interconnect

interoperable solutions
connecting smart homes,
buildings and grids

WP2 – Interoperable IoT Smart Homes and Grid Reference Architecture

D2.1

Secure interoperable IoT smart home/building and smart energy system reference architecture

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant agreement No 857237

DOCUMENT INFORMATION

DOCUMENT	D2.1 – Secure Interoperable IoT smart home/building and smart energy system reference architecture
TYPE	Report
DISTRIBUTION LEVEL	Public
DUE DELIVERY DATE	12/31/2020
DATE OF DELIVERY	12/31/2020
VERSION	V1.0
DELIVERABLE RESPONSIBLE	Sensinov
AUTHOR (S)	WP2 Partners
OFFICIAL REVIEWER/s	WP2 Partners

DOCUMENT HISTORY

VERSION	AUTHORS	DATE	CONTENT AND CHANGES
0.1	Sensinov	26/03/2020	Provided initial draft of the ToC
0.1.1	Sensinov, TNO, INESC TEC, VITO, VLF	02/04/2020	Updated ToC
0.2	TNO, VITO, EDP D, ENGIE, KNX	15/04/2020	Section 4 – Smart Energy Reference Architecture initial draft
0.2.1	Sensinov, EEBus, TNO, KEO, INESC TEC	07/05/2020	Section 2 – SotA analysis
0.2.2	Sensinov, EEBus	13/05/2020	Section 4 – Smart Home/Building IoT Reference architecture initial draft
0.2.3	TNO, VU, Trialog, EEBus, KNX, Sensinov	20/05/2020	Section 5 – Semantically Interoperable Framework Architecture initial draft
0.3	Sensinov, TNO, Yncréa, VITO, VLF, INESC TEC	22/05/2020	Content for sections 3 and 4
0.4	TNO	25/06/2020	Updates to section 5
0.4.1	TNO, VITO, EDP D, ENGIE, KNX	24/07/2020	Updates to section 4
0.4.2	Sensinov	20/08/2020	Updates to section 2 and section 4
0.4.3	TNO, Trialog	20/08/2020	Updates to section 2 and section 4

0.5	TNO	26/11/2020	Section 6 – Ensuring system security
0.6	VLF, Sensinov, TNO	02/12/2020	Section 7 – Functional Architecture implementation in pilots
0.7	TNO, Sensinov, INESC TEC, VLF, VITO, EEBus, KNX	03/12/2020	Final draft for sections 3 and 4
0.7.1	VLF, TNO, Sensinov, KEO, EEBus, Trialog, VU, VITO, KNX	10/12/2020	Final draft for sections 5, 6 and 7
0.8	Sensinov, TNO	17/12/2020	Integrated document ready for QA
1.0	Sensinov	31/12/2020	Final version addressing QA comments - ready for submission

ACKNOWLEDGEMENTS

NAME	PARTNER
Ruben Baetens Mojtaba Eliassi	3E NV
George Limperopoulos	COSMOTE
Cami Dodge-Lamm Andraž Andolšek	cyberGRID
Lieven Demolder	DUCOOP
José Manuel Terras	EDP DISTR
Josef Baumeister Ulrich Bartsch Ralph-Ino Prümm Dr. Maren Fiege	EEBUS
Romain Bonnin Rubion Matthieu	ENEDIS
Gil Vandermarcken	ENGIE
Sebastian Wende Von Berg Lars-Peter Lauven	Fraunhofer
Donatos Stavropoulos	GRIDNET S.A.
Steven Marks Kim Verheij	Hyrde (iCity)
Esteban Municio Johann Marquez-Barja	IMEC
Fabio Coelho Filipe Ribeiro Ruben Queiros	INESC TEC
Thomas Fichedick	KEO
Joost Demarest	KNX
Stefaan Aelbrecht Chaim de Mulder	OpenMotics
Stefano Fava Fabrizio Tortonese	Planet Idea
Nour Sobh	RDGFi

Maria Perez	
Miguel Gonçalves	Schneider Electric Portugal
Eliana Valles Mahdi Ben Alaya	Sensinov
Amandio Ferreira (Elergone)	SONAE
Arnor Van Leemputten	TH!NK-E
Pol Olivella Klaas Charlier	ThermoVault
Kristian Helmholt Laura Daniele Barry Nouwt Wilco Wijbrandi Gerben Broenink Joost Laarakkers	TNO
Amélie Gyrard Olivier Genest	Trialog
Lars Lauven Sebastian Wende-von Berg	UNI KASSEL
Dominic Ectors Jung Georg Chris Caerts Enrique Rivero Puente	VITO
Milenko Tosic Dragan Boscovic Ognjen Ikovic	VIZLORE LABS FOUNDATION
Kim Verheij (Hyrde)	VOLKERWESSELS ICITY B.V.
Ronald Siebes	Stitching VU
Dieter Roefs Thierry Coosermas	VUB
Andreas Georgakopoulos Vassilis Foteinos Ilias Romas	WINGS
Anaïs Galligani Ghislain Oudinet Stephane Vera	Yncréa Méditerannée

DISCLAIMER:

The sole responsibility for the content lies with the authors. It does not necessarily reflect the opinion of the CNECT or the European Commission (EC). CNECT or the EC are not responsible for any use that may be made of the information contained therein.

EXECUTIVE SUMMARY

This document introduces the deliverable D2.1 Secure interoperable IoT smart home/building and smart energy system reference architecture. It is the first deliverable produced by WP2 – Domain Interoperable IoT Reference Architecture.

This deliverable uses and develops the output and ongoing work of WP2 and other WPs. Hence, this deliverable and its related task:

- Defines the **Secure Interoperable IoT Smart home/building and smart energy reference architecture (SHBERA)** for InterConnect. The latter can be defined as a system-agnostic architecture for the IoT and Energy domains, built iteratively from WP1 output and WP5 initial specifications and requirements. The resulting SHBERA describes the different layers and domains introduced by the **Smart Home/Building IoT Reference Architecture (SHBIRA),** produced by task T2.1, and the **Smart Energy Reference Architecture (SERA**), produced by task T2.2;
- Defines the **Semantically Interoperable Information Architecture**, by specifying the semantic technology and semantic reasoning mechanisms that will be integrated into the architecture to achieve cross-domain and cross-platform interoperability;
- Defines a **set of privacy and security strategies and guidelines**, based on international best practices and standards, for ensuring data protection, security and end-users' right to privacy;
- Collaborates closely with WP3 on defining the **set of interoperable services and applications needed for pilot implementation and validation of results**, due to take place within WP7.

More precisely, D2.1 and its associated tasks are an essential entry point for other project activities, namely by:

- Fostering **early-alignment across WPs** to help define and integrate the set of known **roles, requirements and stakeholders** into the architecture;
- Providing different **architectural viewpoints (i.e., SHBERA, SHBIRA and SERA)** that cover the full set of interactions between the different domain and actors specified in WP1;
- Providing a **high-level specification of the Semantically Interoperable Information Architecture Framework**, including the required enablers for achieving interoperability across project stakeholders;

- Presenting a more **in-depth overview of each (sub)pilot's functional architectural implementation**, helping develop a more resonant synchronisation across pilot members.

These concepts and the methodology used to achieve these results are described in detail in the document.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

AE	Application Entity
AI	Artificial Intelligence
AMI	Advanced Metering Infrastructure
API	Application Program Interface
BEMS	Building Energy Management System
BUC	Business Use Case
CA	Consortium Agreement
CEM	Customer Energy Manager
CIM	Common Information Model
DER	Distributed Energy Resources
DMS	Distribution Management System
DR	Demand Response
DRES	Distributed Renewable Energy Sources
DSF	Demand Side Flexibility
DSO	Distribution System Operator
EDSO	European Distribution System Operators
ESCo	Energy Service Company
ETSI	European Telecommunications Standards Institute
EV	Electric Vehicle
FSP	Flexibility Service Provider
HBAM	The Home and Building Architecture Model
HBES	Home and Building Electronic Systems
HEMS	Home Energy Management System

HLA	High Level Architecture
HLUC	High Level Use Case
IEC	Internal Electrotechnical Commission
IC	InterConnect
IDS	International Data Spaces
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IoT	Internet of Things
IIRA	Industrial Internet Reference Architecture
ISO	International Organization for Standardization
KB	Knowledge Base
KD	Knowledge Directory
KE	Knowledge Engine
KIs	Knowledge Interactions
M2M	Machine to Machine
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
oneM2M	Global Standards Initiative for Machine-to-Machine Communication
RAMI	Reference Architecture Model Industrie
SAREF	Smart Appliances Reference ontology
SaaS	Software as a Service
SHBERA	Secure Interoperable IoT Smart Home/Building and Smart Energy Reference Architecture
SHBIRA	Smart Home/Building IoT Reference Architecture
SERA	Smart Energy Reference Architecture
SGAM	Smart Grid Architectural Model

SPINE	Smart Premises Interoperable Neutral-Message Exchange
TA	Technical Aggregator
TC	Things Consumers
TD	Things Description
TSO	Transmission System Operator
UC	Use Case
WoT	Web of Things
WP	Work Package

1 INTRODUCTION

Within the InterConnect project, WP2 is in charge of carrying out the following activities and attaining the following objectives [38]:

- Define the **Secure Interoperable IoT Smart Home/Building and Smart Energy System Reference Architecture (SHBERA)**. The latter can be defined as a technology-independent, device-agnostic system architecture for the Energy and IoT domains, derived from the integration of the **Smart Home/Building IoT Reference Architecture (SHBIRA)** and the **Smart Energy Reference Architecture (SERA)**, introduced in tasks T2.1 and T2.2, respectively;
- Define the set of **privacy and security strategies and guidelines supporting a privacy-by-design approach** (T2.3). WP5, particularly T5.3, will use these guidelines to specify each pilot's action plan and reports on the result of the security and risk analysis, as well as the requirements for mitigation and analysis of compliance readiness;
- Define **the Semantic Interoperability Framework** (T2.4) supporting semantic interoperability among the different existing devices, services and platforms within the project ecosystem. This includes possible adaptations and extensions to the SAREF suite of ontologies that are required from WP1 use cases and WP7 pilots, and all the relevant semantic reasoning mechanisms and related components to be integrated into the SHBERA resulting from tasks 2.1 and 2.2;
- Foster interoperability between devices, systems and domains (i.e., smart homes, buildings, energy, and grid) by defining the **domain-specific abstraction layers and basic APIs needed for their implementation** (in T2.5). This work is carried jointly with WP3, in charge of the specification and development of interoperable functions, i.e., software services/applications and physical devices/appliances, that are needed for the WP7 pilots.

Moreover, by fostering early-alignment across most WPs, notably WPs 3, 5 and 7, **WP2 defines and integrates the set of known roles, requirements and stakeholders into the architecture**. The design and combination of all these critical components (e.g., ontologies, standards, abstraction layers and security concepts) - in close cooperation with industry

players - should result in an interoperable, secure, open system architecture, capable of handling complex scenarios, like those described in WP1 on use cases.

1.1 RELATION TO OTHER WPS

As shown in Figure 1, the work carried out in WP2 is based on the work conducted in other technical WPs, while at the same time providing key enablers for those same WPs, namely:

- From WP1, this WP **utilizes the use case requirements to infer the architectural requirements** for the project's Reference Architecture and Interoperability Framework;
- The work carried out in WP5, particularly in T5.1, allowed for **various iterations of the resulting SHBERA, SERA and SHBIRA**. This deliverable presents the latest version of each of these viewpoints; however, these iterations containing input and feedback from other WPs and pilots should pursue until M36 (September 2022), culminating with the publication of deliverable D2.4 Secure Interoperable IoT smart home/building and smart energy system reference architecture V2.0, the second version of this document.

The concepts and functions (e.g., data models, interfaces, protocols, security and privacy requirements) introduced here are further developed in WP5 and WP3, which subsequently provide:

- WP3 with the **service store specification and generic adapter** for achieving semantic interoperability of the services;
- WP4 with the **interoperable interfaces towards energy markets** and especially DSOs while WP5 provides integration with the interoperability framework and services;
- WP7 pilots with the **interoperable digital platforms and supporting services** necessary for realizing the project use cases;
- WP8's cascade funding projects/partners with the **interoperability toolbox** necessary for making their platforms and services interoperable with the interoperability framework and established pilots.

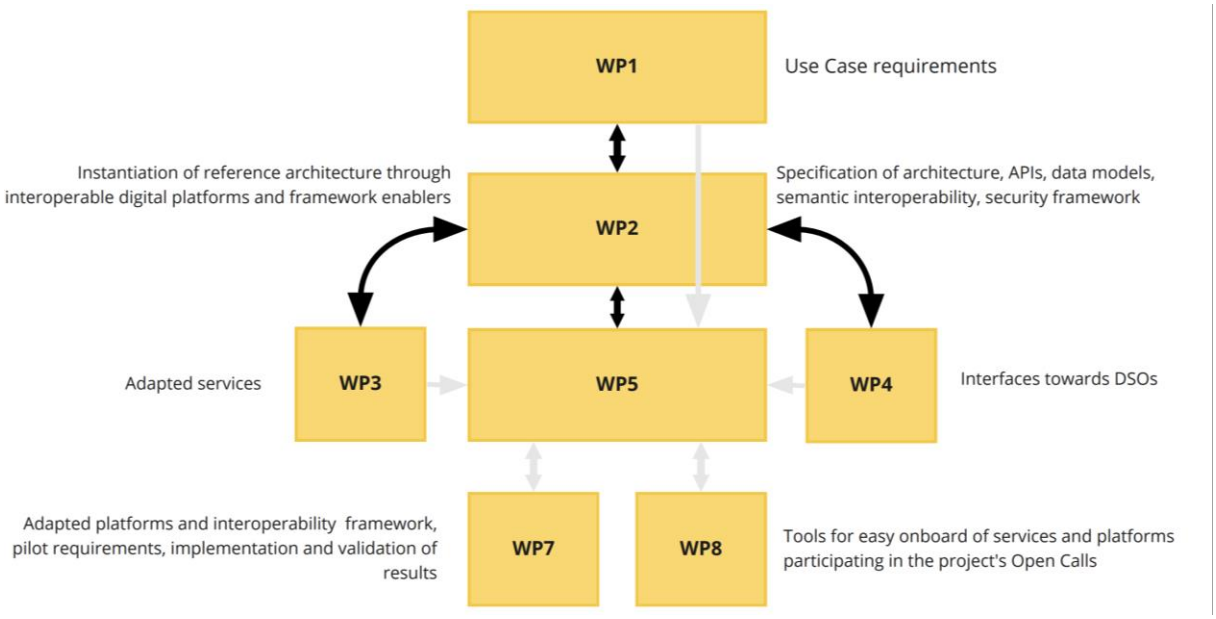


FIGURE 1 – RELATION OF WP2 TO OTHER WPS

1.2 D2.1 OBJECTIVES

This deliverable is one of the results of the work carried out within most of the WP2 tasks. Its main objectives can be detailed as follows:

- Carry out a **detailed analysis of the project's use cases, digital platforms and services** as well as their interoperability capabilities and requirements;
- Provide an **initial overview of the InterConnect Reference Architecture** and each (sub-) pilot's architectural implementation;
- Specify **InterConnect's Interoperability Framework** and other interoperable resources and services;
- Contribute to the **specification of the Semantic Interoperability Layer,** by identifying the set of connectors and adapters needed to integrate the benefits of ontologies and semantic technology into the InterConnect reference architecture.

To attain these objectives, the present document introduces:

- An overview and analysis of relevant IoT, Smart Home, Smart Building, Energy and Industrial Reference Architectures;
- The list of architectural principles, methodologies, and requirements that guided the architectural choices made by this project;
- The description of InterConnect's Secure Interoperable IoT Smart Home/Building and Smart Energy System Reference Architecture (SHBERA), resulting from the integration

of the project's Smart Home/Building IoT Reference Architecture (SHBIRA) and the Smart Energy Reference Architecture (SERA);

- Different architectural viewpoints introduced within this WP2 and WP5 (i.e., SERA, SHBIRA, and IC's Interoperability Framework) to cover the full set of interactions between the different domain and actors;
- The high-level specification of the Semantic Interoperability Layer, further developing the work already covered in WP5, which identified the set of connectors and adapters (see the Glossary and Terminology table) required to convert frequently used data formats in InterConnect into Semantic Web standards, and map the existing IC devices, services and platforms into SAREF-compliant specifications;
- The set of privacy and security requirements and guidelines supporting a privacy-by-design approach; Note that another deliverable D2.2 [42] will address the Practice for security and privacy policies compliance;
- A more in-depth overview of each (sub-)pilot's architectural implementation. First introduced within D5.1, this ongoing work helps improve, step-by-step, coordination across pilot participants.

As previously stated, the content covered by this deliverable will be discussed and iterated until M36, date of publication of the second version of this deliverable (D2.4). Therefore, the work presented here should not be considered static nor exhaustive, but rather the structure upon which other tasks, WPs and other projects can already build upon to further detail the project's pilot architectural instantiations.

1.3 DOCUMENT STRUCTURE

This document is structured as follows:

This introduction is part of Section 1. Its followed by the **Glossary and Terminology** table, used within this document and other technical and non-technical deliverables published by the InterConnect project.

Section 2 – State of the art collects and analyses other existing reference architectures within the Smart Home, Smart Building, Smart Energy, and Industrial domains. These reference architectures provide the basis upon which the Consortium wishes to converge and extend to achieve interoperability. Each section concludes by offering a synthetic view of each project's key features. The last subsection provides an analysis and comparison to the architecture proposed by InterConnect.

Section 3 – Methodology, Principles and Architectural Requirements for InterConnect's Reference Architecture describes the methodology used to derive the project's reference architecture, alongside the key principles and requirements that impacted the early stages of architectural specification of the SHBERA. These notions were mainly derived from the High-Level Use Cases (HLUC) produced by WP1 and the specification of the project's Interoperability Framework, specified within WP5.

Section 4 – InterConnect's Secure Interoperable IoT Smart Home/Building and Smart Energy System Reference Architecture introduces InterConnect's Secure and technology-agnostic high-level architecture for achieving interoperability across domains and devices. Moreover, this chapter includes a set of architectural views, mapping the project's key functions, domains, actors and their interactions. Especially the Smart Energy Reference Architecture (SERA) and the Smart Home and Smart Building IoT Reference Architecture (SHBIRA) views are highlighted and explained in this section.

Section 5 – Semantically Interoperable Information Architecture introduces semantic interoperability and proposes, based on high-level requirements, an inventory and analysis of the semantic solutions existing among the partners in InterConnect. The analysis of these semantic solutions results into a recommended, shared IC solution based on the knowledge engine technology, which is further explained, elaborating on which semantic components will be embedded into the SHBERA to realize it. Finally, the section concludes with guidelines for the pilots and other WPs concerning what steps need to be taken to make their device/service/platform compatible with the recommended solution when using the InterConnect's semantic interoperability layer.

Section 0 – Functional Architecture Implementation in Pilots extends and completes the initial work presented in D5.1 – Chapter 6 [43], providing an overview of each pilot and sub pilot's use cases and requirements in terms of cross-platform interoperability and initial mapping of the interoperability adapters Building upon this result, this chapter focuses on providing a unified view of each (sub-)pilot mapping to the SERA, the SHBIRA and the InterConnect Interoperability Framework.

1.4 GLOSSARY AND TERMINOLOGY

The glossary table, presented below, will be maintained throughout the project. Definitions introduced hereafter might be updated to accommodate project progress and key results from technical WPs. New terminology definitions might also be added in future deliverables.

CONCEPT	DEFINITION
InterConnect Framework-related terminology	
IoT platform (provider)	A collection of tools, software and hardware that makes it possible to connect 'things' (i.e., sensors, actuators or other types of physical devices) to the Internet and the Web. Also used for managing the connection to the devices as well as the devices themselves.
(An) IC Platform	A digital platform that complies with IC Framework requirements in terms of software and/or hardware that enables the actual interconnection of devices and services. Often implemented on the basis of an IoT platform.
(The) IC Framework	A collection of tools and enablers that describes and prescribes how to interconnect devices from different vendors and services from different providers, enabling interoperability and the intelligent interaction of many devices and services from different domains (e.g., home automation, energy management, etc.). The IC Framework includes services, like service store for all interoperable services, P2P marketplace enablers, access control mechanisms, generic interoperability adapters, reasoning and compliance tests.
Project Pilot	A collection of tools, software, hardware, building and users that provide a working demonstration one of more aspects of the generic IC Framework in one or more EU countries in terms of platform interconnected devices and services.
High Level Use Case	A demonstration of application of the generic IC Framework in terms of using a specific set of services and a specific set of devices, that are interconnected by the platform, in a specific way.
Service-related terminology	
Technical Service Provider	A hardware or software component, possibly representing other components, that is capable of offering certain functionality in the form of an (IC) Service to

	other components. The other component could be owned by the same actor or by a different actor.
Commercial Service provider	A business actor that provides a service to another actor (e.g., consumer, but also another commercial service provider).
Service user	An entity that uses a service as provided by another entity. This can be from a commercial viewpoint or a more technical one (e.g., 'software using services offered by other technical components'). The context of this term determines the viewpoint.
Customer	A business actor that uses/consumes a service and in return (generally) rewards the (commercial) service provider for the use of that service.
Service Level Agreement (SLA)	Agreement between (commercial) service providers and users/customers.
Service Level Management (SLM)	Management of agreements and commitments between (commercial) service providers and users/customers through tracking and documentation of service level delivery and usage.
(IC) Service	The offering of certain functionality from one entity/component to another authorized entity/component (e.g., service or software component) using (standardized) interfaces, compliant to certain IC Framework requirements.
(IC) Regular services	IC Services that are offered via, not by, the IC Framework. Regular services are listed in the IC Service Store.
Service interface	An (technical) interface that exposes the functionalities of an IC Service. Within the IC Framework, this includes a metadata interface for exposing service capabilities
Meta data interface	Part of a (technical) service interface in the IC Framework, that provides functionality for interacting with service at a 'meta' level. This part of the interface can be used for example to interrogate the service about its capabilities and semantic framework. Thus, it can be used for reasoning about using a service.
IC Framework Service	A service that supports offering and using services on an IC platform, as prescribed by the IC framework. Examples are registration and discovery services for interfaces, enabling humans and technical entities to find a particular regular service offered through an IC platform.

Energy service	A service that offers the ability to accomplish an objective (mainly in) in the domain of energy, like balancing demand and supply or the reduction of energy usage. This is a special category of services within the IC Framework, as energy services (often) require the coordination of tasks across different Smart Homes and Smart Buildings across the Smart Grid and thus requires multiple levels and domains of control to be interconnected.
Non-energy service	Non-energy service are services that do not relate to energy and/or do not enable clients to accomplish and energy objective (as a main objective). Examples of non-energy services are services that have as objective comfort, well-being, entertainment or safety of their users. Non-energy services can be used by and/or 'become part of' an Energy service. For example, a non-energy service that sends events when a door remains open, can be used by an Energy service to reduce loss of heat in a house by closing doors.
Technical service implementation related terminology	
Software as a Service (SaaS)	A software licensing and delivery model in which software is licensed on a subscription basis and is hosted (de)centrally. It is sometimes referred to as "on-demand software". SaaS applications are also known as Web-based software, on-demand software and hosted software. The term "software as a Service" (SaaS) is considered to be part of the nomenclature of cloud computing.
Local / Remote Services	Software services can be either implemented as code that is run at 'remote' server (i.e., on the cloud), or on a 'local' server, i.e., as code that runs on a digital platform that is in a Smart Building or Smart Home.
IC Service run-time platform	Code that is hosted on a digital platform and acts as an abstraction layer for the underlying software platform (e.g., specific operating systems). The digital platform hosting the IC service run-time platform can be any kind of digital platform, ranging from resource constrained embedded systems up to (virtual) cloud servers. IC services compliant with the IC service run-time platform are called IC² service and digital platform agnostic as they interface with IC service run-time abstraction layer and not directly with the underlying software platform.
(IC) Native Service	A service implemented as software/code that runs on a specific vendor's digital platform, making use of specific functions and characteristics of this specific platform.

(IC) IC² Service	A service implemented as software/code that runs on top of the IC service run-time platform.
Semantic and Syntactic Interoperability-related terminology	
Semantics	Semantics is the study of meaning, i.e., the meaning of the data being exchanged via the IC Framework
Semantic Interoperability	Semantic Interoperability concerns the exchange of meaningful information on the basis of agreed, formalized and explicit semantics
(IC) Semantic Interoperability Layer	A logical concept within the IC Framework that enables semantic interoperability. The semantic interoperability layer comprises ontologies, interoperability adapters and smart connectors with supporting orchestration enablers.
Ontology	The formal specification of a conceptualization, used to explicit capture the semantics of a certain domain of discourse. In the IC Framework, ontologies like SAREF are used to capture the agreed, formalized and explicit semantics for the exchange of meaningful information via the semantic interoperability layer.
IoT Platform specific Information Model	In a specific IoT platform, it is a representation of concepts and the relationships, constraints, rules, and operations to specify data semantics for a chosen domain of discourse, related to a specific IoT platform.
(IC) Sarefized Services	A Software Service whose capabilities and data for the Service Interface are expressed using the SAREF ontologies. (IC) Sarefized Services are automatically recognized by the IC Semantic Interoperability Layer. The capabilities of an (IC) Sarefized Service automatically become available to other Sarefized Services/Devices.
Knowledge Engine	An open-source, ontology-agnostic software component, originally developed by TNO in cooperation with VU Amsterdam, but whose development is further extended to the InterConnect project partners. The Knowledge Engine helps improve interoperability by making data exchange more dynamic and smarter through orchestration and semantic reasoning. It creates a new way for software and devices to communicate with each other.
Knowledge Directory	A central component of the knowledge engine that registers the knowledge offered and requested by Smart Connectors. It does not perform any reasoning.

IC (Smart) connectors	Generic software responsible for orchestration and reasoning. The Smart Connectors are peers, that can communicate directly with each other through SPARQL+. Based on the information in the Knowledge Directory, each Smart Connector can perform orchestration and reasoning for itself. Smart Connectors configured to use the same Knowledge Directory can communicate with each other through SPARQL+.
IC adapters	The Interoperability Framework provides a set of adapters to allow vendors that are already compliant with industry standards to quickly connect their device/service to the Interoperability Framework. Ideally, for each industry standard (i.e., SPINE, WoT, Modbus, S2) an adapter would be available. IC adapter includes IC connector and also the underlying mapping of legacy data models and interfacing functionalities onto the InterConnect unifying protocol (SPARQL+) and SAREF based data model.
Knowledge Base	Any device/service or platform with a Smart Connector attached is called a Knowledge Base. A Knowledge Base will consume and produce knowledge that needs to become available for other Knowledge Bases in the network (i.e. needs to be come interoperable). Every Knowledge Base describes its capabilities using Knowledge Interactions.
Knowledge Interaction	A description of a type of interaction that a Knowledge Base supports. There are four types of interactions: Ask, Answer, Post, and React Knowledge Interactions. The Ask and Answer Knowledge Interaction each have one Graph Pattern associated with it, while the Post and React Knowledge Interaction have two (one for the argument, one for the result). A Knowledge Base typically has multiple Knowledge Interactions of different types. Knowledge Interactions are registered in the Knowledge Directory.
SPARQL+	It is a term specifically coined in the InterConnect project, used as internal jargon to identify a unifying interfacing protocol for the InterConnect semantic interoperability layer. It is based on the W3C's SPARQL standard and provides additional interfacing functionalities required for realization of the project use cases (thus, the "+" in the name).
IC Interoperability Framework-related terminology	
(IC) Service store	Complete catalogue of all interoperable services from energy and non-energy domains. The service store is implemented as a web application providing frontend interface for onboarding new interoperable services and browsing existing (already onboarded services) by category and other metadata

	parameters. The service store is part of the interoperability framework and can be utilized by local reasoners to find appropriate remote services (running on 3rd party platforms) needed for completing a task at hand. Service store enables users or local reasoners to find interoperable services of interest and provides them with information on how to access the services running on their hosting digital platforms.
(IC) Deployment Orchestrator	This is integral part of the service store responsible for facilitating instantiation of interoperable services packaged as containers for specific runtime environments including the service store sandbox.
P2P marketplace enablers	Set of enablers for P2P marketplaces include: Hyperledger Fabric configuration as blockchain basis for trusted data access and transaction management; set of smart contract templates representing supported transactions, reports and audits; white labelled web application utilizing blockchain network through integrated smart contract interfaces. These enablers can be configured and deployed for specific use case, on the level of a pilot or on the level of the whole project.
IC security and data protection framework	Set of best practices for ensuring data and privacy protection in integration/interoperability scenarios between two or more stakeholders with digital platforms, services, end users and databases. On the level of the project, a specific access control mechanism will be implemented with user/service/platform authentication and authorization procedures directly integrated with semantic interoperability layer (discovery and reasoning).
Interoperability compliance certification	Set of automated tests of achieved interoperability minimum defined for each service and platform category. The tests will include dummy data exchanges to showcase that defined data models are properly parsed and understood and services are capable of exchanging information through unifying communication layer/protocol. The interoperability compliance test will be part of the service onboarding process in the IC service store. After successful compliance test, a certification of interoperability compliance will be issued and written in immutable record of all interoperable endpoints based on Hyperledger Fabric blockchain established on the level of the IC project.

2 STATE OF THE ART

The following section provides an overview of twelve of the main reference architectures defined by key European Standardisation Organisations and other alliances in the IoT, smart home, smart building, smart energy, and industrial domains.

IoT Reference Architectures provide a high-level view of the entities and relationships that exist in the IoT domain. The main reference architectures covered in the following sub-sections are:

AIOTI's High Level Architecture, consisting of a three-layered model that interprets the relations between users, virtual entities and things. Each of the layers contains a set of functions and services that interact via the secure interfaces defined by the project.

oneM2M's Reference Architecture uses a layered approach to depict common services functions that enable applications in multiple domains, using a common framework and uniform APIs, built around the concept of a distributed operating system for IoT. oneM2M also provides an open basic ontology model, describing the core classes, relations and properties found within compatible and non-compatible oneM2M systems and technologies. This sub-section also introduces a simple example for understanding how oneM2M's semantic annotations model uses SAREF to describe an application entity (AE).

FIWARE's Reference Architecture is an open, public and free architecture, enabling the adoption of new services and solutions. The initiative offers a cloud-oriented open-source ecosystem for implementing IoT platforms, strengthened by the participation of several alliances and a rich ecosystem, built from a growing array of data models.

W3C's Web of Things (WoT) Architecture offers a flexible, scalable and interoperable approach to improve usability across the IoT domain. It builds on the concept of "Things, Consumers" (TC) and "Things Description" (TD) to provide human and machine-readable descriptions. The latter allowed for semantic annotation of its structure and described contents and can be exchanged using multiple formats commonly used in the web.

Smart Home/Building Reference Architectures, and more precisely, The Home and Building Architecture Model (HBAM), provides a framework for the home and building domains. The HBAM focuses on modelling the interactions between end-users and an interoperable ecosystem, often including standards in other domains, such as energy, mobility and home/building.

CENELEC's Reference Architecture aims to achieve interoperability across devices or system of devices that provide energy flexibility. It also describes the S2 communication protocol, which can be defined as an intermediate protocol that can function with many already existing protocols, e.g., SPINE, KNX, etc.

Smart Energy Reference Architectures provide common architectural specifications which provide a high-level view of the entities and relationships that exist in the energy and smart grid domains. The main reference architectures covered in this sub-section are:

The **Smart Grid Architectural Model (SGAM)** defines a set of common concepts, across five distinct layers (i.e., business, functional, information, communication, and component layers). This framework focuses on providing a technological-neutral approach, supporting the creation of smart grid use-cases across various zones (i.e., levels from a power systems management perspective) and domains in the energy field (e.g., generation, transmission, distribution, distributed energy resources, and consumers).

The **International Electrotechnical Commission's (IEC)** Smart Grid Reference architecture introduces key concepts (e.g., processes, stations, field, operation) and actors (e.g., enterprise and market) spanning across the generation, transmission, distribution, DER, consumption, the communication, and crosscutting tiers. It also provides a series of considerations for data modelling and semantically driven reasoners using ontologies tailored for the Energy domain.

Industrial Reference Architectures serve as a foundation for the development of real-life application architectures across numerous industrial sectors. Three reference architectures are covered in this sub-section: The Industrial Internet Reference Architecture (**IIRA**) is a standards-based open architecture for IIoT systems, based on the ISO/IEC/IEEE 42010:201 standard. The IIRA defines a set of viewpoints (e.g., business, usage, functional, implementation viewpoints) representing top-to-bottom and bottom-to-top interaction across stakeholders.

The **International Data Spaces (IDS) Reference Architecture** focuses on the link between the creation of data on the internet of things (IoT) and the use of this data in machine learning (ML) and artificial intelligence (AI) algorithms. One of the core values put forth by the IDS is data sovereignty, allowing for the exchange and sharing of data between partners independent from their size and financial power.

The following subsections describe in more detail each of the reference architectures mentioned above.

2.1 IOT REFERENCE ARCHITECTURES

2.1.1 AIOTI

The Alliance for the Internet of Things Innovation (AIOTI) encourages interactions among the European IoT stakeholders. The areas of action range from experimentation, replication, deployment to supporting the convergence and interoperability of IoT standards. Within AIOTI, the WG03 on “IoT Standardization” led to work that resulted in the production of a high-level architecture based on ISO/IEC/IEEE 42010 standard (HLA) [1], leveraging the IoT-A domain model. AIOTI's architecture reduces complexity by offering a comprehensive IoT landscape standardization framework that achieves semantic interoperability.

AIOTI's domain model describes entities in the IoT domain and their relationships, at the highest possible level; namely user (human or otherwise), a virtual entity (digital representation of the physical entity), and the thing (physical entity).

The IoT Service interface allows for different functionalities, including data representation and enrichment (semantic metadata), identification schemes, interaction with external IoT systems, security and privacy, and device management.

AIOTI's functional model defines functions and interactions inside the IoT domain. It is composed of three layers:

- The **Application layer** contains the communications and interface methods used in process-to-process communications.
- The **Network layer** provides various services ranging from data plane services, data forwarding between entities to control plane services (e.g., location, device triggering).
- The **IoT layer**, which uses the network layer's services to expose and share data through an application layer, commonly referred to as APIs or application programming interfaces.

Other layers are also present to interface between planes. The commands/data structure interface describes the structure of the data exchanged between app entities while networks provide the connectivity for exchanged data on this interface. The interfaces to access IoT capabilities allows access to services exposed by an IoT Entity. The data plane interface supports sending/receiving of data across networks of other entities. The network control plane interfaces authorize the requesting of network control plane services. The horizontal Services interface allows the inclusion of other IoT entities, trough exposing/requesting services.

AIOTI includes propositions for unlocking semantic interoperability features in large-scale pilots[1] such as the need to create a high-level approach to semantic interoperability and to develop domain-specific ontologies based on WG03 IoT standardization by the Semantic Interoperability Expert Group.

2.1.1.1 LINKS AND GAPS WITH THE INTERCONNECT REFERENCE ARCHITECTURE

AIOTI's HLA model offers a global, comprehensive, technological agnostic and highly evolutive model that can be deployed on large scale pilots. AIOTI's provides a basis for the HLA of InterConnect, particularly in its "IoT Entity" layer, where semantic metadata and identification services are comprehended. This layer from AIOTI also establishes the groundwork between applications and services at the application layer, the abstraction in InterConnect for the digital platforms and services.

AIOTI's reference architecture provides the base considerations that are required to assemble InterConnect's HLA, particularly for the smart home, smart building and IoT encapsulation of concepts. Nevertheless, AIOTI's generic modelling does not fully address the requirements that consider a truly vertical abstraction. The need for semantic abstractions, mainly covering how ontology mappings are brought into the focal point of InterConnect's architecture is currently not covered by AIOTI's architecture. InterConnect considers AIOTI's reference architecture as foreground and considers and embeds complementary energy reference architectures into its core, exploring the SAREF ontology family.

Finally, AIOTI's architecture does not address the energy domain. While it might comprehend some concepts that derive from device support, it does not showcase important layers/roles to accommodate needs related to energy trading, support or even interoperability of systems.

[1] The **IoT European Large-Scale Pilots Program** is an EU-initiative fostering innovation and collaboration for the deployment of IoT solutions all across Europe. The program consists of seven innovation consortia (5 LSPs and 2 Communication Support Actions), including: **AUTOPILOT** (AUTOmated driving Progressed by Internet of Things), **SynchroniCity** (SynchroniCity: Delivering an IoT enabled Digital Single Market for Europe and Beyond), and **ACTIVAGE** (ACTivating InnoVative IoT smart living environments for AGEing well), amongst others. More information on this program and related initiatives can be found here: https://european-iot-pilots.eu/

2.1.2 ONEM2M

The oneM2M Global Initiative, established by ETSI, defines a globally agreed machine-to-machine (M2M) service, with contributions from seven SDOs in the world and various alliances and industries.

oneM2M architecture comprehends three layers, namely: the application layer, the service layer and the network layer, respectively providing standardized interfaces for application communication, software middleware services for IoT applications and corresponding hardware and network services [2]. Each layer contains a common services entity (CSE), an application entity (AE), or both.

An AE provides application logic (e.g., remote power monitoring), a CSE comprises a set of service functions called common services functions (CSFs) that can be used by applications and other CSEs. CSFs include registration, security, data management and repository and device management, amongst others. Since oneM2M adopted a RESTful architecture, all services are represented as resources to provide the defined functions.

To address semantics, oneM2M provides a base ontology[2] describing a set of classes, relations, and properties for compatible and non-compatible oneM2M systems and technologies. In terms of interoperability, the oneM2M standard allows for various approaches, including but not limited to: **pure ontology-based solution** (RDF/OWL serialization format), such as the oneM2M base ontology extended with a domain-specific ontology (e.g., SAREF); **common vocabulary** or a basic serialization format, such as XML or JSON; **resources specializations**, for instance, the oneM2M *FlexContainer* resources specialized with a technology-specific data model; or, **blackbox resources**, which are basic oneM2M resources (e.g., container, and group) extended with an external domain-specific data model. Semantic annotations provide meaning for the data encapsulated, and enable:

- **Semantic discovery**, allowing for locating and linking resources or services;
- **Semantic reasoning**, deriving new relations and classifications according to the semantically annotated data;
- **Semantic mash-up**, offering the possibility of creating virtual devices and new services.

[2] https://git.onem2m.org/MAS/BaseOntology

2.1.2.1 LINKS AND GAPS WITH THE INTERCONNECT REFERENCE ARCHITECTURE

InterConnect's Smart Home and Building reference architecture resemble ETSI's oneM2M high-level architecture. Both comprehend layers for device, gateways and higher-level services. However, oneM2M focuses on providing technical and syntactic interoperability, allowing devices to establish data flows among them. A common data model introduces a first ontology mapping and step towards semantic interoperability.

ETSI's oneM2M standard provides a robust reference architecture upon which the project can build. It provides a strong basis for building and extending a reference architecture for the building, home and energy domains. However, since oneM2M's core concepts do not provide a fine-grained model for interoperating energy flexibility management with home and building architectures, some work needs to be done to further detail such concepts in the resulting global reference architecture.

While oneM2M offers considerable experience with the use of ontology-based solutions (including SAREF), it is closer to the device layer. InterConnect will provide the capabilities as foreground, ensuring compliance with devices, but will shift its focus to higher-level abstractions, particularly the ones conveyed by higher-level software data services that can operate at all levels of the HLA (separately or together). Moreover, InterConnect will also sponsor evolutions within the SAREF family specification, enabling them also to address needs coming from interoperability requirements of the energy domain that are currently not part of it (e.g., flexibility).

2.1.3 FIWARE

The FIWARE Foundation is a non-profit organisation funded by the European Union and the European Commission, aiming to encourage the adoption of open standards. It provides an open, public, and free architecture, enabling the adoption of new services and solutions by new stakeholders, without compromising the openness characteristic of the environment. It provides a market-ready framework that can combine software interfacing with IoT devices and cloud-based big data cloud platforms. Central to the design is the smart data usage that enables specific APIs for data exchange while ensuring compliance with legacy applications via a set of harmonised data models.

FIWARE introduces three core main data model concepts: context entities, attributes, and metadata. An entity represents a physical or logical object and is uniquely identified by two attributes: id and type. The entity type follows a given semantic definition. Attributes are properties describing the context entity. Metadata, which is also an optional part of attributes, is used to convey extra information.

FIWARE's flexible architecture is enriched by several alliances and an ecosystem built from a growing array of data models. Even though NGSI's version 2 information model introduces the capability to drive a semantical expansion of the data models, there is yet no direct semantic reasoning capabilities [3] provided by the base framework. The inclusion of a semantic processing engine would allow the seamless usage of distinct ontologies while maintaining legacy systems and devices interoperable.

2.1.3.1 LINKS AND GAPS WITH THE INTERCONNECT REFERENCE ARCHITECTURE

FIWARE provides a flexible architecture and an ecosystem built from a growing array of data models. Even though NGSI's version 2 information model introduces the capability to drive a semantical expansion of the data models, there is yet no direct semantic reasoning capabilities [4] provided by the base framework. The inclusion of a semantic processing engine would allow the seamless usage of distinct ontologies while maintaining legacy systems and devices interoperable.

InterConnect builds upon the experience from FIWARE, to provide a framework that can be used by adopting platforms and digital services, making them interoperable at both the technical/syntactic levels, but most notably at the semantic level. Semantic interoperability will provide means for the discovery of service capabilities and will sponsor data translations between digital services and devices. FIWARE also provides as groundwork to explore the logic surrounding a generic adapter that can attach to an already existing service and provide new interfaces with the ecosystem.

2.1.4 W3C'S WEB OF THINGS (WOT)

The World Wide Web Consortium's (W3C) Web of Things (WoT) standards aim to solve different interoperability issues across IoT platforms and application domains. Its architecture

(introduced in [6]) is an abstract architecture designed by industrial partners such as Huawei, Fujitsu, Oracle, Panasonic, Hitachi. WoT architectural goals are to improve the interoperability and usability of the IoT. Common principles include mutual interworking of different ecosystems using web technology, namely RESTful interfaces, and the use of multiple standard formats for data encoding [5].

One of the core concepts upon which the W3C's reference architecture is built is things. A thing can be defined as an abstraction of any physical or virtual entity, where each entity is uniquely identified. W3C things functionalities include: reading, updating or subscribing to information or invoking or subscribing to input/output functions or notifications.

Things interact with consumers, that is, entities that can process Things Descriptions (TD). TD's building block provides interoperability for machine-to-machine communication and a uniform format for developers to document and to create applications that can access IoT devices and their data.

The core WoT concepts can be combined to address most use cases introduced in [5]. Namely, it introduces the concept of a "web thing", containing four key architectural aspects:

- **Behaviour** includes autonomous behaviour and handlers for the Interaction affordances;
- **Interaction Affordances** model consumer and thing interactions through abstract operations;
- **Security configuration** regroups all relevant security mechanisms used to control access to Interaction Affordances and related public/private security Metadata and Data;
- **Protocol Bindings** provides additional details, making it possible to map Interaction Affordances to messages from a particular protocol.

The resulting architecture offers the following benefits:

- **Flexibility**, which are heterogeneous physical device configurations for WoT implementations. The WoT abstract architecture could map to and cover the heterogeneity;
- **Compatibility**, to provide a bridge between existing IoT solutions, ongoing IoT standardization activities and Web technology based on WoT concepts;
- **Scalability**, since WoT must be able to scale for IoT solutions that incorporate thousands to millions of devices even if different manufacturers create them;

- **Interoperability** across device and cloud manufacturers is provided. It must be possible to take a WoT enabled device and connect it with a cloud service from different manufacturers out of the box.

W3C's WoT uses structured data (i.e., thing description or TD) to describe Things. A TD can be further defined as a "standardized, machine-understandable representation format that allows Consumers to discover and interpret the capabilities of a thing (through semantic annotations) and to adapt to different implementations (e.g., different protocols or data structures) when interacting with a thing, thereby enabling interoperability across different IoT platforms, i.e., different ecosystems and standards" [5].
TDs are processed using a JSON-LD processor. The latter also enables semantic processing, including transformation to RDF triples, semantic inference and accomplishing tasks given based on ontological terms.

2.1.4.1 LINKS AND GAPS WITH THE INTERCONNECT REFERENCE ARCHITECTURE

WoT provides a framework to describe existing interfaces with potentially multiple ontologies semantically. In that sense, the InterConnect reference architecture can be seen as a subset of WoT, where an interface is prescribed, and only one ontology (SAREF) can be used. WoT works with multiple transport protocols, such as MQTT, COAP, and HTTP, and does not necessarily require an adapter/connector. However, the semantic reasoning itself is not covered by the WoT model, as it concerns only the description of message structure and their ontological annotation. This is where a Knowledge Engine could fill a crucial gap.
A link can be made via the InterConnect adapter/connector, which must transform the messages described by the TD into an appropriate format for the InterConnect RA. The ontological descriptions can be re-used as long as the ontology is SAREF. Descriptions in terms of other ontologies must be mapped to SAREF or discarded. As far as it relates to WoT with EEBUS, SAREF will be used wherever possible, so the ontologies are not an issue. However, this means that a WoT adapter/connector would be specific to EEBUS, and not necessarily applicable to every protocol that can be described with WoT-TD.

2.2 SMART HOME/BUILDING REFERENCE ARCHITECTURES

2.2.1 THE HOME AND BUILDING ARCHITECTURE MODEL (HBAM)

The Home and Building Architecture Model (HBAM) was developed by the German Commission for Electrical, Electronic & Information Technologies of DIN and VDE (DKE)3, as a derivative of the SGAM framework for the building and home domains. The DKE is an organization responsible for producing electrotechnical standards in domains such as energy, mobility, and home and building.

In 2019 the HBAM model was presented in IEC SEG9-WG3 and updated according to the discussions which took place. The HBAM focuses on end-users to describe and model an interoperable ecosystem framework and the required interfaces for cross-domain interworking. It describes three main aspects:

- The **interoperability aspect**, which consists of various levels covering the technical, organizational, social, and regulatory objectives;
- The **application domains aspect** maps currently loosely connected systems that can be further integrated to improve end-users' added value;
- The **integration zone domain** introduces a physical or logical abstraction level for defining complex products and systems interworking.

Layer	Objectives
Component Layer	This layer groups primarily physical parts and elements. But also, software components like applications or operating systems
Communication Layer	This layer covers the entire OSI layer model on communications[4]. The physical layer (OSI layer 1) interfaces to the component layer
Information Layer	This layer distinguishes data from applications (OSI layer 7) and communication as fundamental to interoperability
Functional Layer	This layer defines use cases that can be created by any stakeholder of the ecosystem

TABLE 1 – HBAM MODEL LAYER DESCRIPTION

[3] https://www.dke.de/en/ueber-uns

[4] Open System Interconnection (OSI) – Basic Reference Model (ISO/IEC 7598-1)

2.2.1.1 LINKS AND GAPS WITH THE INTERCONNECT REFERENCE ARCHITECTURE

Although the HBAM model is still under development, it is expected to be used in the InterConnect project. All three aspects are represented in various pilots striving the domains from energy resources to audio-visual communication entertainment.
Mapping the high-level use cases onto the HBAM model will help to analyse the interactions in the respective pilots as well as helps to verify the HBAM model itself.

2.2.2 CENELEC

CENELEC provides standards for interoperability touching the energy domain. With the European Mandate M490, the Smart Grid Coordination Group (SG CG) developed a High-Level Architecture for (Energy) Flexibility. Based on this architecture, CENELEC TC59x/WG7 - smart household appliances - started in 2012 to develop a common standard for all smart appliances (whitegoods and HVAC devices) to ensure interoperable communication with the customer energy manager (CEM). The communication language and protocol is called SPINE[5] (Smart Premises Interoperable Neutral message Exchange).
As interoperability is a key objective of EN 50631-x and may not be the only language and protocol, from the very beginning, SPINE was made available to become part of the SAREF ontology and is fully compliant with SAREF4Ener.
The CENELEC EN50491-12 standard series, produced by CENELEC TC205 ‘Home and Building Electronic Systems (HBES)’ WG18 ‘Smart grids’ describes an architecture and data model for influencing the energy behaviour of devices or systems of devices in order to optimize the (local) power grid. The objective of the architecture is to achieve interoperability between any device or system of devices that provides energy flexibility, and between any system that utilizes energy flexibility. This way, lock-in for a specific technology or company can be avoided. There are many ways flexibility can be utilized; for example, local objectives, such as balancing a microgrid, maximizing self-consumption or avoiding having to upgrade to a grid connection with a higher capacity can be defined. Many devices can provide energy

[5] SPINE defines a neutral layer which helps to connect different communication technologies to build an energy ecosystem from grid to device level. For more information, please visit: https://www.eebus.org/technology/

flexibility, such as EV/EV chargers, batteries, curtailable PV panels, HVAC systems and whitegoods.

