energy Flexibility at business park: from the buildings and from the EV chargers
  - Enhance local grid resilience through detection & prevention
- Context: A business park, with multiple buildings with different building age, layouts, infrastructure and end-users (tenants):
  - Two grid connections to the DSO
  - Public EV chargers through the park
- Two possible sub-pilots identified:
  - Sub-pilot A) The owned grid with its connected energy nodes/buildings belonging to the same owner. Being used by known tenants
  - Sub-pilot B) The (to be added) V2G charging infrastructure, with unknown users.
  - Sub pilot A and B are related to the same BUC's and SUC's.

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.

- Initial privacy concerns:
  - In general: compliance, governance and traceability
  - Ensure full compliance with legal and regulatory requirements (e.g. GDPR)
  - Establish clear data processing and storage agreements between stakeholders
  - Maintain comprehensive logging and audit trails to guarantee accountability and transparency
  - Specific focus on the information needed for transactions, when implementing V2G (via dataspaces)
- Initial cybersecurity concerns:
  - Data Confidentiality and Integrity: Protect sensitive energy and user data from unauthorized access, tampering, and breaches. This includes encryption, strict access controls, and safeguards against data manipulation (e.g. man-in-the-middle attacks).
  - System and Device Security: Secure all energy components (such as IoT nodes, EMS/BMS) against vulnerabilities, ensuring proper authentication, firmware updates, and protection against both physical and cyber-attacks that could impact system availability or reliability.

For the Dutch pilot, even with two sub-pilots, it was decided to perform the X-CCP practice through a unique analysis. If there is a need, a specific focus could be done on sub-pilot B.

6.2.1.5 Portuguese Pilot

Brief description: The Portuguese pilot connects the complete energy value-chain from users to system and market operators. The first, now prosumers, own assets capable of offering flexibility services while the operators are responsible for managing the grid and the market in a secure and optimal manner. The pilots' goal is to value the flexibility assets within an energy community by focusing on dynamic operation of the energy community using federated learning strategies that allow the optimization of the different assets and fulfilling the differentiated objectives set by the community participants.

- Use cases:
  - GreenVale: Harnessing the potential of energy communities by leveraging Federated Learning strategies.
  - Participation of industrial and residential energy communities in ancillary services market for the TSO.
- Environment: 2 Energy Communities, one represented by the DSO (CEVE) and the other one residential. The role of market operator within the pilot will be RDN, CEVE and Elergone (Aggregator and Flexibility provider role).
- No sub-pilot identified: The Portuguese pilot does not include sub-pilots given that it was structure as a complete end-to-end chain of actors and processes that depend one on another for achieving their own specific goal. In the case, it is needed data from other DSO (e-Redes), it is not part of the Consortium.
- Initial privacy concerns:
  - Users' privacy, including CEVE's clients and Sonae/Elergone information.

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 exchange is tagged but anonymised.
- Initial cybersecurity concerns:
  - communication protocols and data exchange
  - For those being subjected to cybersecurity threats, it is expected to implement authentications and firewalls as required.

For the Portuguese pilot, the X-CCP will be performed through a unique analysis.

6.2.1.6 Slovenian Pilot

Brief description: The Slovenian pilot aims to strengthen the resilience of the power grid by leveraging advanced data management and grid flexibility techniques. The primary focus is on optimizing the management of key grid components, particularly distribution and transmission transformers, through the application of advanced Dynamic Thermal Rating (DTR) algorithms. By integrating artificial intelligence and IoT data, the project enhances the visibility of the low-voltage distribution network. Implementing DTR methods at the edge helps extend equipment lifespan and mitigate overloads in critical grid elements. A key aspect of the pilot is the semantic integration of large datasets, enabling improved operational decision-making through a standardized and secure data exchange platform.

- Use cases:
  - Maximizing asset capacity for increased lifetime of DSO and TSO equipment
  - Enhanced Network Manageability and Observability
- Environment:
  - Substation assets for the use cases (Distribution Transformer in the EDGE, the IoT devices in DT for temperature and metering centre).
  - On the cloud (database and SUMO).
- Two sub-pilots were identified as they are independent of each other
  - Sub-pilot 1: Maximizing asset capacity for increased lifetime of DSO and TSO equipment.
    - Sub-pilot 2: Enhanced Network Manageability and Observability. (Data from the cloud).
    - Stakeholders:
  - Sub-pilot 1:
    - Elektro Gorenjska: leader of the pilot and in charge of providing the pilot facilities (DSO)
    - Jozef Štefan Institute (JSI): Responsible for the development of DTR/DLR edge calculations.
    - Operato: Provider of IoT assets in the distribution grid.
    - ELES: TSO (it will provide the pilot facilities in TSO grid).
  - Sub-pilot 2:
    - UNIZG: Responsible for the development of ML algorithms.
    - Operato: Provider of IoT assets in distribution grid. (SUMO Cloud)
    - KONČAR: A technology partner that provides a platform for the semantic model of the substation.

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.

- Initial privacy concerns:
  - In Sub-Pilot 1, no personal or business-sensitive data will be processed. However, during the development of IoT services, user access controls will be implemented. All data transmissions will be encrypted with an additional layer of encryption, alongside the existing encryption in transport and lower network layers.
  - In Sub-Pilot 2 most of the shared data does not contain sensitive information without knowing the specific context that is not shared. Specific identifiers of substations will be anonymized in such a way that their unique label will be replaced by a randomly generated string that does not contain any sensitive information.
- Initial cybersecurity concerns:
  - Securing data transmission channels
  - Protecting critical infrastructure components from unauthorised access or cyberattacks
  - Ensuring the integrity and availability of monitoring data to maintain operational reliability.

For the Slovenian pilot, the X-CCP will be performed on one of the two sub-pilots, to be defined.

6.3 Workshop 2 - AI Trustworthiness analysis

6.3.1 Introduction

This activity was divided into four main steps:

1. Training and awareness: A session was held on the topics of trustworthiness, AI trustworthiness, associated regulation and standardisation, workshop preparation, and questionnaire preparation.
2. AI Impact assessment (one by AI system studied): This preparatory work took the form of a guided questionnaire with the aim of:
   - provide initial analysis and basis for the workshop in a form of a high-level AI impact assessment,
   - allow a best possible workshop preparation for the participants by understanding the topics to be covered,
   - perform an impact assessment of their AI system guided by the predefined framework,
   - allow participants to find relevant information in advance even if unknown by them, which is crucial for the workshop's success and
   - finally allow a more efficient workshop
3. Workshop: This collaborative and guided workshop could be titled "AI system categorisation and risk/threats/controls analysis" and goes through the following steps:
   - review and validation of the AI system information based on the completed AI impact assessment,
   - estimation, justification and agreement of the studied AI system risk category according to the AI act,
   - identification of the relevant risks or harms for the AI system studied,
   - categorisation of identified risks by types of impact,

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.

- For each identified risk:
    I. risk map completion considering likelihood and impact,
    II. identification of threats or hazards that may lead to the risk,
    III. identification of controls or mitigation maneuvers possible to prevent, mitigate or avoid the risk, and
- identification of trustworthiness gaps.

4. Results summary report: This report summarises the activities performed and results obtained.
5. The following elements are the main outputs of the AI trustworthiness related activities:

- A recorded training session (to prepare the workshop) including a slide deck on the topic of AI trustworthiness (definitions, references, AI trustworthiness, AI regulation, AI Act, AI standardisation, AI Act harmonized standard, AI impact assessment methodology, AI trustworthiness analysis methodology, workshop preparation).
- One AI impact assessment by pilot on a selected AI system
- One report by pilot summarizing their workshop results and conclusion

AI Impact Assessment

The AI Impact assessment, was achieved following the structure of the table below:

TABLE 7 : AI TRUSTWORTHINESS QUESTIONNAIRE STRUCTURE (BASED ON ISO/IEC 42005)[11]

Section	Sub-section	Key items
Plan and AI system characterisation	Plan information	• Generic information about the plan like version management, confidentiality and contacts.
	AI system characterization	• ID information about the AI system like system purpose, life cycle stage, objectives, context, infrastructure, location, and accountability.
Impact assessment	AI risk management	• Relevant interested parties • Uses information • AI Risk management • Ethical, societal and environmental impact
	Data, Algorithm and Model information	• Data information and quality • Algorithms and models information and quality
	Regulatory and standards compliance	• Regulatory compliance • Standard Alignment
	AI Trustworthiness	• AI Cybersecurity (including logging functionalities) • AI privacy • AI Robustness, resilience and accuracy • AI Transparency (transparency, explainability, documentation) • AI management (governance, human oversight)
	AI Trustworthiness assurance	• AI trustworthiness assurance expectations • AI trustworthiness process
Continuous improvement	Continuous improvement	• Continuous monitoring • Continuous maintenance • Continuous development
Other items	Other items and complementary information	• Open section for additional information

Workshop

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.

During the workshops, a collaborative online tool named Mural was used by all participants. Seven steps were followed throughout the session. The results were identified, and each report will receive a dedicated report which summarizes the results and conclusions.

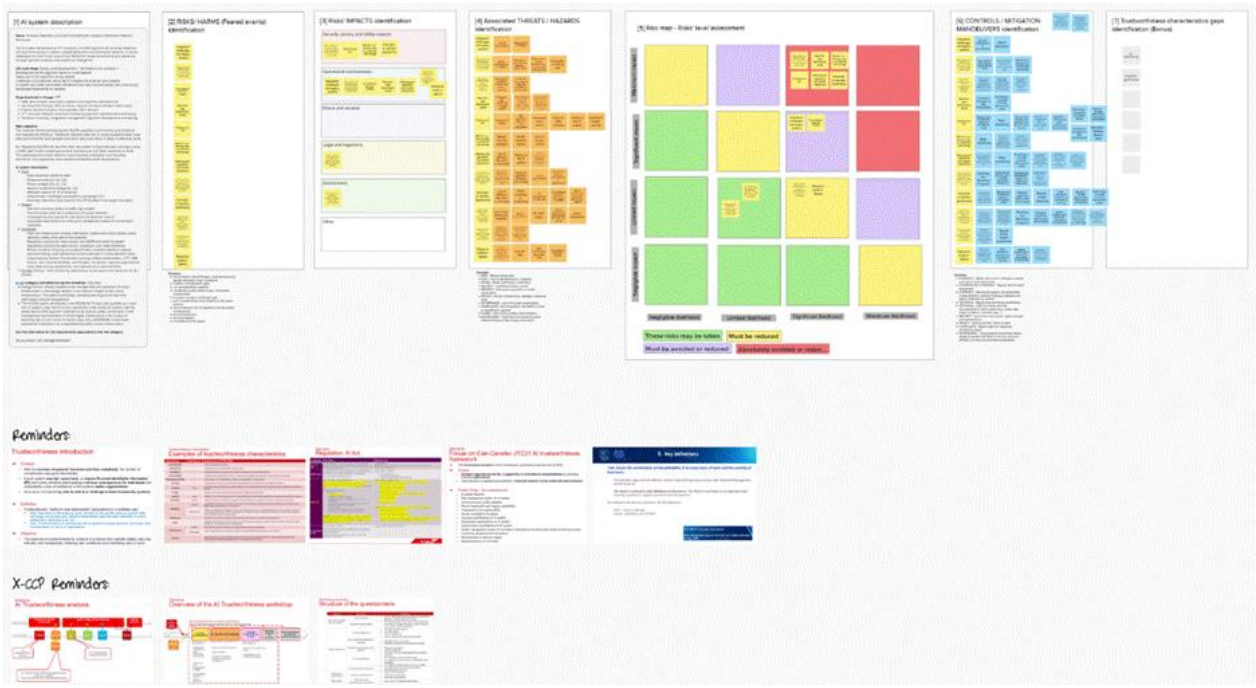


FIGURE 16 OVERVIEW OF A COMPLETED COLLABORATIVE TOOL USED FOR THE WORKSHOP (MURAL)

6.3.2 High-level results Summary

For each pilot, one AI system was analysed. The AI trustworthiness analysis reports for each pilot are available in annexes. This section presents an overview of the workshops' results and an example summarising the threats, risks and controls identified for one specific pilot.

6.3.2.1 Finnish Pilot

Table 8 FINNISH PILOT OVERVIEW

AI system name	Anomaly Detection and Fault Forecasting to Increase Distribution Network Resilience
Main objective	The AI system developed by VTT employs an HLSTM algorithm for anomaly detection and fault forecasting in medium voltage (MV) electrical distribution networks. It will be integrated into the Finnish pilot of the HEDGE-IoT project to enhance grid resilience through real-time analytics and predictive intelligence.
Life cycle stage	Design and development > Verification and validation
AI Act category estimation	High-Risk

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.

Number of risks/harms identified (Feared events)	12	
Number of threats/hazards identified* (for the risks)	43	
Number of controls/mitigation measures* (for the risks)	52	
Main trustworthiness gaps identified (for the AI Act category)	Clear, sufficient and regular impact assessment	Partially covered
	Clear, sufficient and regular risk management	Partially covered
	Clear, sufficient and regular quality management	Gap
	Sufficient AI system life cycle process	Gap
	Clear, sufficient and regular fundamental rights impact assessment	Gap
	Compliance with the regulatory framework	Partially covered
	EU High-risk AI system registration and requirements	Gap
	Clear governance and accountability (system and data)	Partially covered
	Sufficient cybersecurity level	Gap
	Sufficient privacy and data protection level	Partially covered
	Clear and operational human oversight; sufficient controllability	No gap
	Sufficient AI logging (automatic) and record-keeping capabilities	No gap
	Clear technical documentation and documentation keeping capability	No gap
	Sufficient robustness and resilience	Partially covered
	Sufficient safety	Partially covered
	Sufficient accuracy and reliability	No gap

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.

	Sufficient transparency	No gap
	Sufficient explainability	Partially covered
	Sufficient data/algorithm quality and suitability	No gap

*: Some are similar from one risk to another.