The first standard in the series, EN50491-12-1, is published. The second part, which describes the data model, responsibilities, and interactions, is currently in the enquiry stage. Several InterConnect project' partners (TNO, KNX and EEBus) are involved in CLC TC205 WG18.

2.2.2.1 LINKS AND GAPS WITH THE INTERCONNECT REFERENCE ARCHITECTURE

TC59x architecture approaches the communication of a smart appliance with the Energy Manager. Other uses and use cases for SPINE in the grid connection, HVAC and e-mobility domains are included in upcoming national German standards CENELEC and IEC activities.

The TC205 architecture offers the capabilities to enable energy management with many kinds of Smart Devices and protocols. They are complementary parts of the InterConnect Architecture, and both are already existing or upcoming standards.

2.3 SMART ENERGY REFERENCE ARCHITECTURES

2.3.1 SGAM

The Smart Grid Architectural Model (SGAM) specified in CEN-CENELEC-ETSI defines a set of common concepts, enabling their architectural specification across five distinct layers (i.e., the Business, Functional, Information, Communication and Component Layers). The SGAM focuses on supporting a neutral positioning towards the creation of smart grid use-cases, allowing a representation of interoperability viewpoints in a technologically neutral approach. The interoperability concept itself, the focal topic of this project, refers to the ability for multiple devices, despite the manufacturer, to exchange data enabling information to be used for the correct co-operation of a functionality [6].

This mechanism encompasses a three-dimension model, that merges the five interoperability layers enumerated above (Business, Functional, Information, Communication and Component Layer) with the two dimensions from the Smart Grid plane, namely: the concept of zones (hierarchically describing several levels from a power systems management perspective, and,

the concept of domains, covering the large spectrum conversion chain within the energy field (generation, transmission, distribution, DER, and consumers).

The roll-out of the SGAM architecture pertains to highlight which zones of cross-interaction between layers need to be detailed in the scope of a given use case. This methodology enables to start a design process by sketching a high-level global functional architecture and progress to define a system by using a characterization of the underlying infrastructure, components, communication protocols and exchanged data models and considered standards.

2.3.1.1 LINKS AND GAPS WITH THE INTERCONNECT REFERENCE ARCHITECTURE

SGAM presents a good departing point for InterConnect, especially in the different layers and the energy domains. It is also well suited to map (smart grid) use cases on it. We do not see the need to use the concept of zones in InterConnect directly since we in the component layer only address the DSO level. The principles of the layering, the universality and scalability of SGAM can be taken over.

InterConnect requirements call for a broader approach, especially in the IoT, smart home, home device and sensors domains. Moreover, the advantages to connect the InterConnect architecture to SGAM is that the latter is very well established in the smart grid world and the SDOs CEN-CENELEC and ETSI.

InterConnect requires a more in-depth focus on the function/service layer and the information layer. Information is in InterConnect exceeds a set of data models: InterConnect will use ontologies and, as such, make semantically enriched interoperability possible.

The main architectural difference between InterConnect's IoT HLA and this initiative is that the project's Reference Architecture differentiates less (or not at all) the domains or zones in at least the layers communication and information, given InterConnect's architecture and its objective of achieving semantically enriched interoperability.

2.3.2 IEC

The International Electrotechnical Commission (IEC) is a global organisation which provides international standards. The standards produced serve as a basis for national and cross-border regulatory frameworks and legislation for the sector. The IEC has had a significant role

in sponsoring the integration of several parts and players from the energy sector. Most notably, the creation of several standards has opened the possibility to integrate parts and services from different vendors, sponsoring Interoperability.

The IEC's vision[6] towards the smart grid architecture covers several tiers, spanning the generation, transmission, distribution, DER, consumption and the communication and crosscutting tiers. Moreover, the architecture matches these tiers with a rationale for the positioning of concepts with their main actors, namely: processes, stations, field, operation, enterprise and market. Focusing on interoperable capabilities, other standards address from an ICT perspective how control data should be transmitted and modelled, namely through the standards IEC 62357. This standard encompasses a series of considerations for data modelling, including the possibility to encourage the use of semantically driven reasoners through the use of ontologies tailored for this domain.

There are several points of views drawn from the analysis of this standard, from the establishment of profiles and service modelling to the actual communication and information data model exchanged. These features can be viewed as a group of IEC reference documents, as they all together provide detail and positioning. The IEC architecture also covers relevant topics such as Advanced Metering Infrastructure (AMI) or the inclusion of EVs – electric vehicles, respectively in IEC 62051-62059 and IEC 61851.

2.3.2.1 LINKS AND GAPS WITH THE INTERCONNECT REFERENCE ARCHITECTURE

IEC possesses a unique role in this state-of-the-art section as it does not directly configure an architecture model, from which we can establish a comparison with InterConnect HLA. It provides a set of standards that establish key characteristics for the IoT and energy, that directly tackle some of the challenges in providing interoperability within the smart grid landscapes.

[6] Please note that the IEC Smart Grid Reference Architecture is not a dedicated architecture but a landscape for existing IEC standards related to the Smart Grid Architecture Model (SGAM)

2.4 INDUSTRIAL REFERENCE ARCHITECTURES

2.4.1 IIRA

The Industrial Internet Reference Architecture (IIRA) is the result of the work carried out by the Industrial Internet Consortium (IIC)[7]. It is a standards-based open architecture for IoT systems, based on the ISO/IEC/IEEE 42010:201 standard [8]. It serves as a foundation for the development of real-life application architectures across numerous sectors. Based on the ISO architecture specifications, IIRA defines a set of viewpoints (i.e., representation of architecture views) to help model and resolve the different concerns and stakeholders that compose each architecture view.

Four viewpoints help frame and analyse the various IoT use cases that were considered:

- The **Business Viewpoint** develops the concerns identified by the business vision and objectives. By conceptualising IIoT requirements of systems that integrate business logic, factors such as regulatory constraints, external influences, and technological trends participate in shaping the resulting system characteristics;
- The **Usage Viewpoint** expresses the concerns of the system's users (e.g., humans or systems) and the system's capacity for delivering intended functionalities;
- The **Functional Viewpoint** focuses on the functional components that compose an IIoT system. Their relationships and interactions are modelled by IIRA and are the subject of the next section;
- Finally, the **Implementation Viewpoint** details the technologies and concepts needed to instantiate the functional viewpoint.

IIRA's architectural viewpoints (business, usage, functional) are organised in a way that demonstrates top-to-bottom and bottom-to-top interactions. The higher-level viewpoints (e.g., Business Viewpoint) guide and impose design requirements of lower-level viewpoints (e.g., Usage Viewpoint). In contrast, lower-level viewpoints can impose, in some cases, a revision of higher-level viewpoints. IIC decomposes an IIoT system into five functional domains:

[7] The IIC is a global partnership of Industry, Government and Academia members. Founded in 2014, it provides guidance and resources in the digital transformation domain. Specifically, the IIC members are concerned with developing, implementing, and testing collaborative IIoT (Industrial Internet of Things) solutions through the development of Testbeds (experimentation platform), Test Drives (short-term pilots), and the creation of an ecosystem for increased interoperability and security via reference architecture frameworks and open standards.

- The **Control Domain**, which contains the set of rules and logic that exercise control over physical systems. These components or systems are usually stationed close to the physical system they control (e.g., control units in an electricity utility plant);
- The **Operations Domain** represents the set of functions responsible for managing and operating the components in the Control Domain;
- The **Information Domain** allows for data collection and transformation from the control domain. The data is then analysed and modelled to obtain a high-level overview of the IIoT system;
- The **Application Domain** can be defined as the application logic that carries out business functionalities. Low-level operations are not performed at this stage, but rather delegated to functions in the Control Domain;
- The **Business Domain** contains the processes and business activities needed to implement the business logic within IIoT systems.

The data flows and control flows between the domains are represented as green and red arrows, respectively, in Figure 2. Concurrently, new forms of data and control flows are generated within each domain (horizontal arrows). The functional domain also covers other essential enabling system functions as "crosscutting functions" (i.e., available across components such as connectivity and data management functions). The emergent properties resulting from the interaction of the different parts are labelled "system characteristics" (e.g., reliability and system security).

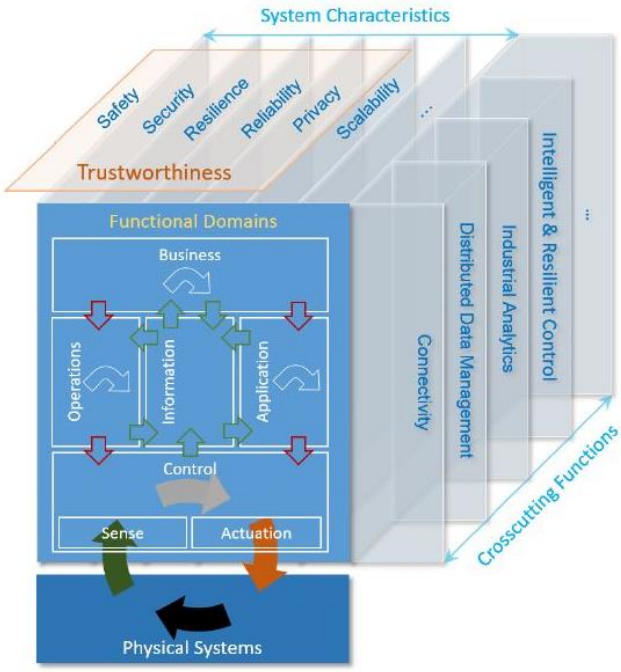


FIGURE 2 – IIRA'S FUNCTIONAL MODEL

2.4.1.1 LINKS AND GAPS WITH THE INTERCONNECT REFERENCE ARCHITECTURE

IIRA provides an industrial architecture that focuses on addressing key domains within product development such as operations, information, application and business. While focusing on IoT, IIRA aids in mapping functionalities and the business logic behind use-cases, detailing them via several domains.

This architecture does not directly cover a domain (even when addressing IoT) such as energy, appliances, or services for comfort control and automation. Moreover, there is no particular focus on interoperability (independent of the level that is considered, namely syntactic or semantic). InterConnect establishes a very distinct architecture and splits it a by launching an HLA for IoT (SHBIRA) and for Energy (SERA) where semantic interoperability addresses the crosscutting entities of each one of them where layers cover the main actors for the SERA and the main ICT building blocks for the SHBIRA, therefore distancing from this approach.

2.4.2 IDS

The International Data Spaces' (IDS) Reference Architecture, also known as DIN SPEC 27070 "Requirements and reference architecture of a security gateway for the exchange of industry data and services" [7], is an architecture of a data infrastructure based on European values, i.e. data privacy and security, equal opportunities through a federated design, and ensuring data sovereignty for the creator of the data and trust among participants. It forms the strategic link between the creation of data in the internet of things (IoT) on the one hand and the use of this data in machine learning (ML) and artificial intelligence (AI) algorithms on the other.

The IDS Association (IDSA) defines this reference architecture, which supports sovereign exchange and sharing of data between partners. Whether data of IoT devices is concerned, in on-premise systems or cloud platforms, the IDSA aims at providing the guidelines for sharing data between different endpoints while ensuring data sovereignty.

The architecture contains four essential components, namely:

- The **IDS Connector**, which acts as an organization's interface into the network and handles all IDS-specific protocols and security functionality. The organization's back-end systems, IIoT-devices, end-users, etc. interface with the IDS Connector to access the IDS space. The IDS Connector can load IDS Data Apps from the app store, which enables domain-specific standardized data handling. Moreover, the IDS Connectors

automatically publish their self-description (i.e. metadata such as organization, functionality) to the IDS Broker;

- The **Broker** acts as a yellow page and has an overview of the connected connectors. Brokers can be queried by all connectors to route information to the available partners dynamically;
- The **Identity Provider** (i.e., Dynamic Attribute Provisioning Service) manages the certificates of the organizations present in the IDS space and contain an elaborate stack of security functionality. Moreover, it should be noted that the complete IDS architecture is highly flexible. For example, it is possible to have zero or multiple of the central components in the IDS space (e.g. Broker, DAPS, Clearing House). Moreover, there are various implementations of all components, ranging from enterprise-graded connectors which interface with ERP software components to components which directly interface with IoT devices;
- Finally, the **Clearing House** is a centralized component for logging (metadata of) data transfers to a central component. This component acts as a trusted third party which can resolve any disputes which might occur. It is optionally and can be used to log a full copy or a subset of the original data and can be hashed or encrypted.

In order to ensure interoperability within multiple domains, the IDS architecture comes with an overarching ontology, namely the IDS Information Model. This model is used and extended in all domain-specific applications.

2.4.2.1 LINKS AND GAPS WITH THE INTERCONNECT REFERENCE ARCHITECTURE

The IDS reference architecture provides a technically, ICT-focused architecture mapping devices, gateways and other brokers. Given that focus, this architecture is focused on the IoT domain in general, not showing a particular tailor for any specific domain such as energy or comfort, for instance. The reference architecture provided within InterConnect offers a domain focused experience, not only in what regards to the IoT domain (with comfort and user-centric design) but also to energy, with its smart energy reference architecture. Even though InterConnect provides more focused reference architectures in terms of domain, the architectural designs are kept at an actor/layering level. They do not showcase direct components as it happens with this architecture under review.

2.5 COMPARISON AND DISCUSSION

This section provides a discussion regarding the surveyed reference architectures.

	Interoperability			Ontology		ICT Processing Focus			
	Technical	Syntactic	Semantic	SAREF	Proprietary	Edge	Fog	Cloud	Legacy
AIOTI	1	1	4	2	4	3	2	3	2
ONEM2M	2	2	3	4	5	4	1	3	1
FIWARE	4	4	2	2	2	4	2	5	2
W3C WOT	2	4	4	3	3	4	3	4	3
IDS	0	0	0	2	5	1	2	6	3
HBAN	4	4	4	4	2	4	2	2	4
CENELEC	2	4	5	5	4	1	1	1	1
SGAM	4	5	1	0	0	1	1	1	4
IEC	2	4	2	0	2	1	1	1	4
INTERCONNECT	4	5	6	6	4	6	4	6	3

TABLE 2 – COMPARISON OF KEY ARCHITECTURAL FEATURES

Legend

0	not relevant
1	Agnostic
2	Includes Awareness
3	Adopts some concepts
4	significantly relevant
5	very relevant
6	Highly relevant

The analysis is provided in Table 2, where each one of the reference architectures is catalogued in three dimensions, namely: interoperability, ontology and ICT processing focus. The Interoperability dimension identifies and classifies the interoperability level provided in each one of the reference architectures. The ontology dimension highlights if a given architecture comprehends ontology specific characteristics as addressing SAREF or any other (proprietary) ontology. Finally, the ICT processing focus dimension assesses if these architectures can distinguish (and in which layers) the processing focus, namely if the processing can occur at the edge, fog, cloud or legacy (or proprietary infrastructures). The assessment of all these dimensions is achieved via a scale that spans from 0 (not relevant) to 6 (highly relevant). Moreover, it provides a colour scheme that transforms Table 2 into a heat map for visual guidance.

From the interoperability dimension, most reviewed architectures score high (above 4) across the three interoperability levels. It is worth noting that more generic architectures such as AIOTI, oneM2M, IEC or SGAM do not score equally throughout the technical, syntactic or semantic interoperability. While AIOTI and oneM2M aim for supporting semantic interoperability, IEC and SGAM are instead focused on syntactic (and technical for the case of SGAM) interoperability. The remaining architectures - generally more IoT-focused - have better scores regarding syntactical and semantic interoperability. At this particular dimension, InterConnect aims at full interoperability, implying that these three interoperability levels, but mainly the latter two, will have a deep commitment and impact in the results.

Regarding the ontology dimension, its expected that the architectures that scored high regarding semantical interoperability also score high in this dimension. In fact, this is the case (particularly) for AIOTI and oneM2M. Other solutions such as IDS also score high, showing that there is a trend to include (in this case proprietary) ontology notions even if interoperability is not necessarily set as one of their main targets. This might sound counter-intuitive, but for some cases, ontologies are used as look-up-tables to identify data and, even if they are present, they are not considered as a support for reasoning capabilities. On the other hand, architectures which usually cover the industrial spectrum, do not necessarily address the need for ontologies and even SAREF, being HBAN the architecture that is highlighted as it encompasses a significant relevance for SAREF in its construction.

Finally, regarding the ICT processing focus dimension, it is clear that reference architectures that directly map or are closer to the IoT ecosystem, such as AIOTI, oneM2M, FIWARE or W3C do show significant to high relevance on the edge, fog and cloud focus. Most of these architectures include the notion of computational capabilities or business processing at the edge layers (which in this case also includes gateways). They can mix them with other legacy capabilities for processing that are now cloud-based solutions and that leverage from the cloud computing paradigm. On the other hand, industrial architectures are often based on IEC or ISO standards which have an agnostic implementation. Therefore, they score lower. This is not because solutions mapped under these architectures are unable to gain leverage from these structures, but rather that these architectures are agnostic to this type of mapping.

InterConnect establishes a close dependency from ontological developments, particularly to SAREF. Semantic reasoning and what it can covey to interoperability is one of the key exploitable results that InterConnect is expected to deliver. In that sense, InterConnect also addresses the need to distribute processing between the edge devices and to include fog

systems (middleware systems) that can translate and off-load processing when needed. With the cloud computing paradigm at the centre, InterConnect delivers a set of cloud-enabled tools to sponsor interoperability and to provide high-availability capabilities to such services, both from the energy and non-energy realms.

3 METHODOLOGY, PRINCIPLES AND ARCHITECTURAL REQUIREMENTS FOR INTERCONNECT'S REFERENCE ARCHITECTURE

This chapter begins by discussing the project's need for a common reference architecture before introducing the design and security principles, requirements and methodology used to derive the Reference Architectures produced by the InterConnect Project.

3.1 ON THE NEED FOR A COMMON REFERENCE ARCHITECTURE

A common Smart Home/Building and Smart Energy Reference Architecture is a key enabler for successfully interworking the 50 project partners as well as connecting Smart Homes, Buildings and (electrical) Grids in seven European countries (Portugal, Greece, France, Netherlands, Germany, Belgium, Italy). These solutions will help provide people from all over Europe the ability to interconnect devices in their Smart Homes and Smart Buildings to a wide range of services from different providers, using the Smart Grid as a means for efficient exchanging energy.

IC's Secure interoperable IoT Smart Home/Building and smart Energy system Reference Architecture (SHBERA) is the overall architecture view describing the different layers and domains introduced by the **Smart Energy Reference Architecture (SERA)** and the **Smart Home/Building IoT Reference Architecture (SHBIRA)**. It is a technology-independent and device-agnostic architecture that will be used in the development and demonstration of advanced solutions.

The SERA focuses on the energy system point of view and introduces the project's actors, roles and devices in the energy system and the information exchange between these.

The SHBIRA takes on the functional/service layering perspective and focusses on the interoperability and communication of services with each other and with the devices, cloud and local management systems in buildings.

In order to support a relatively easy comparison of implementation architectures, the SERA shows a close resemblance with parts of existing reference architectures in the smart grid

domain. The emphasis is on parts following InterConnect's focus on the interconnection of homes, buildings and grids. As such, the SERA does not replace current Smart Grid reference architectures but instead uses concepts from existing reference architectures used in the smart grid domain to discuss and compare interconnection of devices, services and parties/roles in the energy system.

The SERA can then be defined as an architecture and a tool to help InterConnect focus on the interconnection (by the exchange of information) of devices in homes, buildings with services (available through the Internet for example) and the (electrical/smart) grid. It includes fewer details than many of the existing reference architectures to enable new roles and stay flexible with current and changing legislation as well as to provide project members with an overview and understanding on how their part relates to all other parts of InterConnect.

The SHBIRA also focuses on interconnecting devices, homes and buildings to the Smart Grid. It does so by providing a flexible, device and technology-agnostic high-level architecture, which builds on top of the extensive work already carried out by other initiatives and standards[8] (e.g., AIOTI, oneM2M, SGAM, amongst others). It fully integrates InterConnect's Interoperability Framework and develops on existing standards and technologies, such as SAREF, to allow different stakeholders to develop and implement complex use cases and new innovative services, as such developed within this project.

Without a Reference Architecture, it would have proven difficult to compare the different geographically distributed implementation architectures systematically. This was required for finding out where to introduce layers of interoperability between the different systems across Europe. These layers are important, as this is where information is exchanged between architectural components regarding the status and control of devices, past and planned energy usage, amongst others.

The following section describes the three fundamental principles that guided the design of InterConnect's reference architecture and architectural viewpoints.

[8] See Section 2 for a detailed analysis of the Links and Gaps of the InterConnect Reference Architecture to other initiatives and standards.

3.2 BASIC DESIGN PRINCIPLES

3.2.1 STRUCTURE FOLLOWS USAGE

This principle states that the resulting architecture must primarily relate to its intended function or purpose. In such cases, the resulting system architecture can be "rearranged" to meet the core functional requirements formulated by the project's stakeholders.

Since the project's Reference Architecture is meant as a tool to implement interoperable solutions of 50 project partners that connect Smart Homes, Buildings and (electrical) Grids, it needs to be derived from the needs of these project partners. As such, the overall process:

- Originated from the **collection and analysis of High-Level Use Cases and stakeholder's concerns**, produced by WP1 and WP2 partners. The latter was then generalized, creating a generic, layered structure providing a high degree of adaptability to cover all use cases.
- Was **carried out iteratively**, allowing us to step back if needed when delivering advancements to the overall specification of the required Reference Architecture. By doing so, new information, methodologies or requirements could be included at any step in the derived IoT Reference Architecture.
- Allowed for **collaborative and synergetic effort**, through cross-WP discussions, helping to synchronize and validate the resulting viewpoint.

3.2.2 SEPARATION OF CONCERNS

InterConnect's Reference Architecture (SHBERA) and each of its domain-specific viewpoints (e.g., the SHBIRA and the SERA) are also based on the High Level Architecture (HLA) proposed by AIOTI's WG03 "IoT Standardization". This working group is responsible for identifying standardization problems. The main objective of the AIOTI HLA is to reduce complexity by offering a comprehensive IoT landscape standardization framework that achieves semantic interoperability [1].

Following AIOTI's recommendations, IC's Reference Architecture is described using the ISO/IEC/IEEE 42010 standard which expresses architectures in terms of multiple views "*in which each view adheres to a viewpoint and comprises one or more so called architecture models*". As such, IC's multiple viewpoints enable (business) architects and/or (software) engineers and/or (platform/system) designers to focus on specific directly related topics, while

not being overloaded with other issues/domain views (that are related more indirectly in complex systems). This is one example of Separation of Concerns (SoC).

Another way is applying modularity, which would allow us to keep information that is not needed outside a software module inside. Modularity also requires the creation of a well-defined interface for the information that is required outside the module.

3.2.3 LAYERING

For describing the IC Reference Architecture, the project has adopted the principle of architectural layering. A model consisting of 5 layers has been used, that is the result of merging the Reference Architecture Model Industrie (RAMI) 4.0[9] and the Smart Grid Architecture Model (SGAM)[10]. The following layers are defined:

- **Business Actors and Roles**, this layer contains all (business) actors and/or roles active in the InterConnect system. Examples of those actors are Energy Suppliers, Home Appliance Manufacturers, Service Providers, Consumers, Building owners, and EV drivers;
- **Service/Function**, this layer contains all services and/or functions that will be performed, either directly or indirectly, by or for the actors/roles;
- **Information**, this layer contains all information objects and structures needed by the functions and services mentioned above. This layer is the most 'virtual' since it cannot be coupled directly to a location or actor. In this layer, semantic interoperability should be achieved;
- **Communication**, this layer performs the communication between devices and physical assets (southbound), and to the system layers above (northbound), between applications and services;
- **Device/Asset/Component/Thing**, this layer contains all physical elements, very often clearly described in use cases. For example, it contains devices (like household appliances, EVs) and assets (like DSO infrastructure as networks and substations), other components (like EVSE, buildings, ...) and *things* (as in IoT: physical objects (things) with sensors, software, and other technologies, connected to the internet to communicate with other things, devices and systems).

[9] For more information on the RAMI 4.0, see https://www.plattform-i40.de/PI40/Navigation/EN/Home/home.html

[10] See Section 2.3.1.

The next section focuses on the privacy and security principles enforced by the InterConnect Framework - a core value within the Consortium - and how a suitable level of security across the system can be achieved. The set of security-related requirements, derived from these principles, is discussed Section 3.3.

3.3 ENSURING SYSTEM SECURITY

Ensuring security and privacy throughout the InterConnect Interoperability Framework means that each participant or actor in the InterConnect Framework instance (e.g., instantiation of the framework by the project pilots) can share and retrieve (control) information from any/all other actors and their related devices and services safely and securely. For all data exchange and control processes performed through the InterConnect Interoperability Framework, the following common principles should apply:

- Each endpoint (user, application, service, device) should be authenticated and authorized;
- All communication and data handling should be securely performed with the main focus on data/privacy protection; and
- All participating stakeholders should be ensured that their data is treated with the appropriate security measures. These security measures need to enforce the privacy of the consumer, confidentiality of the data, integrity and availability of the data.

One of our main challenges in this project is the plethora of stakeholders (e.g., consumers, manufacturers, DSO's) and related services or devices, each presenting different security requirements and challenges (e.g., privacy requirements for consumers, safety requirements for DSOs) in different contexts (e.g., end-user hardware for consumer devices is different than substation hardware of a DSO). As a result, different security measures will be taken.
This section will address privacy and security requirements for information/data and for control (actuating systems and devices) in three steps:

- Definition of the set of background principles and required security levels, domains and groups;
- Attribution of responsibilities based on roles and location privacy;
- Lastly, analysis of the impact of these elements in the resulting architecture, namely, how privacy and security will be addressed for the Semantic Interoperability Layer,

participating digital platforms, devices, services and IC's Service Store. As we will see, the InterConnect Framework should be able to facilitate different security and privacy protection groups.

The next sub-sections will focus on detailing the two first steps before introducing the resulting security-related requirements on Table 9. The analysis of the impact on the resulting architecture will be later introduced, in Section 4.5, following the presentation of the SHBERA, and its related architectural viewpoints (SERA, SHBIRA, and IC's Interoperability Framework Architecture or IFA) discussion. Overall security and privacy protection framework for the project pilots is presented in D2.2 [42].

3.3.1 BACKGROUND PRINCIPLES

3.3.1.1 ISO 62443 - SECURITY LEVELS

The Smart Grid Information Security (SGIS) model[11] defines security levels (SGIS-SL), similar to those introduced by ISO 62443, but that are specially described for the energy sector. Each security level describes an impact and varies from 1 (low) to 5 (highly critical). At security level 1, a disruption could lead to a power loss under 1MW, whereas at security level 5, a disruption could lead to a power loss above 10GW.

It is interesting to note that the SGIS-SL model also estimates the required security level for a given SGAM Domain/Zone. This leads to a table combination of a SGAM Domain and Zone, resulting in a different security level.

Like SGIS-SL, InterConnect will require that different security levels be supported in different parts and domains of the framework, which requires the definition of specific "security groups". A security group is a set of security requirements, meant for a specified domain, with a specified security level.

This principle is embodied by the derived requirement **R4.4**.

[11] For more information, see https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_security.pdf

3.3.1.2 INFORMATION SHARING

In [8], the authors suggest a framework to examine information sharing on Smart Grids in a structured way. This framework can be used to analyse related 'remote monitoring' services, and information about a consumer, his energy consumption or service usage, which can then be shared in three 'axis' (or degrees of freedom). Table shows the relationship between these degrees of freedom and the impact on privacy.

Degree of freedom	Impact on privacy
Level of detail	An increase in the level of detail means less privacy for the end-user. Thus, a breakdown of aggregated information into a more detailed level of information (e.g., at the appliance level) means less privacy.
Direction in time	Sharing information about the current or (expected) later use will have an additional impact on consumer's privacy. Information about the future provides insight into predicted or expected consumption of energy carriers reduces consumer's capacity to keep their past or future energy consumption private, entailing privacy risks for end-users.
Additional recipients	Each recipient of consumer's information has an impact on the privacy of the consumer. Moreover, the number and type of recipients are also significant (e.g., the DSO, needs data for sending a bill, whereas a next-door neighbour does not need to access this data). If the number of recipients increases, this usually means less privacy for consumers.

TABLE 3 – RELATIONSHIP BETWEEN THE DEGREES OF FREEDOM AND PRIVACY [8]

Information can be kept private by not sharing it. However, this makes it impossible for certain services to work correctly (e.g., producing an energy bill, or using prediction services requiring extensive data). Another approach that can still ensure data privacy is to share only the required information with actors and service providers that have an explicit service agreement with the customer.

From this analysis, we conclude that the InterConnect interoperability framework should provide users with the ability to set privacy levels for securely sharing information while allowing them to accept (or decline) different provided services. This should also be enabled for service providers and platform operations who are managing consumer's data.

This principle is embodied by the derived requirement **R4.5**.

3.3.1.3 CONTROL SHARING

Connecting devices to services using the InterConnect Framework has a potentially significant impact on Smart Homes and Buildings and Smart Grids. Since this type of interconnection enables remote control of devices that influence the physical reality of the built environment, services interconnection requires the exchange of information, and sometimes also the sharing of control[12]. Table 4 shows the relationship between three axes (degrees of freedom) for control sharing and privacy.

Degree of freedom	Impact on privacy
Predictive window	A large predictive window forces consumers to make early decisions on their energy consumption. For example, when the decision to use no energy after 22:00 is made at 18:00, a consumer cannot change his mind at 21:00
Level of indirection	The higher the level of indirection, the more choice the consumer has, so the lower the impact on personal lives privacy (e.g. if the only control is that the consumer may not consume more than 3000 Watts, the consumer can decide for himself how he uses the 3000 Watts. If the grid decides that the consumer cannot watch TV, because he will be using the washing machine, there will be a significant impact on privacy)
Level of participation	When the control decisions are made by an external party, the owner of the device connected to the grid considerably loses privacy. If the consumer is participating in the control decisions, the impact on his personal life (in terms of privacy and control) will be lower. The more participation there is in the decision-making process, the more privacy for self-control is left for the consumer.

TABLE 4 – RELATIONSHIP BETWEEN THE DEGREES OF FREEDOM AND PRIVACY [9]

This principle is embodied by the derived requirement **R4.6** and **R4.7.**

3.3.1.4 NUMEROUS STAKEHOLDERS, CONFLICTING REQUIREMENTS

InterConnect aims to provide an infrastructure where IoT devices/services and Smart Grid services can communicate and cooperate. To achieve this goal, we have defined several functional requirements that are relevant for the different stakeholders, devices and services in the IC ecosystem. Within the Consortium, different stakeholders have different roles and

[12] For example, when a service enables a washing machine at the optimal time for the energy grid, it is not the consumer who decides when his washing machine is turned on, but the service.

different requirements. These requirements might also conflict. Below, a list of key stakeholders and their main requirements:

- **Service providers:** there are different kinds of service providers within different security groups. For example, a weather forecast service will not be interested in investing heavily in secure communications. On the other hand, a DSO will need to invest heavily in secure communications because of the potential pervasive impact of a failure. Within the project, different service providers will have different/conflicting requirements about the security groups; however, InterConnect should be able to handle and provide different security groups for different Service providers. This situation could be even more problematic if these service providers depend on each other[13].
- **DSOs & TSOs:** DSOs and TSOs want to provide a reliable energy network. Therefore, they require high-integrity measurement values. However, for the DSO and the TSO, conflicting requirements may arise. For some grid-related service, the latter may need or want to provide details on expected congestion and location while ensuring that others do not misuse this information (e.g., commercial aggregators pretending they need grid capacity to reduce it for commercial benefit later).
- **Manufacturer:** A manufacturer wants to design and build devices for users. Implementing security requirements on (IoT) devices can have a heavy impact on the development and production costs. As a result, manufacturers may not want to create devices on a higher security level than needed to exploit its core functionality[14].
- **User:** For most end-users, easy usage is considered essential. For example, a user should be able to buy a new device and install it within his home-environment with just a few (simple) installation steps. As a result, security measures should not result in a complex configuration for the end-user. Moreover, on the privacy of data, there are also potential conflicts of interests. The service provider may like to collect as much data as possible for sometimes future or unknown purposes, while the end-user may only want to share data on a need-to-know basis.

This principle is embodied by the derived requirement **R4.8**. The next subsection will briefly discuss our approach for dealing with cybersecurity challenges within the context of InterConnect.

[13] An example would be households that calculates the expected production of solar panels based on the weather forecast service, an integrity issue of the weather forecast service can have a considerable impact on the DSO.

[14] For example, it may not be commercially viable to manufacture an electronic cat-flap with the security requirements of a distribution station

3.3.2 THE SECURITY AND PRIVACY PLAN PROCESS (SPOCS)

To deal with the constant and ever-evolving challenges of cybersecurity, business groups, government agencies, projects, and other organizations have produced “cybersecurity frameworks”, documents, and tools to help organize and communicate cybersecurity activities. This subsection introduces one of such frameworks, explicitly developed for InterConnect: the **Security and privacy Plan Process (SPOCS)**.

SPOCS is a cybersecurity and privacy combined framework for smart grid and IoT is compliant with ISO/IEC standards. Its main goal is to create a high-level plan to help following security and privacy concern for an application in the context of a smart grid home ecosystem. Additional goals are to 1) identify and analyse threats about security and privacy, and 2) identify and define solutions to the cybersecurity and privacy tasks.

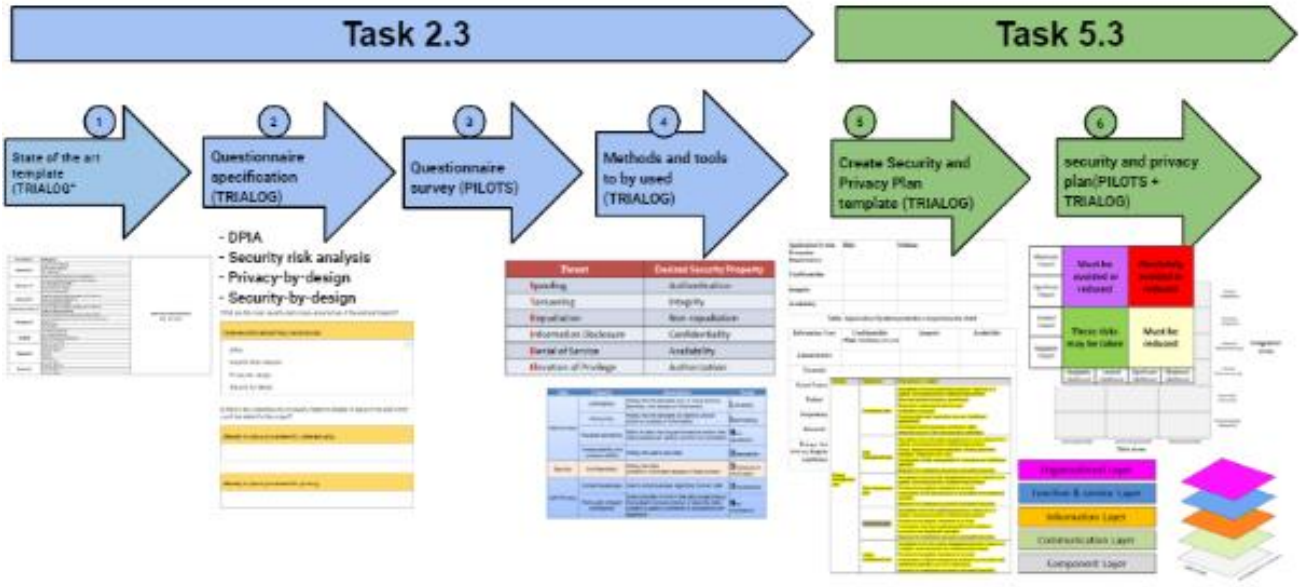


FIGURE 3 – INTERCONNECT’S SECURITY AND PRIVACY PLAN PROCESS (SPOCS)

Figure 3 shows a high-level overview of the SPOCS framework. It consists of 6 steps:

- **Step 1** focuses on the state-of-the-art investigation (e.g., ISO standards, NIST frameworks, STRIDE and LINDDUN methodologies) to analyze their limits and introduce the need of our framework to overcome their gaps;
- **Step 2** designs the questionnaire to be sent to pilots to get an overview with their experience of security and privacy;

- **Step 3** applies the questionnaire to pilots to get an overview with their experience of security and privacy;
- **Step 4** focuses on methods and tools to be used (a selection of tools analyzed in Step 1);
- **Step 5** designs the Security and Privacy Plan;
- **Step 6** applies the Security and Privacy Plan to pilots. Refinement of the plan will be done following the feedback and experience.

The Security and Privacy Plan comprises five sub-plans:

- Governance Management Plan,
- Data management Plan
- Risk management plan
- Engineering Management Plan
- Citizen Engagement Plan

The SPOCS framework and all related concepts are further developed in deliverable D2.2 [42].

3.4 INTERCONNECT'S ARCHITECTURAL REQUIREMENTS

This section introduces the core and derived requirements that InterConnect's Secure interoperable IoT Smart Home/Building and smart Energy system Reference Architecture (SHBERA) should comply to at all times. The following list of high-level requirements will later allow us to verify if the resulting IC architecture complies with the goals and objectives set at the beginning of this project.

Requirement #	Description
R1	IC Reference Architecture **MUST** be technology independent and device agnostic
R2	IC Reference Architecture **MUST** integrate semantic reasoning mechanisms to exploit the benefits of ontologies and semantic technology in the InterConnect ecosystem
R3	IC Reference Architecture **MUST** include a set of InterConnect-compliant energy and non-energy services, and produce extensions for a mainstream uptake and for testing and applying new business models
R4	IC Reference Architecture **MUST** be based on the latest and most stable industry standards and insights for cybersecurity and data privacy protection
R5	IC Reference Architecture **MUST** enable data exchange between all stakeholders, roles and their related services

TABLE 5 – HIGH-LEVEL REQUIREMENTS FOR INTERCONNECT'S REFERENCE ARCHITECTURE

These high-level requirements have been further specified within WP2 and other WPs, so that each introduces a set of scope-specific requirements. Table 6 defines the set of derived requirements from **R1**, covering the IC Ecosystem and core principles:

Requirement #	Description
R1.1	IC Reference Architecture **SHOULD** be based on existing reference architectures in the smart grid and IoT domains
R1.2	IC Reference Architecture **SHOULD** be flexible enough to support pilot-specific use cases and integrate existing (legacy) systems as well as use cases from cascade funding projects
R1.3	IC Reference Architecture **MUST** provide a high level of modularity and be implementable by including different standards/best-practice techniques
R1.4	IC Interoperability Framework **MUST** achieve semantic interoperability without an intermediary digital platform purposefully built for the project to facilitate this interoperability
R1.5	IC Interoperability Framework **MUST** specify an interoperability toolbox that provides enablers and services to speed up the realization of interoperable environments required by the project pilots and defined use cases
R1.6	IC Interoperability Framework **SHOULD** enable interoperability not just within pilots, but among them in overarching use cases
R1.7	IC Interoperability Framework **MUST** support cascade funding partners and integrators to utilize the interoperability toolbox components to make their platforms and services interoperable in the same semantic interoperability framework
R1.8	IC Reference Architecture **SHOULD** allow instantiations of the same service (from the service store) to be hosted on different platform instantiations

TABLE 6 – REQUIREMENTS FOR INTERCONNECT'S ECOSYSTEM AND CORE PRINCIPLES

Table 7 further specifies the requirements derived from **R2**, specific to the Semantic Interoperability Layer.

Requirement #	Description
R2.1	IC Semantic Interoperability layer **MUST** offer a set of dedicated semantic components to discover, make reasoning based on ontologies and translate
R2.2	IC Interoperability Framework **SHOULD** achieve semantic interoperability based on the SAREF ontology and a set of existing, already validated semantic reasoning and orchestration technologies

R2.3	IC Semantic Interoperability layer **MUST** provide a mechanism for the above-mentioned translation, discovery and reasoning
R2.4	IC Semantic Interoperability layer **SHOULD** enable explainability to the user for transparency and privacy protection
R2.5	IC Semantic Interoperability layer **MUST** guarantee the accessibility and open license of the enablers developed within the project
R2.6	IC Semantic Interoperability layer **SHOULD** be easy to adopt by non-ontology experts
R2.7	IC Semantic Interoperability layer **SHOULD** aim for a minimal impact on the operational behaviour of the system. Properties, such as performance of the system, should not be influenced in a way that the behaviour of the entire system changes

TABLE 7 – REQUIREMENTS FOR INTERCONNECT'S SEMANTIC INTEROPERABILITY LAYER

Table 8 provides a list of requirements derived from **R3** and cover the SAREF-compliant services, and Service Store developed within WP3 and WP5.

Requirement #	Description
R3.1	IC Reference Architecture **SHOULD** allow end-users to connect devices, services and applications to multiple other services from different providers
R3.2	IC Reference Architecture **SHOULD** allow the introduction of new services and new devices without requiring a complete restandardization of the IC Framework
R3.3	IC Reference Architecture **SHOULD** allow the introduction of new relevant technologies, such as blockchain and smart contracts technologies to favour the uptake and development of new business models
R3.4	IC Interoperability Framework **SHOULD** implement a mechanism for interoperability compliance test and certification

TABLE 8 – REQUIREMENTS FOR INTERCONNECT'S INTEROPERABILITY FRAMEWORK

Table 9 further specifies the requirements derived from **R4**, specific to the project's system security and privacy.

Requirement #	Description
R4.1	IC Semantic Interoperability layer **SHOULD** allow that data stays at the source (e.g., no duplication of data in RDF)
R4.2	IC Semantic Interoperability layer **MUST** follow the security by design approach

R4.3	IC Interoperability Framework **MUST** ensure that achieved interoperability does not impact or limit the privacy protection regulations and mechanisms already implemented by participating entities
R4.4	IC Interoperability Framework **SHOULD** be able to support different types of security requirements and security levels for different types of threats
R4.5	IC Interoperability Framework **SHOULD** allow data sharing in different granularity levels to different recipients. This process should be fully transparent and under the control of the end-user and data controllers (e.g., BMS, service provider)
R4.6	IC Interoperability Framework **SHOULD** support data and control sharing protocols
R4.7	IC Interoperability Framework **SHOULD** facilitate R4.6 (data and control sharing) by providing end-users and framework integrators with a level of participation on control decisions
R4.8	IC Interoperability Framework **SHOULD** aim to ensure that 'low-level 'security service will not impact 'high-level' security systems. As a result, InterConnect project should be able to evaluate dependencies between services and devices
R4.9	IC Interoperability Framework **MUST** provide a flexible identification and authorization service for its integrators and users
R4.10	IC Interoperability Framework **SHOULD** facilitate the communication between devices, users and services while enforcing the (different) policies given by all the stakeholders
R4.11	IC Interoperability Framework **SHOULD** allow devices, users and services to have their own security capabilities, possibly resulting in different security groups

TABLE 9 – REQUIREMENTS FOR INTERCONNECT'S SYSTEM SECURITY AND PRIVACY

Lastly, Table 10 specifies the requirements derived from **R5**, specific to the project's requirement to achieve interoperability between the stakeholders and the Energy providers.

Requirement #	Description
R5.1	IC Reference Architecture **SHOULD** allow the introduction of interoperable data exchange mechanisms that will enhance grid observability and system coordination using distributed data resources
R5.2	IC Reference Architecture **SHOULD** allow the development of new market tools and energy/non-energy services to increase the penetration of renewable resources
R5.3	IC Reference Architecture **SHOULD** be flexible and technologically agnostic to encompass the operational planning processes between system operators, improve distributed controllability and market interaction, and enhance system coordination

TABLE 10 – REQUIREMENTS FOR ACHIEVING INTEROPERABILITY BETWEEN THE PROJECT'S STAKEHOLDERS AND ENERGY PROVIDERS

The following section describes the methodology that has been used to derive the high-level architectures introduced in this deliverable, based on the aforementioned design principles and requirements.

3.5 METHODOLOGY AND APPROACH

3.5.1 METHODOLOGY FOR DERIVING THE SMART ENERGY REFERENCE ARCHITECTURE (SERA)

This section describes the methodology that was used for deriving the Smart Energy Reference Architecture (SERA. It consists of 5 steps, carried out iteratively, in line with T2.2 activities:

- **Step 1:** Use case collection and analysis;
- **Step 2:** Definition of time sequence flows and information exchange between components;
- **Step 3:** Generalization of architectural components;
- **Step 4:** Validation of results with WP1 use case analysis;
- **Step 5:** Creation of a structure by application of the separation of concerns and layering principles.

3.5.1.1 STEP 1: USE CASE COLLECTION AND ANALYSIS

This first step includes the compilation of the 'Lisbon Use Cases' (WP1) focusing on smart grids[15]. These use cases served as verbal, human-readable descriptions of what was expected of the InterConnect framework/platform, from the different project stakeholders. From this initial analysis, it emerged that the project's architecture needed to contain enough components and inter-component links, supporting the full array of pilot-specific use cases.

During the early stages of this process, only a subset of available use cases allowed for more in-depth analysis. In total, ten use cases from all seven pilots were covered, with the emphasis put on determining which architectural elements exchange what kind of information in what

[15] Please note that Use Cases and related methodologies are also used by the SGCG (CEN-CENELEC-ETSI Smart Grid Coordination Group). For details on their use case methodology see their documentation (e.g., CEN-CENELEC-ETSI Smart Grid Coordination Group – Sustainable Processes, November 2012: Chapter 6 Use case methodology in standardization). Furthermore, BRIDGE, a European Commission initiative which unites H2020 Smart Grid, Energy Storage, Islands, and Digitisation Projects, also makes extensive use of use cases (see also https://www.h2020-bridge.eu/).

chronological order. The rest of the use cases were covered during the second half of the year when more detailed descriptions became available for analysis. The resulting analysis is explained in the remaining subsections.

3.5.1.2 STEP 2: CREATE TIME SEQUENCES OF INFORMATION EXCHANGE

Collecting WP1 use cases allowed us to identify a set of actors, their actions and time sequences. The IEC standard IEC 62559-2 served as a starting point for defining the structure of a standardised use case template[16], facilitating the creation of 'time sequences'.

One of the first usage areas to be analysed was the energy system/smart grid. However, this methodology can be used in other areas, such as the smart home or electric-mobility domains. Figure 4 depicts an example of the description of a step in a sequence diagram.

3.1 Steps – Normal Sequence

Scenario Name:						
Step No.	Event	Description of Process/Activity	Information Producer	Information Receiver	Information Exchanged	Technical Requirements ID
1		User sets dishwasher latest ready time	User	Appliance Service	- End time device (user defined)	

FIGURE 4 – SEQUENCE DIAGRAM STEP TABLE FROM IEC 62559

Pilot teams were each asked to fill in a template for their pilot use cases. In some cases, a less structured format of this template was used, allowing all pilots to provide initial input. Early drafts of sequence diagrams, provided by pilot teams, were directly exploited and used as a basis for building and validating the first Smart Energy Reference Architecture. An example of the French pilot is shown in Figure 5, depicting a possible market design interaction scheme.

[16] This template has been widely used in many projects and overarching activities (e.g., M/490, SGCG and BRIDGE). It also fits the needs of the InterConnect project, and as such, is being used in Task 1.4.

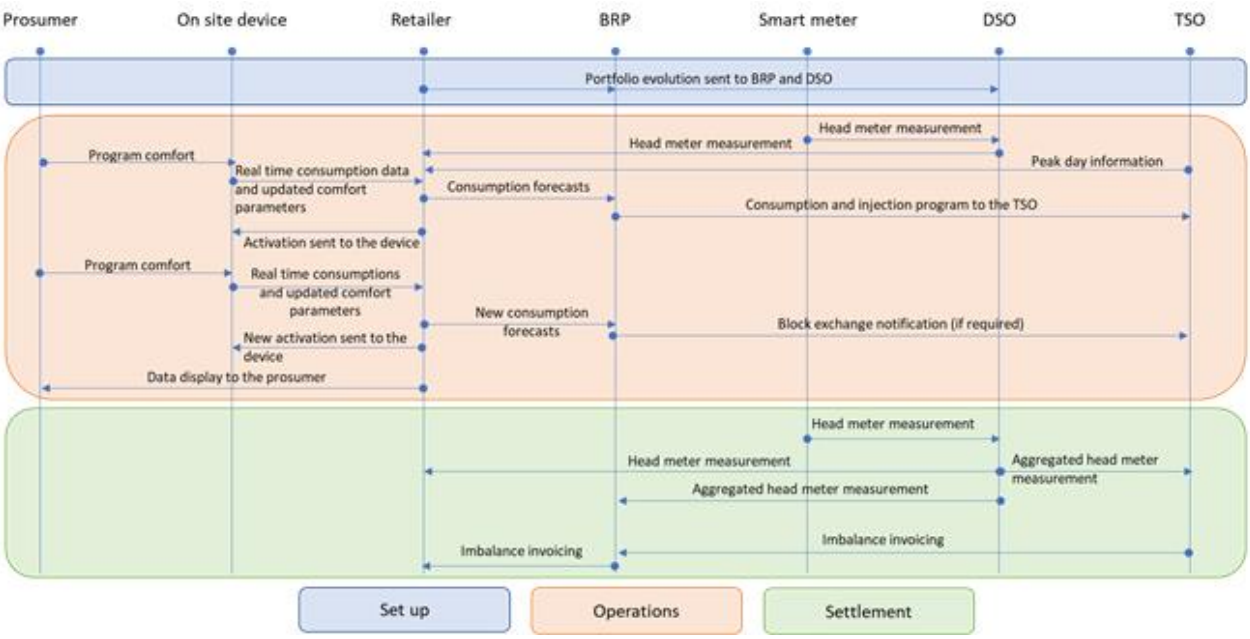


FIGURE 5 – USE CASE SEQUENCE DIAGRAM FROM THE FRENCH PILOT

Another example is from a Portuguese pilot, shown in Figure 6.

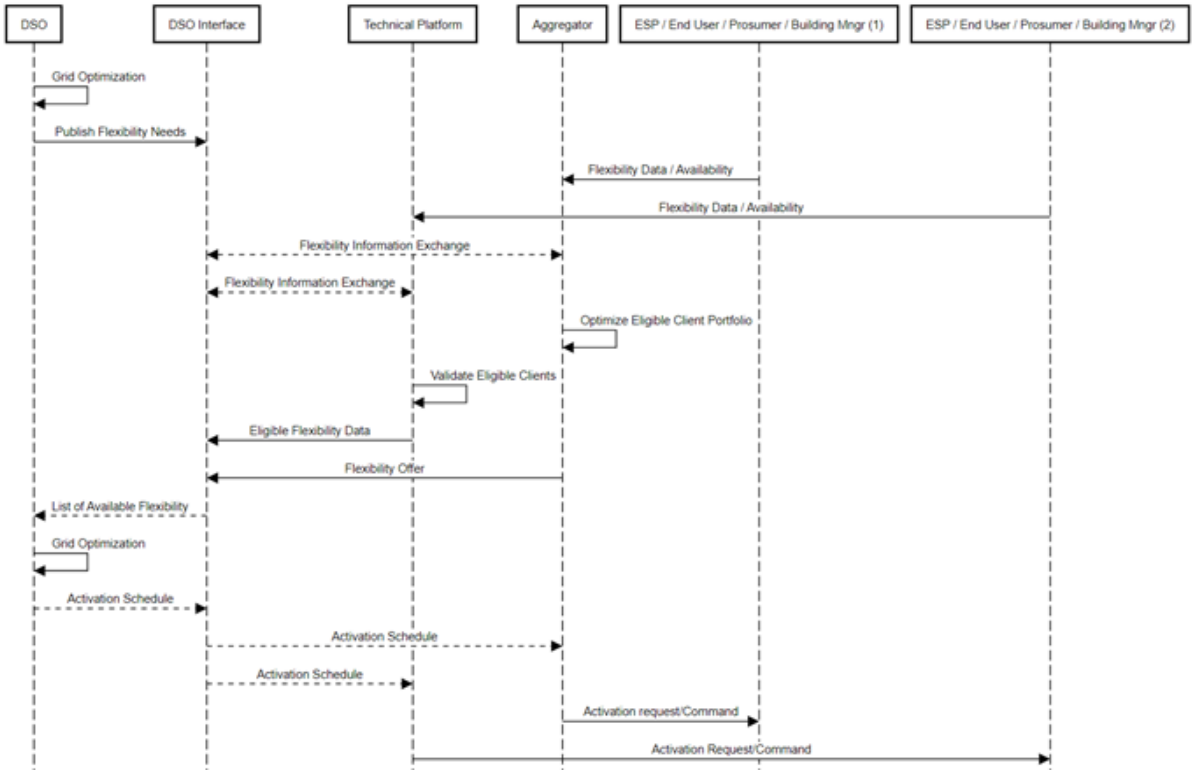


FIGURE 6 – USE CASE SEQUENCE DIAGRAM FROM THE PORTUGUESE PILOT

Use Cases from all seven pilots were analysed, and textual descriptions were modelled into time sequences. An example is shown in Figure 7. The structure of this document, based on the IEC standard, was extended to include the following columns: 'Information via InterConnect', 'Why', 'Information theme type', and 'Subtype'. This document was produced for all use cases, allowing for different views to be discussed and aligned.

Step No.	Description of Process/Activity	Information Producer	Information Receiver	Information Exchanged	Via InterConnect Platform	Why	Information theme type	Subtype
1	Setup	Retailer	BRP	Portfolio evolution	Option	Inter non regulation energy	DSO	DSO flex offer
2	Setup	Retailer	DSO	Portfolio evolution	Likely	DSO	DSO	DSO flex offer
3	Operations	Smart meter	DSO	Head meter measurement	Unlikely	want direct access	DSO	DSO Smart Meter data
4	Operations	DSO	Retailer	Head meter measurement	Likely	DSO	DSO	DSO Smart Meter data
5	Operations	TSO	Retailer	Peak day information (tariff)	Unlikely	TSO etc	TSO	TSO DATA not InterConnect
6	Operations	Prosumer	Device	Program comfort	Very likely	Prosumer	User	User preferences (for device)
7	Operations	Device	Retailer	Real time consumption data a	Yes	Devices	Device	Device flexibility/info
8	Operations	Retailer	BRP	Consumption forecasts	Option	Inter non regulation energy	Forecast	Forecasted power profiles
9	Operations	BRP	TSO	Consumption and injection pr	Very unlikely	TSO etc	TSO	TSO DATA not InterConnect
10	Operations	Retailer	Device	Activation	Yes	Devices	Device	Commands to device
11	Operations	Prosumer	Device	Program comfort	Very likely	Prosumer	User	User preferences (for device)
12	Operations	Device	Retailer	Real time consumption data a	Yes	Devices	Device	Device flexibility/info
13	Operations	Retailer	BRP	New consumption forecasts	Option	Inter non regulation energy	Forecast	Forecasted power profiles
14	Operations	BRP	TSO	Block exchange notification (if	Very unlikely	TSO etc	TSO	TSO DATA not InterConnect
15	Operations	Retailer	Device	Activation	Yes	Devices	Device	Commands to device
16	Operations	Retailer	Prosumer	Data display to consumer	Very likely	Prosumer	User	User feedback
17	Settlement	Smart meter	DSO	Head meter measurement	Unlikely	want direct access	DSO	DSO Smart Meter data
18	Settlement	DSO	Retailer	Head meter measurement	Likely	DSO	DSO	DSO Smart Meter data
19	Settlement	DSO	TSO	Aggregated head meter meas	Unlikely	TSO etc	DSO	DSO Smart Meter data
20	Settlement	DSO	BRP	Aggregated head meter meas	Likely	DSO	DSO	DSO Smart Meter data
21	Settlement	TSO	BRP	Imbalance invoicing	Very unlikely	TSO etc	TSO	TSO DATA not InterConnect
22	Settlement	BRP	Retailer	Imbalance invoicing	Unlikely	TSO etc	TSO	TSO DATA not InterConnect

FIGURE 7 – EXAMPLE TABLE OF USE CASES AND ADDITIONAL FIELDS FOR THE ARCHITECTURE ANALYSIS

From this activity, the following 'Information Themes' were derived: User, Sensor, Forecast, Device, Flexibility, and (Grid) Connection Info. Subtypes for each information there were also identified (i.e., basic information objects). The resulting lists of information producers/receivers, information domains, and information objects will be presented in Section 4.2.4.1.

3.5.1.3 STEP 3: GENERALIZE ARCHITECTURAL COMPONENTS

Step 2 consisted of proceeding to the generalization of the (semantical) concepts commonly introduced by different Use Cases (see for an example Figure 8).

At this stage, it became clear that the SERA should describe relevant components (e.g., devices, platforms, services, and business parties) related to Smart Homes, Buildings and Smart Grids all the while offering a high degree of readability. Thus, overlapping (semantical) concepts were regrouped and mapped from all Use Cases (input from WP1). This work

resulted in a reduced set of components, later partitioned into different types (e.g., device, role), also introduced in Section 4.2.4.1.

Information theme type	Subtype	Information Exchanged
Device	Flex plan to device	Command to do washing
Device	Flex plan to device	Control signals
Device	Flex plan to device	Deploys the updated setpoints
Device	Flex plan to device	Failsafe power limit (production, consumption)
Device	Flex plan to device	Flexibility plan to charging station
Device	Flex plan to device	Load shifting request to appliance
Device	Flex plan to device	Local Flexibility plan
Device	Flex plan to device	Operational restrictions
Device	Flex plan to device	Setpoint (power limit/max device)

FIGURE 8 – EXAMPLE OF THE SAME DEVICE INFORMATION SUBTYPE AND THE DIFFERENT DESCRIPTIONS IN THE VARIOUS USE CASES

3.5.1.4 STEP 4: VALIDATE RESULTS WITH WP1 USE CASE ANALYSIS

Step 4 consisted of comparing the results obtained in Step 3 to the Use Cases produced in WP1. This initial analysis confirmed that all key actors introduced by WP1 were also covered in the actors' list inferred during Step 3 (e.g., Prosumer, DSO, Aggregator, ESCO, TSO and other energy actors like Supplier).

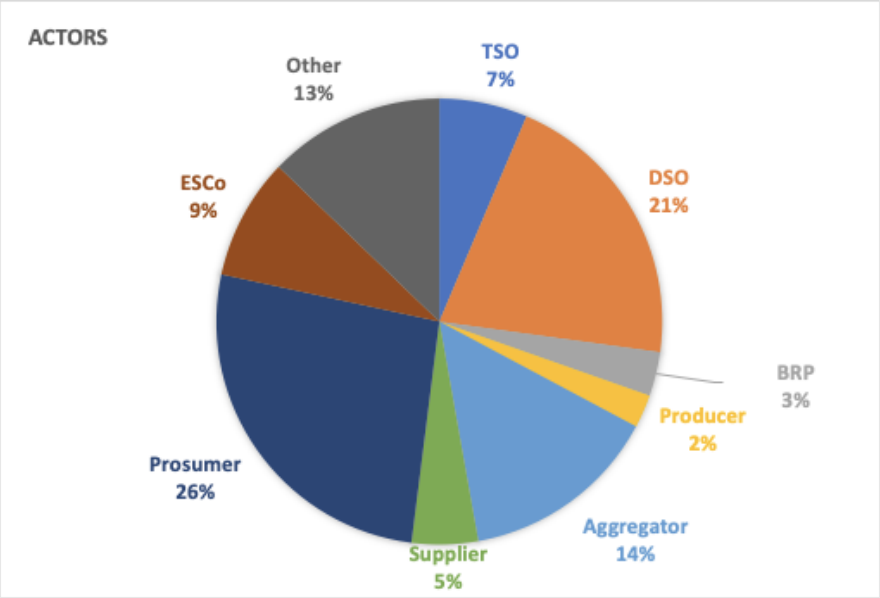


FIGURE 9 – ACTOR'S REPARTITION (BASED ON WP1'S USE CASES)

3.5.1.5 STEP 5: CREATION OF A STRUCTURE BY APPLICATION OF THE SEPARATION OF CONCERNS AND LAYERING PRINCIPLES

The Smart Energy Reference Architecture (SERA) is the result of the efforts carried out during the previous steps and the principles enumerated in Section 3.2. The overall goal for the SERA was to create a structure that showcased the different architectural components and their interactions, as required by WP1 use cases and stakeholders concerns. Three main steps were followed in deriving the SERA:

- **Step 1:** Classification of derived architectural components into domains (User, Smart Home/Building, Smart Grid, Control Service and Energy Service). Components inside a domain are expected to have common characteristics (e.g., physical location, interests), overlapping (semantic) concepts, and require the same type of information. Different domains interact via their specific components, influencing their behaviour (e.g., electrical grids are influenced by the aggregated behaviour in power usage of consumers in Smart Homes and Smart Buildings);
- **Step 2:** Identification of critical interfaces between components and the InterConnect Framework, both logically and technically;
- **Step 3:** Layering of the resulting visualisation, in addition to the initial grouping of components into domains. Devices are considered to communicate with the 'south-bound' interfaces of the platform, whereas service providers communicate with the 'north-bound' interfaces. In this way, the platform shields services from the specifics from devices and vice versa.

3.5.2 METHODOLOGY FOR DERIVING THE SMART HOME AND SMART BUILDING IOT REFERENCE ARCHITECTURE (SHBIRA)

This section describes the methodology and steps followed for deriving the Smart Home and Smart Building IoT Reference Architecture (SBHIRA), consisting of the five following steps:

- **Step 1:** Gather information from project stakeholders and analyse existing use cases;
- **Step 2:** Compilation and overview of existing IoT architectures;
- **Step 3:** Layering and identification of key architectural functions;
- **Step 4:** Identification of information flows;
- **Step 5:** Deriving the Smart Home and Building IoT Reference Architecture.

The methodology introduced henceforth can be associated to the SGAM layered-approach (see Section 2.3.1) for identifying and deriving key zones and domains. In this sense:

- **Steps 1 and 2** are linked to the Business Layer, where the information collected from the project stakeholders is used to guide and infer required system functionalities.
- **Step 3** is strongly linked to the Function Layer in the SGAM model, which describes the set of functions, services and their relationships from an architectural standpoint. These functions are represented independent from actors and physical implementations in applications, systems, and components and are derived by extracting the use case required functionalities (from Step 1).
- The goal of **Step 4** was to allow us to identify the nature of the information exchanges between the different architectural components, functions and services. This approach is aligned with the overall objective and representation of the Information Layer in the SGAM model.
- Finally, the goal of **Step 5** was to provide an initial description of the existing (or needed) protocols and mechanisms for exchanging information in an interoperable manner (Communication Layer). Moreover, this step focused on providing an early mapping of the physical distribution of all participating components (Component Layer), including the key services, actors and applications that need to be made interoperable within the large-scale pilot demonstrators.

The following subsections describe in more detail each of the steps mentioned above.

3.5.2.1 STEP 1: GATHERING INFORMATION AND ANALYSIS OF USE CASES

The goal of this step was to compile relevant IoT reference architectures from a wide array of sources, e.g., standardisation organisations, other European projects, other sectors/domains, a stakeholder's company system architecture, amongst others. More specifically, we aimed to provide an initial outline of what was required by the IC system, which entailed a rough breakdown of the processes, actors, and data involved. This first output was collected via two separate actions:

- The **"InterConnect H2020 Project WP2 Architecture" template,** which was sent to key WP2 and T2.1 partners during the first month of the project (October 2019) to collect early insight on existing architectures and methodologies that could be used to build a unified reference architecture within multiple domains, as in the case of the IoT Smart Home, Smart Building and Smart Grids Reference Architectures. Additionally, partners

were asked to provide suggestions for overcoming the most likely issues that could arise, when trying to provide a unified, interoperable Reference Architecture[17].

- The **analysis of WP1's Use Cases**. WP1 - Use Cases, Business Models and Services carried out extensive work to define new and innovative energy and non-energy services. Use cases were developed using the design thinking methodology, which promotes a user-centric approach. In most cases, the functions described in these Use Cases provided the entire information exchange required to implement the considered use cases and user stories, i.e., in our context architectural and functional layers.

As a result of this approach, it proved hard to set a strict line in what regarded the Energy domain and the Smart Home/Smart Building domain (e.g., most use cases introduced cross-domain actors and roles, with no particular segmentation[18]). Which is why the analysis of use cases introduced in 3.5.1.1, and further developed in 4.2.4.1 holds valid for the IoT Reference Architecture.

3.5.2.2 STEP 2: COMPILATION AND OVERVIEW OF EXISTING IOT AND ENERGY-RELATED ARCHITECTURES

This step consisted of an in-depth analysis of existing relevant initiatives, mostly resulting in Section 2 - State of the art and the analysis on the links and gaps with other architectures developed in that Section.

As required by **R1.1**, the IC Reference Architecture needed to be based on existing reference architectures in the smart grid and IoT domains. This analysis helped fill this requirement by structuring early discussions of the SHBIRA.

The goal was not to create an architecture "from scratch", but rather build on the work already carried out by other initiatives by providing additional capabilities and sponsoring evolutions within the SAREF family specification, allowing for the introduction of new vertical domains (e.g., Energy) and their requirements (e.g., flexibility services).

[17] This deliverable introduces some of the issues and concerns raised by partners at this stage in Section 3.4, as derived requirements from **R1**.

[18] One example is UC18 - Smart EV charging @ private parks with public access, which covered EV charging platforms for tertiary buildings integrated to the Building's Energy Management System (BEMS) and offering some strategies to minimize charging costs, via flexible tariffs.

3.5.2.3 STEP 3: LAYERING AND IDENTIFICATION OF KEY ARCHITECTURAL FUNCTIONS

The SHBIRA aims to describe all relevant components (devices, platforms) and functions relating to Smart Homes and Smart Buildings. As mentioned above, these components were inferred from WP1's High-Level Use Cases, and later linked to standard system architectures found in the IoT domain. Below, a non-exhaustive list of identified functions during this stage:

- **Data access provision:** Expose APIs using standard communication protocols (e.g., RESTful, MQTT, SPINE, web sockets). Data exposed can be consumed by any platform (including local-based clients) or made available for third-party services;
- **Publish/Subscribe patterns:** Communication pattern where message senders (i.e., publishers) do not program the messages to be sent directly to specific receivers (i.e., subscribers) but rather categorize published messages into classes without knowledge of which subscribers there may be. Similarly, subscribers express interest in one or more classes and only receive messages that are of interest, without knowledge of which publishers, if any, there are;
- **Discovery:** Can be defined as a system's capability to automatically and dynamically discover new services, devices, applications, by offering some level of context-awareness;
- **Command and control:** Allows extending data collections from 'simple' sensors and alarms to fully integrate IoT equipment access and remote control (e.g., HVAC systems);
- **Data transformation/Unified data modelling:** Can be defined as the conversion of data into a unified format, exposed by sensors or IoT actuators. A common ontology (e.g., SAREF) is expected to be implemented at this stage;
- **Monitoring and performance:** Centralise data from heterogeneous systems to offer new services to occupants, improve monitoring of building equipment and provide managers with relevant information that facilitates decision-making.

Once these functions were defined, we organized them into a layered view containing all key architectural components, which can be detailed as follows:

- The **Device Layer**, consisting of all of the controllable devices and (home) appliances that exist in the Home and Building domains;
- The **Gateway Layer** consists of a set of nodes (i.e., routers) that send data back and forth between the Device Layer and the Interoperability Layer;

- The **Semantic Interoperability Layer**, which offers the set of enablers and functions needed to fulfil the general requirements for Building, Home and Energy interworking;
- The **Applications Layer**, which communicates with the Building/Home Interoperability Layer's services to retrieve/send data for the execution of a specific task or use case.

These layers are discussed in more detail in Section 4.3.1.

3.5.2.4 STEP 4: IDENTIFICATION OF INFORMATION FLOWS

Relationships between defined components needed then defined to model the task of the system. Once the relationships between classes were understood, the next step was to detail the behaviour the classes will exhibit and how they will interact in order to complete the system. This entails determining how entities communicate and send messages within the system. This information was derived from the roles of the entities previously identified.

Within this step, three separate actions were carried out:

1. **Model standard communication behaviour between the system layers and components**: These message flow examples are introduced in Section 4.3.2.1. The goal was to provide a generic description of the communication behaviour that typically occurs via message interchange between the different architectural components of the High-Level Architecture.
2. **Derive required interfaces**: In total, fourteen interfaces were introduced to describe the set of interactions that may occur between the system components. Each one of these interfaces represents a shared boundary that two or more separate components use to exchange upstream, downstream, and contextual information. These interfaces are discussed in detail in Section 4.3.2.
3. **Categorise interfaces using three distinct typologies:** The "Unified/Interworking/ Specific" typology allows us to categorise interfaces over which interfaces will consist of a unified interface (e.g., SPARQL+/SAREF), interworking proxies (i.e., smart connectors) or vendor-specific interfaces, outside of the scope of the InterConnect project. The "MUST/SHOULD/MAY" offers a view of the interfaces that must, should or may be provided during the architecture's instantiation within large-scale demonstrators. Lastly, the "Interacting Entities" typology offers a view that allows us to categorise interfaces that provide similar functioning. The interfaces typologies are detailed in Section 4.3.2.2.

3.5.2.5 STEP 5: DERIVING THE SMART HOME AND BUILDING IOT REFERENCE ARCHITECTURE

The Smart Home and Smart Building IoT Reference Architecture frames the concerns identified during the previous stages (e.g., functional decomposition of the system into objects, interfaces, amongst others). Based on the layers, functions and components already described, an initial draft was introduced and validated amongst WP2 partners during the first quarter of 2020.

A simplified view of the SHBIRA was also introduced at this stage, including all system layers previously mentioned (i.e., Device, Gateway, Semantic Interoperability and Application Layers) and depicting all key interfaces between the system layers. The resulting reference architecture is detailed in Section 4.3.

Activities carried out during this step included further discussions with other WPs (namely WP1, WP3, WP5 and WP7) to synchronize and validate the resulting viewpoint across WPs and stakeholders. One of such activities was organized in the form of three “Architecture Workshops”, organized in November 2020. This joint action with WP5’s leader helped validate all viewpoints introduced in this document (the SHBIRA, produced by T2.1, the SERA, produced by T2.2, and the IC Interoperability Framework, produced in T5.1), and consolidate them into IC’s Secure interoperable IoT smart home/building and smart energy system reference architecture (SHBERA). The output of this work is presented in Section 0 - Functional Architecture Implementation in Pilots.

The next section introduces the project’s High-Level Architecture (SHBERA) and details its composing viewpoints, namely the SERA and the SHBIRA, before discussing security-related guidelines and how they could embed into the resulting architecture.

4 INTERCONNECT'S SECURE INTEROPERABLE IOT SMART HOME/BUILDING AND SMART ENERGY SYSTEM REFERENCE ARCHITECTURE

This chapter contains the description of InterConnect's **Secure interoperable IoT smart Home/Building and smart Energy system Reference Architecture (SHBERA)**, as derived from the requirements and methodology described in Section 3.

The SHBERA is the overall architecture view describing the different domains and layers introduced by the **Smart Energy Reference Architecture (SERA)** and **Smart Home/Building IoT Reference Architecture (SHBIRA)**. The **SERA** focuses on the energy system point of view and introduces the project's actors, roles and devices in the energy system as well as the information exchanges that occur amongst the latter. The **SHBIRA** takes on the functional/service layering perspective and focusses on the interoperability and communication of services with each other and with devices, cloud and local management systems.

Zooming in further brings us to the InterConnect **Interoperability Framework Architecture (IFA)**, previously introduced in deliverable D5.1 Concept, design and architecture of the interoperable marketplace toolbox [43]. This architecture view focusses on 'platform services' like service store for all interoperable services, P2P marketplace enablers, access control mechanisms, generic interoperability adapters, enabling communication, and others.

Zooming in once more brings us to the **Semantic Interoperability Layer (SIL)**. This is a logical concept within the IC Framework that enables semantic interoperability. The Semantic Interoperability Layer comprises ontologies, interoperability adapters and smart connectors with supporting orchestration enablers.

These viewpoints are further detailed in this section and in Section 5 - Semantically Interoperable Information Architecture.

4.1 THE SECURE INTEROPERABLE IOT SMART HOME/BUILDING AND SMART ENERGY REFERENCE ARCHITECTURE (SHBERA)

The goal of the SHBERA is to provide a unified architecture viewpoint capable of describing how different components relate to each other in an easy, affordable and trustworthy manner, allowing for the interconnection of services and devices in the Smart Grid, connected Smart Homes and Buildings and vice versa.

The initial, simplified high-level reference architecture introduced in D5.1 [43], is shown in Figure 10. This reference architecture was based on the SHBIRA and included all the system layers and key interfaces introduced by the former, namely:

- The **Device layer**, including all end devices which are consumers, producers or prosumers of electric energy as well as smart metering systems, sensors, actuators and other smart home/building connected devices.
- The **Gateway layer**, including home and building management systems, deployed on-site. This layer encompasses communication technologies and protocol gateways bridging the devices and higher-level applications and services.
- The **Interoperability layer** allows the establishment of semantic interoperability. It is important to note that the semantic interoperability layer is not strictly between the gateway and application layers, but a pervasive network of interoperability adapters and connectors (see section 5.7.2.2) spanning all of these four reference architecture layers.
- The **Application layer**, which includes all interoperable services (energy, non-energy and grid-related) as well as applications built for the realization of the project's use cases. InterConnect interoperability framework services also reside on this layer.

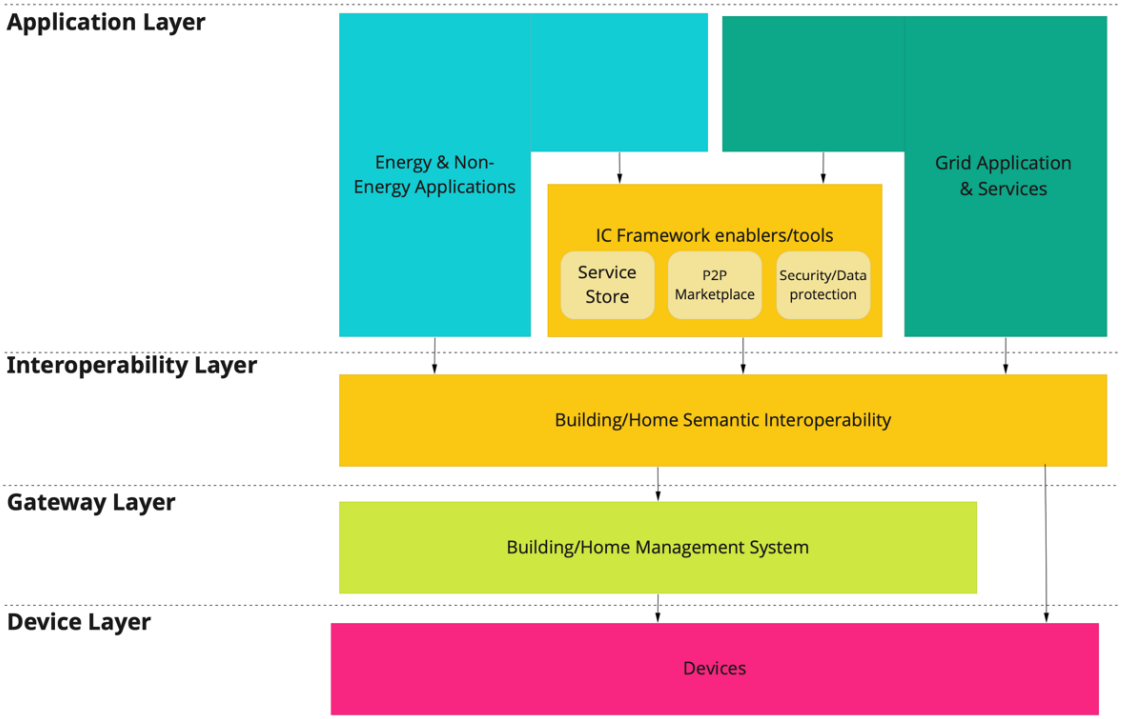


FIGURE 10 – IC'S INITIAL HIGH LEVEL REFERENCE ARCHITECTURE

This initial viewpoint was later improved by including the set of domains put forth by the SERA, namely the Energy System and User domains, and adding the Stakeholder layer.

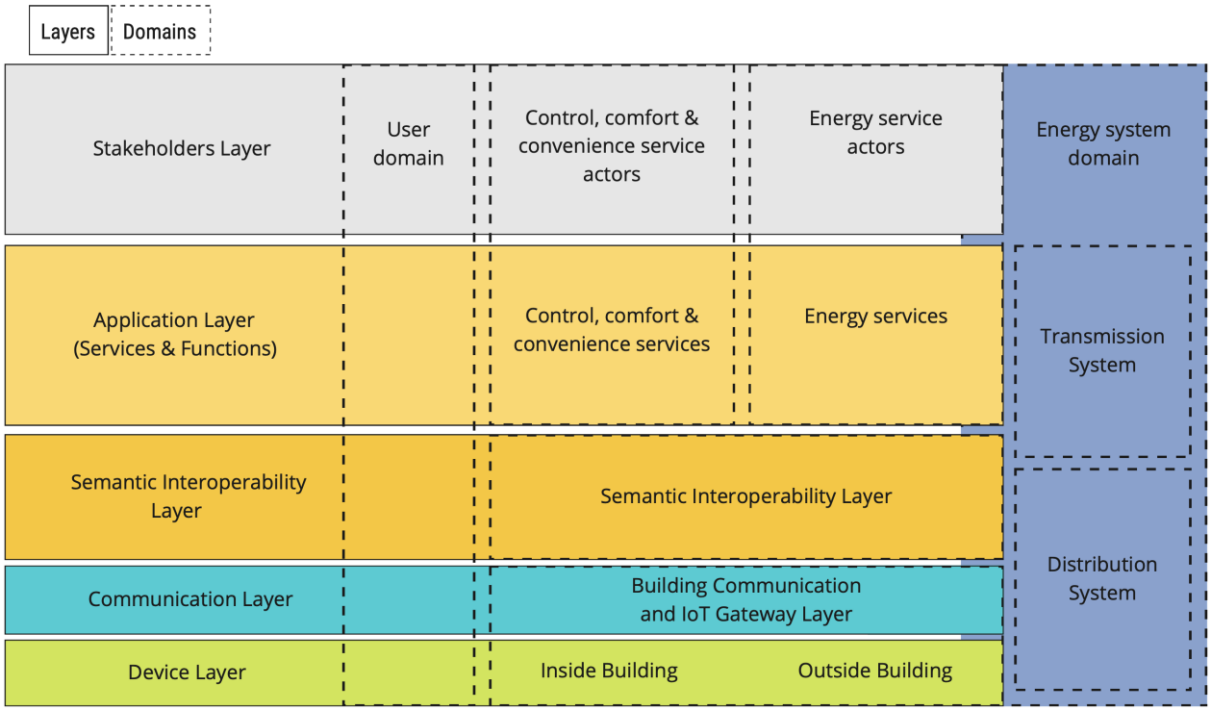


FIGURE 11 – INTERCONNECT'S SMART HOME/BUILDING AND ENERGY REFERENCE ARCHITECTURE (SHBERA)

This new version of the SHBERA has been kept in line with the layered models SGAM (from SG-CG) and RAMI (from AIOTI), and introduces the following modifications:

- The Gateway layer has been renamed **Communication layer**. According to SGAM the emphasis of the communication layer is to describe protocols and mechanisms for the interoperable exchange of information between components in the context of the underlying use case, function or service and related information objects or data models.
- The Interoperability layer has been renamed **Semantic Interoperability layer** to reflect the objective of achieving *semantic* interoperability on top of syntactic interoperability between services and resources on different layers;
- The **Stakeholder layer** was added to include all of the project's stakeholders, end-users, and energy system actors/roles providing or benefiting from the Control, Comfort & Convenience (CCC) and Energy Services.

The (new) SHBERA also introduces the following domains (depicted using dashed lines in Figure 12), further detailed in Section 4.3.1:

- The **User domain**, which expands over multiple layers to depict the set of roles found in the processed use cases. This shows the diversity of roles, but also that these can be architecturally combined;
- The **Control, Comfort and Convenience (CCC) services domain** covers both the key actors providing and benefiting from the control, comfort & convenience services and the non-energy services comprising/enabling the pilot;
- The **Energy services domain**, which covers key actors providing energy services and the services themselves, which comprise/enable pilot use cases;
- The **Semantic Interoperability Layer domain** comprises configured instances of interoperability adapters and smart connectors (see Section 5.7.2) hosted on digital platforms (provided by project partners) and supporting services introduced by the interoperability framework;
- The **Home/Building domain**, which groups the hardware and software components that are deployed within residential or commercial buildings (e.g., appliances, IoT devices, sensors, amongst others);
- The **Energy System domain**, which includes key actors from energy system domain and resources and services from the TSO/DSO domain.

Figure 12 shows how the Smart Home/Building and Energy Reference Architecture (SHBERA) is composed of multiple zoomed-in viewpoints, namely:

- The Smart Energy Reference Architecture (SERA);
- The Smart Home/Building IoT Reference Architecture (SHBIRA);
- The Interoperability Framework Architecture (IFA), introduced in D5.1 [43];
- The Semantic Interoperability Layer (SIL).

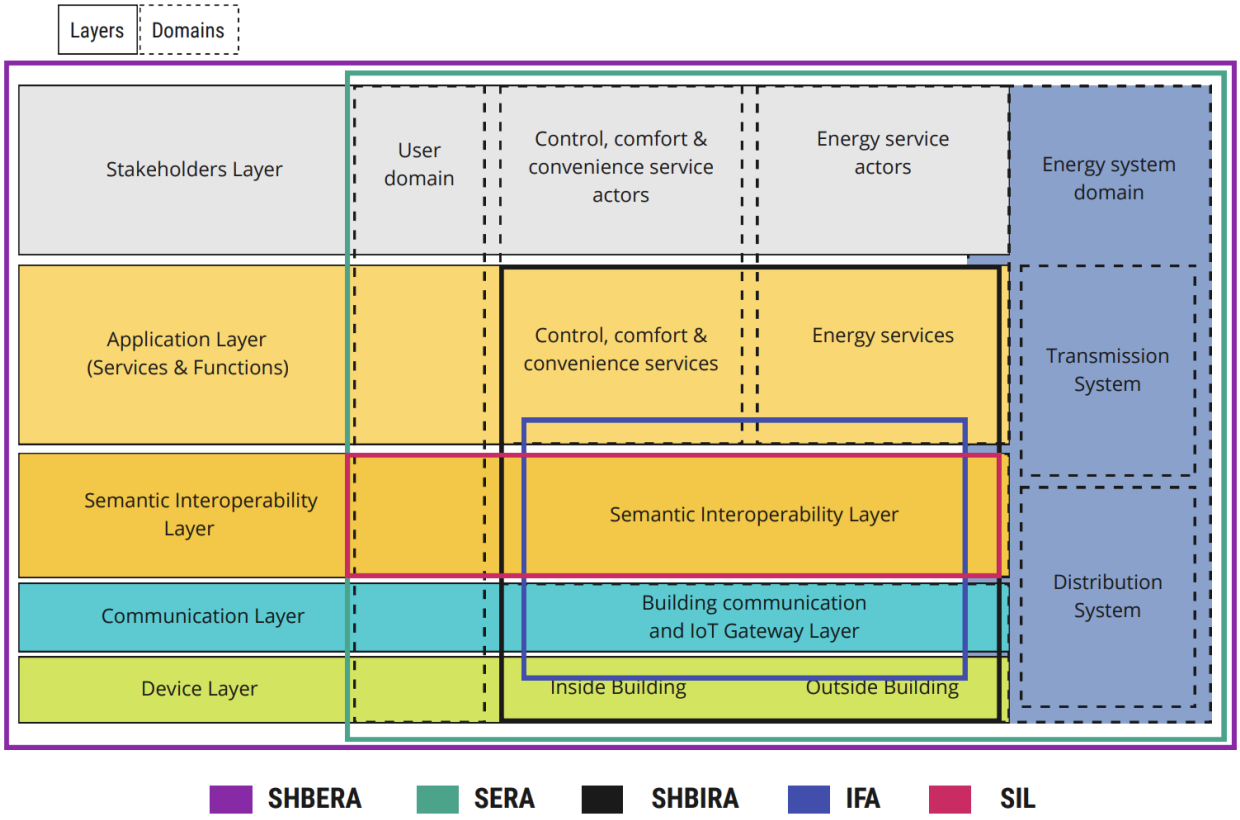


FIGURE 12 – THE SHBERA AND THE DIFFERENT ARCHITECTURAL VIEWPOINTS

The following sections introduce the first three architectural viewpoints (SERA, SHBIRA and the IFA), while the Semantic Interoperability Layer is detailed in Section 5.

4.2 INTERCONNECT'S GLOBAL SMART ENERGY REFERENCE ARCHITECTURE (SERA)

The Smart Energy Reference Architecture builds on previous architectures as these have become commonplace in different domains of expertise, like smart grids, e-mobility, and energy flexibility markets (with aggregators). Below, a stepwise description of the main focal points of the SERA:

- **Physical topology and geographical scale of a system of systems**, describing existing physical entities, identifiable services and their interworking through grids and communication networks;
- **Assets and devices**, which introduces energy-related assets used in Smart Homes and Smart Buildings;
- **Energy flexibility** describes the concept of being flexible in the production and consumption of electricity and also flexible in power capacity;
- **Intercomponent exchange of information**, characterises the kind of architectural components that can be identified from WP1's Use Cases and their relationship to the InterConnect Framework.

The following subsections address these four topics in more detail.

4.2.1 PHYSICAL TOPOLOGY AND GEOGRAPHICAL SCALE OF A SYSTEM OF SYSTEMS

Services, like energy forecasting, flexibility aggregation and communication services (e.g., create any bus so others can subscribe), will be used in the SERA[19]. However, to understand what is needed from system architectures in interconnecting devices and services across smart home, buildings and grids, we need to understand it is necessary to get an idea of the physical reality that is involved.

This section describes a topology of that physical reality, including a 'sense of geographical scale' from a smart energy point of view. The geographical scale is important since physical local grid limitations can only be solved on the same local scale by connected buildings and devices. Based on this representation, it is possible to get an impression of the actual scale of this system (e.g., 'grids') of systems (e.g., 'homes in buildings').

Figure 26 depicts the topology, how the different components (from electricity grid to energy services) of a smart energy system are interrelated from a physical point of view, with a focus on the networks between and in homes and buildings. The electrical low, medium and high voltage grids are less detailed (e.g., 'no transformer stations') since the emphasis is on the

[19] Energy-related service possibilities and needs will be described here while service details and services in general will be described in WP3 and its related documentation.

interconnections of smart homes, buildings and grids - not on the interconnection of grid components.

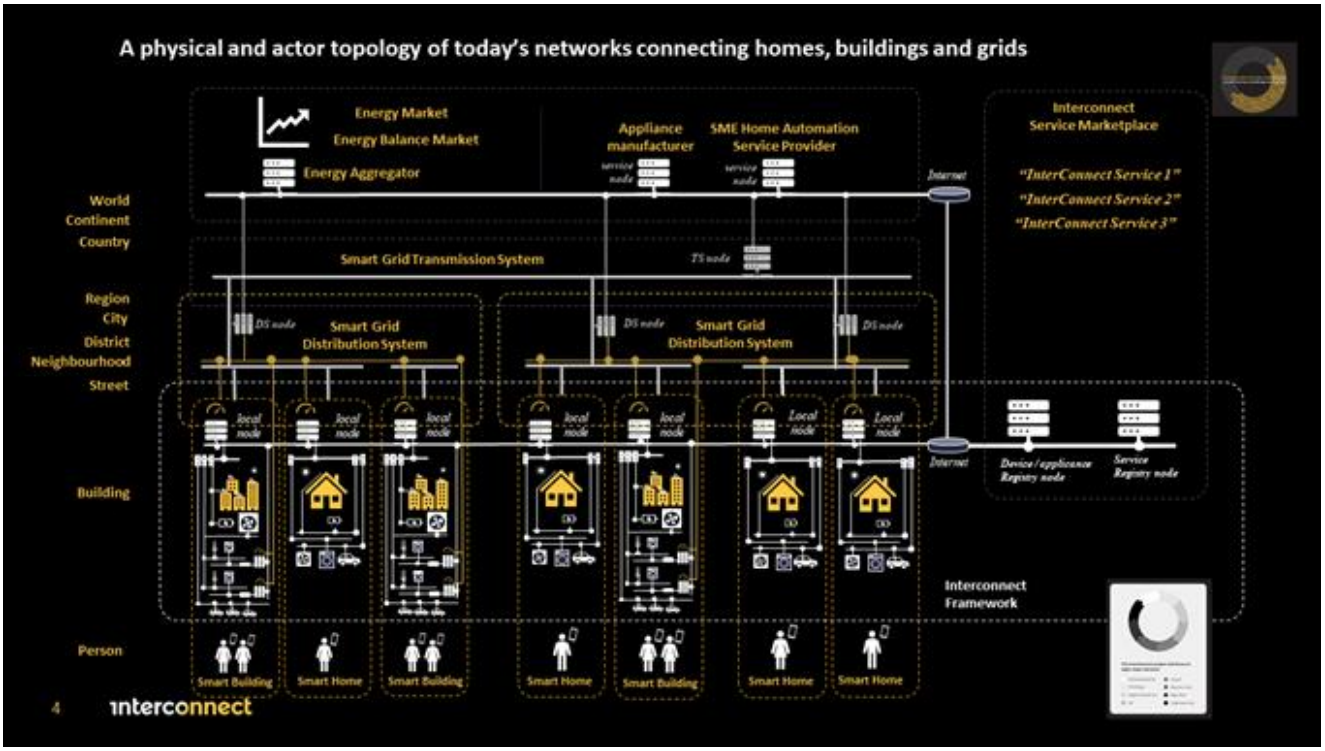


FIGURE 13 – PHYSICAL AND ACTOR TOPOLOGY OF TODAY'S NETWORKS CONNECTING HOMES, BUILDINGS AND GRIDS

The concept of **geographical** scale is visualized from below to top. The higher a component is drawn, the larger the geographical scale at which it is present or at which it operates. It starts at the level of a person (which can be mobile), having a mobile device (e.g., 'smartphone ') with apps that the person can use for interacting with physical and technical systems.

From the level of a person, it goes upwards to the building level. There are **Smart Buildings,** counting multiple **Smart Homes** (e.g., apartments), or single Smart Homes. Each one of the homes can leverage on multiple communication **networks** (e.g., Wi-Fi, wired Ethernet, Zigbee.) that connect to different **devices/appliances** (e.g., cars, heating, washing machines) with communication hubs (e.g., H1, H2). There are also electricity or heat-generating devices present, like Photo Voltaic (PV) panels or heat pumps. Energy can be stored in (home)

batteries. Currently, it is already possible to connect multiple devices to these communications networks[20].

The following are examples of sensors that can send information to the bus:
Light switches
Dimmer switches
Motion sensors
Presence detectors (which can detect whether there is a person in a room even if they are not moving)
Window and door contacts (for security and heating control)
Doorbell buttons for front doors
Water, gas, electricity and heat meters
Overvoltage sensors
Temperature sensors for indoor and outdoor air
Temperature sensors in heating and hot water circuits
Modules for preselecting room temperature setpoints
Brightness sensors for indoors and outdoors, e.g. for constant lighting control
Wind sensors for controlling blinds
Fault and system status messages for white goods (washing machine, clothes dryer, dishwasher, cooker, etc.)
Leak sensors, e. g. in laundry room
Level measurements e. g. for rain water tank, oil tank, wood pellet store
Radio receivers for door locks
Receivers for infrared remote controls
Fingerprint modules and card readers for access control

The following are examples of actuators that can be controlled via the bus:
Relays for switching room lights on and off
Dimmers and DALI-gateways
Electric thermostatic radiator valves
Temperature displays
Drive mechanisms for awnings, blinds, curtains and garage doors
Drive mechanisms for windows
Circulator pumps for heating systems
Valve control systems, e.g. for solar thermal installations
Alarms (lights and buzzers)
Information displays and indicator LEDs
Relays for making and breaking socket outlet circuits (standby cut-off)
Well pumps
Air conditioning systems
Ventilation systems (toilet/bathroom extractor fans, controlled ventilation for living areas)
Control of washing machine, dryer, dishwasher
Consumer electronics
Trigger signals for alarm systems
Telephone systems
Electric door openers and door locking systems

Examples of functional modules (may be self-contained or integrated in devices):
Room temperature controllers
Timer functions
Freely-programmable logic modules
PLCs with KNX interface
Constant lighting control modules
Alarming and alerting
Telephone switchboards connected to the bus
Media control
Heating control
Pump control
Presence simulation
Displays and user interfaces
Modules for connecting bus with telephone
Modules for automatically sending warning messages by text
Modules for accessing building data from outside via the internet or a phone

The KNX Standard – the basics | 3

FIGURE 14 – KNX SENSORS, DEVICES AND SYSTEM LIST

Each home can contain one or more network-connected devices that have (local) storage/computational capabilities for information processing. These devices are called a 'local node' and are visualized as three 'bars' with a gauge on top. The gauge represents a

[20] An example can be found in a basic description of the KNX standard (ISO/IEC14543, CENELEC EN50090, CEN13321) where the communication network is called 'the bus'. For more information, see: https://www.knx.org/wAssets/docs/downloads/Marketing/Flyers/KNX-Basics/KNX-Basics_en.pdf

Smart Meter for the electrical grid connection. Each Smart Home has one node; Smart Buildings have smaller nodes in each apartment. Local nodes can also act as a gateway to the Internet, allowing devices found in homes to connect to the Internet[21].

From the Smart Home and Smart Building level, the geographical scale increases upward. The homes and buildings are connected to the electrical grid at the level of a **Street**. There are metering devices that meter the flow of electricity from the grid to a building and vice versa. It is also possible to have multiple meters inside buildings for apartments. The meters are connected to an independent communication infrastructure from the Distributed System Operator (DSO) that might be outsourced to a telecommunications network operator. The DSO often operates at the geographical Street, Neighbourhood, District, City and Region level[22]. A Transmission System Operator (TSO) operates at the **Country** level, and multiple **TSOs** work together at the **(European) Continent** and **World** level.

The description of the physical reality, in terms of a topology of associated components at different geographical scales, shows how complex the entire system of assets and devices is. Many technical, organizational and geographical relationships between system components can be identified.

The next section describes these components and relationships from a logical (and thus) higher abstraction level - the energy system perspective.

4.2.2 ASSETS AND DEVICES

Usage and behaviour of different assets and devices in Smart Homes and Buildings have a different impact on the Smart (electrical) Grid. Categorizing them helps gain a better understanding of the kind of information they require, and for which interoperability points/layers and type of devices. This section describes these categories on a high level and provides examples.

There are four categories of assets and devices, that can be wrapped around two axes:

[21] Note that for reasons of simplification a separate Internet gateway has not been drawn, but it could be a separate device from the 'local node'. It is an Internet connection that makes it potentially possible to offer services to end-users worldwide.

[22] Note that in some areas certain DSOs also might operate at the country level. This, however, does not alter the geographical scale of the project as a whole, which is at least at a continental level.

1. **Electricity consumption and production-related (major/minor impact).** These are assets and devices that *consume* and/or *produce* electricity or *control* the flow of energy. Some of the assets and devices have a major impact on the grid (e.g., larger batteries, EVs and PV panels), others have a minor or no impact (e.g., Smart Locks). The difference between major and minor is important from an 'energy flexibility service' point of view. Devices and assets in the 'major impact' category are interesting for flexibility in the production and consumption of electricity in order to keep balance.
2. **Sensors (energy /non-energy related).** These are devices that provide data/information about aspects of Smart Homes and Smart Buildings. Some of these devices are related to the flow/usage of electricity, while others are not like CO_2 and movement sensors. However, these non-energy sensors are interesting from a grid perspective, since they help to reveal the amount of energy flexibility.

These two categories and their two subcategories result in four categories, which have been used to categorize the assets and devices put forth by the Use Cases from InterConnect. The results are in the table below that contains several types of devices per category, e.g., 'the *HVAC* type of device for the category of *major electricity consumption and production-related devices*', with examples like heat pumps, ventilation, and others.