6.3.2.2 Greek Pilot

TABLE 9 GREEK PILOT OVERVIEW

AI system name	Flexibility Optimisation Service	
Main objective	The AI system powers a Flexibility Optimisation Service within the HEDGE-IoT platform. It is designed to: • Request flexibility provisions from participating households (prosumers or consumers). • Provide automated forecasts for energy demand and photovoltaic (PV) production using real-time and historical data. • Disaggregate household energy usage into device-level consumption via Non-Intrusive Load Monitoring (NILM). • Optimize bidding behavior for the aggregator in the Local Flexibility Market (LFM), leveraging dispatch plans and customer data. • Optimise Formulate and personalize flexibility offers using incentive optimization based on behavioral predictions and market signals.	
Life cycle stage	Software service test	
AI Act category estimation	High-Risk	
Number of risks/harms identified (Feared events)	10	
Number of threats/hazards identified* (for the risks)	42	
Number of controls/mitigation measures* (for the risks)	46	
Main trustworthiness gaps identified (for the AI Act category)	Clear, sufficient and regular impact assessment	Partially covered
	Clear, sufficient and regular risk management	Partially covered
	Clear, sufficient and regular quality management	Gap

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.

	Sufficient AI system life cycle process	No gap
	Clear, sufficient and regular fundamental rights impact assessment	Gap
	Compliance with the regulatory framework	Partially covered
	EU High-risk AI system registration and requirements	Gap
	Clear governance and accountability (system and data)	Gap
	Sufficient cybersecurity level	Partially covered
	Sufficient privacy and data protection level	No gap
	Clear and operational human oversight; sufficient controllability	No gap
	Sufficient AI logging (automatic) and record-keeping capabilities	No gap
	Clear technical documentation and documentation keeping capability	No gap
	Sufficient robustness and resilience	Partially covered
	Sufficient safety	Partially covered
	Sufficient accuracy and reliability	Partially covered
	Sufficient transparency	No gap
	Sufficient explainability	Partially covered
	Sufficient data/algorithm quality and suitability	Partially covered

*: Some are similar from one risk to another.

6.3.2.3 Italian Pilot

Table 10 ITALIAN PILOT OVERVIEW

AI system name	Application of Machine Learning methods for photovoltaic production forecasting in the context of Energy Communities

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.

Main objective	The AI system forecast the PV plant production leveraging on the data coming from the weather stations, the technical characteristics of the plant, the historical and real time measurements and the diagnostic data. Moreover, it analyses the customers data to forecast EC members load profiles to increase the energy sharing in the communities. It aims to improve the balancing in the energy communities and in the distribution grids. The two forecasts will be shared to an operator; they will not have direct automated actions based on them.	
Life cycle stage	Design and development stage	
AI Act category estimation	Limited	
Number of risks/harms identified (Feared events)	13	
Number of threats/hazards identified* (for the risks)	56	
Number of controls/mitigation measures* (for the risks)	45	
Main trustworthiness gaps identified (for the AI Act category – Limited risk)	Clear transparency	No gap
	Compliance with the regulatory framework	Gap
Other trustworthiness gaps identified	Clear, sufficient and regular impact assessment	Partially covered
	Clear, sufficient and regular risk management	Gap
	Clear, sufficient and regular quality management	Gap
	Sufficient AI system life cycle process	Gap
	Clear, sufficient and regular fundamental rights impact assessment	Gap
	Clear governance and accountability (system and data)	Gap
	Sufficient cybersecurity level	Partially covered
	Sufficient privacy and data protection level	Partially covered
	Clear and operational human oversight; sufficient controllability	Partially covered
	Sufficient AI logging (automatic) and record-keeping capabilities	Partially covered

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.

	Clear technical documentation and documentation keeping capability	Partially covered
	Sufficient robustness and resilience	Partially covered
	Sufficient safety	Partially covered
	Sufficient accuracy and reliability	Partially covered
	Sufficient explainability	Gap
	Sufficient data/algorithm quality and suitability	No gap

*: Some are similar from one risk to another.

6.3.2.4 Dutch Pilot

TABLE 11 DUTCH PILOT OVERVIEW

AI system name	Anomaly Detection and Predictive Maintenance	
Main objective	This AI system aims to provide real-time monitoring of graph data streams between smart devices, aiming to detect technical failures and other anomalies within the system on time, providing real-time alerts and explanations. Detecting anomalies on time is a critical component of building management systems, resulting in more efficient energy use and less wear and tear.	
Life cycle stage	Verification and validation	
AI Act category estimation	High-Risk	
Number of risks/harms identified (Feared events)	13	
Number of threats/hazards identified* (for the risks)	44	
Number of controls/mitigation measures* (for the risks)	57	
Main trustworthiness gaps identified (for the AI Act category)	Clear, sufficient and regular impact assessment	Partially covered
	Clear, sufficient and regular risk management	Partially covered
	Clear, sufficient and regular quality management	Partially

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.

		covered
	Sufficient AI system life cycle process	Partially covered
	Clear, sufficient and regular fundamental rights impact assessment	Gap
	Compliance with the regulatory framework	Gap
	EU High-risk AI system registration and requirements	Gap
	Clear governance and accountability (system and data)	Gap
	Sufficient cybersecurity level	Gap
	Sufficient privacy and data protection level	Gap
	Clear and operational human oversight; sufficient controllability	No gap
	Sufficient AI logging (automatic) and record-keeping capabilities	No gap
	Clear technical documentation and documentation keeping capability	Gap
	Sufficient robustness and resilience	Partially covered
	Sufficient safety	Gap
	Sufficient accuracy and reliability	Gap
	Sufficient transparency	No gap
	Sufficient explainability	Partially covered
	Sufficient data/algorithm quality and suitability	Partially covered

*: Some are similar from one risk to another.

6.3.2.5 Portuguese pilot

TABLE 12 PORTUGUESE PILOT OVERVIEW

AI system name	Vector Autoregressive Model for Energy Time Series 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.

Main objective	This AI system is a decentralized peer-to-peer federated learning approach, focusing on data privacy, with the goal of forecasting energy consumption time series data for residential consumers. The rationale behind the development of this federated learning approach is the need for a scalable model, focused on protecting the private data of end consumers and that uses the processing power at the edge to its fullest extent. Where are used the outputs? Stored in a datalake on INESC TEC's premises and used in an energy community for monitoring, optimization, flexibility. Flexibility module (RECreation) is automatically triggered by the AI system under study.	
Life cycle stage	Verification and validation > Deployment	
AI Act category estimation	High-Risk	
Number of risks/harms identified (Feared events)	12	
Number of threats/hazards identified* (for the risks)	37	
Number of controls/mitigation measures* (for the risks)	51	
Main trustworthiness gaps identified (for the AI Act category)	Clear, sufficient and regular impact assessment	Partially covered
	Clear, sufficient and regular risk management	Partially covered
	Clear, sufficient and regular quality management	Partially covered
	Sufficient AI system life cycle process	Partially covered
	Clear, sufficient and regular fundamental rights impact assessment	Gap
	Compliance with the regulatory framework	Partially covered
	EU High-risk AI system registration and requirements	Gap
	Clear governance and accountability (system and data)	Partially covered
	Sufficient cybersecurity level	Partially covered

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.

	Sufficient privacy and data protection level	No gap
	Clear and operational human oversight; sufficient controllability	Partially covered
	Sufficient AI logging (automatic) and record-keeping capabilities	NA
	Clear technical documentation and documentation keeping capability	NA
	Sufficient robustness and resilience	NA
	Sufficient safety	NA
	Sufficient accuracy and reliability	NA
	Sufficient transparency	No gap
	Sufficient explainability	NA
	Sufficient data/algorithm quality and suitability	NA

*: Some are similar from one risk to another.