Asset, device, and sensor groups	Examples
Major electricity consumption and production related (devices, components, assets, things are expected to be used in the energy domain)	
HVAC (Heating Ventilation Air Conditioning)	• Heat pumps, electrical heater, hot water heating, domestic hot water (including solar) • Ventilation, fan coil • Air-conditioning, split unit, chilled ceiling control • Dehumidifier
Domestic Appliances	• Dish Washer, Washing Machine, Dryer
PV and its inverter	
EV and the related EVSE	• EV (Electric Vehicle) • Charging Points (EVSE EV Supply Equipment)
Energy storage	• Batteries
Office Equipment	

Smart Plugs *(major, but also minor)*	
BEMS	
Minor electricity consumption and production related	
Lighting	• Switching/dimming/colour control
Sun shading	
Audio/Video Control	
Smart locks	
User Smart Phone	• User In Home Display & Control
Scheduling	• Including user agenda, user scenarios
Gateway	
Energy sensors	
Smart Meter	• Heat meter, heat cost allocator, water meter, gas meter • Electricity meter, with information like voltages, phase loading
Non-energy sensors (but often used for energy control and flexibility)	
Climate and comfort sensors	• Room/floor/outdoor temperature • Supply, return air, CO_2 • Flow and return water • Wind speed • Sun intensity, brightness, luminance • Air quality, humidity sensor
Activity sensors	• Movement, presence sensor • Body sensors
Security, alarming	• Fire-Smoke Detection • Intrusion Detection, Window contacts • Alarm sensors • Flood sensors

TABLE 11 – ASSET, DEVICE AND SENSOR LIST DERIVED FROM INTERCONNECT USE CASES

The description of assets and devices in Smart Homes and Buildings at a relatively high abstraction layer, from an electrical energy point of view, allows us to introduce the concept of

flexibility in electricity production and consumption. Readers that already are acquainted with the concept of energy flexibility can skip the following section and move on to Section 4.2.4.

4.2.3 ENERGY FLEXIBILITY

The ability to control assets and devices in Smart Homes and Smart Buildings enables **energy flexibility.** Energy flexibility is the ability of a user, grid connection point or device to be flexible and vary the production and consumption of energy or electricity (e.g., shifting in time, changing power, modulating energy bandwidth).

This section first describes why the concept of being flexible in production and consumption of electricity is essential for the SERA. It then describes energy flexibility in more detail, using technical notions that already have been employed in the field (e.g., trading in flexibility in electricity production and consumption). Although the notions are tested on flexibility in electricity consumption, they are likely applicable to other energy vectors. This description of energy flexibility will enable the reader to (later on) understand the importance of certain energy services, parties/roles in the energy system and their responsibilities as described in the next sections.

Energy flexibility and related protocols are extensively described here since it is a crucial part for almost all energy services and since this part will be used in T2.5 as starting point to create higher abstraction levels and/or ontologies (e.g., in SAREF4ENER) for energy flexibility. A sound basis for that is the basic energy flexibility patterns described in Section 4.2.3.2 since coverage of these can be seen as requirements for any energy flexibility abstraction.

4.2.3.1 IMPORTANCE OF FLEXIBILITY FOR THE SERA

Being flexible, in electricity production and consumption, can significantly influence the flow of electricity on the grid (e.g., power, actual voltage, voltage quality). It has the potential of enabling the energy system to better deal with the arrival and growth of less and/or non-controllable electricity production (e.g., PV panels, windmills). These sources of electricity can sometimes have highly irregular, volatile and/or variable productions patterns, making it difficult to achieve the (technically) necessary balance between production and consumption. The need for balance has gotten so big (quantitively speaking), that 'energy flexibility' has

gotten enough significance in terms of economic value for trading/valorisation. This is also shown by the fact that several countries already experience negative energy prices.

Another important application for energy flexibility can be found in the distribution grid, where a growing number of EV's, PV's and heat pumps increasingly cause congestion issues for the DSO. Energy flexibility can be a valuable asset to reduce peaks in order to postpone costly investments in the distribution grid or even to prevent blackouts from occurring.

Not surprisingly, in the InterConnect Use Cases, there is often a reference to the concept of 'energy flexibility', which in turn has a strong relationship with the architecture in terms of information that is required to be exchanged between different components and/or roles (like organisations and businesses). Energy flexibility information can be exchanged regarding different aspects:

- **Harvesting** flexibility: detection of available flexibility at certain points in the energy system;
- **Processing** flexibility: evaluation of available flexibility in terms of arranging and optimisation;
- **Trading** flexibility: advertising and valorising flexibility;
- **Exploiting** flexibility: triggering assets/devices to employ flexibility when needed.

Energy flexibility is a core concept with high relevance in InterConnect Use Cases. As such, it needs to be universally understood between all project partners. It requires that all **different aspects** of **energy flexibility** shall be **qualified** and **quantified**, which is the goal of the following sections, beginning with a qualitative description of the most basic flexibility patterns that can be used to describe energy flexibility behaviour of smart devices. In isolation, these flexibility patterns are easy to understand; but in reality, there are often complex interdependencies between them. Various solutions have been proposed to capture these complicated relations, three of which are discussed in Section 4.2.3.3.

4.2.3.2 BASIC ENERGY FLEXIBILITY PATTERNS

As described in the section on assets and devices, many different devices are capable of providing energy flexibility. Although devices differ vastly in their functionality, there is only a limited number of “atomic” flexibility patterns required to describe their energy flexibility

behaviour. Atomic, since with the patterns the flexibility of all devices can be expressed. These basic patterns are listed below [10]:

- **Limit production or consumption.** This pattern describes the behaviour of devices that can be provided with a power limit for production or consumption they will not exceed. This is particularly useful for devices for which the consumption or production cannot be controlled directly. The production of a PV panel, for example, is dependent on the sun's radiation which obviously cannot be controlled externally. This may lead to problems if the production of PV panels exceeds the limits of the local power grid. By curtailing or limiting the production of PV panels to a certain threshold, such problems can be avoided;
- **Shift production or consumption in time.** Some devices follow a more or less predetermined energy/power profile while performing their tasks. Whitegoods such as washing machines often exhibit this pattern, where running a selected (washing) program comes with an associated energy/power profile. If the washing machine has a delayed start option, that profile can be shifted in time, thus offering flexibility. Usually, there is a deadline by which the entire profile must have finished;
- **Pause a task.** Some devices can be interrupted while performing their task. It might be possible that the device can be paused at arbitrary times, but more often, there will be some predetermined points in the energy/power profile where a pause can be inserted. In our previous example, the washing machine may be paused in between the heating and washing cycle. The duration of the pause will typically be limited to a maximum. Just like the previous pattern, there will usually also be a deadline by which the task must have finished;
- **Alternative energy profiles.** This pattern applies when there are multiple alternative ways to perform a certain task. Take a heating cycle for instance; it might be achieved by using less power over a longer period or by using more power over a shorter period. This results in alternative energy/power profiles from which one has to be chosen;
- **Power modulation.** A device that follows this flexibility pattern can change its power level (either consumption or production) if so required, without any consequence for its future flexibility. A good example of this pattern is a diesel generator, with a sufficient amount of diesel in its tank, it can produce energy at any power level between zero and its maximum output, and it can almost instantly switch between different power levels. This flexibility pattern is particularly useful for balancing applications, for example, in a microgrid;
- **Buffer energy.** Some devices can buffer energy in some form or another. These devices have one or more components that convert electrical energy, for example, into another energy form and put that in the buffer. Other components can then retrieve the

converted energy from the buffer. The buffer provides flexibility because the (converted) energy that is put into the buffer does not have to be retrieved immediately. A good example of this pattern would be an electric hot water boiler. The water can be heated with an electrical heating element and be retrieved much later when it is needed;

- **Store energy.** In the previous pattern, it was not possible to retrieve energy in the same form as it was put in. A water boiler consumes electricity and converts that into hot water but is not possible to convert that back into electricity again. The “store energy” pattern, however, is capable of retrieving energy from the storage in the same form as it was put in. The stereotypical example of this pattern is of course, a battery. This can be a stationary battery or a battery in an EV;
- **Switch energy type.** The final pattern concerns devices that can utilize different forms of energy to achieve the same objective. A hybrid heat pump is a good example of this pattern. This setup consists of an electric heat pump and a gas boiler. Either one or a combination of both can be used to meet the heat demand. This creates a lot of flexibility on the electrical side. If there is congestion on the local grid due to a combination of EV charging and heat pumps, for example, the hybrid heat pump can switch to the gas boiler. This way, it will still be able to meet the heat demand while the electricity consumption will have been reduced to nearly zero.

On their own, these flexibility patterns are relatively simple and easy to understand. In practice, however, they usually will not occur in their isolated form in a real-life device, but rather as a combination of patterns, e.g., a battery will typically combine the ‘power modulation’ and ‘store energy’ patterns. In that case, the ‘power modulation’ will be limited by the storage. When the battery is almost full, a certain power level cannot be maintained for extended periods. If the battery is already completely topped, it is not even possible to select any power level at all that would result in trying to fill the battery some more. The real challenge is in modelling the interdependencies of these atomic flexibility patterns as they occur in actual devices. The following sections discuss three different approaches for modelling these interdependencies.

4.2.3.3 S2 (EN50491-12-2)

Energy flexibility can also be categorized in terms of different types of control that describe how basic energy flexibility patterns will typically interact in real-life devices. In this subsection, the so-called ‘S2 control types’ are used to describe this.

The name S2 points to an interface between the Resource Manager and the Customer Energy Manager (CEM) in a CEN-CENELEC architecture that is the basis for the 50491-12 standard series (formally standardized in EN50491-12-1)[23]. The S2 interface is used to communicate the flexibility of smart devices to a Customer Energy Manager (CEM) and to allow for control of that flexibility. The full S2 specification is the subject of the upcoming EN50491-12-2 standard (expected release date between Q4 2020 and Q1 2021). Through the S2 interface, the Resource Manager is capable (if supported by the underlying smart device) to provide power/energy measurements and forecasts to a CEM. In addition to these basic and generic functions, the S2 interface also features five control types that represent different types of energy flexibility. A Resource Manager will map the flexibility of the device it represents onto one of these control types. The CEM will only have to implement these control types to be able to connect to all devices via their respective Resource Managers.

Figure 15 shows which sets of basic energy flexibility patterns together act as a basis for the five control types.

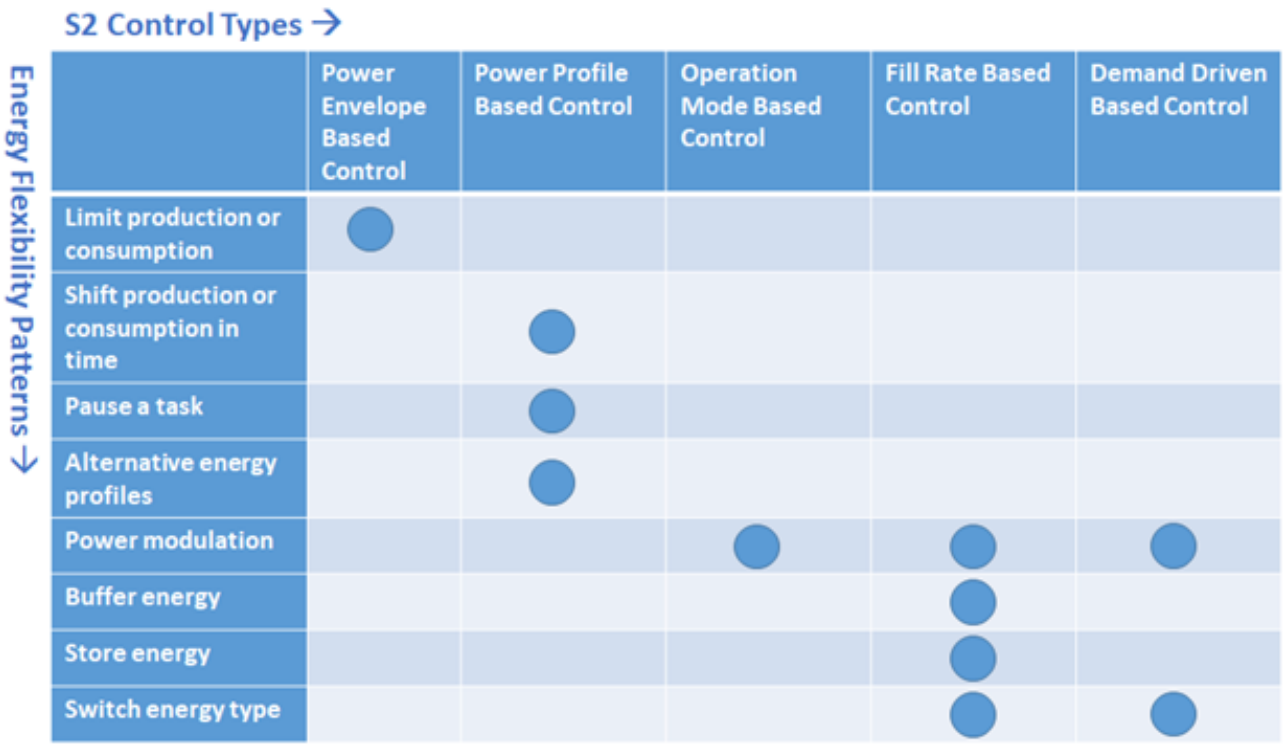


FIGURE 15 – MAPPING OF BASIC ENERGY FLEXIBILITY PATTERNS ON S2 CONTROL TYPES

[23] See also Section 2.2.2, on the CENELEC Reference Architecture.

The S2 Control Types themselves are described in more detail below:

- **Power Envelope Based Control.** This control type is used for devices that cannot be controlled by the CEM to adhere to a specific value for their production or consumption. They can, however, be asked by the CEM not to exceed certain power limits over time. A typical example of such a device would be a PV panel. The CEM cannot directly control its production as this is dependent on the amount of sunshine, but it can ask the PV panel not to exceed a certain production limit, also known as curtailment. This feature is very useful for example for congestion management;
- **Power Profile Based Control.** The power profile-based control type is typical for devices that perform a function with a corresponding power profile that is known or can be predicted. Their main flexibility comes from the ability to change the start time of that power profile. White goods, such as a washing machine with a delayed start option, are good examples of this category. A consumer fills the washing machine, selects a program and chooses the final time by which this program should be finished. This control type offers another type of flexibility since it has the ability to choose between multiple alternative power profiles. The heating cycle of the washing machine might have alternative profiles;
- **Operation Mode Based Control.** Devices that fall within this control type can control the amount of power they produce or consume, without significant effects on their future flexibility options. Typical examples for this control type are diesel generators and variable electrical resistors. Such devices are often useful for balancing microgrids. Operation mode devices offer a lot of flexibility; they can assume a range of power levels at almost arbitrary moments in time. When this type of flexibility would be modelled with power profiles, as used for power profile-based control, the number of possible permutations would rapidly grow beyond practical limits. To avoid such issues, the operation mode control type is modelled as a state machine. Transitions between operation modes are also explicitly specified. This way, the possible transitions between operation modes may be restricted. Transitions can also be equipped with timing constraints;
- **Fill Rate-Based Control.** The fill rate-based control type can be used for devices that can store or buffer energy. How energy is stored or buffered does not matter, as long as there is a means to measure how full the storage or buffer is. There are many examples of devices that can store or buffer energy. Stationary batteries and electric vehicles are examples of devices that store energy in batteries. Heating devices such as CHPs, (hybrid) heat pumps or boilers can buffer energy in a dedicated heat buffer (typically a thermally insulated water tank), but a room with an allowable bandwidth for

the temperature can also be used as a buffer. Finally, there are also devices that produce cold, like air conditioners, fridges and freezers. Just like heat, cold can be buffered. The behaviour of the actuators is described with a state machine, just like the operation mode-based control type. In this case, however, the states also specify what their influence on the fill level of the buffer will be;

- **Demand-Driven Based Control**. Demand-Driven Based Control can be used for systems that are flexible in the type of energy carrier they use but are not capable of buffering or storing energy (in that case Fill Rate-Based Control should be used). A typical example is a hybrid heat pump, that generates heat using either electricity (using a heat pump) or natural gas (using a gas boiler) but does not have a thermal buffer. The hybrid heat pump must deliver a given amount of heat (hence demand-driven) but can still decide whether to generate this heat using electricity or natural gas. Typically, such systems favour the heat pump but use the gas boiler in case the heat demand cannot be fulfilled by the heat pump alone or when there is a shortage of capacity in the electricity grid. Similar to the Fill Rate-Based Control, Demand Driven Based Control has the concept of multiple actuators. Again, the behaviour of these actuators is described using a state machine.

Under certain conditions, energy flexibility can be represented using a generic concept called ‘Flexgraphs’. The following subsection describes this concept.

4.2.3.4 FLEXGRAPHS

A flexible installation or process has several options in time to convert energy, e.g., consume/produce electricity. These different options can be seen as possible ‘paths’ within the electricity consumption/generation plane. A flexgraph is the visualization of the area between the highest and lowest path of this plane (so it is not a profile since it is an area and that offers more flexibility than a set of profiles), this concept has been used in various European research projects such as industRE, Rennovates, and FHP. It is described in [11] for thermal energy storage and applied to a fleet of electric vehicles in [12]. Figure 16 shows four generic examples of a flexgraph: the grey area indicates the flexibility itself, dashed lines are drawn as possible paths to cross the flexgraph. These graphs can be created based on the identification step of some demand response audit, e.g., the information obtained from the flexibility provider about the installations and processes, such as maximum power production/consumption, modulating options, and others.

By means of such characteristics, graphs like the ones shown in

Figure 16 will be created.

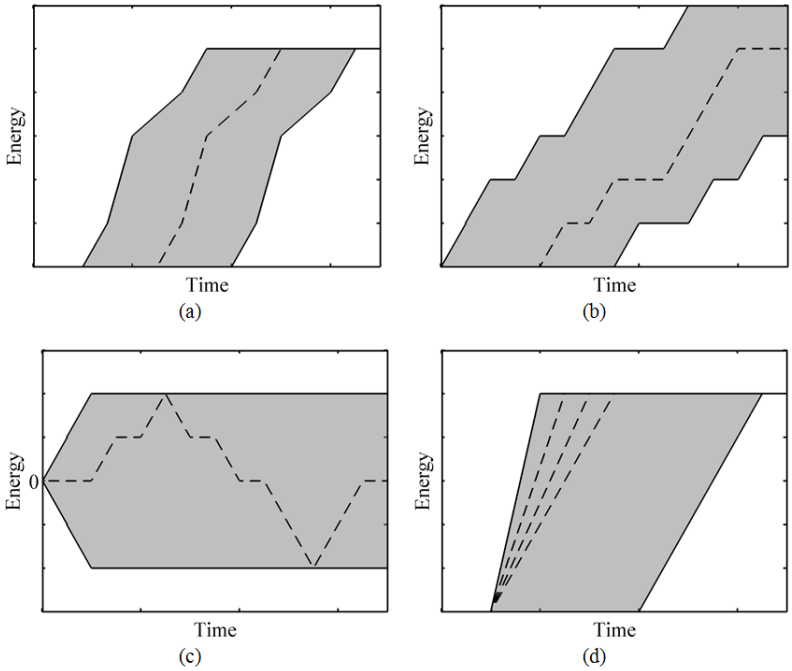


FIGURE 16 – FLEXGRAPH EXAMPLE[24]

The number of possible paths within the graph and the shape of the graph are installation/process specific.

Figure 16(a) shows the profile of a shiftable unit which can delay or bring forward its consumption/production.

Figure 16(b) shows the flexibility of an electric water heater with thermal storage: the power consumption of this device can be interrupted, depending on the heat demand.

Figure 16(c) shows the profile of a battery: when the battery charges, its power is positive, indicated by a path going up, while when the battery discharges, its power is negative, indicated by a path going down.

Figure 16(d) shows the profile of a power modulating unit: the profile has several possible paths with a different slope.

[24] In this example, the grey area indicates the flexibility and the dashed lines indicate possible paths to cross the flexgraph. a) a shiftable unit; b) an electric hot water heater with thermal storage; c) a battery; d) a modulating unit.

The number of possible paths within the flexgraph is a measure for the potential to shift its consumption/production, and thus gives an indication of how much flexibility the installation offers. A unit without flexibility only has one unique path to cross the energy consumption plane, so its flexgraph is just one path. The area of the graph indicates how much energy can be shifted. A flexibility profile with a large area and many paths within indicates that the device can shift a large amount of energy in a lot of different ways. The upper boundary of the graph represents the path in which the energy is consumed as soon as possible; the lower boundary of the graph represents the path in which the energy consumption is delayed as long as possible.

Figure 17 shows an applied example of a flexgraph of a battery system; the top figure represents the energy consumption/production of the battery, whereas the bottom figure displays the power consumption/production. The blue and red dashed lines respectively show the lower and upper boundary of the flexibility; the green area shows the flexibility itself and the black lines show the consumption/production of electricity. Figure 17 also shows the state of the battery on a specific moment in time, namely in between 0.5 and 0.6 days. In the energy plane, it is shown that, at that time, the battery can charge and/or discharge 100 kWh. The power plane shows at which power this energy can be charged and discharged. By looking at the upper and lower boundary in the graphs, it is apparent that the battery can charge at 18 kW and discharge at 15 kW at this specific moment in time. Implicitly, this is also shown in the top graph by the slopes of the solid red (charge) and solid blue (discharge) lines because energy represents the integral of power over time. These two graphs point out that at each moment, the flexibility depends on the state of charge (SoC) of the battery together with the minimum and maximum charge/discharge power.

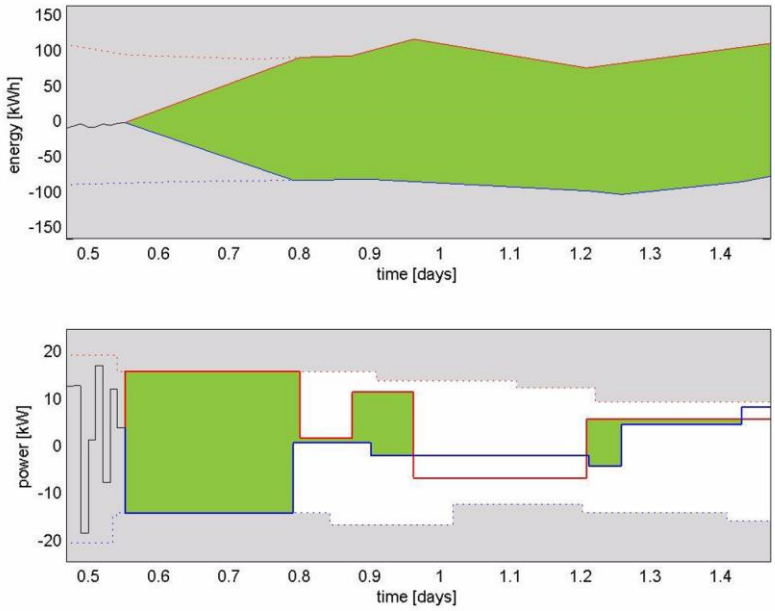


FIGURE 17 – FLEXGRAPH EXAMPLE OF A BATTERY[25]

The flexgraph is a generic concept independent from the type of installation; hereby it is possible to aggregate multiple flexgraphs originating from different types of installations resulting in the overall flexgraph of a device cluster. This is illustrated in Figure 18, where the flexgraphs of two individual installations (light grey) are aggregated and their resulting total flexibility is represented by the flexgraph coloured in dark grey.

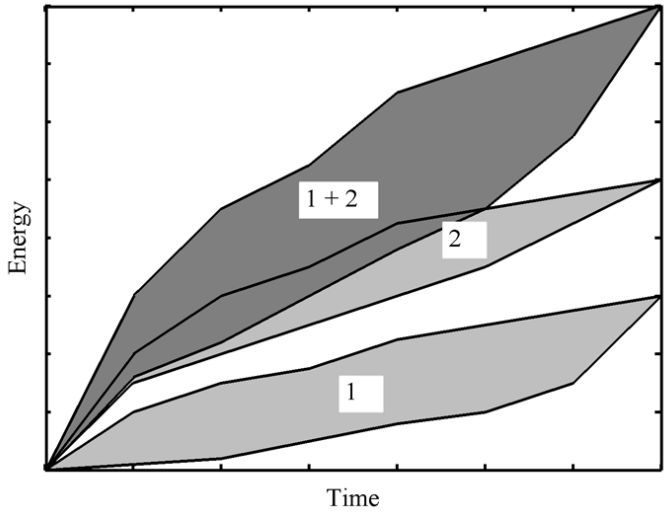


FIGURE 18 – AGGREGATION OF TWO FLEXGRAPH[26]

[25] In this example, the energy consumption/production plane on top and the power consumption/production plane at the bottom; Dashed blue line is the lower boundary of the flexibility, dashed red line is the upper boundary of the flexibility.

[26] In this example, the dark grey area is the sum of the two light grey areas.

The main advantages of using flexgraphs are:

- the simplified quantification of flexibility;
- the ease of aggregation; and
- the abstraction of specific information related to processes/installations.

4.2.3.5 TRACES: FUNDAMENTALS AND SAMPLES

Another way to express flexibility is to make use of a so-called 'traces'-based approach. This was done in the ERA-Net project CALLIA[27], that called it Fundamentals & Samples'. In CALLIA, an alternative approach in which feasible power profiles take a central role as either 'fundamentals' or 'samples' was explored. The flexibility is represented by a set of alternative power profiles. Information about stochastic influences (whether caused by the unpredictable behaviour of a user or by the device itself) is added in a separate step. This is different from flexgraphs (as described above) that express energy flexibility using boundaries in between which physical processes can be modulated. Generally, these boundaries can concern time (e.g., shiftable loads), power (e.g., modulating production capacity), energy (e.g., battery capacity) or an envelope of any combination of these and other dimensions.

A 'fundamental' is a single power profile representing one of (potentially) many feasible alternatives that comply with all device restrictions. To a consumer of flexibility, a set of fundamentals represent flexibility in the form of a discrete collection of alternatives. The stochastic influence of uncertainty is not included in a fundamental itself but presented as a separate set of 'samples' associated with the fundamental (see Figure 19).

[27] https://callia.info/en/

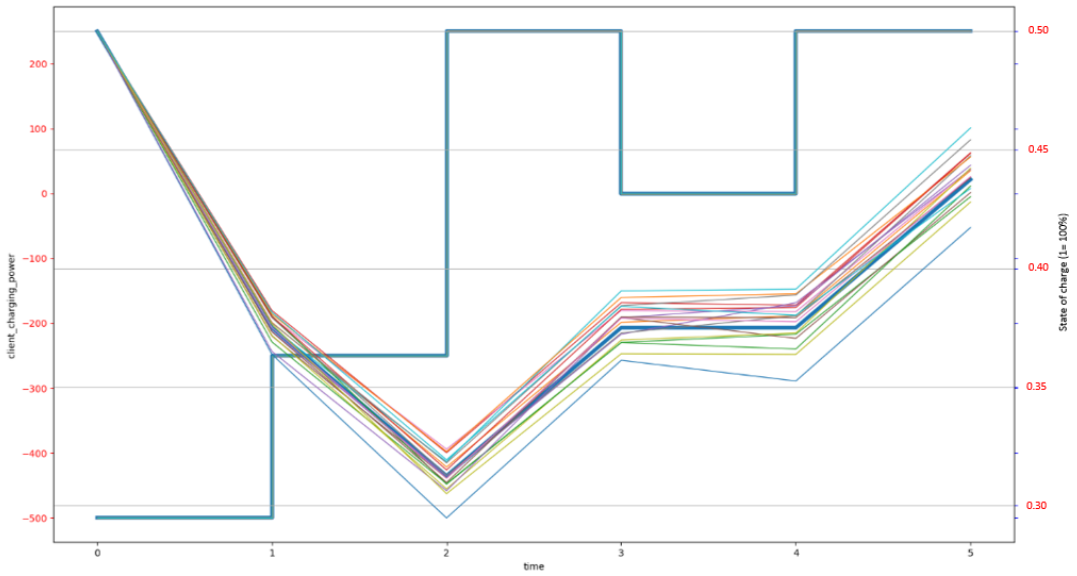


FIGURE 19 – FUNDAMENTALS AND TRACES[28]

A 'sample' is an adaptation of a fundamental to one of (potentially) many possible stochastic disturbances in the process. As the disturbances may sometimes influence if and when physical boundaries are reached, the effect on the fundamental can be profound. To a consumer of flexibility, the set of traces associated with a fundamental indicate what power profiles can really be expected, given stochastic disturbances in the device's behaviour or use.

The information exchanged between two endpoints in the hierarchical flexibility architecture uses the same information scheme independent of the involved layers. Devices exchange the same type of information with the cluster manager as the cluster manager with the aggregator. This means that aggregation levels can be added or removed without having to change the information scheme.

The fundamentals/traces that were practically exchanged within the CALLIA project between the various device agents, cluster managers, and aggregators did not contain any quantified indication on the uncertainty of the forecast. Including this in the data model would improve the optimization at all levels. To accomplish this, (device) models, optimization algorithms, scenario reduction algorithms and communication data models have to be adapted to include and deal with this uncertainty factor.

[28] In this example, the thick blue lines represent a fundamental (stepwise power levels and corresponding SoC evolution). The thin lines are SoC samples deviating from the fundamental.

During the CALLIA project, extensions to the data model were discussed that might prove useful in the context of InterConnect. Among those are:

- the profile uncertainty factor;
- parameters for indicating or tracking deviations;
- locality information;
- potentially, a deviation cost factor could be added to the flexibility and allocation requests to urge a child agent to keep its promises.

All these extensions can influence interoperability. In the data model for flexibility, we need to strive to a flexibility model that does not restrict itself to profile and can aggregate flexibility easily. Multiple models can be used, but an automatic translation between these needs to be possible.

4.2.4 INTERCOMPONENT EXCHANGE OF INFORMATION

Now that (energy-related) assets and devices have been described, and the concept of energy flexibility has been explained, it is now time to describe different domain components in the SERA and their relationships. This description also contains a visualisation of the architecture that shows how different components are related to each other in terms of information exchange.

4.2.4.1 AN INTELLIGIBLE SERA THAT SUPPORTS ALL USE CASES

The previous chapter emphasised the need to generalise the many (semantical) concepts found in the Use Cases produced by WP1. The following subsection introduces the resulting Reference Architecture.

The previous chapter emphasised the need to generalise the many (semantical) concepts found in the Use Cases produced by WP1. The following subsection introduces the resulting Reference Architecture.

Section 4.2.1 introduced the different scales, and more specifically, the Smart Home, Smart Grid and Smart Energy scales, and their actors. After zooming in on the InterConnect scope,

which includes the DSO, the following architecture encloses a pictorial representation, enabling a few simple energy and non-energy use cases.

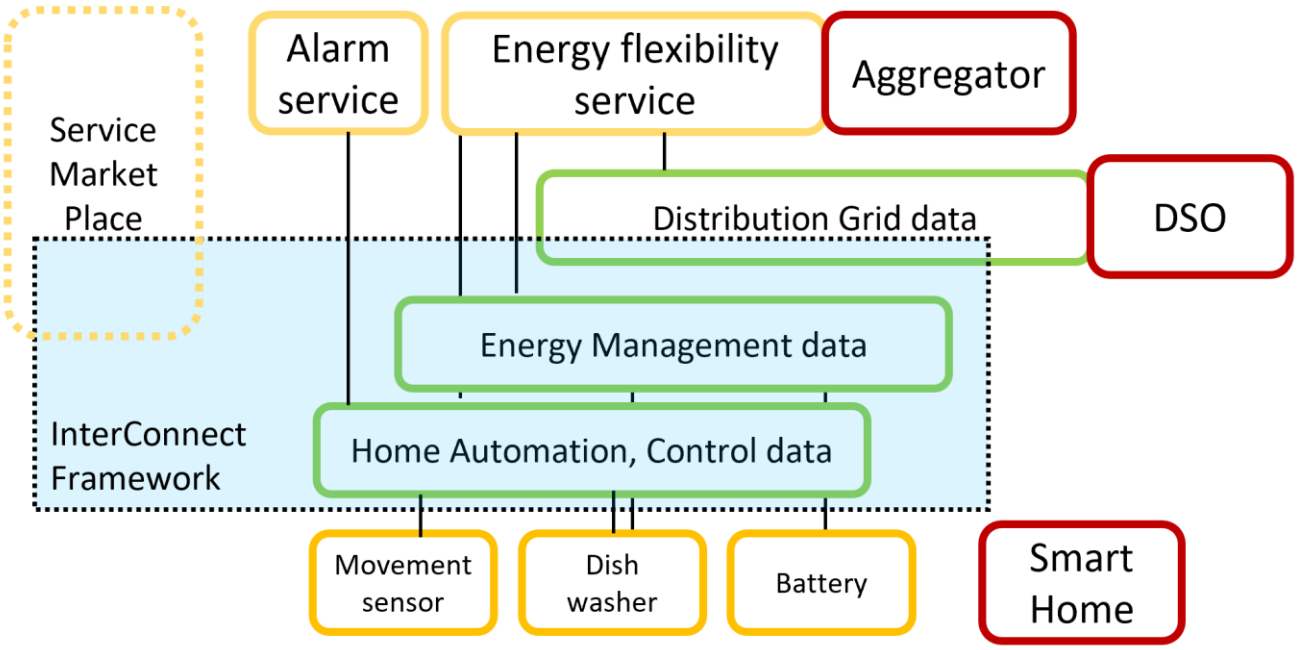


FIGURE 20 – INTERCONNECT'S ARCHITECTURE PICTORIAL ENABLING A FEW SIMPLE USE CASES

Figure 20 already implicitly depicts the use of the five layers from the SHBERA; the Stakeholder layer (e.g., DSO), the Application/Service layer, the Information/Interoperability layer (green data domain), the Communication layer (the connections) and the device/asset layer.

Concerning energy market roles, the goal was to stay in line with the Smart Grid Task Force Expert Group view on Possible relations between market roles [12].

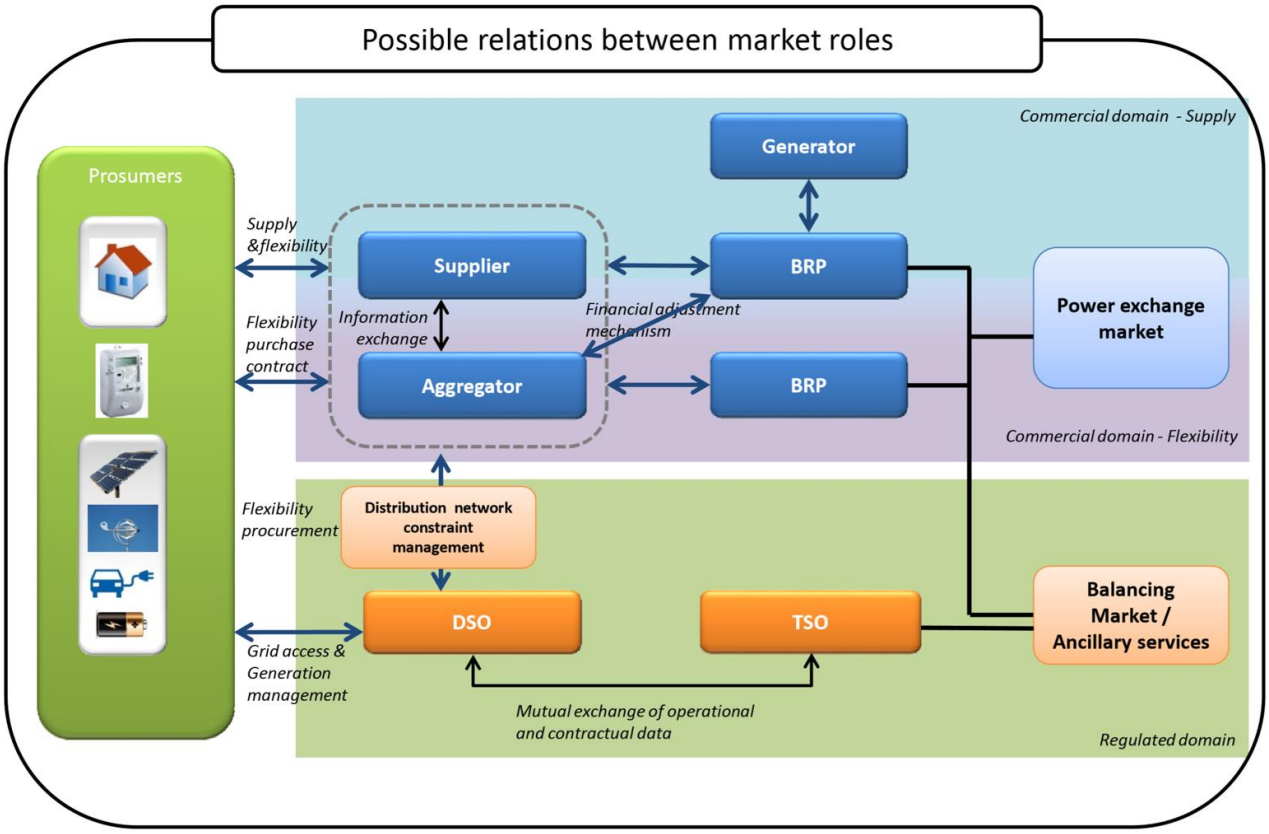


FIGURE 21 – POSSIBLE RELATIONS BETWEEN ENERGY MARKET ROLES [12]

In what regards the energy actors and roles: we noted that although lots of actors (TSO, BRP, and others) and markets (Balancing Market) were clearly defined, there are some differences in countries legislation (and especially around energy flexibility) that introduce different views and possibilities on (local) flexibility markets, actors (technical, commercial aggregators). This was also the outcome of WP1 and leads to our conclusion not to try to standardize these actors roles and markets, but rather focus on *enabling* all these possible actors and markets through providing the right information to the different domains.

In line with the methodology for deriving the Smart Energy Reference Architecture, the steps as described in the previous chapter have been performed. After several iterations with simplification, convergence and generalization, the SERA has been finalized. We identified what kind of information (objects) are to be exchanged between the services (of the actors/roles) and the devices with the help of the InterConnect Framework / Platform. This means that the emphasis in the SERA is on elements that are directly involved in the interconnection of devices and services.

All these steps, actions and iterations have led to the following Smart Energy Reference Architecture (SERA), depicted in Figure 22.

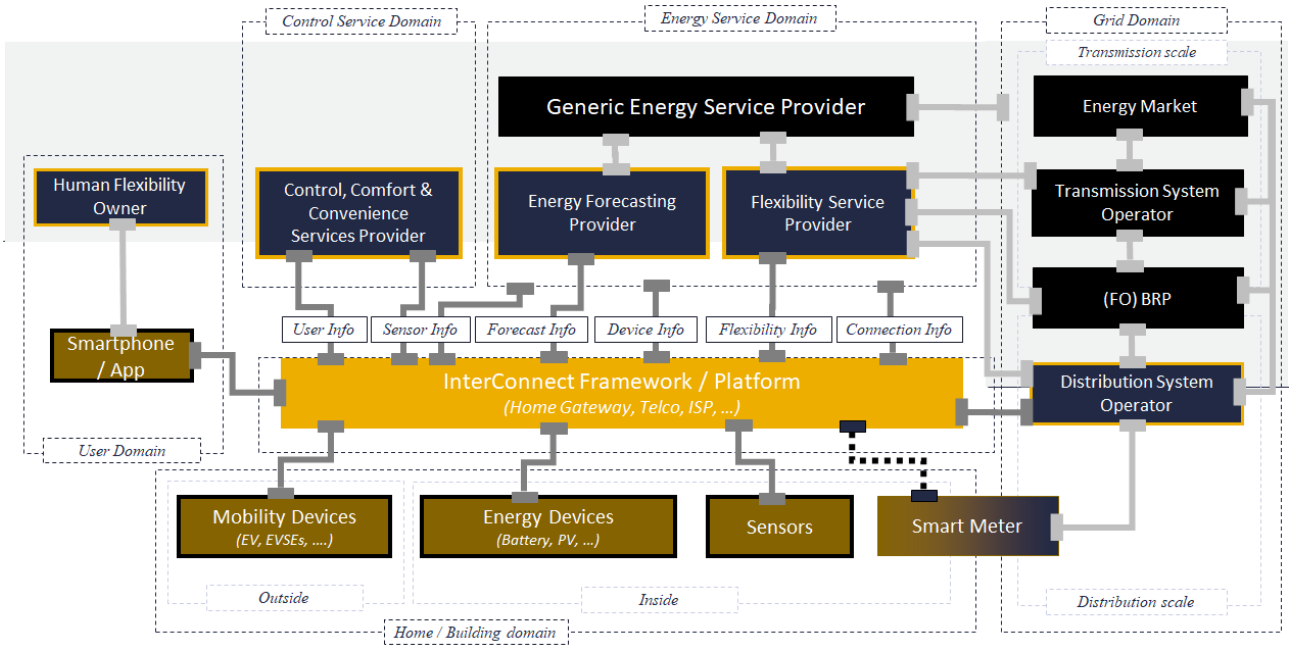


FIGURE 22 – INTERCONNECT'S SMART ENERGY REFERENCE ARCHITECTURE (SERA)

The next four types of categorisation were used to create a structured and more manageable overview:

- **Type of component:** an architectural component can be a Mobility or Energy (related) **Device** (e.g., EV, EVSE, PV, Battery, amongst others), it can be a **Role** (e.g., Human Flexibility Owner, Flexibility Service Provider) or it can be the **InterConnect Framework / Platform** itself.

In the visualisation Devices have a brown fill colour. Roles have a dark blue fill colour. The Smart Meter is depicted as both a Device and a Role, as the Smart Meter is managed by an organisation that has to provide Smart Meter data. This can be a Distribution System Operator, but that does not always have to be the case. The InterConnect Framework / Platform has, by default, an orange fill colour.

1. **Location in a specific domain:** components within one domain tend to share more things with each other (e.g., physical location, interests, reference framework, etc.) than with components in another domain. Different domains do influence each other through the relationships between components in different domains. For example, the Smart

Grid Domain is influenced by the behaviour of people in the User Domain and devices in the Home/Building Domain (and vice versa). The domains are **User**, **Smart Home / Building**, **Smart Grid**, **Control Service** and **Energy Service**. They will be described below (in more detail).

2. **Indirection of Framework / Platform connection:** components can be directly connected to the InterConnect Framework / Platform directly or indirectly. When they are directly connected, they will have to interface logically (and also technically) with the InterConnect Framework / Platform. In the visualisation components that have a direct connection with the InterConnect Framework / Platform have a differently coloured outline. Also, direct connections have a dark grey colour and indirect connections a lighter grey.
3. **Type of 'information theme':** the InterConnect Framework / Platform receives a wide range of information from different archetypical devices and roles. The type of information has been grouped into themes called **User**, **Sensor**, **Forecast**, **Device**, **Flexibility** and (grid) **Connection Info**. This was an outcome of the SERA analysis methodology described in the previous chapter.

The Smart Energy Reference Architecture consists of the following basic elements, for some of these definitions we have made consider the USEF model definitions[29].

- **Human Flexibility Owne**r:
    a. **Prosumer**: A Prosumer can be regarded as an end-user that no longer only consumes energy, but also produces energy.
- **Smartphone / App**: For retrieving user information or giving user feedback in most cases. By default, this is expected to be an App on a Smartphone (or tablet, computer).
- **Mobility Devices**: The energy-related devices we refer here are mainly the Electric Vehicle (EV) or the related EVSE (EV Supply Equipment, the charge point).
- **Energy Devices**: The energy-related devices we refer here are mainly Domestic Appliances, PV panels, in-home battery storage, HVAC (Heating Ventilation and Air-conditioning)
- **Non-energy Devices**: This are devices for controlling lighting, sun shading, locking doors, etc.
- **Sensors**: is a module, component able to measure or detect events in its environment. For InterConnect this are in-home or in-building modules able to measure or detect: activity (motion, door and window, intrusion) climate and comfort (temperature, air flow, CO_2, water, light, humidity) or any other measurement.

[29] For more information, see https://www.usef.energy/app/uploads/2016/12/USEF_TheFrameworkExplained-18nov15.pdf

- **Smart Meter**: In general a Smart Meter is a meter measuring electricity in power and energy (and/or heat, water, gas) and can be read remotely.
- **Distribution System Operator**: The DSO is responsible for the active management of the distribution grid.
- **Transmission System Operator**: The role of the Transmission System Operator (TSO) is to transport energy in a given region from centralised Producers to dispersed industrial Prosumers and Distribution System Operators over its high-voltage grid. The TSO safeguards the system's long-term ability to meet electricity transmission demands and is responsible for keeping the system in balance by deploying regulating capacity, reserve capacity, and incidental emergency capacity.
- **Energy Market**: In general energy markets are commodity markets that deal specifically with the trade and supply of energy. The energy market in our case mostly refers to electricity markets, where trades can refer to capacity, day-ahead, intraday, and balancing products.
- **BRP**. A Balance Responsible Party (BRP) is responsible for actively balancing supply and demand for its portfolio of Producers, Aggregators, and Prosumers. The supplier can contract a BRP.
- **InterConnect Framework**: A collection of tools enabling interoperability and the intelligent interaction of many devices and services from different domains (e.g., home automation, energy management, etc.)
- **Flexibility Service Provider**: The role of the Flexibility Service Provider (can be an aggregator) is to accumulate flexibility from prosumers and their devices and offer or sell it to energy actors (varying from Commercial Aggregators, the BRP, the DSO, or to the TSO)
- **Energy Forecast Provider**: Forecasts are crucial for efficient management of flexibility. For that reason, we foresee dedicated parties (or services) that provide energy forecasts. These forecasts can relate to PV, wind, building consumption, eMobility demand, etc.
- **Generic Energy Service Providers**: These providers offer auxiliary energy-related services to Prosumers. These services include insight services, energy optimisation services, and services such as the remote maintenance of assets. It can also be an Energy Supplier, with the role to source, supply, and invoice energy to its customers. The supplier and its customers agree on commercial terms for the supply and procurement of energy.
- **Control, Comfort & Convenience Services Provider:** This Service Provider executes for their customers different kind of services related to building and in-home

management and control for comfort and convenience in various domains (like heating, lighting, control of domestic appliances, etc.)

The following sections list the names of the information (producer or receiver) mentioned in the specific use cases mapped on the basic elements of the SERA in a table per domain. These tables also contain the generalised use case information objects used in these use cases.

Now that the main structure in terms of grouping and categorisation has been described, it is time to describe the different components and the mapping of (semantical) concepts found in Use Case descriptions. In order to create a manageable overview, each domain has a subsection of its own.

4.2.4.2 USER DOMAIN

The information objects used are mapped on the basic role most connected to this information. Although a retailer can send an activation signal to a device, we allocated this to the device in the tables below.

Basic Roles and System elements	
Human Flexibility Owner	**Use Case Information Producers and Receivers** • End User • Local community • EV user • Prosumer • User, end consumer • Building Manager, Building Owner • Smart parking owner, parking manager, Charging station operator • Community energy manager
	Use Case Information Objects Exchanged • Human preferences (for device) • Human feedback • Human Login & Authentication • Human request
Smartphone / App	**Use Case Information Producers and Receivers** • App • Mobile App • Manufacturer App

	• Living Service Provider's App
	Use Case Information Objects Exchanged • Digitized human preferences (for device) • Digitized human feedback • Digitized human Login & Authentication • Digitized human request

TABLE 12 – USER DOMAIN BASIC ROLES AND COMPONENTS

User Domain Information Objects:

- **User Login & Authentication**: all identification data required to complete the user authentication process.
- **User request**: user requesting sensors reading, commands to do switch off/on lights, HVAC, commands to check building installations.
- **User preferences (for device)**: All preferences the user can set for devices or the (building/home) environment: like comfort settings (temperature or humidity), lightings timing and settings, preferences for low-cost or own generated energy, etc.
- **User feedback**: All kind of user feedback like reporting of actions performed, display feedback to user, charge summary, errors, etc.

The next version of this deliverable, due in M36, will detail this further as more detailed use cases become available (also in line with T2.5 activities). Following the project's DOA, both D2.1 [39] and D1.2 [40] are due in M15. D1.3 (system use-cases) [41] is due in M18. The full details of all use-cases should be available then.

4.2.4.3 SMART HOME / BUILDING DOMAIN

Basic Roles and System elements	
Mobility / Energy Devices	**Use Case Information Producers and Receivers** • Device • Charging stations operator • Charging station • Devices • Device-X Smart Plug • Smart Device • PV inverter devices

	Use Case Information Objects Exchanged • Flex plan to device • Commands to device • Device feedback • Device flexibility/info
Sensor	**Use Case Information Producers and Receivers** • Sensors
	Use Case Information Objects Exchanged • Sensors (data)
Smart meter	**Use Case Information Producers and Receivers** • DSO-Smart Meter • Smart meter • Smart Meter + Internet Interface
	Use Case Information Objects Exchanged • Smart meter (building consumption)

TABLE 13 – SMART HOME/BUILDING DOMAIN BASIC ROLES AND COMPONENTS

Device and Sensor Domain Information Objects:

- **Commands to device**: Sending commands to a device. This can be simply turn on a specific device but can also be an advanced program.
- **Device feedback**: Feedback of the device (to a service) that a plan has been activated or a command has successfully been processed.
- **Device flexibility/info**: This information can be the device energy flexibility, but also real-time consumption data or other device-related information.
- **Flex plan to device**: This energy flexibility plan can be advanced, a simpler power profile, a load shifting request or a power limit.
- **Sensor (data)**: This sensor data can be very diverse (see also chapter on devices and sensors). Data can vary from room temperature to current grid load, energy consumed yesterday, CO_2 level, etc.

These elements will be further detailed in the next version of this deliverable.

4.2.4.4 SMART GRID DOMAIN

Basic Roles and System elements	
Distribution System Operator (DSO)	**Use Case Information Producers and Receivers** • DSO • DSO-Grid
	Use Case Information Objects Exchanged • DSO flex needs/request • DSO flex offer • DSO flex order • DSO Flex order feedback • DSO Heartbeat • DSO Smart Meter data
Transmission System Operator (TSO)	**Use Case Information Producers and Receivers** • TSO
	Use Case Information Objects Exchanged • TSO data is not expected in the InterConnect platform. TSO found in use cases is e.g.: a. Block exchange notification b. Imbalance invoicing c. Imbalance invoicing d. Consumption and injection program • Peak day information (tariff)
BRP	**Use Case Information Producers and Receivers** • BRP
	Use Case Information Objects Exchanged • These are allocated to TSO or other roles

TABLE 14 – SMART GRID DOMAIN BASIC ROLES AND COMPONENTS

Energy Grid Domain Information Objects[30]:

- **DSO flex needs/request**: The request for flexibility from a DSO, often to reduce grid load in order to prevent local congestion. The request can be to the FSPs or CAs that are active in the domain the DSO has the request for.

[30] Some of the objects are inspired by and also used in USEF.

- **DSO flex offer**: Various flexibility offers from multiple FSPs or CAs are expected and will be received and evaluated by the DSO.
- **DSO flex order**: The DSO will accept/order some of the flexibility offered since these have the best value and or are best suited/reliable.
- **DSO Flex order feedback**: The FSP/CA need to confirm the order. Note that also a part of the flexibility offered can be ordered.
- **DSO Smart Meter data**: Measurement data from the smart meter is required for the settlement of used energy and use flexibility. This data (for reliability purpose) needs to be provided by the DSO (or the designated Meter Operator).
- **DSO Heartbeat**: In some cases, DSOs like to send heartbeats to connected parties/devices to signal if these are alive and able to provide or react on flexibility.

These elements will be further detailed in the next version of this deliverable.

4.2.4.5 ENERGY SERVICES DOMAIN

Basic Roles and System elements	
Flexibility Service Provider	**Use Case Information Producers and Receivers** • Living Service Provider's Platform • i-EMS (integrated Energy Management System) • Aggregation Engine ReFlex • Flexibility service provider • Commercial Aggregator • Aggregator
	Use Case Information Objects Exchanged • TA Aggregated flexibility • Flex plan from TA to set of devices (BEMS) • Flex plan to TA • Set of devices (BEMS) feedback • TA feedback to CA • TA Heartbeat
Generic Energy Service Provider	**Use Case Information Producers and Receivers** • Retailer, Supplier • Energy Service Provider • Energy Service Provider's Platform • ESCO • Producer

	Use Case Information Objects Exchanged • These are allocated to Flexibility Service Provider or other roles

TABLE 15 – ENERGY SERVICES DOMAIN BASIC ROLES AND COMPONENTS

Energy Flexibility Domain Information Objects:

Various use cases include a Technical Aggregator (TA), which is called Flexibility Service Provider (FSP) in the architecture to avoid confusion and mixed up with a Commercial Aggregator.

- **TA Aggregated flexibility**: The FSP (or TA) aggregates flexibility of a set of households, buildings or a certain area and sends this to an Energy Service Provider (e.g., a Commercial Aggregator).
- **Flex plan to TA**: An Energy Service Provider exploits the aggregated flexibility on various energy markets and generates a flexibility plan to be executed by the FSP/TA.
- **Flex plan from TA to set of devices (BEMS)**: The FSP/TA disaggregates the flexibility plan and sends it to the devices (or BEMS) of the households or buildings.
- **Set of devices (BEMS) feedback**: The devices (and BEMS) give feedback if the plans can successfully be executed. If not, the deviations will be sent to the FSP too.
- **TA feedback to CA**: The FSP/ TA will collect all deviations (if any) and bundle these and send it to the FSP/TA, so that if needed an adapted plan can be executed.
- **TA Heartbeat**: Sometime heartbeat messages Are sent to devices by the FSP/TA to see if these are still active and online.

These elements will be further detailed in the next version of this deliverable.

4.2.4.6 FORECAST DOMAIN

Basic Roles and System elements	
Forecaster	**Use Case Information Producers and Receivers** • Aggregation Forecaster • Baseline forecaster • Flexibility forecaster • PV forecaster • Weather Forecaster • Forecaster

	Use Case Information Objects Exchanged • Forecasted power profiles • Forecasted Weather • Forecast request

TABLE 16 – ENERGY SERVICES DOMAIN BASIC ROLES AND COMPONENTS

Forecast Domain Information Objects:

- **Forecasted Weather**: Regular weather forecast with different time scale (next week, day, hour) and data (temperature, wind, solar radiation, etc.)
- **Forecasted power profiles**: Various services need forecasted power profiles. This can be baseline load forecast (the load the household will have without the flexible devices), the PV forecast (of the PV panels of the building or an area), but also overall energy consumption forecast (including all flexible loads like EVs and HVAC) are needed.
- **Forecast request**: Certain forecasts can also be made on request of the DSO, and example is to request as DSO the forecast of a set of households (that is, e.g., connected to a certain DSO LV feeder).

These elements will be further detailed in the next version of this deliverable.

4.2.4.7 CONTROL SERVICES DOMAIN

Basic Roles and System elements	
Control, Comfort & Convenience Services Provider	**Use Case Information Producers and Receivers** • Manufacturer Platform • Non-energy service provider • Third parties service provider
	Use Case Information Objects Exchanged • Intra-platform messages, such as: a. Update digital twin b. Sync settings, config, commands, messages

TABLE 17 – CONTROL SERVICES DOMAIN BASIC ROLES AND COMPONENTS

4.2.4.8 INTERCONNECT FRAMEWORK/PLATFORM

Basic Roles and System elements	
InterConnect Framework / Platform	**Use Case Information Producers and Receivers** • Edge/resource manager • BSM/Building energy manager • EMS • IoT GW • Platform • Platform-Device Control • Platform-Logic • Tokenization provider • Token management services
	Use Case Information Objects Exchanged • Use cases do not explicitly list the platform, so the information objects are assigned to other basic roles. We would expect here intra-platform messages, such as: a. Sync settings, config, commands, messages

TABLE 18 – IC FRAMEWORK BASIC ROLES AND COMPONENTS

4.2.5 MAIN CONCLUSIONS AND RECOMMENDATION ON THE SERA

The Smart Energy Reference Architecture (SERA) is established mainly based on the layering principle. Based on use cases business actors, roles and physical devices/components are mapped on this layered architecture. The use cases also reveal information exchanged between the roles (sometimes services) and devices.

Use cases, and also legislation from different countries, use different terminology for actors and roles. Narrowing further down in this architecture phase was therefore not possible, but also not needed since we also require to be able to execute new and future use cases. Therefore, business actors, roles are grouped into different basic roles and system elements per system domain.

Similarly, we dealt with the information exchanged. These were often vaguely described terms (‘flexibility’, ‘forecast’, ‘user settings’). So also here we grouped these into information objects per the same domains.

With this layering, generalizing energy roles, we created an intelligible, understandable and deployable Smart Energy Reference Architecture with lists of basic actors and information elements per domain.

Basic Roles and System elements per domain	
User Domain	• Human Flexibility Owner • Smartphone / App
Smart Home/ Building Domain	• Mobility / Energy Devices • Sensor • Smart Meter
Smart Grid Domain	• Distribution System Operator (DSO) • Transmission System Operator (TSO) • BRP Energy Service Domain • Flexibility Service Provider • Generic Energy Service Provider
Forecast Domain	• Forecaster
Control Services Domain	• Control, Comfort & Convenience Services Provider
InterConnect Framework/ Platform Domain	• InterConnect Framework / Platform

TABLE 19 – SUMMARY OF BASIC ROLES AND SYSTEM ELEMENTS PER DOMAIN

The Use Case Information Objects are also mapped to domains above. The InterConnect Framework / Platform Domain does not contain Information Objects yet since use cases focus on devices and actors and not on the related enabling technology.

Not new but important and further to be worked out in tasks T2.5 and T2.4 and with WP3 is energy flexibility. The main concepts are captured: basic energy flexibility patterns, S2 flexibility control types, flex-graphs and traces).

Rather new was the importance of forecasting information. Together with WP3 services (for forecasting), this is something to be developed further during the next phase.

4.3 INTERCONNECT'S SMART HOME AND BUILDING IOT REFERENCE ARCHITECTURE (SHBIRA)

This section introduces InterConnect's Smart Home/Building IoT Reference Architecture (SHBIRA). Its design takes into account the requirements derived from the pilot use cases as well as industry and academia best practices, including applicable standards and protocols. It was derived following the steps previously described in Section 3.5.2.

The architectural viewpoint proposed for the smart home and smart building IoT domain (SHBIRA) is shown in Figure 23. The latter extends existing work, such as the High-Level Architecture (HLA) R4.0 developed by AIOTI, to include the smart grid and energy domains and to offer a logical/functional view of the different components and interfaces in the InterConnect ecosystem.

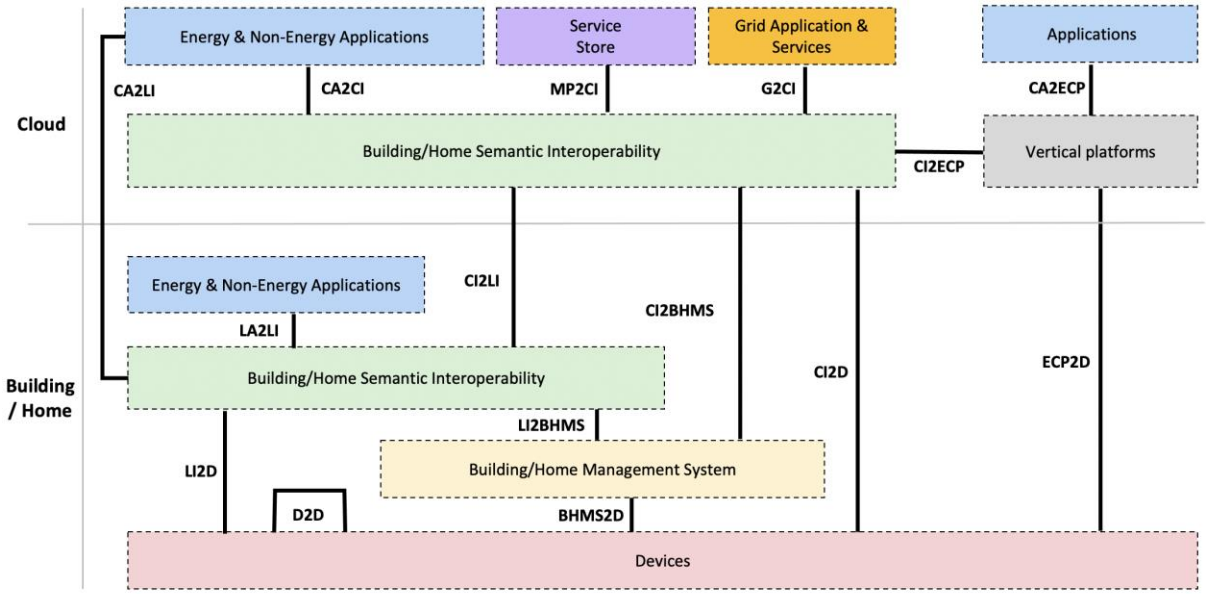


FIGURE 23 – IC'S SMART HOME AND BUILDING IOT REFERENCE ARCHITECTURE (SHBIRA)

The SHBIRA is structured around two domains, depending on where each function resides:

- The **building/home domain**, which groups hardware and software components that are deployed within residential or commercial buildings. These components include appliances, IoT devices and sensors, meters, and software (e.g., building/home energy management system) that run on specific hardware or general-purpose hardware such as a PC or a home gateway. Local communication networks provide the necessary connectivity for those components to exchange data among themselves or connect to

cloud servers via the Internet. While the building/home domain components can operate in an isolated localised manner, they can also connect to a remote cloud-server (located in the cloud domain) for accessing third party energy and non-energy applications. It is generally expected that robust security measures are put in place to protect sensitive (including personal) data and combat cyber-attacks;

- The **cloud domain**, which groups cloud-based systems such as IoT platforms and applications which offer a wide range of energy and non-energy services. Examples of these services include energy efficiency, smart metering, flexibility management, surveillance, amongst others. Typically, hardware and software components, deployed in the edge or central clouds, are responsible for storing and processing data generated from applications. These systems have the advantage of providing highly scalable solutions and address flexibility and adaptability needs of each user.

Within this decomposition, the SHBIRA proposes a layered view for its main architectural components, as shown in Figure 34. It can be detailed as follows:

- The **Device Layer**, consisting of all connected devices and appliances that are deployed in the home and building domain. This layer represents all of the physical hardware (e.g., sensors, actuators, appliances) and related application software that allows devices and appliances to communicate, to share data (e.g., measurements) or receive commands (e.g., demand/response);
- **Building/Home Management Systems (BHMS)** allow to supervise and control appliances and smart devices found within homes and buildings. It may interact with the cloud, e.g., for getting tariffs pertaining to flexibility management and may also include energy management functions;
- The **Building/Home Semantic Interoperability Layer (BHIL)** introduces all of the required functions needed to enable semantic interoperability between devices, applications and services[31]. As such, it represents an instance of the InterConnect Interoperability Framework. The BHIL can either reside locally, i.e., at the home or building level, or remotely in the cloud, depending on the implementation requirements and specifications;
- The **Application Layer**, which communicates with the Building/Home Semantic Interoperability Layer's services to retrieve or send data for the execution of a specific task or use case. Applications, such as home automation and energy efficiency, can be

[31] We define a service (software) component as a software component offering a service via a (digital) interface. A software component can be regarded as an application or part of an application, and it has or represents some functionality. A service (in the real world) is realized by performing some of this functionalities to accomplish a goal with real impact. A software component is hosted on a digital platform. A digital platform can host a service component or not.

instantiated either locally (within the Home/Building Domain) or remotely (within the cloud domain) depending on user needs and service provider preferences. These application instances typically invoke BHIL services, like the Service Store, via APIs.

Moreover, to address the requirements defined by InterConnect (see Section 3.4.), additional components have been included in the SHBIRA, namely:

- **Vertical platforms** and their corresponding **applications** represent any existing cloud-based platform offering a service or domain-specific functionality within the context of the InterConnect project and its partners. Examples include platforms that specifically support Advanced Metering Infrastructure (AMI) applications, or legacy applications made available by one of the project's stakeholders.
- The **Service Marketplace**, which provides a catalogue of all semantically interoperable (SAREF compliant) services in smart building/homes and energy domains. The service store will enable all interoperable digital platforms, services and applications to navigate the ecosystem of available services, integrate and interoperate with IC-regular services (from WP3). The service store will also enable software images of services (e.g., via containers) to be downloaded and instantiated locally. The service marketplace/store was specified within D5.1 [43] and will be implemented during WP5.
- **Grid applications** and their corresponding **services**, provide new tools, mechanisms and ways to improve the capacity of the grid observability for systems operators, market agents and consumers. The applications from and for the grid services are key elements dependent on agnostic data exchange mechanisms (APIs, platforms or others), respecting access, control and compliance according to the GDPR and the different NRA guidelines. The capacity to set and respect standards (such as USEF, ASM Report, CIM, and others) and rules for market-based solutions addressing flexibility provision and/or activation, AMI information and consumer's associated information must respect and enhance the system coordination between TSO, DSO and generic service providers. The actual design and implementation of the Standard DSO Interface is still under discussion in WP4, which started in M13. The second version of this document, due in M36, will provide an update on how these components are embedded into the reference architecture and define all relevant functions & services.

The next section further details all of these layers and components.

4.3.1 FUNCTIONAL LAYERING

4.3.1.1 DEVICE LAYER

The Device Layer consists of all of the physical devices and appliances capable of completing a specific task. These devices interact with their environment by collecting the information provided by embedded sensors, actuators, processors and transceivers and passing them on to the edge of the network or to a remote server for storage and processing. In essence, this layer cumulates four functions:

- **Perception**, which is provided by built-in sensors (e.g., environmental sensors, RFID, location sensors, light sensors, movement sensors) capable of detecting environmental changes or any other relevant information within its reach. Generated data can be collected, combined or inferred from other devices to provide an overview of their surroundings.
- **Actuation**, defined as the ability to mechanically control physical devices and appliances. Actuation requires a control signal (provided by any external entity) and the energy (electric, hydraulic, etc.) to introduce or prevent motion.
- **Pre-processing** consists of processing locally the collected data without excluding further and more centralized processing. Pre-processing refers to data storage, analysis, processing, and filtering. Those functions may be limited depending on the device processing capabilities.
- **Communication or networking** provides transmission of data packets from/to the devices and appliances.

4.3.1.2 BUILDING/HOME MANAGEMENT SYSTEM

This layer generally depicts existing Building and Home Management Systems (BHMS). BHMS are computer-based systems that offer the first layer of interoperability for automating, controlling, and monitoring smart devices and appliances.

In the case of commercial buildings, a Building Management System (BMS) can perform several functions such as managing energy consumption, control user's safety and react to environmental changes (i.e., access control, motion detectors, sensors, alarms, etc.).

Within residential environments, Home Management Systems (HMS) provide comfort and energy efficiency services to users. They are often used to control lighting, occupancy, heating and cooling, window stores, and other home devices/appliances.

For both Building and Home Management Systems, there is not one single technical standard nor technological ecosystem that can facilitate interoperability of installed multi-vendor devices or platforms.

The instantiation of InterConnect's Smart Building/Home Reference Architecture does not require this component to always be present. However, if it exists, it should provide the required interfaces (e.g., APIs, documentation, and credentials) that would allow for interoperability with the Building/Home Semantic Interoperability Layer.

4.3.1.3 BUILDING/HOME SEMANTIC INTEROPERABILITY LAYER

The Building/Home Semantic Interoperability layer provides all of the necessary mechanisms (e.g., smart connectors) and components to facilitate interworking between InterConnect's ecosystem of IoT devices, digital platforms, the energy infrastructure, and energy/non-energy applications.

The Home/Building Semantic Interoperability Layer can be located within the home/building domain, or in the cloud domain:

- The **local-based Building/Home Semantic Interoperability Layer** is deployed within the home/building infrastructure. Typically, users in strategic sectors (e.g., defence, critical infrastructure such as energy or water, amongst others) are expressly concerned with security and may favour on-premises ("local edge cloud") deployments for building's sensitive data. Generally, in these types of scenarios, the data generated by smart buildings can't be exposed to the cloud and needs to be stored and treated on-premises, i.e., hosted by the building's IT infrastructure. The local-based Building/Home Semantic Interoperability Layer serves this purpose. It can interact with the local-based or cloud-based application layer for accessing local and remote applications.
- The **cloud-based Building/Home Semantic Interoperability Layer** is deployed remotely in the cloud. This type of deployment allows for platform functions to run on third-party cloud servers. Data sets exposed by the latter can be discovered by cloud-based applications subject to configured access control. This instantiation of the semantic interoperability layer can interoperate with one or more local-based Building/Home Semantic Interoperability Layers, with specifically configured semantic reasoners and orchestrators, managing what resources and services can interoperate within a building, between multiple buildings and between buildings and smart grid.

This layer should support up to level 4 (of semantic understanding) on the GridWise Interoperability Context-setting Framework (see Section 5.1). This level of interoperability allows for two or more systems to exchange information with the correct syntax (grammatically correct) but can also provide the correct (automatic) interpretation of the meaning of information. These concepts will be further described in Section 5.

Moreover, the Home and Building Semantic Interoperability layer also provides access to InterConnect's ecosystem of interoperable services via the service store. This unlocks services to consider capabilities that are made available by others. Compliance tests and certificates provide the needed assurance while security and cybersecurity protocols guarantees provide the required data boundaries. Moreover, the P2P enablers configure the possibility for services to be made interoperable if they contain a community or distributed orientation. Supporting enablers will provide means to assemble business models and use-cases based on the concept of distributed services accessing data from legacy (now interoperable via InterConnect) services. The key concepts for the design and operation of the interoperability layer are detailed in D5.1 Section 5.1 [43].

4.3.1.4 APPLICATION LAYER

The Application layer contains the set of application instances implementing a certain ‘business’ logic, i.e., functions and custom IoT applications offering a specific service to users.

Resources within the Application Layer can interact with the Building/Home Interoperability layer via standardized APIs, including SAREF-based interfaces. Services offered at this level include data visualization, data analytics, fault detection, and building automation.

This layer will become the layer where a majority of the software services will live, and also where most of the generic adapters will integrate the services and digital platforms they will attach to. Further details and links with the technical architecture of the interoperability layer are provided in D5.1 Section 5.2.2 [43].

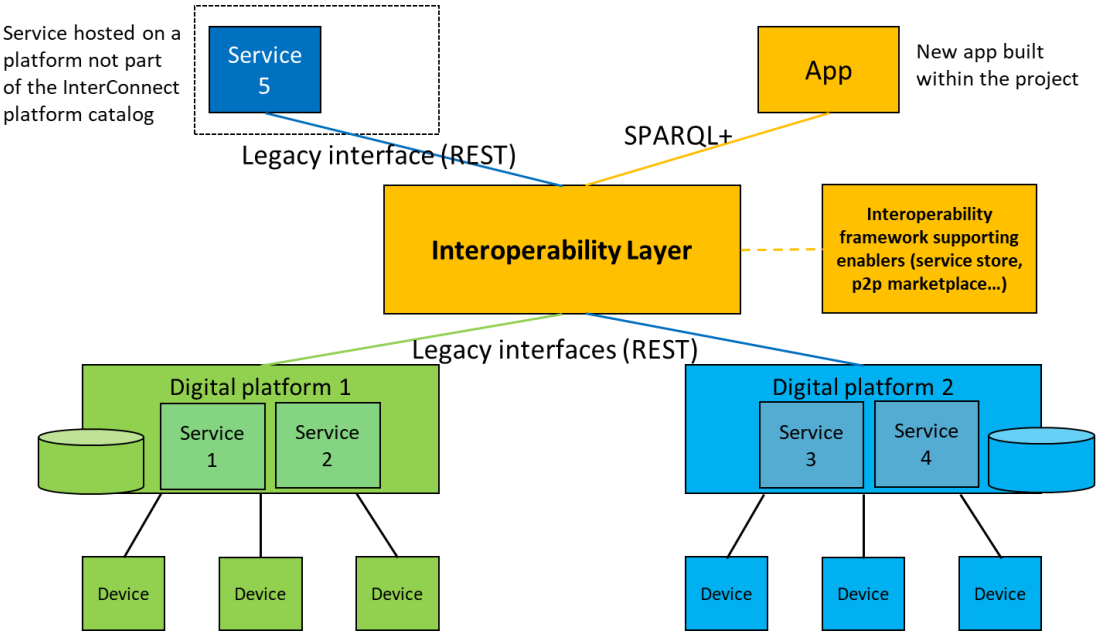


FIGURE 24 – SEMANTIC INTEROPERABILITY LAYER IN CONTEXT OF A TYPICAL PILOT ARCHITECTURE

Figure 24 shows a typical pilot ecosystem comprising:

- Two different **digital platforms**, each with its own set of services[32], managed devices and interfaces;
- A **service** running on a platform that might not be part of the InterConnect digital platform catalogue;
- **Application** (i.e., web or mobile) developed for a project use case and utilizing the interoperable services (not necessarily providing additional services);
- The **IC interoperability framework,** where specific focus is put onto the IC semantic interoperability layer. Here the IC semantic interoperability layer is showcased as a centralized layer/architecture component responsible for bridging/interconnecting services, applications and platforms all utilizing different communication interface technologies/protocols/ standards.

Although services highlighted in Figure 24 can also depict the device and building/home management system layer, the vast majority as a software service will be placed the application layer level.

[32] For the definition of services, please refer to Footnote 31.

4.3.1.5 SERVICE STORE

The Service Store system is specific to InterConnect. It provides a comprehensive catalogue of all interoperable services from the smart home/building and energy domains. The service store also provides a set of generic services (e.g., for data analysis, weather forecast). In order to be featured in the service catalogue, a service needs to be made SAREF-compliant and exposed through the unified interface provided by the InterConnect interoperability framework.

Services can be provided by interoperable digital platforms featured in the project pilots or can be provided as standalone services developed/adapted by project partners. WP3 will be responsible for the SAREF-ization of all services, and WP5 will build service store backend and frontend. Services featured in the service store will be accessible through unified interfaces and interconnected with the InterConnect interoperability layer.

The service store will be specified and implemented in the WP5 (T5.1 responsible for specification and T5.2 responsible for implementation). Further details are provided in D5.1 Section 5.3 [43].

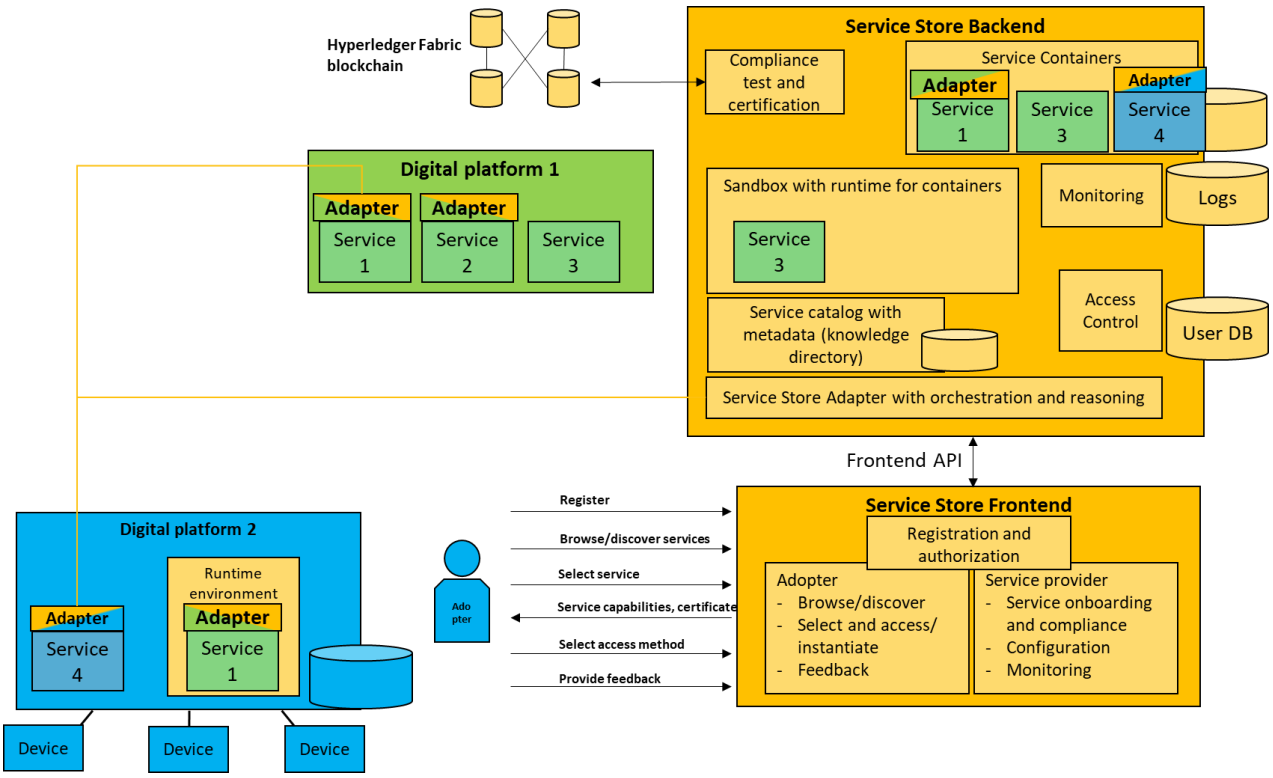


FIGURE 25 – IC SERVICE STORE FUNCTIONAL ARCHITECTURE AND FUNCTIONALITIES

4.3.1.6 KEY FUNCTIONS & COMPONENTS

In this section, key functionalities of a SHBIRA instance (e.g., in project pilots/use cases) are presented. SHBIRA instantiations across already established pilot architectures (e.g., digital platforms, services and resources/devices provided by participating stakeholders) are enabled with properly instantiated and configured building/home semantic interoperability layer. The Building/Home Semantic Interoperability Layer can be established across one or more platforms provided by InterConnect's participating partners. The semantic interoperability layer is instantiated with semantic interoperability enablers (e.g., adapters and smart connectors) deployed on digital platforms. Each digital platform participating in an instantiated SHBIRA provides a set of services (e.g., energy and non-energy services/CCC) and other resources (e.g., data points like devices or edge gateways) which can be made interoperable with properly configured interoperability adapter[33]. Thus, the set of functions and components offered within an instance of SHBIRA will be specified during pilot deployment and will depend on the specific requirements detailed by the Use Cases defined in WP1. Each instance will also have access to InterConnect Service Store, which lists all interoperable services from within and outside of the pilot (from all project pilots and third parties).

Thus, each pilot will potentially produce a different instantiation of the SHBIRA and Building/Home Semantic Interoperability Layer, based on common principles and guidelines defined in this Section and in Section 5 of this document, and further detailed in WP5 and WP3. The following functionalities can be part of a SHBIRA instance (pilot or use case centric)[34]:

- **Data access provision**, responsible for exposing APIs using standard communication protocols (e.g., RESTful, MQTT, SPINE, web sockets). Data herein exposed can be consumed by any platform (including local-based clients) or made available for third-party services by following specified access control rules and privacy protection directives imposed by hosting digital platform or the InterConnect Interoperability Framework;
- **Security and privacy functions**, which provide the necessary tools for safeguarding valuable information assets and comply with business and state regulations. Authentication and authorization mechanisms for users and services (e.g., through

[33] See Section 5 for more details on the interoperability adapters.

[34] This list does not intend to be exhaustive; further refinement will be provided in the scope of WP3 and WP5.

APIs) are a part of this functional group. Access control rules (e.g., role or attribute-based) for specific services or resources provided by a digital platform are an important part of overall security and privacy protection framework established within the instantiated semantic interoperability layer. The semantic interoperability framework should enforce access control rules and privacy sensitivity labelling of data points and attributes within complex data models;

- **Discovery**, defined as a set of software services and network functions that allow for automatic detection of IoT devices, appliances and services. Discovery services considerably reduce configuration efforts by allowing to invoke third-party services with little effort from users. These discovery services will utilize the semantic reasoning capabilities provided by the semantic interoperability layer;
- **South and Northbound interworking**, which supports the inclusion of software "connectors" to include legacy equipment in Smart Buildings, with no interruption of existing Building Operating Systems (BOS). Connectors allow integration of virtually any device, automation server or connectivity network to any enterprise application. They offer the flexibility, through few clicks, needed to integrate endpoints without costly system integration;
- **Data management**, which consists of handling and formatting data explicitly provided by services, devices, end-users' applications and digital platforms. Data processors perform data collection, while data controllers manage access rights and privacy protection.
- **Data transformation**, which allows for the conversion of data into a unified format. The unified data model (for InterConnect project it is based on SAREF ontology, which will describe all the relevant concepts, attributes and interactions within a building, including device taxonomy, measurement and command types, alarm and default categories, locations (e.g., buildings, floors, rooms, etc.), labels, payloads, and other contextual information. A common ontology (e.g., SAREF) is implemented at this stage. Semantic enrichment can enrich data contextualization, for example, by allowing devices to communicate their exact location within a building (Building Information Modelling or BIM);
- **Building Information Modelling (BIM) / Digital Twin**, which can be defined as a digital representation of physical and functional characteristics of a building or a home. Data generated is commonly stored as a model from which information can be extracted or exchanged with other entities, to support the decision from stakeholders. This functionality will/should adopt common data models and modelling techniques represented in the applied ontology standard (e.g., SAREF);

- **Data Abstraction** allows the explicit description of data to be machine-understandable and is compliant with the unified data model (e.g., SAREF);
- **Semantic Enrichment**, by which means the unified data is annotated with additional classes of metadata that can further improve the utility, discovery, and interoperability of content using tagging, mark-up, classification, and categorization techniques;
- **Orchestration**, which is responsible for facilitating data exchange between data sources, data consumers and action/control providers while following an established set of rules (protocol) and adhering to the defined data models. This functionality is part of each service and application, and it will be accomplished in a semantically interoperable manner with the interoperability layer and a network of interoperability adapters and connectors;
- **Data analysis and decision making**, these functionalities implement the main logic behind energy and non-energy/CCC services which rely on collected data set to derive specific actions for other services, for devices and end-users. Data analysis performs mathematical/statistical operations on collected data sets and can also rely on machine learning models to derive specific conclusions about the data or relationships between entities represented by data. Based on data analysis results, reactive and proactive decision making can be configured in support of the main operational protocols and use case logic;
- **Command and control**, functionalities which enable services to perform specific actions on data points, devices, and towards end-user's applications based on collected and analysed data and decision-making logic. Digital platforms which manage devices and complex systems comprising multiple devices and services should enable support action/command/control propagation and execution (e.g., remote control of HVAC systems);
- **Recommendations and predictions**, which are a subset of data analysis functionalities. These procedures are based on advanced machine learning models with the specific role of providing various recommendation on how the system should be used (based on a predefined set of constraints and objectives/targets) and predictions/forecasts on how system/resource might behave in a specific period or moment;
- **Conflict resolution**, set of functionalities for imposing rules in situations where multiple control points compete for managing devices/processes/resources. Semantic reasoning should provide a certain level of conflict resolution;
- **Device Management**, by which means an IoT device or appliance can be remotely controlled and monitored. Device management requires that all devices are configured using a unified standard supporting a common set of applications and functions;

- **System monitoring**, a set of functionalities combining data collection and analysis procedures for assessing status and performance of system components and the system as a whole;
- **System administration**, set of functions for adapting/updating/maintaining system operation within defined performance constraints in (semi)automated manner - based on system monitoring and with a specific set of decision-making procedures.

Listed functionalities (or a sub-set of them) of the SHBIRA instances (comprising digital platforms, services, devices and semantic interoperability layer) can be deployed on devices, edge (e.g., IoT gateway or controller), fog (e.g., local servers and data stations) and cloud system layers. Each SHBIRA instance will feature a subset (or complete set) of presented functionalities. Additional functionalities might be identified as project technical tasks and pilots/use cases progress in their specification and developments.

4.3.2 INTERFACES

Interfaces represent the shared boundaries that two or more separate components use to exchange upstream, downstream, and contextual information, exposed via publish/subscribe and/or request/response protocols. Below, a brief description of interfaces depicted in the SHBIRA.

- **D2D (Devices to Devices):** Communication between two devices crosses the D2D interface. These flows allow devices to exchange data or trigger commands among themselves, without involving other entities at the application level. Device-to-device interfaces are commonly used for local services (i.e., proximity services), emergency communications (i.e., possible lack of reliance of the traditional network) and for within IoT networks. This type of interface is commonly limited to single-vendor or interoperable ecosystems, where all connected devices are capable of communicating via a common semantic model. D2D communications are not within the scope of the InterConnect project and is depicted for completeness purposes only;
- **BHMS2D (Building/Home Management System to Devices):** Communication between devices and the Building/Home Management system crosses the BHMS2D interface. These flows allow each device entity to exchange information with the existing BHMS, to display, monitor and control each node regardless of the particular service they perform. BHMS2D communications are outside the scope of the InterConnect project;

- **LI2D (Local Building/Home Semantic Interoperability Layer to Devices):** Communication between the local Building/Home Semantic Interoperability Layer and devices crosses the LI2D interface. These flows allow devices to exchange upstream, downstream and contextual information to/from the local Building/Home Semantic Interoperability Layer. Within the latter, a set of technology-specific connectors (smart connectors) will provide the necessary translation from/to specific data models provided by the devices and InterConnect's Semantic Interoperability Layer. The InterConnect project covers LI2D communications;
- **CI2D (Cloud Building/Home Semantic Interoperability Layer to Devices):** Communication between the cloud-domain Building/Home Semantic Interoperability Layer and devices crosses the CI2D Interface. These flows allow devices to exchange upstream, downstream and contextual information from/to the cloud-based Building/Home Semantic Interoperability Layer. Within the latter, a set of technology-specific connectors (smart connectors) will provide the necessary translation from/to specific data models provided by the devices and InterConnect's Semantic Interoperability Layer;
- **LI2BHMS (Local Building/Home Semantic Interoperability Layer to Building/Home Management System):** Communication between the local-domain Building/Home Semantic Interoperability Layer and existing Building/Home Management systems crosses the LI2BHMS Interface. These flows allow existing BHMS platforms to exchange information from/to the local-based Building/Home Semantic Interoperability Layer. Within the latter, a set of technology-specific connectors (smart connectors) will provide the necessary translation from/to specific data models provided by the devices and InterConnect's Semantic Interoperability Layer. The InterConnect project covers LI2BHMS communications;
- **LA2LI (Local Energy & Non-Energy Application Layer to Local Building/Home Semantic Interoperability Layer):** Communication between the local-domain energy & non-energy applications and the local-domain Semantic Interoperability Layer crosses the LA2LI interface. These flows allow applications and other resources to exchange information from/to the Semantic Interoperability Layer via a standardized SAREF-based interface. The InterConnect project covers LA2LI communications;
- **CI2LI (Cloud Building/Home Semantic Interoperability Layer to Local Building/Home Semantic Interoperability Layer):** Communication between the cloud-domain Semantic Interoperability Layer and the local-domain Semantic Interoperability Layer crosses the CI2LI interface. These flows allow local-domain platform functions to interact with cloud-hosted platform functions, via a standardized SAREF-based interface. Data exposed by this interface opens access to cloud-hosted

applications and services offered by the InterConnect project. The InterConnect project covers CI2LI communications;

- **CI2BHMS (Cloud Building/Home Semantic Interoperability Layer to Building/Home Management System):** Communication between the cloud-domain Semantic Interoperability Layer and the Building/Home Management System crosses the CI2BHMS interface. These flows allow existing BHMS platforms to exchange information from/to the cloud-domain Building/Home Semantic Interoperability Layer. Within the latter, a set of technology-specific connectors (smart connectors) will provide the necessary translation from/to specific data models provided by the devices and InterConnect's Semantic Interoperability Layer. The InterConnect project covers CI2BHMS communications;
- **CI2D (Cloud Building/Home Semantic Interoperability Layer to Devices):** Communication between the cloud-domain Semantic Interoperability Layer and devices crosses the CI2BHMS interface. These flows allow devices to exchange upstream, downstream and contextual information from/to the cloud-based Semantic Interoperability Layer. Within the latter, a set of technology-specific connectors (smart connectors) will provide the necessary translation from/to specific data models provided by the devices and InterConnect's Semantic Interoperability Layer. The InterConnect project covers CI2D communications;
- **CA2LI (Cloud Energy & Non-Energy Applications to Local Building/Home Semantic Interoperability Layer):** Communication between the cloud-domain energy & non-energy applications and the local-domain Semantic Interoperability Layer crosses the CA2LI interface. These flows allow applications and other resources to exchange information from/to the Interoperability Layer via a standardized SAREF-based interface and interworking proxies (smart connectors). The InterConnect project covers LA2LI communications;
- **CA2CI (Cloud Energy & Non-Energy Applications to Cloud Building/Home Semantic Interoperability Layer):** Communication between the cloud-domain energy & non-energy applications and the cloud-domain Semantic Interoperability Layer crosses the CA2CI interface. These flows allow applications and other resources to exchange information from/to the Interoperability Layer via a standardized SAREF-based interface. The InterConnect project covers CA2LI communications;
- **MP2CI (Service Store to Cloud Building/Home Semantic Interoperability Layer):** Communication between InterConnect's Service Store and the cloud-domain Semantic Interoperability Layer crosses the MP2CI interface. These flows allow third-party and stakeholders to access the marketplace toolbox and establish cross-platform

functionalities via a standardized SAREF-based interface. The InterConnect project covers MP2CI communications;

- **G2CI (Grid Applications & Services to Cloud Building/Home Semantic Interoperability Layer):** Communication between InterConnect's Service Marketplace and the cloud-domain Semantic Interoperability Layer crosses the G2CI interface. These flows allow grid operators, energy and non-energy service providers, market platforms and stakeholders to access the marketplace toolbox and establish cross-platform functionalities via standardized DSO interface. The InterConnect project covers G2CI communications;
- **CA2ECP (Cloud Applications to Existing Cloud Platforms):** Communication between existing cloud platforms[35] and their associated applications crosses the CA2ECP interface. These flows allow applications and other resources to exchange information from/to the cloud platforms via proprietary or non-standardised interfaces. CA2ECP communications are outside the scope of the InterConnect project;
- **CI2ECP (Cloud Building/Home Semantic Interoperability Layer to Existing Cloud Platforms):** Communication between existing cloud platforms and the cloud-domain Semantic Interoperability Layer crosses the CI2ECP interface. These flows allow existing cloud backend services to access the project tools/enablers and establish cross-platform functionalities via a standardized SAREF-based interface. The InterConnect project covers CI2ECP communications;
- **ECP2D (Existing Cloud Platforms to Devices)**: Communication between devices and existing cloud platforms crosses the ECP2D interface. These flows allow devices to exchange upstream, downstream and contextual information from/to existing cloud backend services. ECP2S communications are outside the scope of the InterConnect project.

4.3.2.1 INFORMATION FLOWS

The message flow examples introduced in this section aim to provide a generic description of the communication behavior that typically occurs via message interchange between the different architectural components of the High Level Architecture. The specific symbols that are introduced in these examples can be interpreted as follows:

- **Message exchanges** are depicted as horizontal arrows. These messages can either serve as a basis for exchanging meta-data (i.e., for device discovery and reasoning),

[35] Existing cloud platforms will be made in some cases available by project partners and/or third parties, outside of the Consortium, for the realisation of a pilot's use cases. See Section 0 for more details on this.

core-data (i.e., payloads), or actionable commands (i.e., command and control of devices). In each case, the type of message being transmitted is indicated immediately above the horizontal arrows;

- **Reply (acknowledgement)** messages are represented as dashed arrows;
- Each **entity** (i.e., architectural component) is represented as a box at the top of a vertical line, representing the message exchange lifeline.

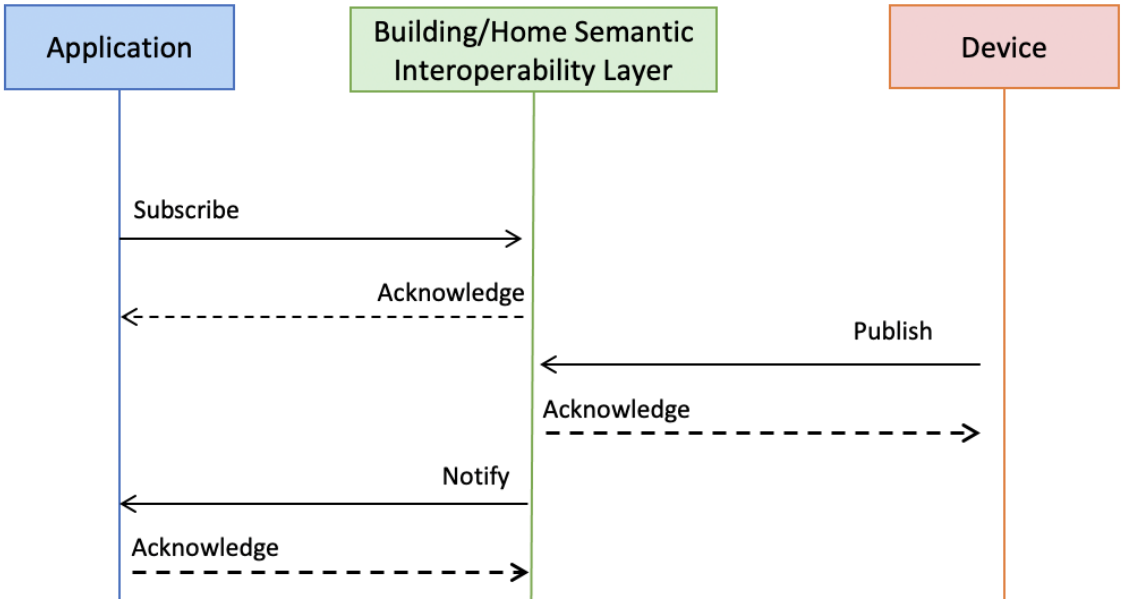


FIGURE 26 – MESSAGE FLOW EXAMPLE FOR PUBLISH/SUBSCRIPTION MESSAGING BETWEEN ENTITIES

Figure 26 depicts a generic example of message transmission that can take place between the following entities:

- **Application to Building/Home Semantic Interoperability Layer:** in this case, an application subscribes to one or more devices registered in the Building/Home Interoperability Layer, which in turn returns an acknowledgment message to the application.
- **Device/ Building/Home Semantic Interoperability Layer:** registered devices publish new information (e.g., measurement, state, etc.) to the Building/Home Interoperability Layer.
- **Building/Home Semantic Interoperability Layer/Application:** Notification to (subscribed) application to indicate that a change has occurred.

Table 20 provides a brief description of the interfaces covered by these three interactions.

Interface	What does it cover?
CA2CI to CI2D	Cloud-based applications interacting with the cloud-based Building/Home Semantic Interoperability Layer that communicates with registered devices found within buildings and homes
CA2LI to CLI2D	Cloud-based applications interacting with the local-based Building/Home Semantic Interoperability Layer that communicates with registered devices found within buildings and homes
LA2LI to LI2D	Local-based applications interacting with the local-based Building/Home Semantic Interoperability Layer that communicates with registered devices found within buildings and homes

TABLE 20 – DESCRIPTION OF INTERFACES COVERED BY THE MESSAGE FLOW EXAMPLE

Figure 27 includes a new entity representing an existing Building/Home Management system, introducing the following additional message transmission between these entities:

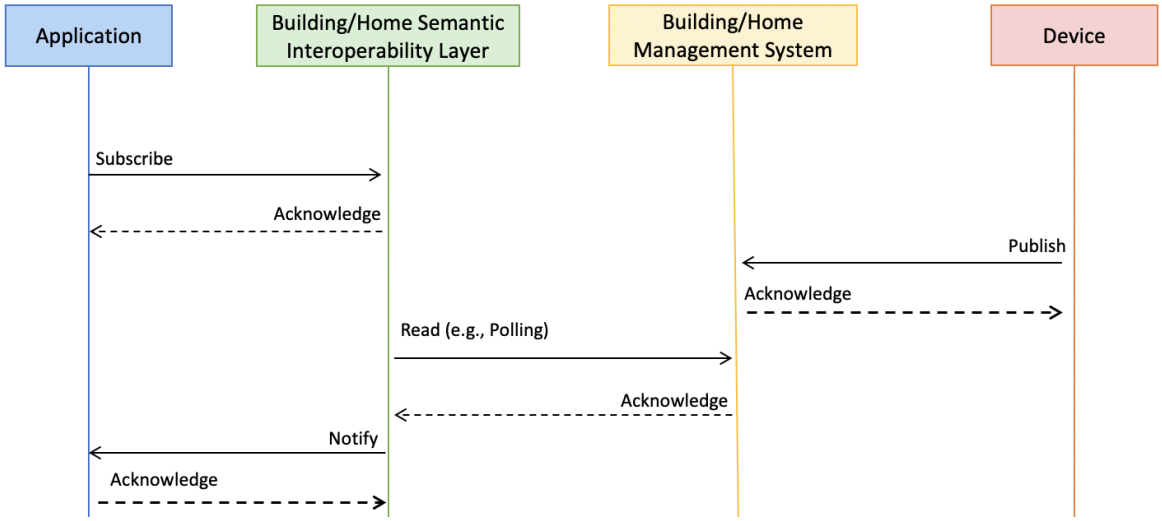


FIGURE 27 – MESSAGE FLOW EXAMPLE FOR PUBLISH/SUBSCRIPTION MESSAGING PATTERN BETWEEN ENTITIES

- **Building/Home Semantic Interoperability Layer/Building Home Management System:** The interoperability layer will actively check the status of the device as provided by the existing Building/Home management system (i.e., polling). If (when) a state change is detected, the interoperability layer will proceed - as in the previous example - to notify the application, that will send in exchange a reply or acknowledgement.