6.3.2.6 Slovenian pilot

TABLE 13 SLOVENIAN PILOT OVERVIEW

AI system name	Local weather forecast for DTR and DLR
Main objective	Dynamic thermal rating calculation / Dynamic line rating calculation depends on the weather data input. The purpose of AI system is to provide short-term local weather forecast based on weather station measurements and local terrain characteristics using AI.
Life cycle stage	Design and development
AI Act category estimation	Limited
Number of risks/harms identified (Feared events)	9
Number of threats/hazards identified* (for the risks)	30
Number of controls/mitigation measures* (for the risks)	31

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.

Main trustworthiness gaps identified (for the AI Act category – Limited risk)	Clear transparency	No gap
	Compliance with the regulatory framework	Partially covered
Other trustworthiness gaps identified	Clear, sufficient and regular impact assessment	Partially covered
	Clear, sufficient and regular risk management	Partially covered
	Clear, sufficient and regular quality management	Partially covered
	Sufficient AI system life cycle process	Partially covered
	Clear, sufficient and regular fundamental rights impact assessment	No gap
	Clear governance and accountability (system and data)	Gap
	Sufficient cybersecurity level	No gap
	Sufficient privacy and data protection level	No gap
	Clear and operational human oversight; sufficient controllability	No gap
	Sufficient AI logging (automatic) and record-keeping capabilities	Partially covered
	Clear technical documentation and documentation keeping capability	Partially covered
	Sufficient robustness and resilience	Partially covered
	Sufficient safety	No gap
	Sufficient accuracy and reliability	Partially covered
	Sufficient explainability	Partially covered
	Sufficient data/algorithm quality and suitability	No gap

*: Some are similar from one risk to another.

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.

6.4 Overview of Workshop outputs – Finnish pilot example

One part is the workshops is the identification of:

- AI system risks/harms
- Threats/Hazards that can lead to the identified risks
- Controls/mitigation measures that can mitigate/control/prevent identified risks.

The following table presents a summary of the outputs coming from the Finnish pilot workshop.

TABLE 14 EXAMPLE OF THE FINNISH PILOT AI RISK ANALYSIS SUMMARY

THREATS	RISK	CONTROLS
• Lack of documentation • Interoperability challenges	Integration challenges with legacy systems	• Ensure a sufficient level of documentation • Use of standards
• Lack of representativity in datasets • Processed or preprocessed data (e.g., sensor data) • Biases due to wrong feedback loop (wrong output reuse as input) • Incomplete or missing data	Data quality and integrity issues (e.g., processed or preprocessed sensor data)	• Data validation before feeding into the HLSTM model • Use of redundant data sources to minimize the impact of missing data • TECHNICAL - Regular bias and fairness audits/tests
• High quantity of data to analyse (real time or historical) • Limited/low computational resources allocated to the AI system	Big datasets analysis issue due to computational resource limitations	• Secure data storage and processing in compliance with GDPR and internal security policies. • TECHNICAL - Data quality checks (e.g., data input accuracy, completeness and representativity) • computational resources estimation and design of the system accordingly
• Integration and interfacing with Edge systems • Wrong configuration and connection between the substation or Feeders Scenario modeling on RTDS simulator • Data streaming issue: Pilot site Substation or Feeders real-time input data streaming	Real-time data transmission issues	• End-to-end encryption of data transmissions • FUNCTIONAL - Complete functional testing of the system
• Cybersecurity attacks • Data poisoning attacks or model manipulation • Adversarial inputs attacks • Insecure data handling • Abuse of the AI system	Cybersecurity Risk	• Regularly audit AI systems to detect and eliminate any biases • Risks monitoring • Adherence to cybersecurity standards and access control 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.

• Insufficient access controls		• SECURITY - AI cybersecurity watch to continuously improve system security. • SECURITY - Compile and apply cybersecurity best practices • TECHNICAL - Adversarial robustness testing • SECURITY - Simulate attacks to test model behavior and resilience • End-to-end encryption of data transmissions • SECURITY - Reliable backup ready
• Biased training datasets • Model inversion attacks • Lack of access control	PRIVACY risk - Personal data or confidential data leakage	• Risks monitoring • Secure data storage and processing in compliance with GDPR and internal security policies. • SECURITY - Control and track access, rights, changes and authentication
• Lack of testing in real-world or rare cases • Failure of the AI system • Lack of continuous risk identification, monitoring, management and control	Affecting grid operations and market interactions	• Use of redundant data sources to minimize the impact of missing data • Risks monitoring • FUNCTIONAL - Complete functional testing of the system • OVERSIGHT - Define clear human oversights, controls and human-in-the-loop review • TECHNICAL - Continuous system monitoring and assessment (e.g., system performance and anomalies) • TECHNICAL - Be ready for system failure with defined remediation plans and fallback mechanisms
• Ignorance of regulations and compliance requirements in the development and/or management team • No/lack of logging for traceability and oversight • Lack of documentation • Lack of role clarity or accountability or responsibility	Non-compliance with national or EU regulations (e.g., GDPR, AI Act, CRA) leads to lawsuits or penalties.	• Reskilling and Retraining Programs • COMPLIANCE - Develop AI ACT and GDPR compliance frameworks • GOVERNANCE & OVERSIGHT - Regular Risk analysis and assessment • GOVERNANCE - Training and awareness-raising (developers, top management)
• Lack of testing in real-world or rare cases • Model overfitting or underfitting • Poor generalization to edge case • Inconsistencies across AI model versions or updates • Lack of maintenance and model (re)training on dataset	Incorrect or harmful predictions	• Integration of human-in-the-loop decision support, avoiding full automation • Regularly audit AI systems to detect and eliminate any biases • Feedback loops from team in pilot environments • Regular model retraining • Clear roadmap for scalability and maintenance planning • SECURITY - Simulate attacks to test model behavior and resilience • FUNCTIONAL - Complete functional testing of the system
• Lack of user training and expertise • Lack of documentation	Lack of user adoption (e.g.,	• Integration of human-in-the-loop decision support, avoiding full automation

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.

• No clear output • Lack of explainability, opaque (black-box) decision-making • Lack of transparency	due to explainability or transparency concerns)	• Develop AI systems with explainable models that allow decision-making processes to be easily understood by humans • Reskilling and Retraining Programs • Feedback loops from team in pilot environments • Iterative prototyping and testing with users before full deployment • TECHNICAL - Use explainability tools/methods to improve outputs understanding (e.g., SHAP, LIME) • TECHNICAL - Use interpretable models to foster outputs explainability
• Significant computational power needed leading to high energy consumption • No monitoring of environmental risks and possible changes around the AI system.	Environmental risks (e.g., massive increase in electricity consumption)	• ENVIRONMENT - Incorporate environmental metrics: design AI systems that factor in not only economic efficiency but also environmental sustainability • Regular ethical impact assessment
• Lack of continuous risk identification, monitoring, management and control • Lack of data • Data transmission issue (real time) • Computational ressources limitation	Failure to scale or deploy	• Continuous performance evaluation of the HLSTM model during simulation phases • Clear roadmap for scalability and maintenance planning • Iterative prototyping and testing with users before full deployment • TECHNICAL - Simulate misuse scenarios to test model behavior and resilience

6.5 Trustworthiness profiles

This section presents the methodology selected to investigate the HEDGE-IoT trustworthiness profiles.