Table 21 provides a brief description of the interfaces covered by these interactions.

Interface	What does it cover?
CA2CI to CI2BHMS to BHMS2D	Cloud-based applications interacting with the cloud-based Building/Home Semantic Interoperability Layer. The latter interfaces with existing BHMS regrouping various registered devices found within buildings and homes
CA2LI to LI2BHMS to BHMS2D	Cloud-based applications interacting with the local-based Building/Home Semantic Interoperability Layer. The latter interfaces with existing BHMS regrouping various registered devices found within buildings and homes
LA2LI to LI2BHMS to BHMS2D	Local-based applications interacting with the local-based Building/Home Semantic Interoperability Layer. The latter interfaces with existing BHMS regrouping various registered devices found within buildings and homes.

TABLE 21 – DESCRIPTION OF INTERFACES COVERED BY THE MESSAGE FLOW EXAMPLE

Figure 28 describes the different message transmissions that take place between the previous entities and an existing vertical platform:

- **Vertical platform/Building/Home Interoperability Layer:** in this scenario, the vertical platform provides the necessary mechanisms to notify the interoperability layer if (when) changes are detected in registered devices. As in the previous example, the interoperability layer then notifies the application that returns an acknowledgement reply message.

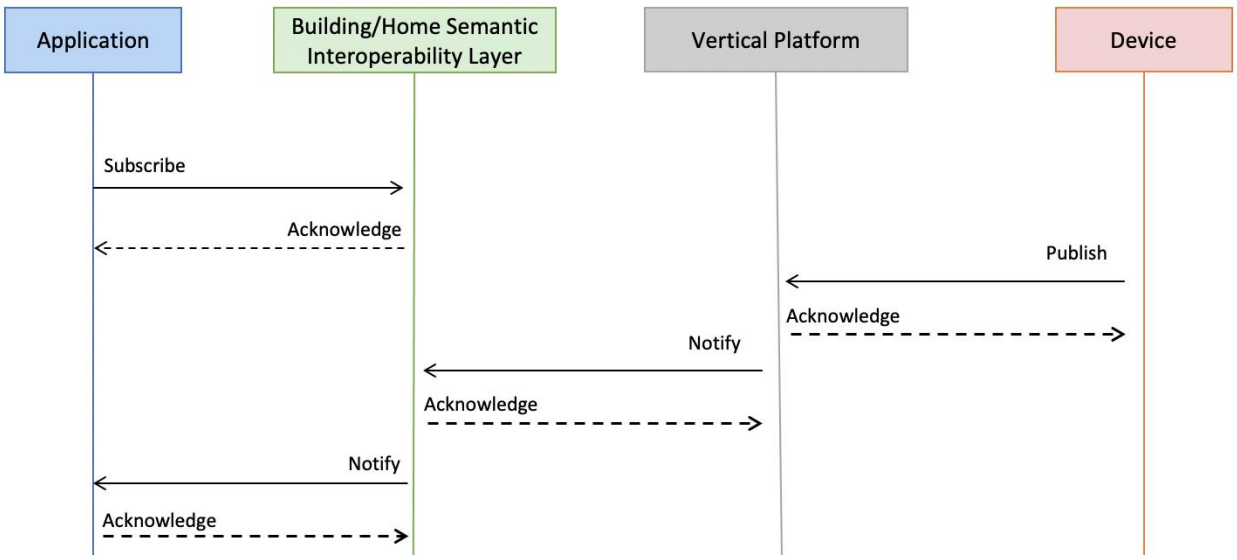


FIGURE 28 – MESSAGE FLOW EXAMPLE FOR PUBLISH/SUBSCRIPTION MESSAGING PATTERN BETWEEN ENTITIES

Table 22 provides a brief description of the interface covered by these interactions.

Interface	What does it cover?
CA2CI to CI2ECP to ECP2D	Cloud-based applications interacting with the cloud-based Building/Home Semantic Interoperability Layer. The latter interfaces with existing vertical platforms regrouping various registered devices found within buildings and homes

TABLE 22 – DESCRIPTION OF INTERFACES COVERED BY THE MESSAGE FLOW EXAMPLE

Figure 29 provides an overview of the different message transmissions that take place between the previous entities and a cloud-, local-interoperability layer, alongside an existing Building/Home Management System:

- **Cloud-based Building/Home Interoperability Layer/ Local-based Building/Home Interoperability Layer:** in this case, the cloud-based interoperability layer subscribes to one or more devices registered in the local-based Building/Home Interoperability Layer, which in turn returns an acknowledgement message.
- **Local-based Building/Home Interoperability Layer/ Building/Home Management System:** the local-based interoperability layer will actively check the status of the device as provided by the existing Building/Home management system (i.e., polling). If (when) a state change is detected, the local-based interoperability layer will proceed - as in the previous example - to notify the cloud-based interoperability layer, that will send in exchange a reply or acknowledgement.

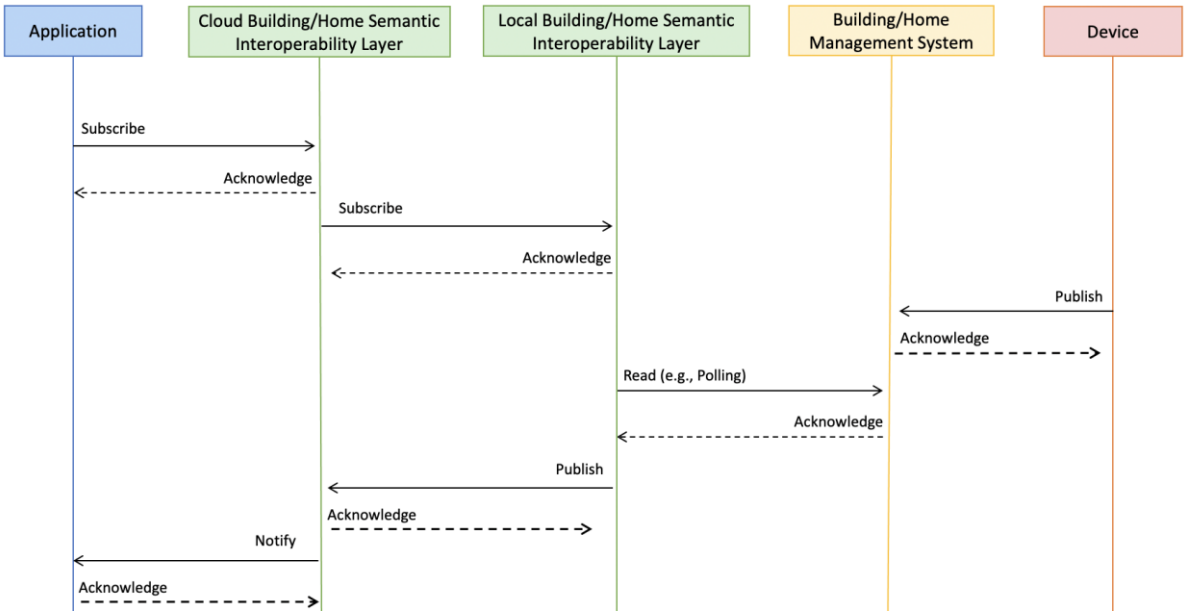


FIGURE 29 – MESSAGE FLOW EXAMPLE FOR PUBLISH/SUBSCRIPTION MESSAGING PATTERN BETWEEN ENTITIES

Interface	What does it cover?
CA2CI to CI2LI à LI2BHMS to BHMS2D	Cloud-based applications interacting with the cloud-based Building/Home Semantic Interoperability Layer. The latter interfaces with existing local-based Building/Home Semantic Interoperability Layer and existing BHMS, regrouping various registered devices found within buildings and homes

Table 23 provides a brief description of the interface covered by these interactions.

Interface	What does it cover?
CA2CI to CI2LI à LI2BHMS to BHMS2D	Cloud-based applications interacting with the cloud-based Building/Home Semantic Interoperability Layer. The latter interfaces with existing local-based Building/Home Semantic Interoperability Layer and existing BHMS, regrouping various registered devices found within buildings and homes

TABLE 23 – DESCRIPTION OF INTERFACES COVERED BY THE MESSAGE FLOW EXAMPLE

All of the previous examples described the core-data message exchanges that can occur between the different entities described by the high-level architecture. Figure 30 and Figure 31 describe the case of actionable commands (i.e., command and control) where an application pushes a demand to update the device state via the interoperability layer. The device replies with an acknowledgement message, to indicate that the command has been executed.

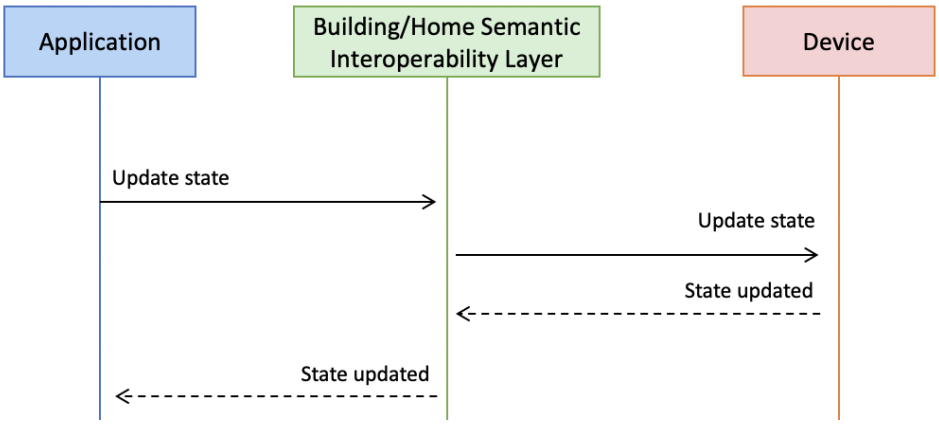


FIGURE 30 – MESSAGE FLOW EXAMPLE FOR ACTIONABLE COMMANDS

In Figure 31, the Building/Home Management System is introduced to depict the usage of generic/standardized (e.g., SAREF/SPARQL+) and specific (e.g., HTTP) messaging protocols for controlling existing devices.

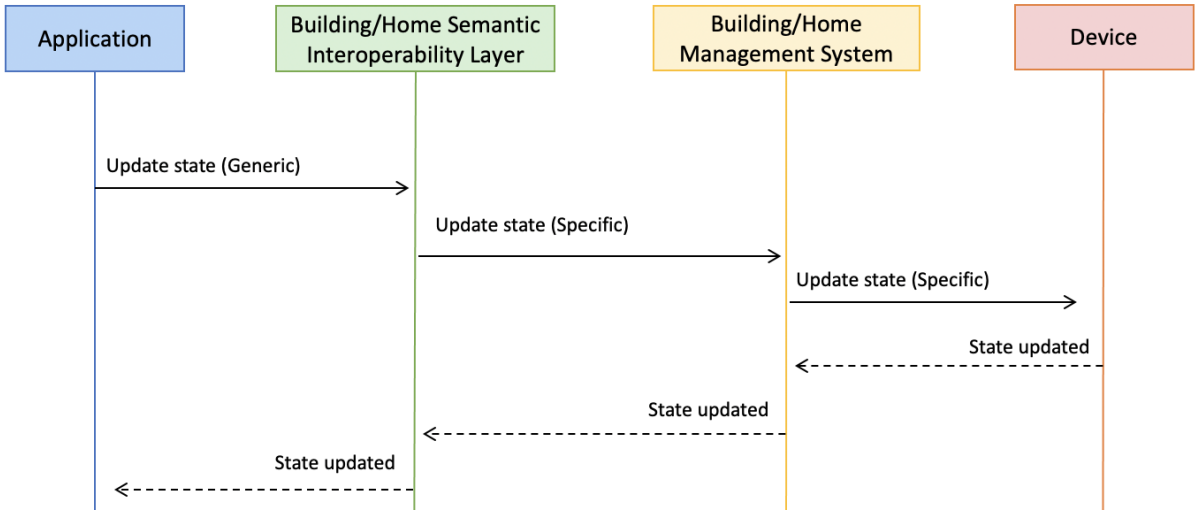


FIGURE 31 – MESSAGE FLOW EXAMPLE FOR ACTIONABLE COMMANDS FOR SPECIFIC/GENERIC MESSAGING PROTOCOLS

Lastly, Figure 32 covers the meta-data message flows between the application, Building/Home Interoperability and device entities. In this scenario, devices register to the semantic interoperability layer, which then sends a reply to the device that acknowledges its registration. Applications are then able to discover registered devices within the interoperability layer, that sends a reply message containing the device's meta-data

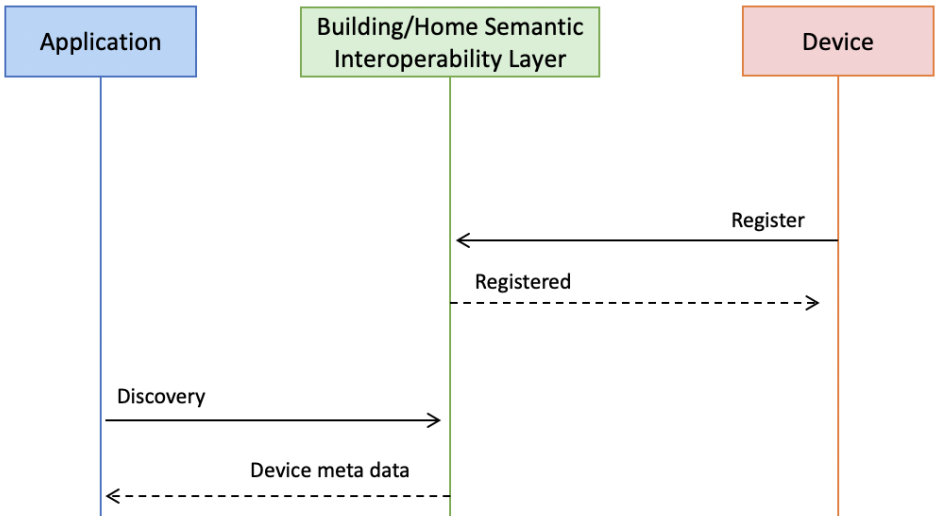


FIGURE 32 – MESSAGE FLOW EXAMPLE FOR META-DATA EXCHANGE

Deliverable D5.2 [44] provides more detailed message flow diagrams with focus on the role of semantic interoperability layer and semantic interoperability adapter in data exchange between interoperable endpoints and in the scope of the InterConnect service store.

4.3.2.2 INTERFACES TYPOLOGY

4.3.2.2.1 TYPOLOGY UNIFIED/INTERWORKING/SPECIFIC

This typology allows us to categorize interfaces into 'Unified' (e.g., SPARQL+/SAREF), interworking proxies (i.e., smart connectors) or vendor-specific interfaces, outside of the scope of the InterConnect project.

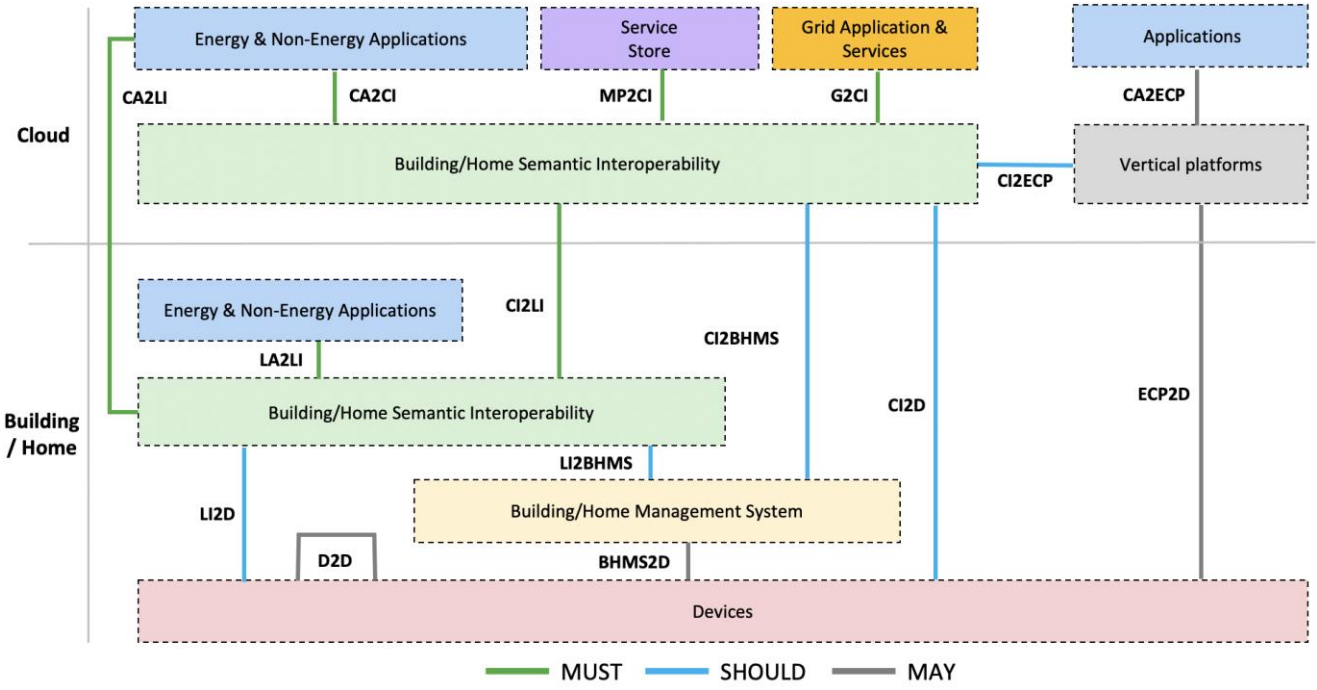


FIGURE 33 – TYPOLOGY UNIFIED/INTERWORKING/SPECIFIC

4.3.2.2.2 TYPOLOGY MUST/SHOULD/MAY

This typology offers a view of the interfaces that must /should /may be provided during the architecture's instantiation. "MUST" interfaces necessarily exist in all pilot site's deployments and need to be proposed by the InterConnect Interoperability Framework either through unified interfaces (e.g., SPARQL+/SAREF) or interworking proxies. "SHOULD" interfaces can exist in specific pilot site's deployments and should be proposed by the IC Interoperability Framework using the same methods that "MUST" interfaces employ. "MAY" interfaces represent components that may exist on one pilot site deployment but not in others, mostly related to

local-based legacy Building/Home Management Systems and devices, and their interaction with the cloud-based Building/Home Interoperability Platform.

These interfaces will mostly be covered through interworking proxies, capable of translating specific data models to InterConnect's common semantic model. Finally, vertical platforms and dependant vertical applications are represented in this figure as out of scope.

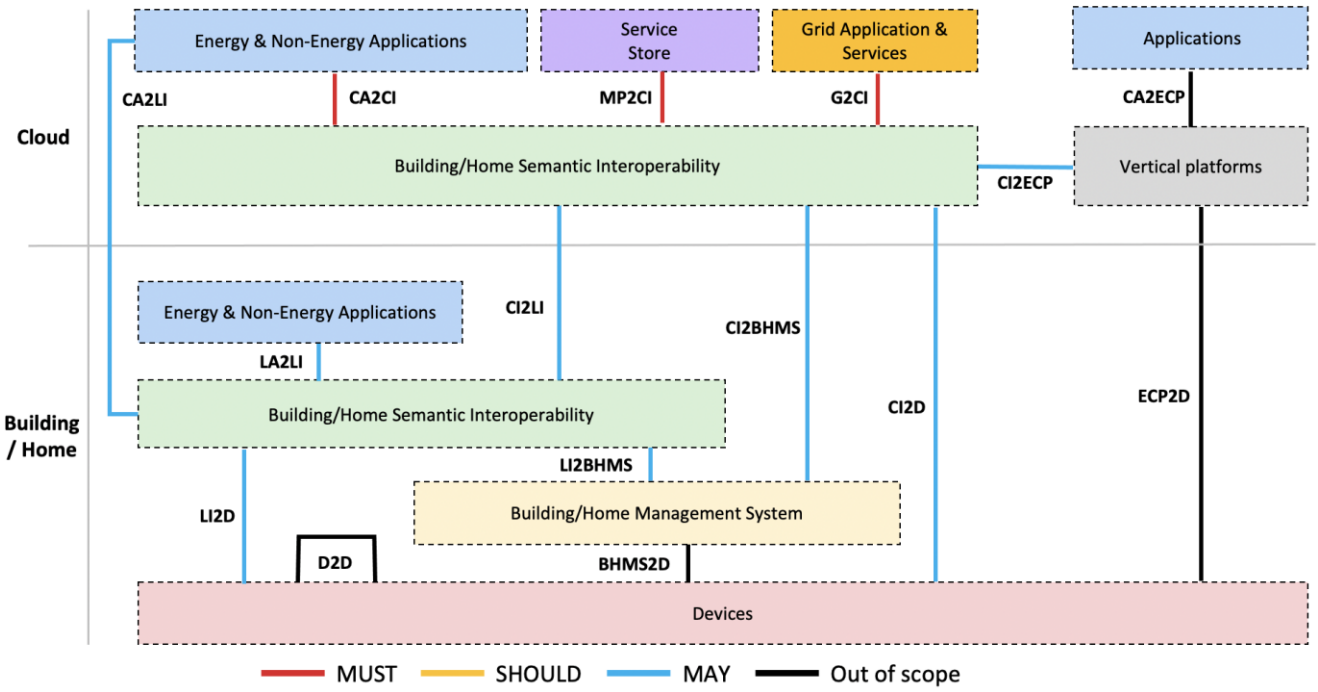


FIGURE 34 – TYPOLOGY MUST/SHOULD/MAY

4.3.2.2.3 TYPOLOGY INTERACTING ENTITIES

This typology offers a view that allows us to categorize interfaces that provide similar functioning. In this case, we can denote four types of interfaces: local-, cloud-domain apps to local-, cloud-domain interoperability platform; local-, cloud-domain interoperability platform to devices, local-, cloud-domain Interoperability platform to existing Building/Home Management Systems, and others, covering specific interfaces such as the service marketplace and grid interfaces to the Interoperability platform, and the interfaces provided by cloud-domain vertical platforms and vertical applications to devices and to the Semantic Interoperability Layer.

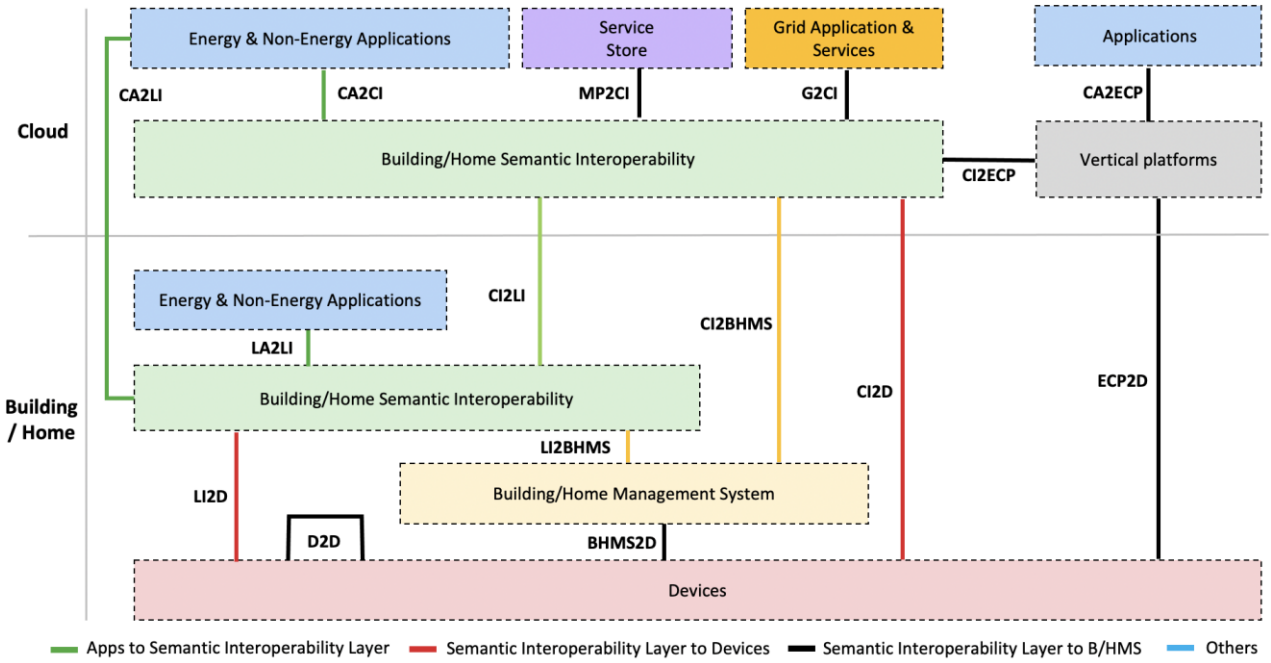


FIGURE 35 – TYPOLOGY INTERACTING INTERFACES

4.3.3 INTEROPERABILITY MAPPING GUIDELINES

This section discusses the set of guidelines designed to aid mapping any new service to the SHBIRA. The latter is mainly split into two large dimensions, the home and building dimension and the cloud dimension. A service, that is, the offering of a certain functionality from one to another entity or component, can be spread into both dimensions and does not necessarily requires to be isolated. This is a first crucial step to promote the mapping process into the SHBIRA.

The set of guidelines is presented in Table 24.

Step	Description	Action
Service type	The type of service will allow to map it to the cloud or building/home layer, or both.	Map the service to the cloud, building/home or both layers.
Vertical service	A vertical service requires multiple layer objects from the home/building and cloud layers	Identify which layer objects does the service needs.
EMS system service	The service relates to EMS Gateway functionalities	Map the service to the Building/Home Management System. If there are digital twin

		services, map it to the application object in the cloud layer.
Grid services	Services provided from the DSO or grid stakeholders for smart home and building features. Grid specific services are mapped according to the SERA.	Grid services are mapped to the grid object in the cloud layer.
Interfaces	The selected interfaces will be the basis for message flows between layer objects.	Map the needed interfaces required between layer objects.
Message Flows	The message flows link the interfaces and messages between object layers	Establish the message flows between layer objects.
Interoperability	The need for interoperability will establish service interoperability and exposed capabilities	Identify the interoperability features (to consume from other parties and to expose to other parties) that the service provides.

TABLE 24 – SMART BUILDING/HOME INTEROPERABILITY GUIDELINES [43]

The technical specification should consider the inner components of the interoperability layer according to the detail provided in the scope of WP5, namely via D5.1 [43].

4.4 INTERCONNECT'S INTEROPERABILITY FRAMEWORK ARCHITECTURE

Each project pilot comprises a set of digital platforms, services, applications, devices and other resources provided by participating partners. The InterConnect Interoperability Framework enables semantic interoperability of all participating digital platforms, providing energy and non-energy services (control, comfort and convenience) and devices, thus ensuring proper instantiation of the SHBIRA across pilots infrastructures.

Some functional layers of the SHBIRA are already represented in the digital platforms provided by project partners for the realization of the pilots and use cases. Especially in platforms which provide vertical solutions for individual or multiple smart buildings. What is missing in most cases is interoperability achieved in a unified way and not per-interface/service type. In order to enable instantiation of the reference architecture on digital platforms and other endpoints constituting the project use cases, the InterConnect is introducing the Interoperability Framework.

The Interoperability Framework enables digital platforms with standard, or custom architecture to interoperate with other platforms and get access to additional services and data streams necessary for building innovative use cases and applications.

The overall functional architecture of the InterConnect Interoperability Framework is shown in Figure 36. The central component is the semantic interoperability layer which interconnects existing digital platforms, and services they offer, among themselves and with the interoperability framework services (service store, P2P marketplaces, compliance certification, data protection and access control and supporting services for production-level operation).

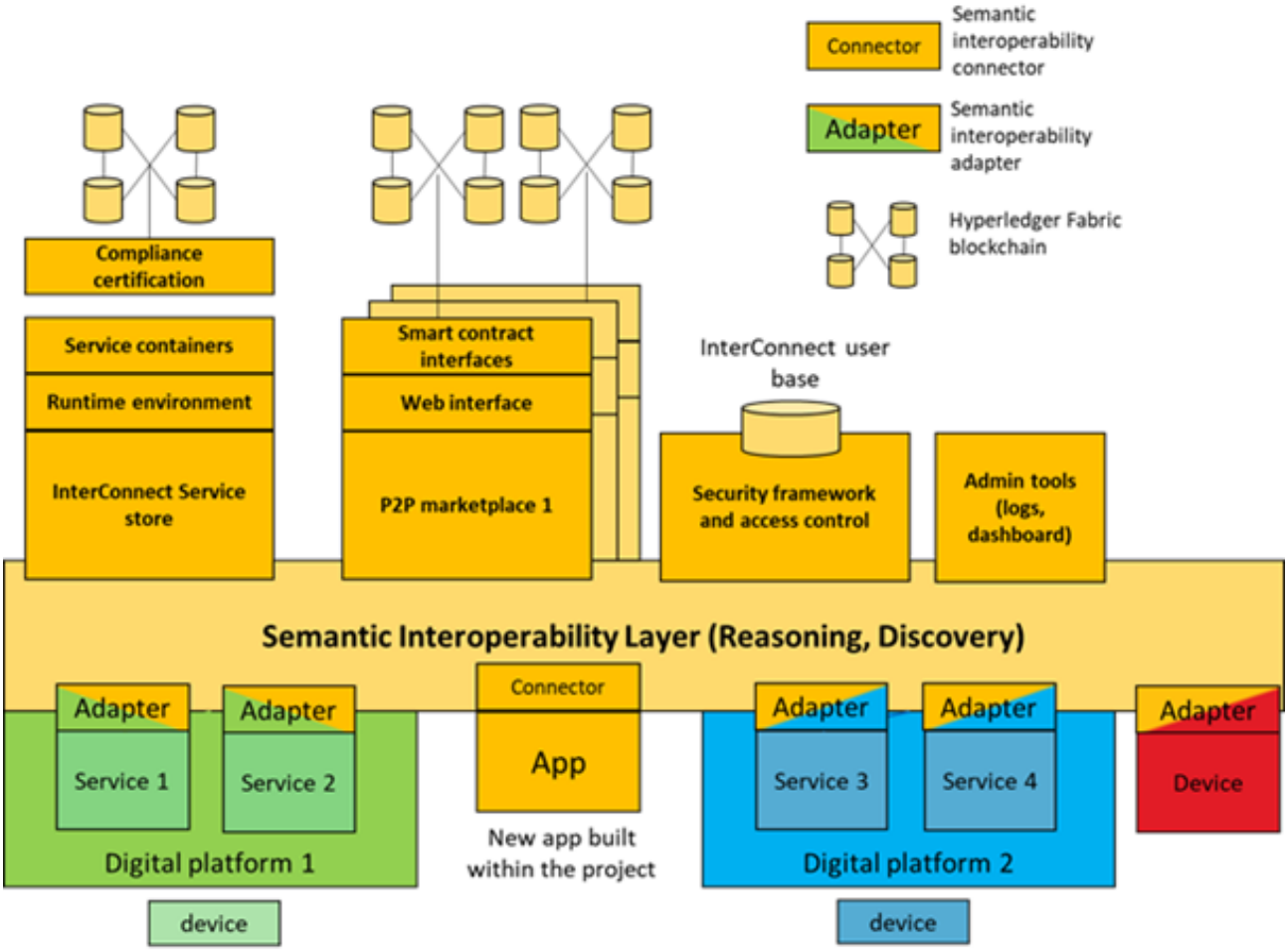


FIGURE 36 – INTERCONNECT INTEROPERABILITY FRAMEWORK ARCHITECTURE (IFA)

More details about IFA and Interoperability Framework components can be found in D5.1 [43].

4.5 SECURITY GUIDELINES FOR IC'S REFERENCE ARCHITECTURE

This section introduces security-related recommendations and guidance on privacy and security considerations for the SHBERA and its key composing views, namely the IFA and the SIL. These recommendations are based on the security-related discussions and derived requirements introduced in Section 3.4.

The next section begins by discussing where the security responsibility is deposited, depending on which environment (local or cloud-based) executes the tasks. It uses the SHBIRA as a departure point, the latter being responsible for introducing this distinction**,** as shown in Figure 23 and discussed in Section 4.3.

4.5.1 LOCATION OF THE SECURITY RESPONSIBILITY

Within the SHBIRA architecture, there is a cloud domain, and a local domain. These domains share a common responsibility for several security tasks. Especially:

- **User's profiles**, namely, which devices are used in which home, with which configurations;
- **Security services**, allowing for secure communication, ensuring that only trusted code is executed, authentication services, amongst other;
- The ability for **services and devices to communicate with each other**. This would for example, make a change of ISP (change of IP-address) cause a malfunction in InterConnect);
- The **resilience** of existing functionalities, in case of temporary network failure, all devices should still be able to function (possibly in a less optimal way, but the basic functionalities should still be available).

Different architectural approaches would allow us to achieve these objectives:

- **The cloud environment executes all tasks:** in which case all devices connect directly to the cloud environment; This will require a higher security level for all these devices since they have to communicate over the internet. It will also cause the home environment to be highly dependent on an internet connection and the cloud environment. An advantage is, however, that the user does not need to install a gateway in the home environment.

- **The local environment executes most tasks**: this would mean that all local configuration is only stored in the gateway layer, and the gateway layer directly communicates with all services. There are only a few functions that need to be executed by a cloud environment:
    a. A **trust anchor for validating applications**, comparable with a Certificate Authority in TLS connections and authentication users/devices;
    b. Ability for services and smartphones to connect to the devices;
    c. A **hybrid system, where the cloud platform executes some functions and other functions are executed in the local environment**.

4.5.2 EMBEDDING SECURITY INTO IC'S KEY COMPONENTS

The next subsections propose for each of the project's key components, guidelines on how to embed security & privacy capabilities, based on the discussions and requirements introduced in Section 3.3 and Section 3.4, respectively.

4.5.2.1 THE SEMANTIC INTEROPERABILITY LAYER (SIL)

The Semantic Interoperability Layer needs to support the following security capabilities:

- **Authentication**: Since (interoperable) devices and services communicate via the semantic interoperability layer, the semantic interoperability layer needs some identification for users, devices and services. Note that different user, devices and services might require a different level and/or type of authentication (see Section 3.3.1.1);
- **Authorization**[36]: to protect data and guarantee control to authorized users, not all users/devices/services can have access to all data. As a result, some authorization scheme needs to be part of the semantic interoperability layer. Authorization requires a model capable of deciding which user/device/service might have access to which data. Within the semantic interoperability layer, however, this will be more complex. Traditional authorization schemes store which role or user can access which data. Within InterConnect, different types of data will be combined with reasoning technologies, and new data will be inferred; thus, making it challenging to implement a *traditional* users' access-permissions storage system. So, for instance:

[36] In D2.2 [42], several examples of authorization control are mentioned in other (comparable) projects (especially RBAC and ABAC). These are taken in consideration in InterConnect.

a. In some cases **combining data will lead to requiring a higher/lower security group**: for example, by aggregating (and removing personal information) the data will be less privacy-sensitive.
b. It might be challenging to communicate in (full) transparency with end-users on how their data is/will be used since this might not be known beforehand. As a consequence, user-consent is more difficult.

- **Secure communication**: the semantic interoperability layer should be able to enforce secure communication for all interfacing devices/services/users. Note that, when TLS communication can be combined with authentication; however, this would require that a Certificate Authority is implemented as well.
- **Security Levels and Groups:** the semantic interoperability layer should support different kinds of services/devices having different security requirements. In which case, the security features of the semantic interoperability layer should be at least of the same security level as the highest connected service/device. Moreover, the possible security groups should be described, and contain the minimal security requirements which each service/device should achieve.

4.5.2.2 DIGITAL PLATFORMS

Digital platforms within the InterConnect ecosystem will act as intermediaries between the devices and the semantic interoperability layer and services. As a result, digital platforms should comply with the security recommendations and guidelines made on the previous Section for the semantic interoperability layer. Nevertheless, digital platforms are also responsible for enforcing security and privacy within their platforms and when communicating with devices; thus, the same requirements need to be implemented to ensure secure communication towards the devices.

In terms of risk, it is essential to differentiate whether all device-to-SIL communications occur via digital platforms[37]. Two scenarios may arise:

- **Devices are directly connected to the Semantic Interoperability layer**: in this scenario, devices communicate directly with other semantically interoperable endpoints (services, platforms and even devices). In terms of privacy & security, and as we now have seen, different devices have different contexts, requiring different security groups. They also have distinct hardware capabilities, so not all devices can commit to the

[37] This is an important distinction since any failure in the security measures of the digital platforms might impact have a significant impact on the devices, and all future usage of the measurement data extracted from those devices.

highest security groups. In that case, devices are expected to comply with the following requirements:

a. Each device should specify what security group they require;
b. Each device should implement all requirements of the specified security group.

Depending on the chosen security group, different security measures can be taken. The semantic interoperability layer will enforce specific measures for specific groups. However, specific for devices which send measurement data to the interoperability layer, signatures will be used to avoid tampering with the measurement data.

- **Devices communicate via Digital Platforms**: in this scenario, digital platforms act as a *man-in-the-middle* enabler for device-to-SIL communication. This configuration introduces additional risk to all measurement data coming from devices, and all control statements sent to devices. Therefore, devices sending data via a digital platform will have to comply with the security measures which are demanded by the digital platform. In turn, the digital platform should comply with the measures demanded by the interoperability layer. Furthermore, devices sending measurement data to the interoperability layer can use signatures to ensure the integrity of the data. In case of a digital platform, this signature has extra added value, because the digital platform is in a *man-in-the-middl*e position, and signatures can be used to prove the integrity of the data is not changed.

4.5.2.3 APPLICATIONS

There are different kinds of services, e.g., forecasting services, application to enable/disable a washing machine, application to give the consumer advice on his energy consumption, and so on). In this section, a high-level view is taken on these services.

A service or application can be used to give a consumer access to his data, who can then read, add and manipulate his data. For this type of service and application, the following requirements should apply:

- For each service or app, it should be clear what security group it can comply to;
- A user should authenticate to the application, and for each user, it should be clear to which security group the user belongs to[38];
- The application should not receive/send any data from/to the interoperability layer that is not compliant to the applicable security group(s);

[38] Please note that this is only relevant when the services directly communicate with the user.

- Each application should identify the devices it can interact with (e.g., for an app to switch a washing machine on/off, it should be defined with which washing machines it can interact). This can be based on brand, model, support security group or supported protocols.

Note that the application could also give a lot of added value for the consumer's privacy. When the consumer can see what data about the user and its devices are in the interoperability layer, and how this data is being used, it will add significant transparency, and give end-user's more control over their data's privacy and willingness to share data for relevant purposes.

4.5.2.4 SERVICE STORE

The InterConnect Service Store plays an essential role in the InterConnect framework. The Service Store hosts a catalogue of all interoperable services which can be accessed by end-users and framework integrators.

For IC's Service Store the following requirements should apply:

- The service store should check whether a service complies with the security requirements of the security groups they serve (e.g., a service that's using privacy data, should comply with the corresponding security group)
- The service store should enable the user to check whether the used service is 'correct'. This means that the service store should sign each service instance and that a consumer should be able to check this signature.

The next section will provide an example to demonstrate how all of the aforementioned guidelines could be coordinated within a specific use case.

4.5.3 APPLYING IC'S SECURITY REQUIREMENTS - AN EXAMPLE

Description

A manufacturer constructs an IC-compliant washing machine, which can be used by a 3rd party app to aggregate energy flexibility. A consumer buys this washing machine and installs an app allowing him to save money on his energy bill by enabling the app to turn on his washing machine on the optimal point in time.

Important security/privacy principles

The following security & privacy principles apply in this scenario:

- The consumer is sharing part of the control of his washing machine (since the application decides the exact point in time when the washing machine is turned on). To protect privacy as much as possible, the consumer should have a level of participation in the decision-making process (e.g., set some boundaries within the service can make control decisions). The InterConnect framework should facilitate this;
- The manufacturer of the washing machine will have to specify what security group applies to the washing machine. This security group will also contain requirements for controlling the washing machine (e.g., only authenticated and authorized services should be able to send control signals to the washing machines);
- The service provider should build the app in such a way that each washing machine is started on the optimal point in time while utilizing the user participation in the decision-making process to preserve the privacy of the consumer.

Resulting requirements

From these principles, the following requirements can be derived:

- The InterConnect framework should contain a security group for consumers' whitegoods, which would include requirements such as:
    a. Level of authentication of the user;
    b. Level of encryption of all communication;
    c. Storage/logging of all command data (e.g., needed for billing, and non-repudiation);
    d. Integrity measures on measurement data (e.g. needed when devices send usage data back to the cloud)
- The manufacturer service/app should define to which security groups the app applies, and also take care that the app complies to all requirements;
- The manufacturer service/app should specify with which devices the app can communicate (e.g., all washing machines (regardless of vendor), or all washing machines of brand X);
- The service store should check whether the application complies with the given security groups, and also sign the application, so its integrity is guaranteed;
- During the usage of the application/service, the latter should check the identity of the consumer. The application or service could use the authentication and authorization solution of the Interoperability layer to do so;

- Only after authentication, the application should get access to the user profile, which is stored in the interoperability layer. The consumer can then configure the application/service. For example, the consumer has first to authenticate to the app, and then configure his washing machine.

4.5.4 CONCLUDING REMARKS

The goal of this section was to provide an overview of the initial privacy and security requirements for information/data and control (actuation) for the different roles and system elements introduced in this section. The consequences of the security-related requirements covered in Section 3.4 were also discussed, namely for the Semantic Interoperability Layer, Service Store, and the digital platforms, services and devices within the project's ecosystem.

Our initial discussions and findings have led to the conclusion the project needs to facilitate the creation of different security groups. For the time being, we foresee the need for the following groups:

- A Security Group for **Home appliances and home sensors**, focusing on preserving the privacy of the consumer;
- A Security Group for **User (online) services and applications**, focussing on preserving the privacy of the consumer;
- A Security Group for **Billing services**, for all data and systems for the billing process, focussing on preserving the integrity of the data and privacy of the consumer and service provider;
- A Security Group for **Energy system and applications**, focussing on the integrity of their energy data/services.

Please note that one device could be part of multiple security groups. The following recommendations can be made for the next steps for the security guidelines and process:

- Specify the different security groups;
- Specify security requirements for each security group;
- Specify for each device/app/service which security group applies;
- Assess the consistency in the overall architecture of these security group specifications;
- Implement the resulting requirements in each device/app/service and pilot architecture instantiation.

5 SEMANTICALLY INTEROPERABLE INFORMATION ARCHITECTURE

This section addresses what semantic interoperability is, why a semantic interoperability layer is needed in the InterConnect reference architecture, and how this layer can be realized. In particular, based on the requirements necessary for the semantic interoperability layer outlined in Section 3.4. This section proposes an inventory of the semantic solutions existing among the partners in InterConnect. It analyses whether they fulfil (part of) the envisioned requirements. The analysis of existing semantic solutions results in a recommended, shared, solution based on the Knowledge Engine technology, which is used as a common basis to create the semantic interoperability layer in InterConnect. The recommended solution is further explained, elaborating on which semantic components will be embedded into the reference architecture to realize the semantic interoperability layer. Finally, the section concludes with guidelines for the pilots concerning what steps need to be taken to make their device/service/platform compatible with the recommended solution when using the InterConnect's semantic interoperability layer.

As explained in the IoT Standardization Landscape by AIOTI [13], the main challenge in the Internet of Things (IoT) landscape is the fragmentation of existing platforms, protocols and standards. In this fragmented landscape, in which there is not a Winner-Takes-It-All market, vendor lock-in should be avoided to preserve essential values in the European context, such as openness and level playing field. At the same time, consumers should be provided with the flexibility to integrate their devices, solutions and services of choice as they like. To that end, cross-platform interoperability among various platforms from different vendors is essential.

In addition to cross-platform interoperability, another major challenge consists of cross-domain interoperability among various vertical domains (such as, for example, the smart home, buildings, and energy domains that are of interest for the InterConnect project). In our interconnected world, not only is it crucial to share data and become interoperable within each of these domains but especially across these domains. That is where the full potential of combining data still needs to be unlocked.

By using semantic technologies and ontologies, it is possible to address both the cross-platform and cross-domain interoperability challenges at the semantic (information) level,

rather than at the technical communication level, as it used to be in the past [14]. To that end, a semantic interoperability layer can be used to interpret, link and harmonize the concepts in the message data structures exchanged by the multitude of existing platforms, regardless of their specifics at the underlying technical level. In the past years, the IoT industry understood the impact that semantic technologies and ontologies can have to enable the missing interoperability, also as a result of significant standardization efforts such as SAREF[39] [13, p. 103 264], [13, pp. 103 410 parts 1-10].However, most industrial practitioners are not familiar with these technologies and are not willing to learn them, as they believe the learning curve is too steep. IT developers - either device manufacturers or application developers - ask for practical solutions that can be applied in operational environments. In contrasts, the information on semantic technologies and ontologies appears abstract and scattered over the Internet, thus, not as easily applicable.

In this context, promotion, experimentation and roll-out of interoperability innovation based on semantic technologies and ontologies is of paramount concern. Most of the technical barriers have been tackled in R&I projects, national initiatives and EU funded projects. Abundant and mature research on enabling technologies has been validated and demonstrated in industrially relevant environment (TRL 5 and 6). However, concrete guidelines and successful stories of large scale semantically interoperable implementations, which are at the same time easy to be adopted by developers that are non-ontology/semantic technology experts, are still missing. There is now a need to take the current results to a higher TRL level, into (distributed) operational environments that go across vertical domains (silos) and are deployed on a large scale, in a way that is reasonably easy to adopt also for developers that are non-ontology/semantic technology experts (the vast majority). This is the real added value that the InterConnect project aims at delivering for making interoperable smart homes, buildings and grids become a reality.

5.1 INTEROPERABILITY LEVELS

To position the concept of semantic interoperability and show the need for it, this section introduces the main levels of interoperability as defined by the GWAC (GridWise Architecture

[39] https://saref.etsi.org

Council) Interoperability framework [15], which is also the definition adopted by AIOTI. According to GWAC, the following three main levels of interoperability can be identified:

- **Technical Level (Syntax)** covering the aspects of basic connectivity, network interoperability and syntactic interoperability;
- **Informational Level (Semantics)** covering the aspects of semantic understanding and business context;
- **Organizational Level (Pragmatics)** covering the aspects of business procedures, business objectives and regulatory policy.

Each of these levels is divided into sub-levels in order to reference the degree of interoperability accurately. Figure 37 gives an overview of this framework, called GWAC stack.