The notion of trustworthiness was extensively described in HEDGE-IoT D4.1 [6], however, a reminder of the definition is below.

> Note: Depending on the context or sector, and also on the specific product or service, data, technology and process used, different characteristics apply and need verification to ensure stakeholders' expectations are met.
>
> Note: Trustworthiness is an attribute that can be applied to services, products, technology, data and information as well as to organisations.
>
> The list of trustworthiness cross-cutting characteristics can vary according based on stakeholder expectations.

Applying trustworthiness to AI ensures that systems tend to be reliable, fair, and secure, and remain responsible and valuable for society.

6.5.1 Trustworthiness construction method

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.

HEDGE-IoT has selected a trustworthiness profile construction method initiated by the ongoing ECLIPSE-Digital project [5] in which TRIALOG is also involved. The initial methodology is described in deliverable D3.2 "Specific Data Protection Analysis" [5].

6.5.2 Profile

A profile is a standards-writing concept defined in ISO/IEC TR 10000-1:1998.

In essence, a profile is a named set of requirements on an object of conformity assessment.

Profile definitions can be used to add structure to standards documents, making them easier to navigate, and also to create subsets or supersets of the requirements in already-existing standards documents.

In other words, a profile is a viable list of requirements in a specific context.

ISO TR 10000-1 (Information technology — Framework and taxonomy of International Standardised Profiles - Part 1: General principles and documentation framework) provides guidance on profiles. The main concepts associated with the profile approach are as follow:

- **Base standard:** Refers to a standard that can be referenced in a profile.
- **Profile:** Set of base standards subsets, options, parameters.
- **Taxonomy:** Refers to a classification of profiles.

6.5.3 Application to HEDGE-IoT

In HEDGE-IoT, profiles represent an agreed selection of requirements designed to make pilots implementations more trustworthy, i.e. overall, a target level of trustworthiness to be achieved in each project use case context. Profiles will be defined per cross-cutting characteristic and for each pilot. Profiles will explore and construct specific trustworthiness profiles accordingly.

6.5.3.1 Construction of Trustworthiness profile

The trustworthiness profiles will be defined with mandatory fields of information within a specific context according to pilots' generalizable assumptions:

TABLE 15 TRUSTWORTHINESS PROFILE FIELDS

Field	Description
Context	The context is the one provided by the HEDGE-IoT project that is constituted by the Reference Architecture (RA) and the system use cases (SUCs).
Characteristic	Characteristics are the ones that trustworthiness objectives have been identified.
Goal / Risk	The Goals/Risks are the ones identified during the X-CCP characteristics analysis.
Capability / Measure	The Capability/Control / Measure are the ones selected/suggested to achieve the Goals or to reduce the Risks.
Requirement	Functional and non-functional requirements to achieve the Capabilities/Controls / Measures. Requirements include the "... shall ..." statement in the requirement sentence.
Guidance	Recommendations on solutions to apply to bring to completion or reality the requirement.

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.

	Requirements include the "… should …" statement in the recommendation sentence. A recommendation can also include justifications for applying or not previously defined requirements.
Description	A complete description of the recommendation, including references to characteristics base standards and rules for the selection of the lists, subsets, options and parameters if needed.

Hence, for reference, Capabilities and Measures identified during the X-CCP characteristics analysis will be summarised in the table below for further usage within the requirements:

TABLE 16 EXAMPLE OF A TRUSTWORTHINESS PROFILE STRUCTURE

Characteristic	**Goal / Risk**	**Capability / Control / Measure**
CH-CH1	GL-GL1	CP-CP1 CP-CP2
	RK-RK1	MS-MS1
CH-Privacy	GL-Safety	CP-Protect_PII
…		

6.7 Next steps

T4.5 will continue the X-CCP practice execution in collaboration with the pilots. First, by finalising the Data privacy workshops and then going through the security and progress assessment ones.
In parallel, exploration work will start to define HEDGE-IoT trustworthiness profiles. First, the task will capitalise on a methodology developed in the ECLIPSE Digital project, continue its development and adapt it to HEDGE-IoT needs. This method will then be used to explore HEDGE-IoT trustworthiness profiles based on the results of the X-CCP practice.

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. CONCLUSIONS AND NEXT STEPS

7.1 Summary of Achievements Since D4.1

Compared with Deliverable D4.1, this report presents substantial progress:

- **EDC Integration**: The connector was extended beyond its initial setup, incorporating control/data plane separation and first implementations of programmatic clients.
- **MVD Dashboard**: A functional prototype of the data dashboard was introduced, providing monitoring of assets, contracts, policies, and transfers, and offering mock-based validation.
- **App Store**: An alpha version was developed, enabling registration, publication, and search of applications, with a roadmap defined towards a fully DSP-compliant App Store.
- **Semantic Interoperability**: The adoption and alignment of SAREF, IEC CIM, PowerCIM, and Semantic Treehouse were advanced, ensuring semantic consistency across pilots.
- **Pilot Integration**: Concrete validation activities were carried out in Dutch, Greek, Italian, Finnish, Slovenian, and Portuguese pilots, demonstrating interoperability levels 3 to 5 across multiple contexts.
- **Cross-Cutting Security and Privacy**: The implementation of the X-CCP continued with workshops on AI trustworthiness and the construction of preliminary trustworthiness profiles.

Together, these accomplishments highlight the transition from a conceptual framework (D4.1) to a consolidated and partially validated interoperability solution (D4.2), setting the stage for full-scale validation and replication in the next phase.

Conclusions

Deliverable D4.2 consolidates the progress of WP4 towards building an interoperable and operational framework for data sharing in the energy ecosystem. The integration of the Eclipse Dataspace Connector (EDC), the development of the MVD Dashboard, the evolution of the Open Services Catalogue and App Store, and the validation of semantic interoperability enablers have collectively strengthened the maturity of the HEDGE-IoT interoperability framework. Through pilot-driven validation and architectural refinements, the project has demonstrated its capacity to bridge technical, semantic, and organizational layers of interoperability, while also reinforcing security, privacy, and trustworthiness aspects. The results achieved confirm that the project is on track to deliver a scalable and replicable dataspace model for cross-domain applications in the European energy sector.

Next Steps

Building on the current achievements, the next phase will focus on:

- Advancing from prototype-level implementations to fully operational deployments across pilot sites.
- Refining the integration of services within the App Store and aligning them with the latest Dataspace Protocol (DSP) specifications.

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.

- Expanding semantic interoperability activities, including ontology lifecycle management, PowerCIM enhancements, and the use of Semantic Treehouse for broader cross-pilot harmonisation.
- Strengthening the security and privacy framework by consolidating the Cross-Cutting Characteristics Plan and further developing trustworthiness profiles.
- Enhancing testing and validation activities to support large-scale adoption and replication across pilots and external stakeholders.

These steps will pave the way for Deliverable D4.3, which will represent the final technological release of the interoperability framework, showcasing full operational maturity and cross-sector integration.