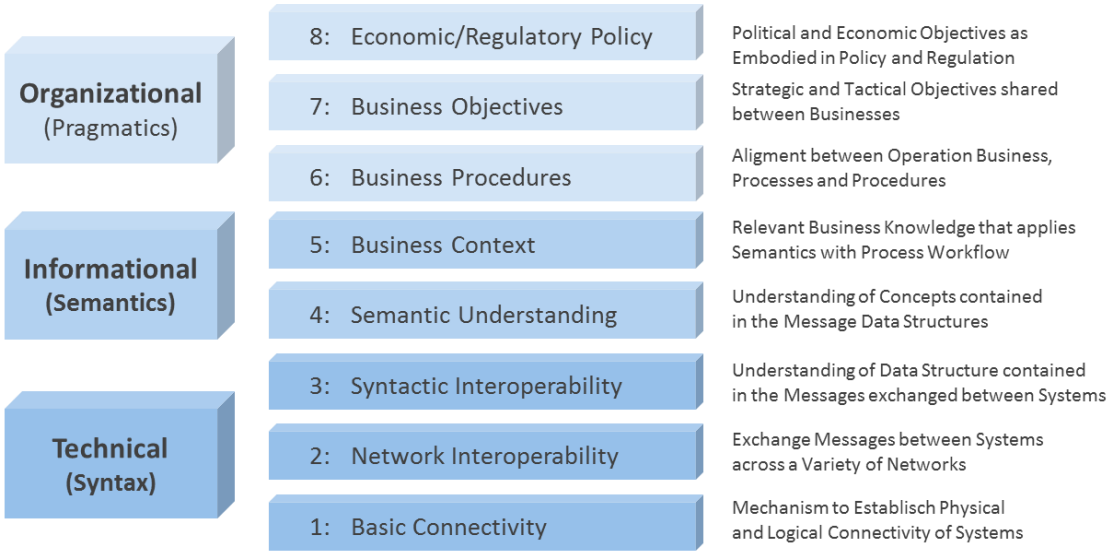


FIGURE 37 – LEVELS OF INTEROPERABILITY - GWAC INTEROPERABILITY FRAMEWORK [15]

In smart homes, buildings, and grid systems, the sublevels of basic connectivity, network interoperability and syntactic interoperability, and semantic understanding are relevant. They are discussed in more detail below:

- **Basic connectivity:** Basic Interoperability concerns the digital exchange of data between two systems and the establishment of a reliable communication path. This requires an agreement on the compliant use of specifications that describe the data transmission medium, the associated media-related data encoding and the transmission rules for the media access;

- **Network interoperability:** Network interoperability supposes an agreement on how the information is transported between interacting parties across multiple communication networks. The protocols agreed upon in this category are independent of the information transferred;
- **Syntactic interoperability:** Technical interoperability guarantees the correct transmission of bits. The correct syntax of transferred information is the task of standards such as XML or EDIFACT. Syntactic interoperability refers to the exchange of information between transacting parties based on agreed format and structure for encoding this information. Assuring that transmitted information has a proper meaning is not in the scope of syntactic interoperability;
- **Semantic interoperability:** Beyond the ability of two or more systems to exchange information with correct syntax (i.e., grammatically correct), semantic understanding concerns the (automatic) correct interpretation of the meaning of information. To achieve semantic interoperability, both sides must refer to a common information exchange reference model. This reference model must define the meaning of the exchanged information (the words) in detail. This is the only way to ensure that the communicating systems will correctly interpret the information and commands contained in the transferred data and will correctly act or react. Reference ontologies, such as SAREF, can be used to represent the common reference model. They may also model constraints about the information concepts by specifying assertions and inferences that can be used in reasoning mechanisms (e.g., *if this, then that*). This allows resolving interpretation conflicts in situations where two differently named classes in different models mean the same or when a class is a subset or superset of another class.

5.2 REASONING

As explained in the previous section, ontologies will be used as common reference models to achieve semantic interoperability. The SAREF suite of ontologies created and maintained by ETSI since 2015 is used in InterConnect for this purpose[40]. Part of the functionality of the semantic interoperability layer is to support reasoning that enables inferring new knowledge and orchestrating the data exchange. The SAREF ontology and its extensions can be used to

[40] The ETSI Technical Specifications and RDF/OWL files of the SAREF suite of ontologies (including SAREF core, SAREF for Energy and SAREF for Buildings that are of significant interest for InterConnect) can be found at https://saref.etsi.org/extensions.html. The future InterConnect deliverable D2.3 will contain all the details of the additions to these ontologies that are currently developed by the InterConnect project. A detailed presentation of SAREF and its extensions is out of the scope of the present document, which is focused on the architectural components of the InterConnect semantic interoperability layer.

support both types of reasoning. Section 5.2.1 introduces some background information about ontologies (i.e., classes, properties, instances and namespaces) using an example scenario based on SAREF. Sections 5.2.2 and 5.2.3 further elaborate on reasoning to infer new knowledge and reasoning for orchestration, respectively.

For illustration purposes, we consider a scenario in a kitchen containing a smart-stove (which can be controlled remotely), a ventilation regulator, a smoke detecting sensor, an infrared temperature sensor, an occupation sensor (detecting people in the kitchen), a local fire alarm bell and an application that automatically warns the fire brigade. In this scenario, the food on the stove ignited and caused a flame and smoke. This can have two reasons: an accident, or by purpose a controlled 'flambe' dish (which would require some extra ventilation to get rid of the smoke). If it is an accident, it matters if somebody is in the house (and can take out the fire him/herself) or the fire-brigade has to be warned. This situation is being monitored by the smart home and will derive by reasoning if a fire-hazard situation is likely and which, if at all, an alarm has to be raised if the stove has to be turned off, the ventilation has to be increased (controlled fire, just smoke) or reduced (reduce oxygen levels), etc.

In this example, we can observe two types of reasoning, i.e., to infer new knowledge and orchestrate data exchange[41], required by the Smart Home system:

- An example of **reasoning to infer new knowledge:**
  - `IF smoke(true) AND rapid_increase_temp(true) AND rapid_decrease_temp(true) THEN uncontrolled_fire_situation(false)`
  - `IF smoke(true) AND rapid_increase_temp(true) AND rapid_decrease_temp(false) THEN uncontrolled_fire_situation(true)`
- An example of **reasoning to orchestrate data exchange:**
  - `IF uncontrolled_fire_situation(true) AND occupied(house,true) THEN ring_local_alarm_bell(true) AND call_fire_brigade(false)`
  - `IF uncontrolled_fire_situation(true) AND occupied(house,false) THEN ring_local_alarm_bell(true) AND call_fire_brigade(true)`

[41] Please note that the reasoning to infer new knowledge concludes facts (i.e., it infers new knowledge), while reasoning to orchestrate data exchange triggers actions, invoking their execution by other existing services.

Further details and examples on deductive and orchestration reasoning can be found in Sections 5.2.2 and 5.2.3.

5.2.1 CLASSES, PROPERTIES, INSTANCES AND NAMESPACES

In the realm of the Semantic Web and Linked Data, *classes* can be interpreted as a group of things for which we have an explicit word (e.g., buildings, devices, cars, trees) and *properties* are the characteristics that hold for that group of things (e.g., location, energy consumption, speed, height).

An *ontology* is an explicit description of a domain, intended as a means for achieving a shared understanding both for humans and computers. An ontology consists of classes and their properties. Linked Data is web-based; anyone can create an ontology and publish it online. The URL of an ontology often coincides with its *namespace*, which is basically the identifier of the ontology[42]. A *prefix* (such as saref: for SAREF or s4ener: for the SAREF for Energy extension), is normally used in front of each class, property and instance of the ontology to avoid repeating the full namespace (such as https://saref.etsi.org/core).

Figure 38 shows an overview of the main classes and properties of SAREF. In total SAREF contains 81 classes, 35 object properties and 5 data properties.

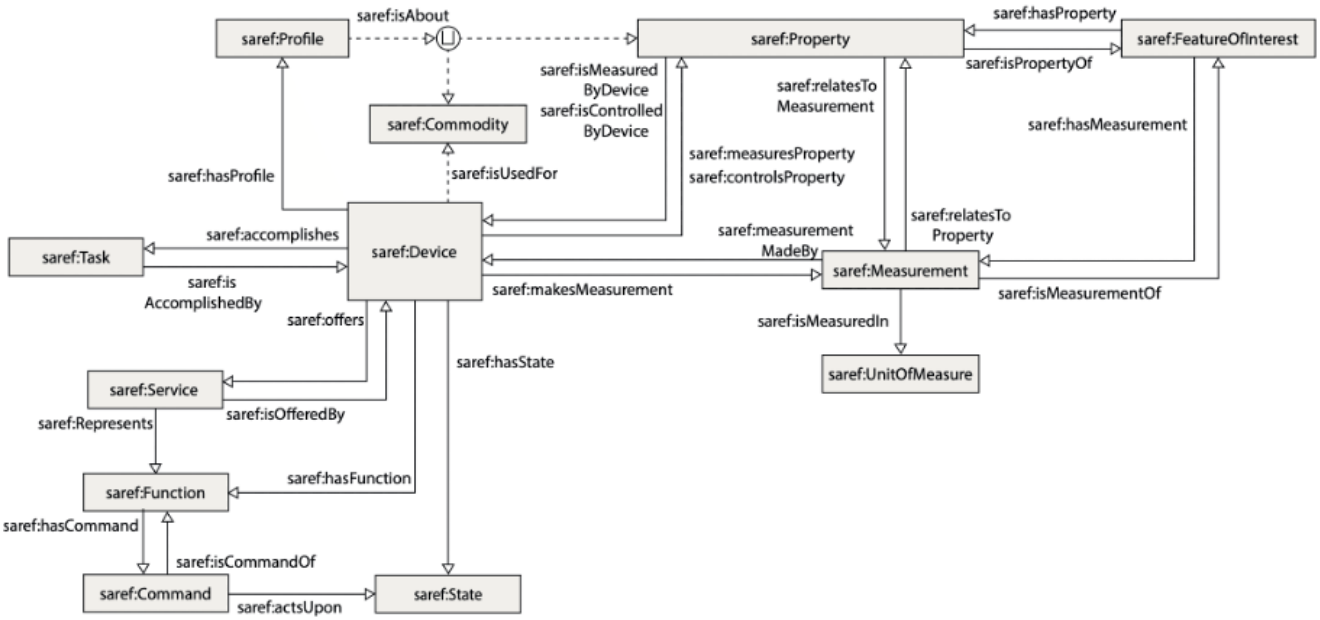


FIGURE 38 – OVERVIEW OF SAREF CORE ONTOLOGY [16]

[42] For SAREF, the namespace for the core ontology is: https://saref.etsi.org/core

As described in [17], the starting point in SAREF is the concept of *Device*, which is defined as a tangible object designed to accomplish a particular *Task*. In order to accomplish this task, the device performs a *Function*. For example, a temperature sensor is a device of type `saref:Sensor`, is designed for tasks such as `saref:Comfort`, `saref:WellBeing` or `saref:EnergyEfficiency`, and performs a `saref:SensingFunction`. Functions have commands. A *Command* is a directive that a device needs to support to perform a certain function. Depending on the function(s) it performs, a device can be found in a corresponding *State*. A device that wants (a certain set of) its function(s) to be discoverable, registerable, and remotely controllable by other devices in the network can expose these functions as a *Service*. A device can also have a *Profile*, which is a specification to collect information about a certain *Property* or *Commodity* (e.g. Energy or Water) for optimizing their usage in the home/building in which the device is located. A *Property* is defined as anything that can be sensed, measured or controlled by a device, and is associated to measurements. For example, a temperature sensor measures a property of type `saref:Temperature`. A *Measurement* is the measured value made over a property and must be associated to an unit of measure and a timestamp. The *Feature of Interest* concept further allows to represent the context of a measurement, i.e., any real world entity from which a property is measured. For example, whether the measured temperature is that of a room or of a person. A more detailed description of the SAREF classes and properties can be found in [16].

Instances are specific individuals that belong to a class, for example the 'PRITY' wood stove belongs to the class "Stoves", or "Ada Lovelace" belongs to the class "Mathematicians", which in itself is a subclass of the class "Persons".

In our example scenario, various instances can be identified. Figure 39 shows that the SAREF core ontology plus a small part of the SAREF4BLDG extension can be used to describe these instances, which are depicted in blue[43]. For example, the `ex:temperatureSensor_x` device is an instance of the `saref:TemperatureSensor` class that measures the temperature in the home and inherits all the properties specified in the SAREF ontology that belongs to that class and its superclasses (such as the `saref:hasFunction` property).

[43] Note that the `ex:` prefix (meaning 'example') is used to distinguish our example instances from the classes defined in SAREF (which in contrast are characterized by the `saref:` prefix).

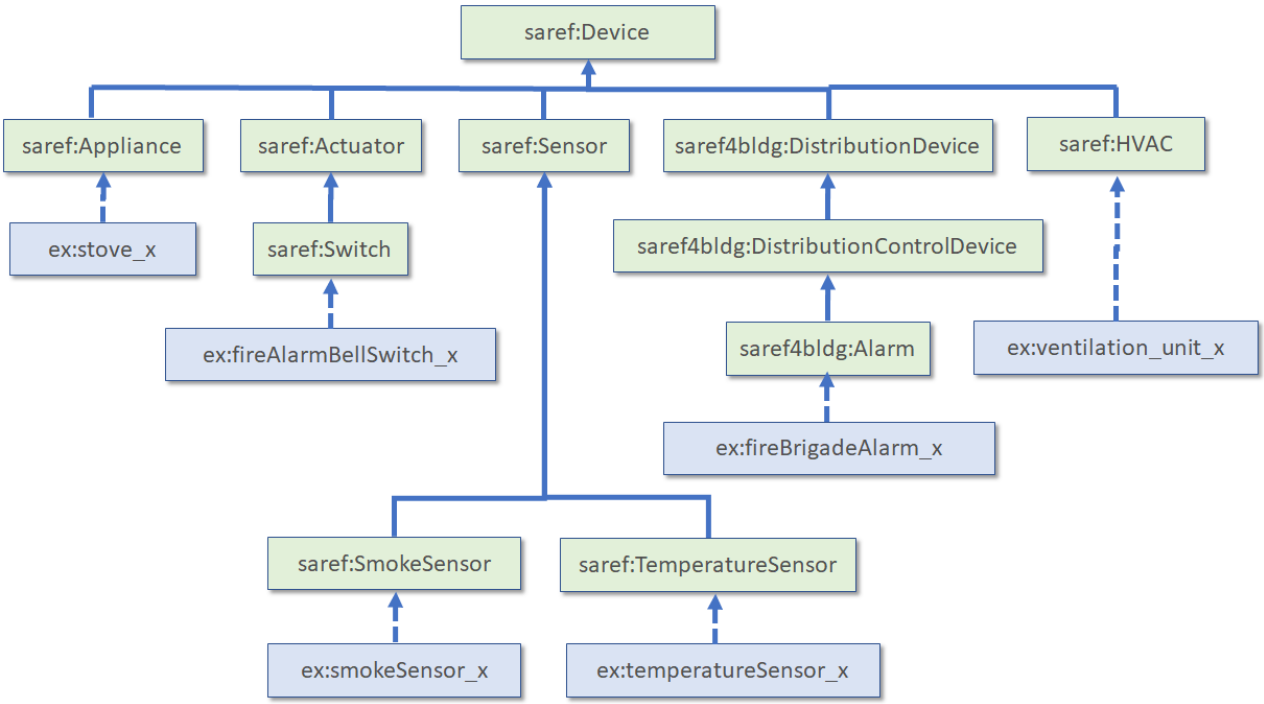


FIGURE 39 – SUBCLASS HIERARCHY OF DEVICES AND THE EXAMPLE INSTANCES. SOLID LINES DEPICT SUBCLASS RELATIONS AND DASHED LINES INSTANCE RELATIONS

5.2.2 REASONING TO INFER NEW KNOWLEDGE

Infer new knowledge is what is usually meant when talking about (semantic) reasoning in the context of the Semantic Web. Detailed information on this type of reasoning can be found in the white paper on semantic interoperability by AIOTI [18]. In the considered smart-home scenario, we have the following example:

- `IF smoke(true) AND rapid_increase_temp(true) AND rapid_decrease_temp(true) THEN uncontrolled_fire_situation(false)`
- `IF smoke(true) AND rapid_increase_temp(true) AND rapid_decrease_temp(false) THEN uncontrolled_fire_situation(true)`

which contains a collection of facts, rules and conclusions as follows:

- a collection of original facts, such as `smoke(true)`, `rapid_increase_temp(true)`, and `rapid_decrease_temp(true)`

- a set of rules the reasoner uses to infer new facts, such as `IF smoke(true) AND rapid_increase_temp(true) AND rapid_decrease_temp(true) THEN uncontrolled_fire_situation(false)`
- derived facts from the reasoning rules, such as `uncontrolled_fire_situation(false)` and `uncontrolled_fire_situation(true)`

The original facts are called the *asserted facts* and the derived facts are called the *inferred facts*, as shown in Figure 40).

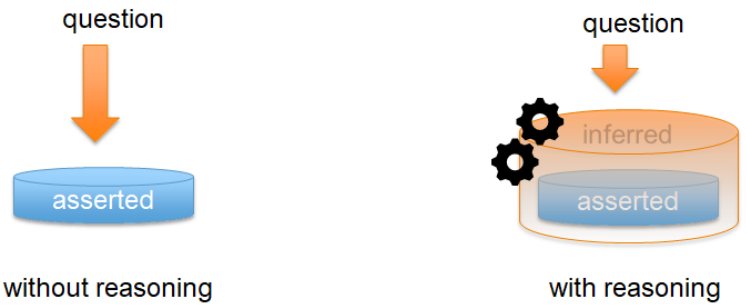


FIGURE 40 – REASONING TO INFER NEW DATA: THE DIFFERENCE BETWEEN ASSERTED AND INFERRED FACTS

The left database in Figure 40 only contains asserted facts and whenever a user asks a question to this database, the answer will be sought within these asserted facts. In the right database, in addition to the asserted facts, a collection of inferred facts is also available. The reasoner derives these inferred facts from the asserted facts by applying a set of rules, such as the ones in our example scenario (further details on this type of rules and reasoning can be found in [18]). This means that whenever a user asks a question to the database on the right, the answer will be sought in an extended knowledge base, consisting both of the asserted facts and in the inferred facts. This will result in more answers to the users, sometimes even unexpected due to the additional links that the reasoner is able to infer, compared to the case of only consulting the database without reasoning.

5.2.3 REASONING FOR ORCHESTRATION

The previous section describes how reasoning is typically used to infer new knowledge from asserted facts, while this section focuses on how a reasoner can be used to also orchestrate

data exchange in a distributed environment where knowledge is scattered among multiple components (e.g., devices, platforms and/or services). The role of the reasoner is then to make sure that the information is exchanged in such a way that it is at the right place and at the right time, according to the different needs of the various components.

InterConnect promotes decoupling of the semantics of the data to be exchanged from the actual data exchange, envisioning the use of so-called *capability descriptions* in the shared semantic interoperability layer. Capability descriptions are descriptions used in the orchestration process of the data exchange among components (e.g., devices, platforms and/or services) based on a shared, common semantics that abstracts from the specific internal technical details of each component (since different components are often developed by different parties and have quite different internal logic), focusing instead on the common aspects of the knowledge to be exchanged. For this purpose, the SAREF ontology presented in Section 5.2.1 can be used. Figure 41 shows an example of capability description for a thermometer that measures the temperature of a room in degree Celsius using a graph pattern expressed in SPARQL.

```
?room rdf:type ex:LivingRoom .
ex:LivingRoom rdfs:subClassOf saref:FeatureOfInterest .
?room ex:hasName ?room_name .
?data rdf:type saref:Measurement .
?data saref:isMeasurementOf ?room .
?data saref:isMeasuredIn om:degree_Celsius .
om:degree_Celsius rdf:type saref:TemperatureUnit .
?data saref:hasValue ?temperature_value .
```

FIGURE 41 – EXAMPLE OF A CAPABILITY DESCRIPTION AS A GRAPH PATTERN USING SAREF

A graph pattern in SPARQL consists of so called *triples*, which are expressions made of a <subject> <predicate> <object>. An example of triple in Figure 41 is `ex:LivingRoom rdfs:subClassOf saref:FeatureOfInterest`, where `ex:LivingRoom` is the subject, `rdfs:subClassOf` is the predicate and `saref:FeatureOfInterest` is the object). In the graph pattern in Figure 41, the terms starting with question marks, such as `?room`, represent variables. Note that these variables are given informative names for human comprehension sake (i.e., `?room`) but those names could in principle be anything for the computer (i.e., we could have called the same variable `?a` or `?xyz` instead of `?room`). The `?room` variable

identifies a living room (type `ex:LivingRoom`), which is in turn a subclass of `saref:FeatureOfInterest` (which in SAREF represents some physical object, such as a room or a person, we can make measurements of). The `?data` variable identifies a measurement (`?data rdf:type saref:Measurement`) of the living room previously defined (`?data saref:isMeasurementOf ?room`). The measurement is made in degrees Celsius (`?data saref:isMeasuredIn om:degree_Celsius`), with degrees Celsius being a type of `saref:TemperatureUnit`. Finally, the measurement holds the numeric value of the current temperature measurement (`? data ?saref:hasValue ?temperature_value`).

To clarify the role that a reasoner can have in the orchestration process, let us consider a scenario in which the data sent by a thermometer in the living room is a measurement of the temperature in Fahrenheit, while the thermostat in the same living room uses the temperature, but in Celsius. A simple matcher (as opposed to a reasoner) could conclude that the capability description of the thermostat (temperature in Celsius) does not match the capability description of thermometer (temperature in Fahrenheit), resulting in no data exchange between them. Or, even worse, it could wrongly conclude that the capability description of the thermostat (temperature in Celsius) matches the capability description of the thermometer (temperature in Fahrenheit), allowing a data exchange that would mix up values in different units of measure, resulting in errors and undesired behaviours in the system. In contrast, a reasoner would be able to infer that the capability description of the thermometer can be made to match the capability description of the thermostat, if the temperature in Fahrenheit is first converted into temperature in Celsius by a third component (where this component capability description is that it is able to convert temperature in Fahrenheit to temperature in Celsius).

As an additional example, the benefits of a reasoner for the orchestration of data exchange (as opposed to a simple matcher) become evident in the scenario in which a component requests from the Interoperability Layer some data that is not available in a single component but can be combined from multiple components. While a simple matcher would not be able of doing that (as the full request is not satisfiable), a reasoner would be able to infer that the original request from the component can be fulfilled by combining the original capability description with several capability descriptions from different components.

5.3 COMPLIANCE

For the sake of readability, we will refer to the type of reasoning to infer new knowledge described in Sections 5.2.2 and 5.2.3 simply as *reasoning support*, while we will refer to the use of/ compliance with the SAREF ontology described in Section 5.2.1 simply as *SAREF compliance*. This section elaborates on the two aspects of reasoning support and SAREF compliance in terms of a corresponding scale of levels from 0 to 3. Note that the aim of InterConnect for both aspects is to start at least from level 2 and ideally reach level 3.

Reasoning support

- Level 0: no reasoning support. With reasoning support, we mean reasoning based on ontologies using semantic web technologies, such as RDF, OWL and SPARQL (as described in Section 5.3);
- Level 1: basic reasoning to infer new knowledge (according to section 5.3.1). That is, the use of a reasoner for consistency checking to validate that there are not violations in RDF/OWL. For example, if two classes are declared as disjoint (e.g., black and white), but a certain instance (e.g., snow) is declared as rdf:type of both these classes (therefore, meaning that snow is both white and black), then the reasoner will throw a violation.
- Level 2: advanced reasoning to infer new knowledge (according to section 5.3.1). That is, the use of a reasoner for deriving new knowledge via, for example, subclassing, axioms and rules. This is the most powerful feature of ontologies and semantic web technology, and sometimes it can lead to unexpected results, even for the ontology developers themselves. Therefore, it must always be checked by means of a reasoner what are the implications of the relations, axioms and rules linking the concepts defined in an ontology.
- Level 3: additional reasoning to orchestrate data exchange (according to section 5.3.2), on top of the advanced reasoning to infer new knowledge at level 2. That is, the use of a reasoner for the composition of knowledge coming from various, distributed data sources (which can be devices, services or platforms in the InterConnect ecosystem) to meaningfully orchestrate their data exchange. This orchestration is not simply based on an exact matching of explicitly defined RDF/OWL triples but makes use of a reasoner for an advanced matching of these triples.

SAREF compliance

- Level 0: no SAREF compliance. That is, SAREF is not used at all. Note that this is decoupled from the reasoning support mentioned above (in other words, level 0 in SAREF compliance does not automatically imply level 0 in reasoning support. In fact, reasoning support can be guaranteed using other ontologies than SAREF).
- Level 1: basic SAREF compliance. That is, SAREF is taken into account and an explicit mapping to SAREF exist via a document, such as a textual file, a table or a spreadsheet[44]. Note that this type of mapping, however, is not automated nor directly machine processable, but requires manual human interpretation.
- Level 2: intermediate SAREF compliance. That is, not only SAREF is taken into account, but machine interpretation is enabled. For example, data that is already encoded in a certain format (e.g., XML or JSON) can be annotated (labelled) using SAREF concepts in RDF/OWL. In this way, the mapping to SAREF becomes machine processable, as an automated script, for example, can be used to convert the original data format into SAREF compliant RDF/OWL triples.
- Level 3: full SAREF compliance. That is, direct use of SAREF concepts in RDF/OWL. A SAREF compliant file in RDF/OWL exists and it is fully machine interpretable, also using a reasoner. Note that this level has a relation with the reasoning support mentioned above, as level 3 in SAREF compliance enables levels 1, 2 and 3 of reasoning support (but not vice-versa, as reasoning support can be guaranteed using other ontologies rather than SAREF).

The goal of InterConnect is to reach level 3, for both reasoning support and SAREF compliance, and to be able to interconnect with systems having level 2. These scales for reasoning support and SAREF compliance have been used, together with some additional criteria derived from the high-level requirements in Section 3.4, to create a template for collecting candidate solutions for semantic interoperability already in use by InterConnect partners that could be used to realize the semantic interoperability layer. The next section proposes an inventory of these solutions based on this template.

[44] See for example the mappings in the form of a look-up table elaborated during the first Smart appliances study for the European Commission [6], also available as a more detailed mapping spreadsheet at https://sites.google.com/site/smartappliancesproject/documents

5.4 SEMANTIC INTEROPERABILITY SOLUTIONS

This section presents the solutions that the various consortium partners bring to the project as possible candidates to realize the semantically interoperable information architecture. These solutions have various states of maturity, varying from conceptual and prototype to implementation and tested. We analyse these solutions based on the high-level requirements specified in Section 3.4, and propose and improve the perfect blend of these solutions to realize the semantically interoperable information architecture. These solutions are described according to the template available in Annex 1 – Template For Semantic Solutions.

5.4.1 KNOWLEDGE ENGINE BY TNO/VU

Category	Objectives
Title and Proposer(s)	Knowledge Engine (KE) by TNO and VU Amsterdam
Context and Project(s)	The KE enables integration and/or cooperation among multiple heterogeneous data producers and consumers. It has been developed and applied in more than 10 research projects in diverse sectors like Agriculture and Safety & Security.
Maturity	The generic components (i.e., Smart Connector and Knowledge Directory) are sufficiently mature and stable (applied in 10+ projects). We successfully tested the Knowledge Engine in two demonstrators using scenarios with different requirements. Therefore, the starting point is TRL 5, i.e., technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies), and we are moving towards TRL 6, i.e., technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies). Currently, in cooperation with VUA, we are working on a demonstrator that interconnects several Raspberry Pi's with different sensors and actuators to show how the KE solution can be deployed also on IoT devices.
Overview	The Knowledge Engine provides semantic interoperability by means of two features: translation and discovery. Both these features require a common ontology, such as SAREF. From here on we consider SAREF as the common ontology used by the InterConnect interoperability framework. The underlying idea is that the KE is able to interconnect different Knowledge Bases (KB), which are depicted in Figure 42 as cylinders. Knowledge bases can be anything, from devices and services to algorithms, apps, machine learning models or platforms from different vendors. To become semantically interoperable with other KBs, each KB is provided with a specific

	component, called Smart Connector (SC), which realizes the translation mechanism to/from a common ontology (e.g., SAREF). As a requirement, SCs must know both SAREF and the specific language that needs to be translated to SAREF. Each SC registers itself in a Knowledge Directory (KD) with a description of the capabilities that it wants to make available to other SCs. This description is defined as a graph pattern in SPARQL[45] that refers to concepts in SAREF. These patterns are used for the discovery of knowledge by other SCs. When a SC (and its corresponding KB) is no longer available, or when a new SC becomes available, the Knowledge Directory is dynamically updated. With this up-to-date information, the knowledge exchange among KBs (enabled by the SCs) can take place. This is shown by the arrows in Figure 42. The knowledge is exchanged using a combination of SPARQL[46] and RDF messages that refer to SAREF concepts.
Semantic Components Description	• **Smart Connectors:** Figure 12 shows how a SC is the main component of the KE as it relates to the KD, SAREF, devices (via south bound interface) and services (via north bound interface). Figure 12 further shows that the mapping to/from SAREF occurs within the interoperability framework. This mapping is realized by the SCs, that should know, as a requirement, both SAREF and the specific language (API) that needs to be translated into SAREF. • **Knowledge Directory:** The Knowledge Directory is a repository of all KB (i.e., services, devices and algorithms) and their capabilities. Smart Connectors register and unregister themselves with the KD and retrieve updates about available SCs. • **Common Ontology:** Both SC and KD refer to a common ontology for the knowledge exchange. In this figure we use SAREF as our common ontology. SAREF can be extended with additional concepts, if needed by the knowledge exchange.
Reasoning support	**[Level 3]** reasoning to orchestrate data exchange AND advanced reasoning to infer new knowledge. The SC contains a reasoner[47] to infer new facts about the data using the ontology. The same reasoner also allows to reason about metadata that is used not only for discovering devices and services, and their capabilities, but also to actually orchestrate the knowledge exchange.
Compliance with SAREF	**[Level 3]** full SAREF compliance, direct use of SAREF concepts in RDF/OWL. As mentioned, the KE can in principle work with any ontology, including SAREF, which can be directly used with the KE.

[45] Basic Graph Pattern (BGP), see https://www.w3.org/TR/sparql11-query/#BasicGraphPatterns

[46] Basic Graph Patterns (see above) and SPARQL Result Set in JSON (https://www.w3.org/TR/sparql11-results-json/).

[47] Apache Jena GenericRuleReasoner, https://jena.apache.org/documentation/inference/#rules

Supported data formats	Anything behind the south and north bound interfaces (like JSON, XML, CSV), because the SCs will map it to/from the data format supported by the interoperability framework (SPARQL[48] and RDF[49]).
Supported standards and protocols	Anything behind the south and north bound interfaces (that's the strength of SAREF), because the SCs will map it to/from the standards and protocols supported by the interoperability framework. Those are HTTPS[50], Java Messaging Service (JMS51), SPARQL[52] and RDF[53].
	The Knowledge Engine uses Ontology-Based Access Control (OBAC) [19] to describe and enforce security policies for access control in terms of a common ontology (i.e. SAREF). Current work aims to restrict the knowledge exchange within the interoperability framework to HTTPS (and the certificates that are required for it).
	The KE is freely available and open source.
	• **Flexible setup:** SCs can be used with individual devices, a hub that connects multiple devices, a gateway in the home, or the interface of any proprietary solution. • **Discovery and orchestration:** it automatically picks up/looks for new relevant knowledge that becomes available (possible relation to InterConnect Service store and Marketplace). • **Push/pull:** it supports both request/response and publish/subscribe mechanisms. • **Explainability:** because it contains a reasoner that fully exploits the reasoning capabilities of the ontology, the KE supports explanations about devices/services behaviour/decisions and their internal processes. • **Human-in-the-loop:** can automatically involve humans in critical processes. • **Access control:** enforces XACML based security policies that use SAREF concepts
	• **The Knowledge Engine is still under development:** new features are added and improved on a weekly basis. • **Not yet stress tested:** to be tested how it will perform in large-scale environments with dozens of devices/services(a stress test is planned for this year in the context of another project). • **Small development team**: currently a few people developing on the Knowledge Engine within TNO.

TABLE 25 – TNO/VU'S SEMANTIC INTEROPERABILITY SOLUTION

[48] https://www.w3.org/TR/sparql11-query/
[49] https://www.w3.org/TR/rdf11-concepts/
[50] https://en.wikipedia.org/wiki/HTTPS
[51] https://en.wikipedia.org/wiki/Java_Message_Service
[52] https://www.w3.org/TR/sparql11-query/
[53] https://www.w3.org/TR/rdf11-concepts/

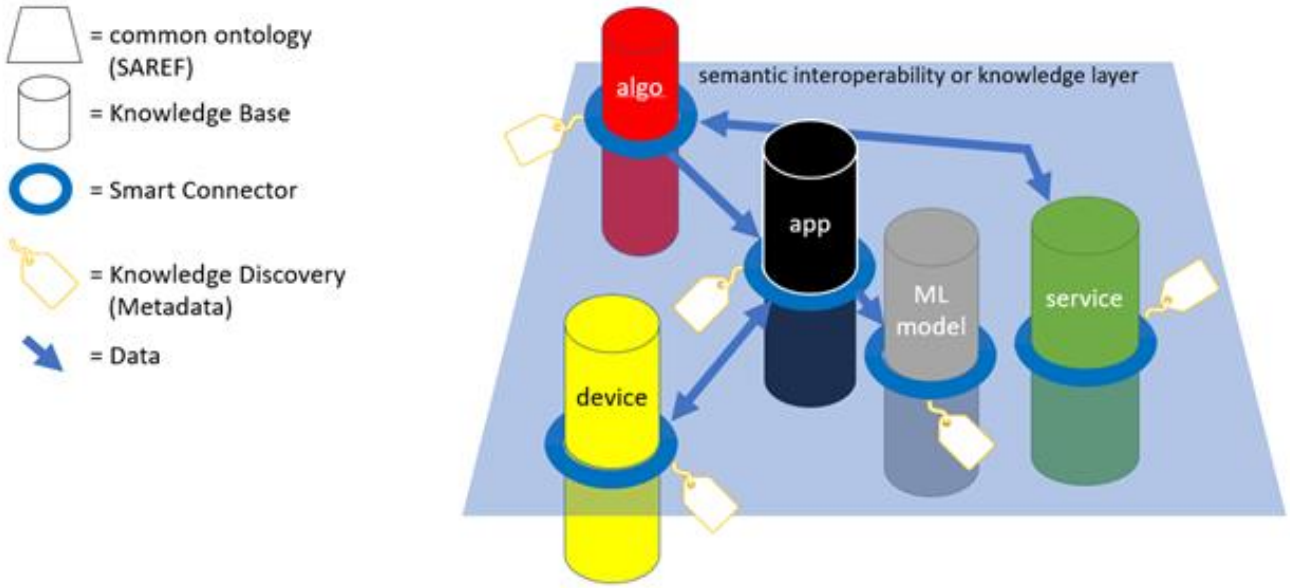


FIGURE 42 – KNOWLEDGE ENGINE OVERVIEW

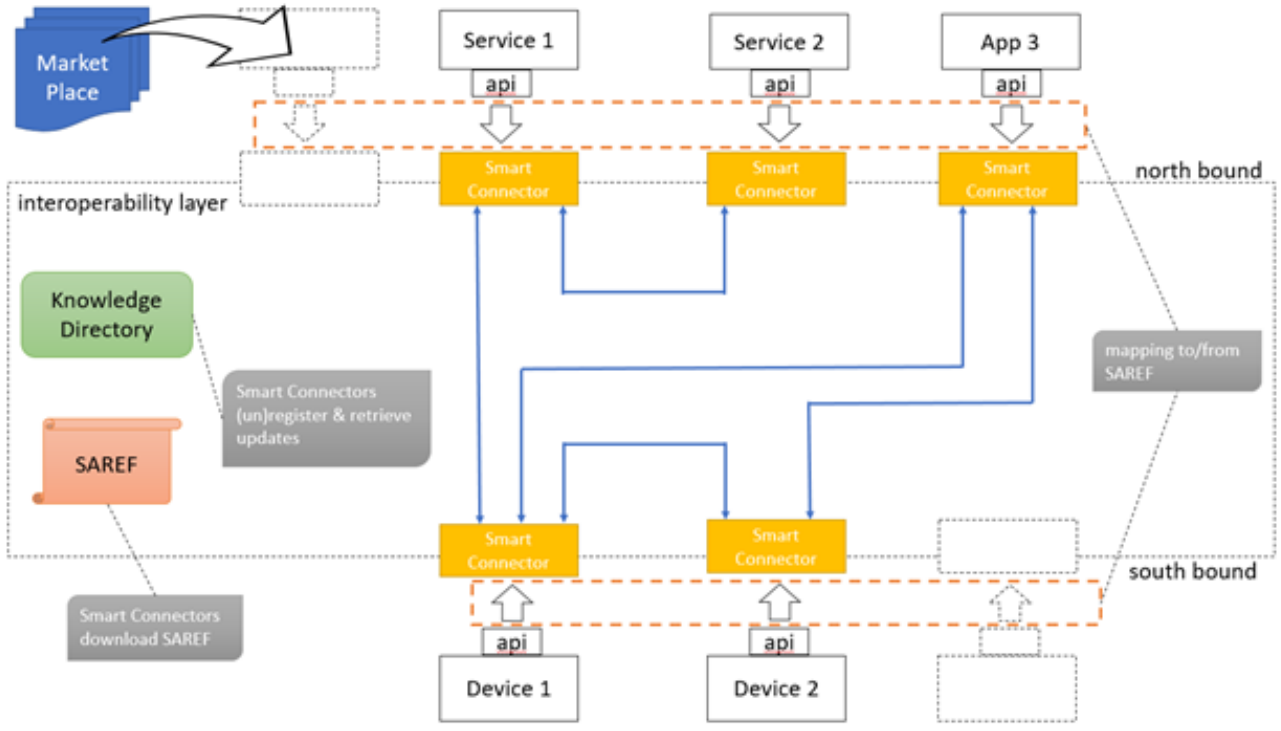


FIGURE 43 – TNO'S / VU SEMANTIC COMPONENTS

5.4.2 WOT FRAMEWORK BY KEO, DFKI, FH DORTMUND AND EEBUS

Category	Objectives
Title and Proposer(s)	EEBUS WOT Framework by KEO GmbH, DFKI, FH Dortmund and EEBUS Initiative
Context and Project(s)	KEO is a founding member of the EEBUS Initiative (2012) and providing software solution sets based on the standardization output of the EEBUS Initiative. EEBUS Initiative is realizing a secure, interoperable machine to machine language for energy relevant devices. KEO has been realizing EEBUS communication by the help of their framework for the mass market for several years. Over 70 companies and Initiatives within the EEBUS Initiative are focussed on bringing their ideas into that standard and their products. Besides that, KEO was member in several research projects on EU, on German government and on Federal State level. Within InterConnect, the KEO EEBUS SAREF Framework will be enlarged with a Web of Things Semantic Interface of the DFKI to an EEBUS WOT Framework. DFKI and FH Dortmund are already successfully designing WoT based applications in smart home and smart living projects like SENSE and Foresight (SENSE WOT).
Maturity	The KEO EEBUS Framework is running in mass market products since more than three years (TRL 9). The main idea of EEBUS is to realize an interoperable machine to machine language. Therefore, the open source EEBUS standardisation documents (Use Case descriptions, Protocol Specifications, Resource Specifications, etc.) will be constantly enhanced with new demands and the implementations tested within ongoing so called EEBUS-Plugfests. Web of Things is accepted as a standard by the W3C for describing IoT applications in a manufacturer and application independent fashion (TRL 8). The new InterConnect Use Cases and the EEBUS WoT Framework will be further developed within the running project. The general concept was already presented at lab level within the Sense Research Project (TRL 4) founded by the Ministry for Economic Affairs and Energy of Germany.
Overview	Communication between the EEBUS devices is managed by the EEBUS WoT Framework (see Figure 44). It has to be integrated within the device software and connect their data and application to the EEBUS WoT Framework. The interface details are depending on the Use Cases which should be used. Using the stack in the InterConnect Southbound/Northbound -System is nearly the same. To get everything up and running in a very fast way all InterConnect parties get the opportunity to use and test the EEBUS SAREF Framework (C++) free of charge for non-commercial use only within the InterConnect project. Examples, different IPC interfaces,

	Doxygen documentation and training is included. All pilots can be equipped with EEBUS device communication. The device communication can support the following energy domains: HVAC, Inverter (PV, Battery), E-Mobility, Metering, White Label Devices, Grid-Interaction. The following solution clusters are depictable based on the current defined Use Cases: Grid defines Power Limit, Market sets Price of Energy (€/kWh), Offer of Flexibility Potential, Increase of Self Consumption, Monitoring and Comfort, System Setup.
Semantic Components Description	Using JSON-LD as description format, Web of Things describes IoT devices and applications as Things defined by their properties (readable values like sensor values), actions that offer affordances to interact with them and events systems can subscribe to. Additional semantics can be added by adding the corresponding namespaces to the JSON-LD context and annotating the respective fields with the appropriate semantic type from that given namespace. Moreover, making use of Binding Templates allows for interacting with a range of different protocols for addressing already existing devices independent of their specific implementation details. Figure 45 shows the SENSE WoT TD model conceptually, which has a device-centric view of the modelled relationships. The primary class of a TD is the Thing, which has been extended by a Location-View (building centric view) related to a building. The exact modelling of this structure is currently not finalized and should adapt to other ongoing developments (e.g., BIM, BOT, SAREF4BLDG). Furthermore, an extension of the TD model for the device and hardware description has been made (Hardware View). The linking of the above views with the TD is done according to the Linked-Data principle. This procedure does not violate the TD specification. The generated TD instances/individuals are still valid. Systems that do not process location or hardware information can ignore the links to these data structures. Figure 46 shows more details of the EEBUS WoT Framework and the communication to other devices. Only few decisions must be taken before the integration work can be started. The goal of the EEBUS WoT Framework including the KEO JSON API or the Use Case API is to offer a programming interface to manufacturers that is much more akin to the high-level description of EEBUS Use Cases and does not required a deep understanding of EEBUS SPINE. An EEBUS device equipped with the KEO JSON API reads all relevant resources from remote devices automatically and discovers which EEBUS Use Cases the remote device supports. Then it presents the relevant data in an easy and user-friendly way.
Reasoning support	**[Level 2]** - advanced reasoning to infer new knowledge.

	While plain WoT Thing Descriptions do not provide any reasoning support, by adding semantic annotations and lifting the description to a semantic level, reasoning can be used to its full extent as with any other semantic representation.
Compliance with SAREF	**[Level 2]** - intermediate SAREF compliance. Within the EEBUS network the device to device communication is running via SHIP (Smart Home IP) and SPINE (Smart Premises Interoperable Neutral-message Exchange) which is SAREF4Ener compliant. The JSON Data on local energy manager (Northbound) will be enhanced to WoT (Web of Things) which is based on W3C standardized concept for semantic descriptions of selected data, functions and interactions. SAREF can be fully integrated into these descriptions as annotations to the existing JSON-LD properties, or a SAREF representation of the entire Thing Description can be derived based on the JSON-LD document (therefore Level 2).
Supported data formats	The supported data formats are JSON-LD, JSON (SHIP).
Supported standards and protocols	For the device to device communication the supported protocol is EEBUS SHIP and SPINE. The interface on a device level can be chosen as an IPC-interface like MQTT, WebSockets, RESTful or dBus which shares data in a JSON format or as a direct C++ function interface. In addition to EEBUS the SENSE WoT Adapter e.g., to SML, KNX, (W-)M-Bus, ZigBee, Z-Wave, DALI.
	Sense WoT and on SHIP level the communication is based on TLS 1.2. For the EEBUS one-time registration process must be released by the end and uses certification sharing mechanisms. The used security algorithms are proofed by the German BSI which is used within also responsible.
	KEO offers all InterConnect parties the opportunity to use and test the EEBUS SAREF Framework (C++) free of charge for non-commercial only. Examples, different IPC interfaces, Doxygen documentation and training is included. The documentation of the EEBUS Specification is Open Source under: https://www.eebus.org/media-downloads/ Web of Things is an established W3C standard presented at https://www.w3.org/WoT/, the specification can be found at https://www.w3.org/TR/wot-thing-description/.
	EEBUS is interoperable and secure machine to machine communication based on standardized Use Cases. It defines in detail the shared data and if it is optional, recommended or mandatory but not the way how to use it. This gives the manufacturers the opportunity to differentiate. If devices are EEBUS compliant the interaction with devices of other manufacturer is included and the end customer can get the same service from different manufacturers.

	Fields of research concerning SENSE WoT: • Interoperable description of payload data structures (data schemas); • Consideration of ontology constraints; • Ontology mapping; • Enhanced Query APIs (SPARQL) and Reasoning. Strengths of WoT: • Use of a manufacturer-neutral, standardized data model (W3C Web Thing Description); • Data model is based on ontologies and is therefore machine-readable and explicit; • The additional use of iot-schema allows a more detailed description of device types/capabilities and an extended functional description; • The Linked Data principle allows for loose coupling and leaves room for future extensions (e.g. detailed hardware description). Dynamic modification of individual model properties. e.g., subsequent location/room modification.

TABLE 26 – EEBUS'S SEMANTIC INTEROPERABILITY SOLUTION

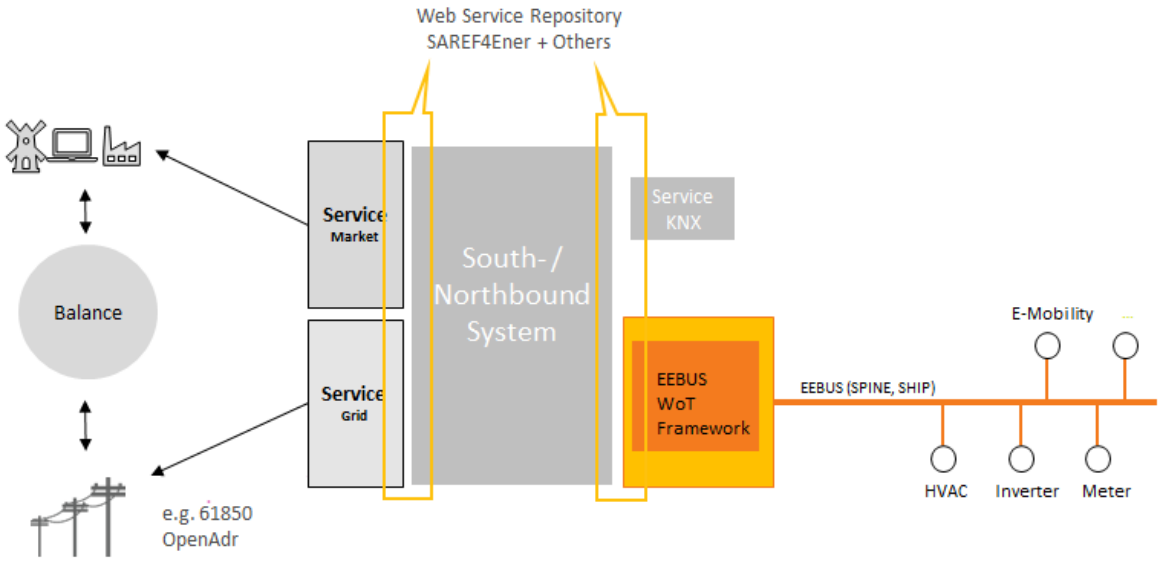
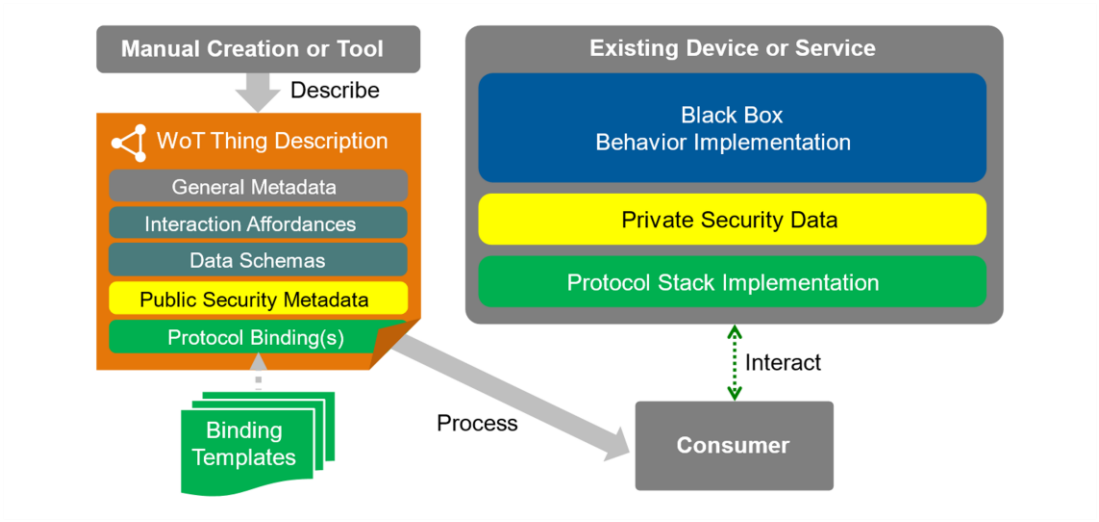


FIGURE 44 – EEBUS'S WOT FRAMEWORK



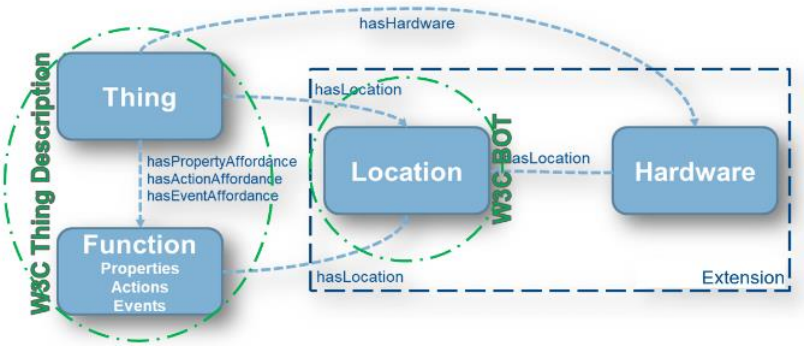


FIGURE 45 – EEBUS'S WOT FRAMEWORK

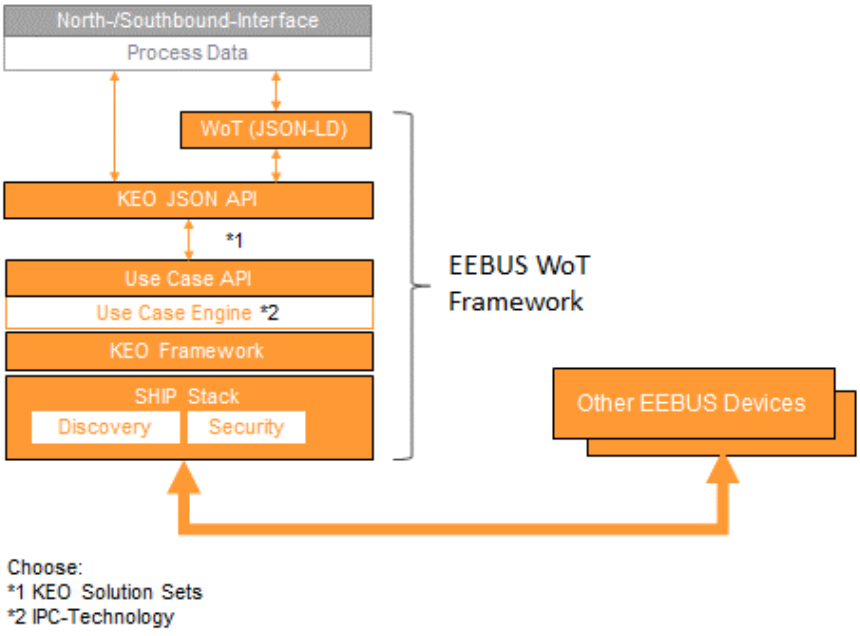


FIGURE 46 – EEBUS'S WOT FRAMEWORK

5.4.3 IOT ONTOLOGY BY KNX

Category	Objectives
Title and Proposer(s)	KNX IoT Ontology
Context and Project(s)	The KNX IoT Ontology is currently under development between KNX Association and its members and aims at achieving three different goals: • System Documentation of current KNX installations (e.g., for BIM purposes) - referred to as the KNX Information Model; • System Representation (for easier and IT-friendlier access to useful data generated by KNX devices in existing installations) - referred to as KNX IoT Type 3; • System Communication (for IP field level device to device communication) - referred to as KNX IoT Type1. The KNX IoT Ontology is already submitted to become part of the EN50090 series as Part 6-2 and the current version can be accessed via: https://schema.knxiot.org/ontology (link will possibly be updated in the future).
Maturity	The KNX IoT Ontology is currently at TRL4 level. A proof of concept is being developed by the KNX Association itself. Some KNX members are currently developing KNX IoT Type 3 gateways, while others are concentrating on readying KNX IoT Type 1 devices.
Overview & Semantic Components Description	The KNX system is designed for direct exchange of information (i.e. communication) between networked devices controlling applications in and around buildings. These different aspects of the KNX environment are shown in Figure 47 and reflected by an individual “model” for Location, Devices, Applications as well as the Communication for exchange of control information (depicted in Figure 48). All individual model parts together form the entire KNX IoT Information Model as a single ontology. Figure 48 describes the KNX Information Model parts. It contains the following: • Equipment (devices and other physical assets); • Application Software (software to run the intended system behavior); • Point (interface to interact with data points mainly provided by devices); • Aspects (grouped points that identify a specific view/perspective to the system); • Location (structural building elements). The current KNX Information Model does not consider other aspects of a HBES installation such as for instance topology or device models.