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] HEDGE-IoT "D3.3: HEDGE-IoT Technological Enablers (First Release)", 2025

[2] HEDGE-IoT "D3.4 Technological Enablers (Intermediate Release)", 2025

[3] International Data Spaces Association (IDSA), Semantic Interoperability in Data Spaces, Position Paper, v1.0, Mar. 2024. [Online]. Available: European Commission, https://internationaldataspaces.org/download/50890/?tmstv=1758274720

[4] "Next Generation EIF – Survey," Interoperable Europe Portal. [Online]. Available: Next Generation EIF - Survey | Interoperable Europe Portal

[5] Eclipse Digital, Eclipse Digital, 2024. [Online]. Available: https://eclipse-digital.eu/

[6] HEDGE-IoT "D4.1 – Interoperability Framework and Integrated Solution (First Release)", 2025.

[7] SYNERGY Project (H2020), Deliverable D3.5 – Semantic Interoperability in Smart Grids, 2023.

[8] Joint Research Centre (JRC), Code of Conduct for Energy Smart Appliances (ESA) Interoperability Test Method, 2023.

[9] ISO/IEC 21823-5:2022, Internet of Things (IoT) – Interoperability for IoT Systems – Part 5: Behavior and Policy, ISO/IEC, 2022.

[10] ETSI TS 103 264 V3.1.1, SmartM2M; Smart Appliances Reference Ontology (SAREF), 2023-06.

[11] ISO/IEC 42005:2023, Artificial Intelligence – Trustworthiness, ISO/IEC, 2023.

[12] EEBUS Initiative e.V., SPINE IoT Working Group – Specifications and Interoperability Framework, 2023.

[13] Eclipse Foundation, Eclipse Dataspace Connector (EDC) Documentation, 2024. [Online]. Available: https://projects.eclipse.org/projects/technology.edc

[14] International Data Spaces Association (IDSA), Dataspace Protocol (DSP) Specification v2024.1, 2024. [Online]. Available: https://internationaldataspaces.org/dsp-specification

[15] M. Larhrib, M. Escribano, C. Cerrada, and J. J. Escribano, "An Ontological Behavioral Modeling Approach with SHACL, SPARQL, and RDF Applied to Smart Grids," IEEE Access, vol. 12, pp. 82041–82056, 2024.

[16] T. R. Silva, J. L. Hak, and M. Winckler, "A behavior-based ontology for supporting automated assessment of interactive systems," in 2017 IEEE 11th International Conference on Semantic Computing (ICSC), Jan. 2017, pp. 250–257.

[17] R. Chen, Y. Liu, and X. Ye, "Ontology based behavior verification for complex systems," in International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, vol. 51739, p. V01BT02A038, Aug. 2018, American Society of Mechanical Engineers.

[18] Object Management Group, Business Process Model and Notation (BPMN) version 2.0.2, 2014. [Online]. Available: https://www.omg.org/spec/BPMN/2.0.2/

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.

8. ANNEX A: ODC-TESTER – BEHAVIORAL TESTING STATE OF THE ART

This chapter completes the section about the semantic enabler ODC-Tester available in the core of the deliverable **Error! Reference source not found.**. It describes:

- the literature review performed in the context of the project to identify and study existing content on bahavioral testing,
- the datasets and the associated actions done or ongoing to enable testing with both simulation and real data, [8]
- a draft of the ODC-Tester behavioral testing methodology, and
- a description of the ISO/IEC 21823-5 contribution [9]

Behavioral testing - Literature review

Behavioral testing plays a vital role in validating dynamic system behaviors such as state transitions, timing constraints, and compliance with policy rules conform to defined specifications and standards. As part of our methodology design, we conducted a targeted review of 25 research publications related to behavioral testing within ontology and Semantic Web contexts. From this, three key studies were identified as particularly influential in shaping our framework

Main references studied:

- Larhrib, M., Escribano, M., Cerrada, C., & Escribano, J. J. (2024). An Ontological Behavioral Modeling Approach with SHACL, SPARQL, and RDF Applied to Smart Grids. IEEE Access, 12, 82041-82056. [15]
- Silva, T. R., Hak, J. L., & Winckler, M. (2017, January). A behavior-based ontology for supporting automated assessment of interactive systems. In *2017 IEEE 11th International Conference on Semantic Computing (ICSC)* (pp. 250-257). IEEE.[16]
- Chen, R., Liu, Y., & Ye, X. (2018, August). Ontology based behavior verification for complex systems. In *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference* (Vol. 51739, p. V01BT02A038). American Society of Mechanical Engineers.[17]
- Object Management Group. (2014). *Business Process Model and Notation (BPMN) version 2.0.2*. https://www.omg.org/spec/BPMN/2.0.2/[18]

Larhrib et al. (2024) propose an ontology-based behavioral modeling approach utilizing RDF graphs combined with SHACL constraints and SPARQL rules. Their lightweight meta-ontology includes four key classes: tasks, states, transitions, and conditions, enabling the construction of executable semantic workflows. This methodology was validated through compliance testing under the CGMES (Common Grid Model Exchange Standard) standard in the smart grid domain. However, it exhibits limitations in modeling complex temporal logic and iterative workflows due to SHACL and SPARQL expressivity constraints. Crucially, the authors explicitly mention BPMN and UML activity diagrams

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.

as examples of visual languages employed during early requirement specification stages, providing a clear literature grounding for BPMN's relevance in behavioral modeling.

Silva et al. (2017) developed a behavior-based ontology tailored to automated functional testing of interactive systems under Behavior-Driven Development (BDD). They address the abstraction challenge that BDD tests are often tied to low-level UI events by raising the level of representation: tests are expressed over an ontology capturing high-level user behaviors that span across prototypes and implemented interfaces. Through a case study in a flight-booking e commerce context, this approach enabled automated assessment of functional requirements across low-fidelity prototypes and final UI artifacts. While it enhances reusability and semantic traceability, its focus remains on UI-driven behaviors and does not address rigorous timing semantics or complex control flows.

Chen et al. (2018) present a framework for transforming UML behavioral diagrams into OWL ontologies, supplemented with rule-based verification for early behavioral validation. This approach facilitates the identification of inconsistencies in behavioral models during early design phases. However, reliance on OWL description logic creates scalability challenges, particularly in scenarios involving complex temporal constraints or concurrent processes.

Beyond these ontology-based methods, alternative modeling techniques were reviewed. Petri Nets offer formal verification of temporal and concurrency properties, but lack semantic interoperability. Network-based behavioral profiling emphasizes communication patterns but omits semantic state management and fine-grained timing semantics.

Following the literature review, Business Process Model and Notation (BPMN) was selected as the most suitable modeling formalism for our behavioral testing framework. Its broad industrial adoption, particularly in sectors such as energy, manufacturing, and digital systems, supports process transparency and regulatory compliance. BPMN offers a standardized and intuitive graphical representation of system behaviors, enabling collaboration between technical and non-technical stakeholders. It is explicitly referenced in Larhrib et al. (2024) as a recognized modeling language for early requirements, reinforcing its relevance in ontology-driven contexts. Moreover, BPMN aligns well with Semantic Web technologies as its constructs can be systematically mapped to RDF-based models and enriched with SHACL constraints and SPARQL rules, enabling executable workflows and semantic validation. Compared to other reviewed methods (e.g., Petri Nets, OWL-based logic), BPMN provides a balanced solution combining expressiveness, scalability, and interoperability, making it a solid foundation for modeling and validating complex behavioral scenarios within our semantic architecture.

Dataset

For the testing and validation of the ODCT (Ontology-Driven Constraint Tester) tool, particularly in the context of behavioral testing, identifying an appropriate dataset is crucial. In our initial version focused on static and semantic testing developed in the Int: Net project, we selected Scenario 1, titled *"Announcement of Plan"* from the Flexible Start use case defined by the *JRC (Joint Research Centre) Code of Conduct*. In the extended version aimed at behavioral testing, we initially selected Scenario 3, titled *"Select Alternative Power Sequence"*. However, this selection is flexible and subject to change based on future requirements and project needs.

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.

As part of our efforts to collect relevant data, we contacted smart appliance manufacturers, specifically Miele and Beko, to request datasets that fully align with the Flexible Start use case scenarios. However, the datasets we obtained were limited in scope: Miele provided data covering Scenario 1 ("*Announcement of Plan*") and Scenario 2 ("*Shift Preferred Power Sequence*"), while Beko provided data covering only Scenario 1. Neither manufacturer provided datasets corresponding directly to Scenario 3 ("*Select Alternative Power Sequence*"), as they do not currently have any smart appliances that fall under this scenario.

Therefore, to meet the precise testing and validation requirements for Scenario 3, we developed a simulated dataset. This simulated dataset strictly adheres to the detailed specifications of the *JRC's Code of Conduct Flexible Start* use case, including clearly defined optional power sequences, associated schedule constraints (such as earliest start and latest end times), state transitions (preferred, optional, invalid), and accurate mechanisms for transitioning between optional and preferred power sequences. This rigorously structured simulated dataset enables comprehensive and precise behavioral testing, thereby enhancing the reliability and robustness of our semantic validation processes within the ontology-driven behavioral testing framework.

Draft behavioral testing architecture

Behavioral testing requires the following capability: flow management

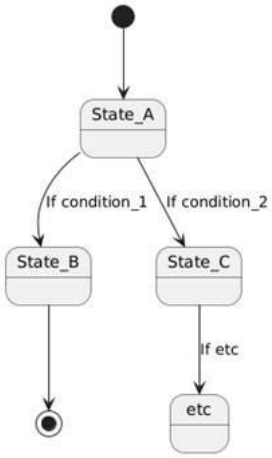


FIGURE 17 EXAMPLE OF STATE MANAGEMENT

Building on the findings of our literature review and motivated by the need to validate specifically whether appliances follow the correct sequence of actions, respect time-based conditions, and transition between states, we have initiated the design and prototyping of a dedicated behavioral testing architecture aimed at evaluating how a system transitions between states, reacts to time based events, and follows predefined control logic. A high-level overview of the proposed architecture is illustrated in Figure 3, which provides a simplified view of the core components and their interactions.

This ontology-driven testing architecture will be validated in the 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.

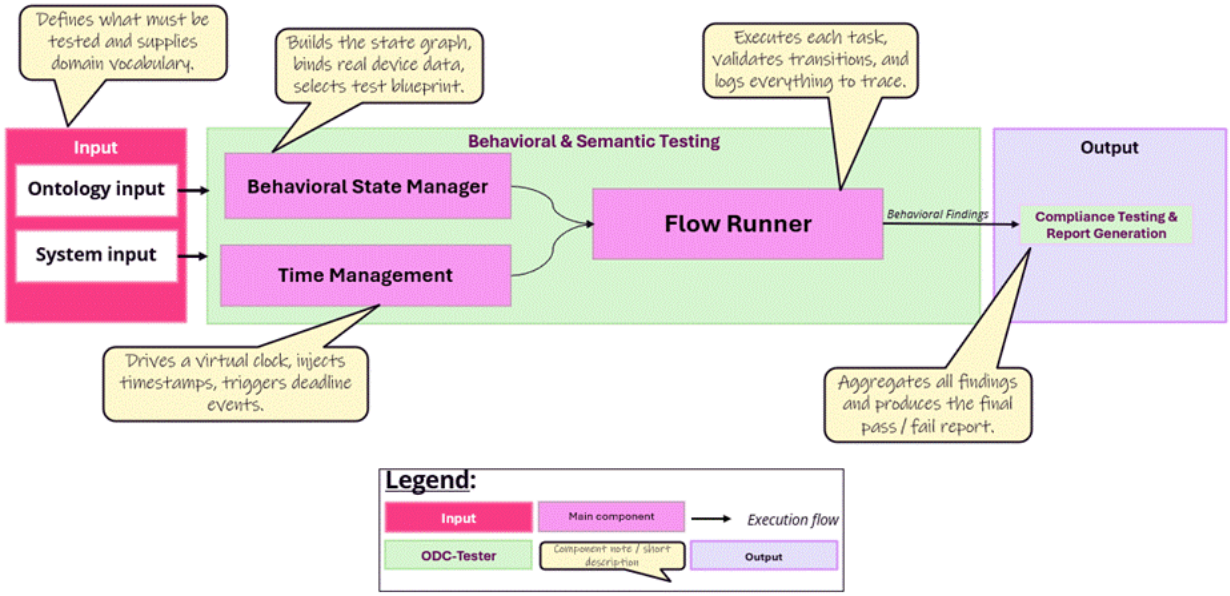


FIGURE 18 SIMPLIFIED VIEW OF ODCT BEHAVIORAL TESTING ARCHITECTURE

Ensuring that smart appliances behave correctly over time rather than just complying with static semantic constraints requires the ability to observe and evaluate how they react across sequences of states and timing conditions. While the current ODCT framework focuses on validating compliance with ontological definitions at a specific point in time, it lacks the mechanisms necessary to test whether appliances behave as expected during ongoing operation. To address this gap, the proposed architecture introduces an execution environment capable of interpreting time-aware behavioral flows, validating transitions, and capturing results through semantic reasoning.

This architecture is structured into three main layers:

- input,
- behavioral and semantic processing, and
- output (compliance reporting).

The input layer begins with two core inputs:

- 1st input: The ontology input provides the formal vocabulary and behavioral constraints to be tested
- 2nd input: the system input supplies real or simulated appliance data for a specific test session.

The Behavioral and semantic processing layer:

- These inputs are processed by the Behavioral State Manager (BSM), which maps the Conformity Aspect of Interest (CAI) to a behavioral test blueprint, injects system-specific values, and generates an executable flow graph representing the expected state transitions and timing logic.

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.

- In parallel, the Time Management component simulates the progression of time by generating timestamps and triggering time-bound events, such as delays, deadlines, or expiration conditions. This allows the system to test not only structural correctness but also temporal compliance, which is critical for evaluating smart appliance behavior in realistic operational scenarios.
- The Flow Runner serves as the core execution engine. It processes each task in the behavioral flow graph by validating pre and post-conditions using for instance, e.g., SHACL constraints, executing SPARQL updates to reflect state changes, and handling control logic such as branching, synchronization, and timeouts.

The output layer: Finally, the Compliance Testing & Report Generation module aggregates the results of each test run, producing a structured report that summarizes the validation status of each behavioral requirement, backed by detailed trace evidence. This report enables both human-readable interpretation and machine-level auditability.

Contribution to ISO/IEC 21823-5

On the initiative of Trialog and the support of AIOTI (task force on semantic interoperability), the standard ISO/IEC JTC 21 21823-5 was started (end of 2021 as a study, end of 2023 as an approved project) and it is currently at a CD stage.

Here is the scope:

This part of ISO/IEC 21823 specifies interoperability from a behavioural and policy viewpoint. In this document, the following specifications for interoperability from a policy and behavioural point of view are included:

- a principle of how to achieve behavioural and policy interoperability;
- requirements on information related to behavioural and policy interoperability, and
- a framework for processes on developing information exchange rules from a behavioural and policy viewpoint

Part 5 contains the following:

- a set of principles:
    - Principle: digital representation based on information models
    - Principle: concept profiles
    - Principle: single source of truth
    - Principle: technology neutrality
    - Principle: behaviour models and policies
    - Principle: semantic interoperability in the IoT system lifecycle
- a definition of constraint profiles

ODC-Tester is based on this standard, and the results of the project will be used to consolidate the standard.

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. ANNEX B EDC INTEGRATION PLAYBOOK

How to onboard apps/services and consume external assets (DSP-compliant), in plain terms

Purpose and scope (read this first)

This annex provides a clear, non-technical sequence for integrating an application/service into the Eclipse Dataspace Connector (EDC) and for consuming services offered by other participants. It complements the main architecture by translating it into actionable steps that align with The Dataspace Protocol (DSP).
Audience: product owners, tech leads, and integrators who need a checklist they can follow without diving into implementation details.

1) From app to service asset (Provider view)

Publish an API/compute service through the connector

Goal. Make your app discoverable via the EDC Catalog and deliver its results through the Data Plane.

a) Wrap the app as a "service asset"

- Expose a stable HTTP endpoint that EDC can call (pull) or from which it can fetch the output.
- For compute-to-data or asynchronous jobs, provide a staging location (e.g., object storage) that the Data Plane can read.

b) Define the HTTP/endpoint DataAddress

- Point the DataAddress either to the app endpoint (sync pattern) or to the output storage (async pattern).
- If useful, adopt a broker pattern: the contract/transfer triggers the app → the app produces an artifact → the Data Plane delivers it.

c) Asset + Policy + Contract

- Register a service asset with concise metadata (title, description, format, version, expected latency).
- Add access and usage policies (who may access, allowed purpose/retention, redistribution limits).
- Create the contract definition linking asset → access policy → usage policy.

d) Document the interface

- In the asset description, spell out inputs, output format, and timing (e.g., parameters, MIME types, SLA hints).

e) End-to-end validation

- Simulate a consumer request to verify that the app produces the output and the Data Plane delivers it as expected.

From catalog to data-in-hand (Consumer view)

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.

Discover, contract, transfer, and use others' services

a) Discover the Provider's Catalog (DSP)

- Call the provider's Catalog endpoint and filter assets of interest.

b) Contract negotiation

- Accept the provider's policies (or negotiate if supported).
- Obtain the agreementId confirming the contract.

c) Data transfer

- Start a transfer process, specifying protocol and destination (e.g., HttpProxy, S3).
- Monitor the state: *started* → *in progress* → *completed*.

d) Consumption & logging

- Validate the received content; respect usage policies (purpose, time, derivatives).
- Track usage for audit/compliance.

Practical notes that reduce friction

Design choices that de-risk adoption

- Endpoint consistency. Ensure the Data Plane is reachable from the consumer (NAT/proxy/HTTPS).
- Start simple. Use permissive policies for test phases (e.g., "allow all within consortium"), then tighten.
- Transfer types. Begin with HTTP consumer-pull (easiest path), then consider S3/Azure Blob.
- Helpful metadata. Provide versions, schema, units, update frequency, and technical contacts.
- Efficient testing. Use Postman or MVD collections to speed up discovery/negotiation/transfer checks.

Following these steps makes an app discoverable, contractable, and deliverable through EDC. Start with the simple HTTP consumer-pull path and clear metadata; once the first transfers are reliable, iterate on policies, performance, and automation. This sequence is intentionally lightweight—enough to align teams and reduce integration risk without overloading the deliverable with implementation detail, as shown in Figure 19.

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.

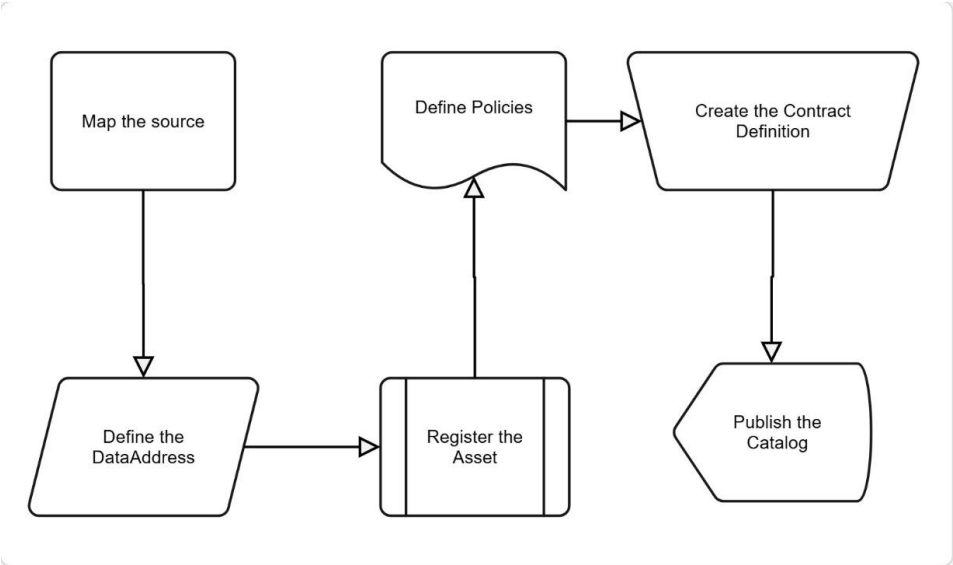
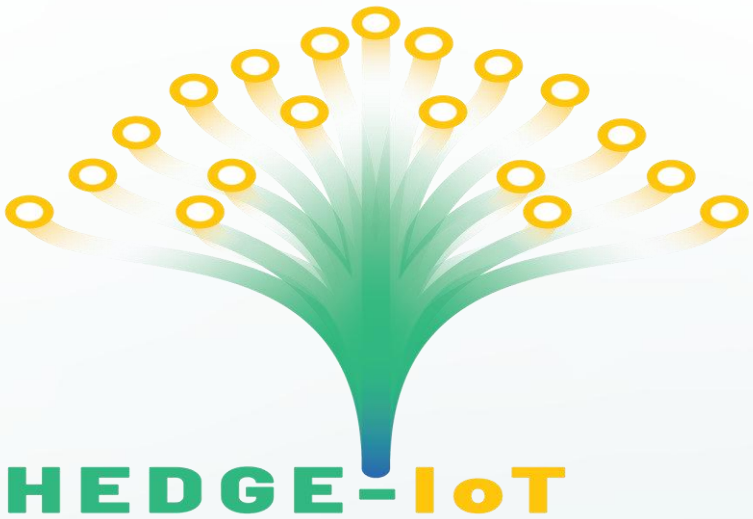


FIGURE 19 EDC APP INTEGRATION FLOW

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.


HEDGE-IoT