	The KNX Information Model does not yet foresee an explicit mapping to SAREF with a so called “bridging” ontology. If concepts are identical in both ontologies, a mapping is technically possible. The KNX Information Model uses the location concepts from IFC and allows a semantic representation to utilize its flexibility and extensibility. For this the KNX Information Model supports an explicit mapping to IFC with a so called “bridging” ontology. The HBES-IFC mapping, respectively the bridging is available as electronic turtle file under https://schema.knxiot.org/ontology/owl-mapping/knx-ifc-mapping (link will possibly be updated in the future). The KNX IoT Type 3 interface can be accessed via RESTful webservices specified with the OpenAPI framework. Some of the semantic information of the KNX IoT Ontology (those related to building elements and functions) are accessible via this Type 3 interface. In the data exported from the KNX common design and configuration tool ETS, all semantic information related to a KNX installation is included.
Reasoning support	**[Level 2]** - advanced reasoning to infer new knowledge. Semantic reasoning supported for the KNX IoT ontology.
Compliance with SAREF	**[Level 1]** SAREF is taken into account and an explicit mapping to SAREF exist via a document
Supported data formats	For KNX IoT Type 1 communication it is foreseen that devices will use JSON or CBOR to exchange data. For KNX IoT Type 3 the data is exchanged in JSON. KNX Classic Devices exchange their data still in binary format.
Supported standards and protocols	The KNX IoT Ontology is available in the following triple serialization formats: TTL (turtle), RDF/XML, JSON-LD. The protocols that are used are: • Southbound: KNX Classic (EN50090) Northbound Type 3 interface: REST-API
Security and Privacy	Security that is implemented is: • **Southbound:** KNX data Security and/or KNX IP Secure (see EN50090-3-4 and ISO EN 22510); • **Northbound:** oAuth2 for KNX IoT Type 3 (RFC 6749), dTLS for KNX IoT Type 1
Accessibility and License	The KNX IoT Specifications are being established as we speak. The KNX IoT Ontology in its current state is freely available (see above link) and is in the process of being standardized as EN (see above). The KNX IoT Specifications will become available as part of the KNX Standard, which can be freely downloaded in MyKNX.

	If companies wish to brand solutions based on the EN or KNX standard with the KNX trademark, then the device needs to be submitted to KNX certification (during which KNX membership is needed).
Strengths	In the framework of the InterConnect Project, the KNX IoT Ontology is a way to interact with KNX
Weaknesses	The mapping to SAREF (for those concepts for which this would be possible) is still missing

TABLE 27 – KNX'S SEMANTIC INTEROPERABILITY SOLUTION

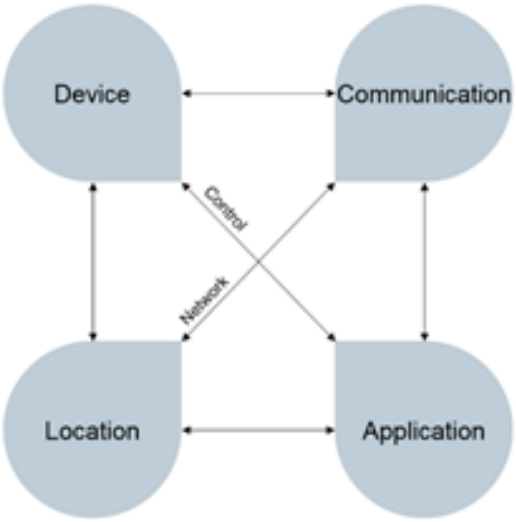


FIGURE 47 – KNX ENVIRONMENT

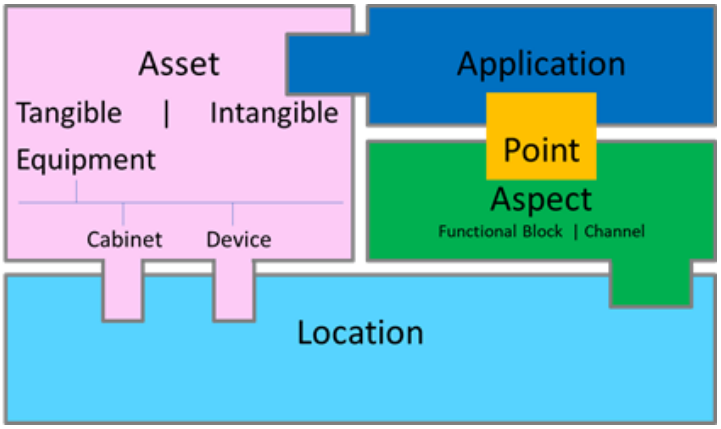


FIGURE 48 – HBES INFORMATION MODEL

5.4.4 SENSOR-BASED LINKED OPEN RULE (S-LOR) BY TRIALOG

Category	Objectives
Title and Proposer(s)	Sensor-based Linked Open Rules (S-LOR): A semantic reasoner for IoT
Context and Project(s)	The Sensor-based Linked Open Rules (S-LOR) project is a PhD research outcome [21] (2012-2015) that has been afterwards refined for the needs of the following projects: • European projects such as the FIESTA-IoT EU H2020 project (2015-2018) that covers domains such as IoT, smart cities and smart buildings; • USA National Institute of Health (NIH) projects (2018-2020) for healthcare and well-being domains, more precisely, asthma, depression, and obesity. Ideally, for the needs of the InterConnect project, we could extend the S-LOR project to cover and refine those domains: home, building, energy, and grid.
Maturity	TRL 5 - technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies), as it is the outcome of PhD research implemented and refined for the needs of various projects (FIESTA-IoT EU H2020, USU NIH Health) mentioned above. For instance, the FIESTA-IoT project integrates the reasoning/inference engine to interpret IoT data. The rule-based reasoning engine is compatible with the M3/M3-lite ontologies[54].
Overview	InterConnect Task 2.4 is focused on semantic interoperability and introduces the need of a semantic reasoning. We suggest a semantic reasoner compliant with ontologies (e.g., SAREF). Our current semantic reasoning is a rule-based reasoner compliant with ontologies (e.g., the M3 ontology that extends the W3 SSN ontology V1). The rule-based reasoner has been also integrated with FIESTA-IoT ontologies that integrates various IoT ontologies such as M3, IoT-lite, SSN, etc. within the FIESTA-IoT H2020 project. The end-to-end architecture provided in Figure 49 below uses data generated by devices (e.g., temperature, humidity) to be stored and managed within the InterConnect Framework/Platform. The Semantic Annotator API component explicitly annotates the data (e.g., unit of the measurement, context such as body temperature or outside temperature) and unifies data when needed (e.g., a same temperature sensor provided by various companies can generate different open or proprietary descriptions). The semantic annotation uses ontologies that can be found through ontology catalogs (e.g., LOV4IoT ontology catalog http://lov4iot.appspot.com/). The ontology chosen must be compliant with a set of rules to infer additional information. The Reasoning Engine API

[54] More information can be found in:

- A Review of Tools for IoT Semantics and Data Streaming Analytics. Book: The Building Blocks of IoT Analytics - Internet-of-Things Analytics [Serrano et al. 2016]. Our Figure 6.5 IoT reasoning data framework within FIESTA-IoT is explained page 18.
- Paper: Experimentation as a Service Over Semantically Interoperable Internet of Things Testbeds [Lanza et al. IEEE Access Journal 2018] See Section 3) Reasoning tools, page 11.

	(inspired from [20] [21] [22] [23] [18]) deduces additional knowledge from data (e.g., abnormal temperature) with the usage of inference engine (e.g., rule-based reasoning comprises IF THEN ELSE rules). The rules executed by the inference engine will add new data in the InterConnect data storage (e.g., triplestore). Finally, enriched data can be exploited within end-user services available within the InterConnect Service Marketplace (e.g., call the firefighter when the temperature is abnormally high, and smoke is detected; a fire might have been detected; it might be an emergency) or any services offered in InterConnect.
Semantic Components Description	The reasoning engine for IoT devices to infer meaningful information specification is inspired from [20] [21] [22] [23]. We can contribute as follows (also explained within the semantic interoperability for IoT white papers [24] [25]): A rule-based reasoning provides simple IF THEN ELSE logical rules. It will enable deducing meaningful information from semantic sensor data (e.g., IF the room temperature is below 15 Degree Celsius, THEN the temperature in the room is considered as cold). It can be achieved, for instance, with the Apache Jena framework, an open-source Java RDF library which also provides an inference engine (rule-based reasoning) to deduce meaningful knowledge from semantic datasets. AndroJena, a light version of the Jena framework, compatible with Android devices, also provides the query engine and the inference engine for constrained devices if needed. The Jena inference engine is used to infer high-level abstractions by executing a set of 'common sense' rules (e.g., following guidelines from experts such as those from the pilots). Ideally, the rule is compliant with: • The Jena framework; • The W3C Sensor Observation Sampler and Actuator (SOSA)/Semantic Sensor Networks (SSN) ontology and its extension; • The Machine-to-Machine-Measurement (M3) [22] [26] ontology that classifies sensor type, measurement type, units, etc. to do analytics and reasoning using semantic information, and • The SAREF ontology and its extensions for specific domains (e.g., SAREF4ENER, SAREF4BLDG). Table 29 explains each step of the Figure 50 that illustrates the data workflow.
Reasoning support	**[Level 2]** - advanced reasoning to infer new knowledge
Compliance with SAREF	**[Level 2]** intermediate SAREF compliance (not only SAREF is taken into account, but machine interpretation is enabled). The M3 ontology[55] can be considered as a SAREF extension with a focus on the concepts describing data generated by devices (saref:Device):

[55] http://sensormeasurement.appspot.com/?p=m3

	• saref:Measurement (e.g., Temperature) or saref:Property. We need more explanations to clearly see the difference between the two concepts. • saref:UnifOfMeasure • saref:FeatureOfInterest
Supported data formats	Within past projects, we developed tools that supported the XML format compliant with the SenML format. A required step for the semantic annotation to be compliant with the M3 ontology. More developments are required to support more formats.
Supported standards and protocols	• **Southbound interface:** We have tools that support XML format compliant with the SenML format. A required step for the semantic annotation to be compliant with the M3 ontology, to be able to execute the semantic reasoner compliant with the M3 ontology. Ontology development is based on semantic web languages such as RDF, RDFS, and OWL. The semantic reasoner is based on the Jena inference engine. • **Northbound interface:** In case, the developers are familiar with semantic web technologies they can execute the Jena reasoner and the Jena rules files. Otherwise ideally, web services could be provided to hide the complexity of using semantic web technologies.
Security and Privacy	In the same way, we unify IoT ontologies, we unified security ontologies within the STAC project (explained hereafter). However, the semantic reasoner itself, does not implement security mechanisms. Security Toolbox: Attacks and Countermeasures (STAC)[56] is a parallel project that we developed to assist developers in: • Designing secured applications or architectures; • Being aware of main security threats; • Exploring security in various technologies such as: Sensor Networks, Cellular Networks (2G, 3G, 4G), Wireless Networks (Wi-Fi, WiMAX, Zigbee, Bluetooth), Mesh/M2M/MANET, Network Management, Web Applications, Cryptography, Attacks & Countermeasures, Security Properties (e.g., authentication, integrity), etc. We developed the STAC Security Knowledge Graph to unify security ontologies from various security domains relevant for IoT.
Accessibility and License	We have online demos[57]. S-LOR is under GNU GPLv3 license, a component of the M3 (Machine-to-Machine Measurement) framework. The are numerous publications describing the project[58]. In the INESC TEC presentation, they highlight the issues regarding Intellectual Property when a project is refined with several projects.
Strengths	SLOR has been developed and refined following agile development methodologies. It is a PhD research outcome then refined for the needs of various projects to cover more and more domains such as: • FIESTA-IoT EU H2020 project covers Io, smart cities and smart buildings;

[56] http://securitytoolbox.appspot.com/

[57] http://linkedopenreasoning.appspot.com/?p=slorv2

[58] http://linkedopenreasoning.appspot.com/?p=publication

	• Health projects to cover healthcare, well-being, and Affective Sciences. For instance, kHealth is dedicated to asthma; ACCRA H2020 EU project to cover robotics, assist elderly people, Ambient Assisted Living (AAL).
Weaknesses	• For the InterConnect project, extensions are needed to cover the domains relevant for this project: smart home, building, energy, and grid; • We need the help force to enrich the system and have a clear vision of end-user applications (provided by the pilots) that are required for the project to verify that the semantic reasoner will be relevant for the needs. Help is needed for the development part, and the integration with other tools within the project.

TABLE 28 – TRIALOG'S SEMANTIC INTEROPERABILITY SOLUTION

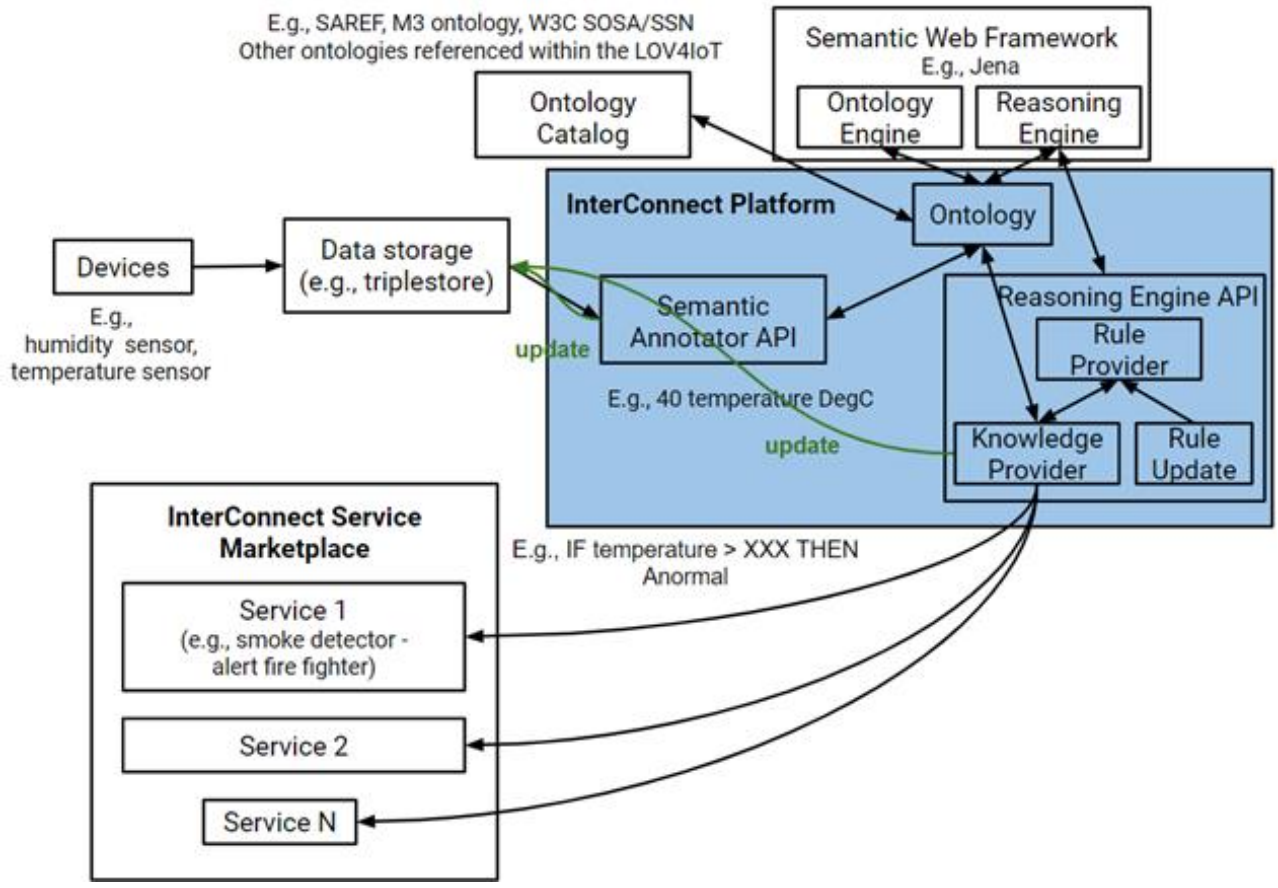


FIGURE 49 – ONTOLOGY-BASED REASONING ARCHITECTURE FROM SENSOR DATA TO END-USER SERVICES

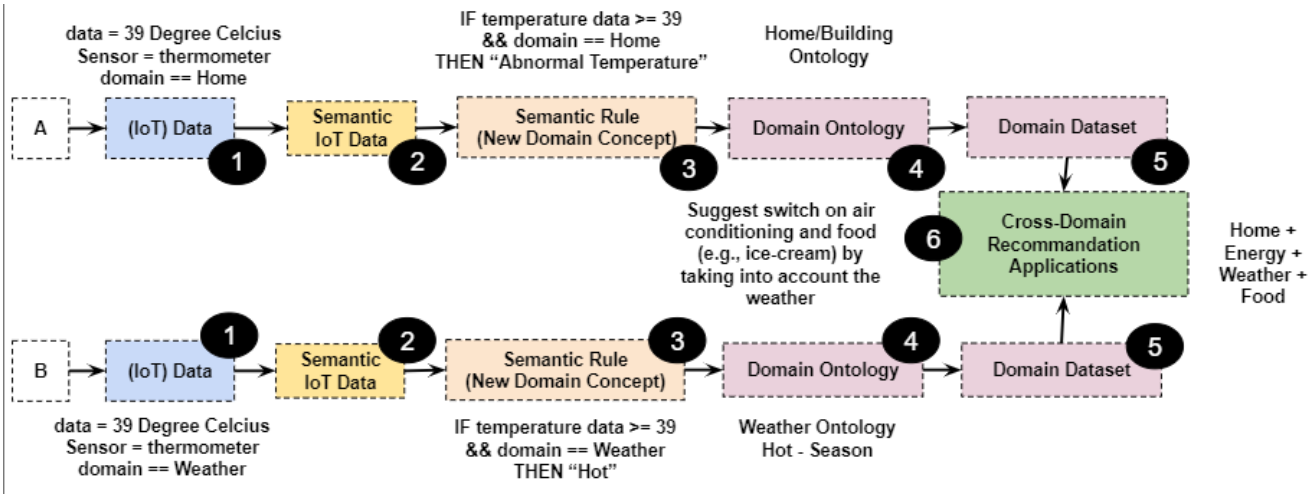


FIGURE 50 – THE IOT KNOWLEDGE-BASED CROSS-DOMAIN RULE-BASED ENGINE & DATA WORKFLOW [26]

Steps	Description
Step 1	The raw measurements generated by the sensors are transformed into metadata with additional attributes: (1) Unit of Measurement, (2) Timestamp, (3) Software Version, (4) Name, (5) Type, and (6) Domain of Operation. Ideally, it could support heterogeneous data formats (e.g., JSON, XML), but requires wrappers to unify sensor metadata descriptions.
Step 2	The framework encodes the metadata using Sensor Markup Language (SenML) to unify sensor metadata before converting into RDF compliant with ontologies (e.g., M3, SAREF ontologies), a key step to later execute the rule-based reasoner.
Step 3	Semantic reasoning drives higher level abstractions as new domain concepts. In the health domain, the reasoning engine explicitly deduces the 'flu' concept; in the weather domain, the 'hot' concept.
Step 4	The respective domain ontologies are used to classify these new concepts; 'flu' as a disease and 'hot' as a seasonal condition.
Step 5	The respective domain datasets are used to link data (e.g., food with diseases, menu with season).
Step 6	The concepts, rules, and datasets of the two domains, are combined and cross-domain semantic reasoning takes place. In this example, the cross-domain reasoning produces suggestions for recipes appropriate for a given state of health and the prevailing weather conditions. The recommendations can be acted upon both by end-users and intelligent machines.

TABLE 29 – STEP DESCRIPTIONS OF THE IOT KNOWLEDGE-BASED CROSS-DOMAIN RULE-BASED REASONER [26]

5.4.5 SEMANTIC LAYER BY GFI

Category	Objectives
Title and Proposer(s)	GFI's Semantic Layer
Context and Project(s)	The Semantic Layer acts as an engine that enables services to be used in many different domains of operations. The focus within InterConnect will be towards IoT (connectivity features) and energy domains for advanced discovery, reasoning and marketplace capabilities. This layer is proposed to be embedded in an IoT platform that facilitates the smart appliance interoperability & smart energy ecosystem.
Maturity	The IoT layer is TRL 9, while the semantic layer is TRL 5 since it has been validated in small-scale pilots. Overall, our objective with the integration of these layers is to reach TRL 9 across the solution. • TRL 5 – technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies) • TRL 9 – actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space).
Overview	See Figure 51. Everything that can be described semantically can be made to automatically be exposed as a semantic service that will be made available in the marketplace where it can be found by users. These services will expose observable and actionable properties of the feature of interest in the physical world. For example: a smart washing machine can be considered as a feature of interest having a load sensor observing the kind of cycle stage that it is at corresponding with its energy consumption as well as the capability to reschedule the program to start later if possible. Thanks to the semantic service it is possible to interact with any kind of smart washing machine using our platform as soon as the capabilities are described semantically using ontologies. In order to increase the level of interoperability the use of standard (upper) ontologies like SAREF will be introduced.
Semantic Components Description	The IoT layer provides the capabilities to connect IT systems with the physical world through the use of many different communication networks and protocols, provides storage facilities next to visualization and reporting functionalities. Whereas the IoT layer may provide syntactical interoperability between the physical world and the IT systems through the use of open standards like REST, the semantic layer adds semantic interoperability to the table. Thanks to the semantic layer the MPP allows the IoT to come to its full potential within the enterprise (ex: smart factory) or open ecosystem context (ex: smart city) by adopting the Semantic Web of Things paradigm. The Semantic Web of Things (SWoT) is an

	emerging vision in Information and Communication Technology (ICT), joining together some of the most important paradigms of the decade: the Semantic Web and the Internet of Things. The Semantic Web initiative aims at allowing available information in the World Wide Web to be seamlessly shared, reused and combined by software agents. Each available resource in the semantic-enabled Web should be properly described in order to infer new information from the one stated in the semantically annotated resource descriptions.
Reasoning support	**[Level 2] -** advanced reasoning to infer new knowledge. As in most situations our platform does not operate in a green field. IoT data use different models and formats (JSON, XML, SenML, CSV, …). Open data sources even use other formats and models. Out platform does not impose a specific data model as it should be as multipurpose as possible. Within our platform we rely on semantic web technology. As a result it does not impose any specific data model. Using our RDFizer component (transforming data into semantic data in RDF format) this data is lifted to a semantic model of choice like SAREF. The semantically rich information obtained is than stored in our triplestore which allows us to enable reasoning when querying the data and metadata supporting our value-added services like data discovery, composition and the marketplace.
Compliance with SAREF	**[Level 2]** - intermediate SAREF compliance (not only SAREF is taken into account, but machine interpretation is enabled). Within our platform we rely on semantic web technology. As a result it does not impose any specific data model. Using our RDFizer component (transforming data into semantic data in RDF format) this data can be lifted to a semantic model of choice like SAREF.
Supported data formats	The Semantic Layer makes use of open standards to communicate internally as well as with external components. We mainly use RESTful APIs with JSON data format.
Supported standards and protocols	• **Southbound interface**: See Figure 52. Currently we support following southbound interfaces: 2G, 3G, 4G, LoRa, Sigfox, LTE-M, NB-IOT through the operator API and open standards like HTTPS, MQTT, SFTP, SNMP, CoAP, OPC-UA. This list can be extended according to the needs using the underlying framework. The use of a gateway component to communicate with our platform is optional. • **Northbound interface:** We provide interfaces using protocols like HTTP, CoAP, WebSockets, OPC-UA, REST. This list can be extended according to the needs using the underlying framework.
Security and Privacy	• GDPR guidelines are adopted to ensure ethical principles involving informed consent, anonymization and controlling access to data. Gfi and its Third Parties will not be collecting or using any non-anonymous data, our contribution will be part of an architecture that does not interface directly with individuals, so we

	expect data to be encrypted and aggregated by partners. Confidentiality is ensured and any breach will be reported.
Accessibility and License	• Refer to the consortium agreement for guidance on access rights. A dual license will be considered based on either research or commercialization purposes.
Strengths	• This solution is highly flexible: a. Different domain verticals could be plugged into the platform b. Interface is available for any of devices, users or developers could c. A variety of protocols & data formats are available d. potential for re-use and integration of knowledge through ontological extension, re-use and alignment. • The ontologies previously used already are either documented to map to SAREF (e.g., SSN/SOSA Ontology) or functionally similar to SAREF. • Enables sharing / trading of data without human involvement • Enables interaction with services without human involvement between HEMS, grid (DSO) and other parties in the ecosystem • Distributed system of systems – no central point • Every node is part of the ecosystem / marketplace
Weaknesses	In order to fulfil InterConnect objectives, the following adaptation should take place: • For InterConnect, there is a need for extensions to cover the domains relevant for this project: smart home, building, energy, and grid; • Pilots implementation will support with to enrich the system, and have a clear vision of end-user applications that are required for the project to verify that the semantic reasoner will be relevant for the needs; • Complete SAREF exploitation will take place within the scope of InterConnect to reach full maturity (level 4); • Extending the application of the semantic engine to reach full maturity at TRL 9.

TABLE 30 – GFI'S SEMANTIC INTEROPERABILITY SOLUTION

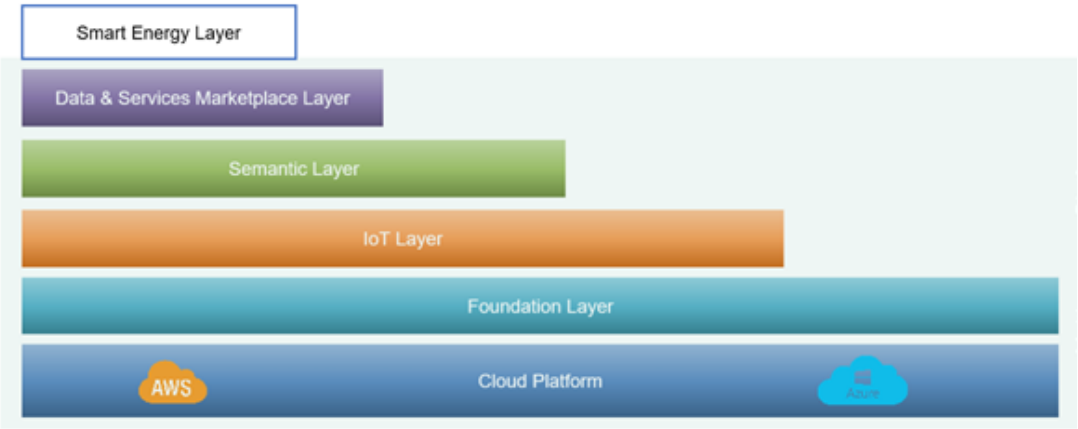


FIGURE 51 – GFI'S DATA SHARING SOLUTION

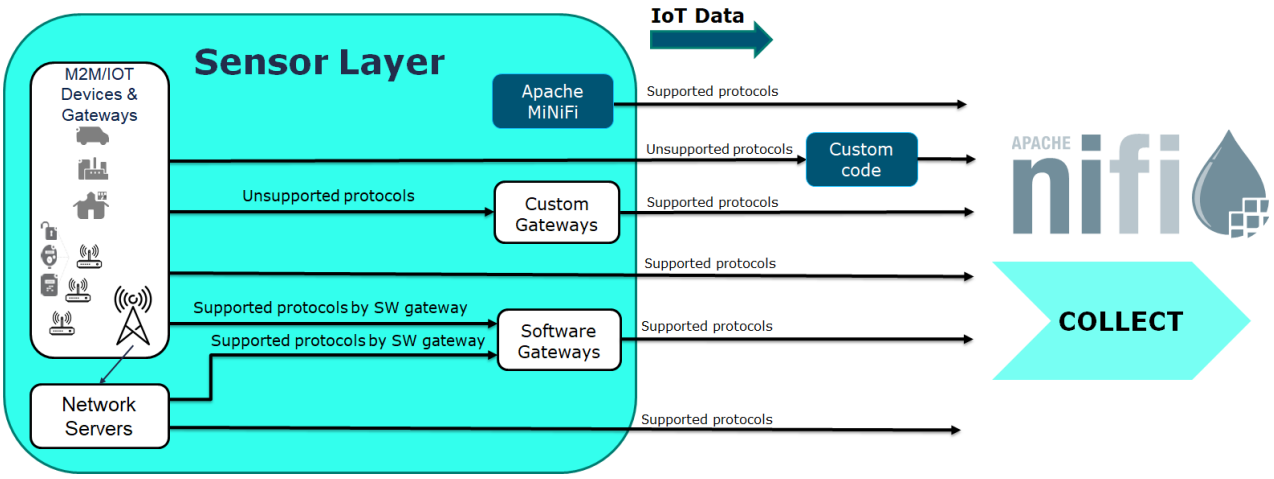


FIGURE 52 – GFI'S DATA SHARING SOLUTION INTERFACES

5.4.6 BOS SOLUTION BY SENSINOV

Category	Objectives
Title and Proposer(s)	Sensinov's BOS (Building Operating System)
Context and Project(s)	Sensinov's BOS (Building Operating System) provides a helicopter view of the facilities management processes, regardless of existing building installations. Sensinov's BOS addresses Smart Building needs in terms of automation and semantic interoperability currently deployed in office and retail sectors, by providing: • Continuous solution integration and operation for Buildings; • Efficient data exposure through modern APIs. Centralised management of heterogenous buildings by supporting global policies, quicker reactions and optimized decisions across all buildings for increased energy efficiency;
Maturity	Sensinov's BOS is TRL 9.
Overview	Sensinov's BOS offers a unified data model and single interface to control any building installation regardless of their vendors. It provides. Building and facility managers can make better-informed decisions, enforce cross building policies and pave the way for automation and wider integration.
Semantic Components Description	Sensinov's BOS interoperability is achieved using the following components, which are shown in Figure 53 and Figure 54: • Hot pluggable and rich set of connectors allowing to integrate virtually any device, automation server or connectivity network to any enterprise application;

	• Data transformation and unification to a common data model using simple structures based in JSON: • Semantic enrichment, where unified data is annotated with additional class of metadata to further improve utility, discovery, and interoperability; • Efficient data exposure, via open and standard interfaces regardless of their vendor or technology; • The mapping from devices to SAREF and vice-versa (Southbound interface) is achieved by mapping module capable of bidirectional translation of Sensinov's data model (JSON) to SAREF ontology (RDF). Sensinov's BOS provides a triple store repository to semantically publish and discover service using a SPARQL over HTTP endpoint.
Reasoning support	**[Level 0]** No reasoning support
Compliance with SAREF	**[Level 2]** Sensinov BOS data model is Level 2 in terms of compliance with SAREF, i.e., intermediate SAREF compliance (not only SAREF is taken into account, but machine interpretation is enabled)
Supported data formats	JSON
Supported standards and protocols	Sensinov's BOS supports the following interworkings: • **Southbound interworking:** MODBUS, Profibus, BACnet, Zigbee, Z-wave, Sigfox and LoRa; • **Northbound Interworking:** HTTP, WebSocket and AMQP.
Security and Privacy	Sensinov's BOS offers Authentication, Authorization and Accounting. (SSL/TLS, JSON web tokens and Role Based Access Control).
Accessibility and License	Sensinov's BOS is a commercial product. A free license will be delivered to InterConnect pilots for the duration of the project. Beyond the duration of the project, continuation of the pilot requires bilateral agreement.
Strengths	Rich device catalogue, Continuous solution integration, unified data model, SAREF support, Efficient data exposure, Centralized management of heterogenous buildings, Wider integration within the city, Cloud native architecture, commercially deployed, etc.
Weaknesses	The current SAREF mapping is limited in terms of device actuation capabilities.

TABLE 31 – SENSINOV'S SEMANTIC INTEROPERABILITY SOLUTION

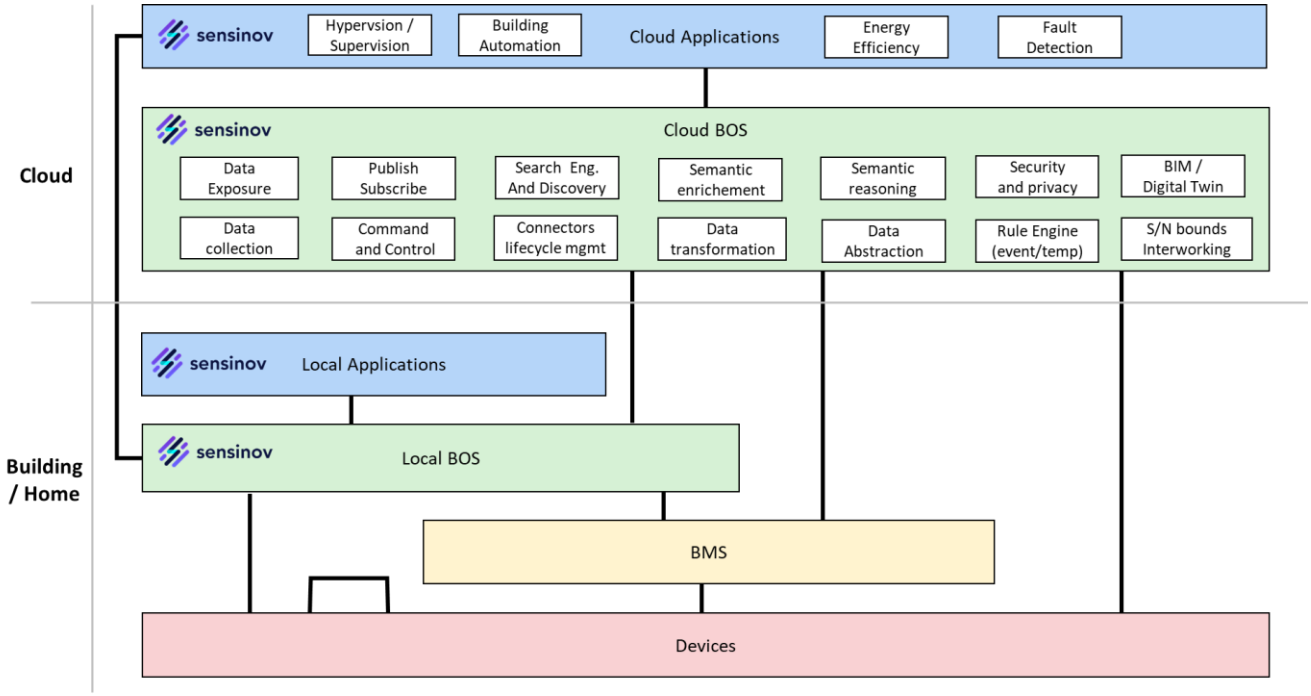


FIGURE 53 – SENSINOV'S FUNCTIONAL COMPONENTS

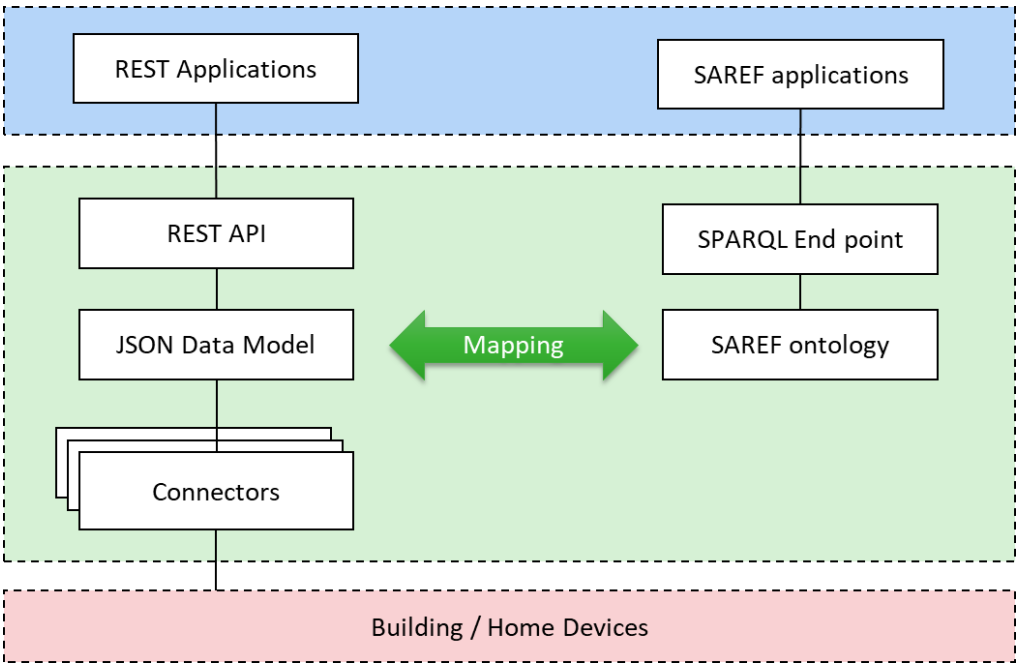


FIGURE 54 – SENSINOV'S DATA MODEL & MAPPING TO SAREF ONTOLOGY

5.5 ANALYSIS

The characteristics of the solutions detailed in the previous section are summarized in Table 32 below.

Solution	Maturity	Reasoning support	SAREF compliance	Data formats	Supported standards & protocols	Security & privacy	License & availability
TNO/VU	TRL5	Level 3	Level 3	any (e.g., JSON, XML, CSV, RDF, etc.)	any (e.g., HTTPS, JMS, SPARQL, etc.)	-/+	Open-source
EEBus/ KEO/ DFKI	TRL 4 (TRL 9)[59]	Level 1	Level 2	JSON (SHIP), JSON-LD, XML	SPINE, SHIP, W3C Web of Things (WoT), MQTT, WebSockets, RESTful, dBus; SENSE WoT Adapter e.g. to SML, KNX, (W-)M-Bus, ZigBee, Z-Wave, DALI	++	Binary freely available for IC partners
KNX	TRL4 (TRL9)[60]	Level 2	Level 1	JSON, JSON-LD CBOR RDF	KNX classic (binary), KNX type 3 (rest API)	+	Specifications publicly and freely available. KNX branding requires membership
Trialog	TRL5	Level 2	Level 2	XML SenML, but potentially any RDF	SPARQL	-	GPL v3 (open source)
GFI	TRL5 (TRL 9)[61]	Level 2	Level 2	JSON over REST	2G, 3G, 4G, LoRa, Sigfox, ZigBee, Z-Wave, LTE-M, NB-IOT and open standards like HTTP, MQTT, FTP/SFTP, SNMP, OPC-UA, CoAP, WebSockets, REST	++	dual license for research or commercializati on binaries
Sensinov	TRL9	Level 0	Level 2	JSON RDF	MODBUS, Profibus, BACnet, Zigbee, Z-wave, Sigfox and LoRa, HTTP, WebSocket and AMQP	++	free license to the InterConnect pilots binaries until 2023

TABLE 32 – SUMMARY OF AVAILABLE SOLUTIONS

[59] Note that (TRL9) is between brackets as it denotes the maturity of the full commercial solution, while the maturity of the semantic aspects of this solution is actually much lower

[60] Same as above

[61] Same as above

We can make the following observations from this table and the descriptions in Section 1.5.

MATURITY

The maturity levels for all six solutions vary from TRL4 ‘Standalone: The functionality has been implemented and passed standalone methodological and functional validation tests’ to TRL9 ‘The class has been used successfully in production-grade analysis work’. This means that all the software is implemented and can be deployed, tested and compared in the various use-cases. We further note that the solutions that are already commercially available, such as the ones provided by KEO/EEBUS, KNX, GFI and SENSINOV have the highest TRL (i.e., TRL 9). However, when looking at the semantic aspects of these commercially available solutions, the maturity becomes lower (e.g., TRL 4 for KEO/EEBUS and KNX, and TRL 5 for GFI). Therefore, we can conclude that the maturity of the semantic solutions that the various consortium partners bring to InterConnect starts at TRL 4 to 5. We acknowledge the need to take these results to a higher TRL level, bringing them into (distributed) operational environments that go across vertical domains (silos) and are deployed on a large scale, in a way that is reasonably easy to adopt also for developers that are non-ontology/semantic technology experts (who are the majority out there).

REASONING SUPPORT

Most solutions are equipped with some level of semantic reasoning support, albeit only part of them (TNO/VU, KNX, TRIALOG, GFI) uses semantic web technology which makes it easier to combine, align and compare their functionality. We further see that only one solution (i.e., TNO/VU) offers the highest reasoning support (level 3) which allows not only to infer new knowledge, but also to orchestrate the data exchange. It is important to note that in this deliverable the reasoning capabilities of only the semantic interoperability layer are discussed (intended as reasoning based on ontologies using semantic web technologies, such as RDF, OWL and SPARQL). The eventual reasoning capabilities of other components, like, for example, the machine learning algorithms underlying the forecasting services, or the flexibility management operated by the home/building energy manager, lies out of this scope.

SAREF COMPLIANCE

Compliance with SAREF is one of the requirements specified in IC, and as can be seen, not all solutions are yet able to natively 'speak' SAREF or have converters to make the translation to SAREF concepts. We note that although several solutions (KEO/EEBUS, TRIALOG, GFI, SENSINOV) present a fair level of SAREF compliance (level 2), only one solution (TNO/VU) presents the highest level of compliance (level 3).

DATA FORMATS

As can be seen from Table 10, most of the solutions support JSON and often RDF and/or JSON-LD. Therefore, we conclude that a mapping of these formats to RDF/OWL via adapters can be fairly straightforward. For an extensive analysis of the platforms available in InterConnect and their supported data formats, refer to D5.1 – "Concept design and architecture of the interoperable marketplace toolbox" [43].

SUPPORTED STANDARDS AND PROTOCOLS

The so-called South-bound interface capabilities of the various solutions vary a lot, both in type and number of supported standards and protocols. In general, we note that support for adapting the most adopted specific technology in Table 10 (such as REST, MQTT, SPINE/SHIP) to semantic technologies like RDF/OWL/SPARQL will be needed. For an extensive analysis of the platforms available in InterConnect and their supported standards and protocols, we refer to D5.1 - "Concept design and architecture of the interoperable marketplace toolbox" [43].

SECURITY AND PRIVACY

The strength of the security is as strong as its weakest link. It can be noted that commercially available solutions (such as, KEO/EEBUS, KNX, GFI and SENSINOV) have a stronger security and privacy level than prototype solutions in small-scale demonstrators, such as TNO/VU and TRIALOG. Since our goal is to have all solutions being part of the semantic interoperability layer, it is key that every solution has the highest security and privacy standards implemented. As can be derived from the descriptions, some solutions will need to work on that, which will be a key effort during the following period.

ACCESSIBILITY AND LICENCE

As long as the specifications of the interoperability layer, the vocabularies, schema's and communication standards are open and free to use by the public, commercial implementations of various components do not limit, but actually stimulate a vibrant development community. As we can see from the matrix, most solutions are shared only with the consortium members in binary format, with two exceptions (i.e., TNO/VU and TRIALOG) which are open source.

5.6 COMPARISON

From the analysis in Section 5.5 we can conclude the following:

- The maturity of the semantic solutions that the various consortium partners bring to InterConnect starts at TRL 4 to 5. The project will bring this to a higher TRL level, deploying its recommended semantic solution into large-scale operational environment into the various InterConnect pilots.
- Only the Knowledge Engine solution provided by TNO/VU offers the highest reasoning support (level 3) which allows not only to infer new knowledge, but also to orchestrate the data exchange.
- Similarly, also concerning SAREF compliance, the Knowledge Engine solution provided by TNO/VU is the only one to present the highest level (level 3), namely the direct use of SAREF concepts expressed in Sematic Web standards such as RDF/OWL.
- Most of the solutions support the JSON data format; some sloutions provide support also for Semantic Web standards such as RDF and/or JSON-LD; but only one solution, namely the Knowledge Engine solution by TNO/VU, in addition to Semantc Web support, provides in principle the flexibility to work with any data format (via mappings).
- Similarly, concerning supported standards and protocols, the Knowledge Engine solution by TNO/VU provides the flexibility to work in principle with any of the standards and protocols supported by all the other solutions (via adapters).
- Commercially available solutions, such as, KEO/EEBUS, KNX, GFI and SENSINOV, have a stronger security and privacy level than prototype solutions in small-scale demonstrators, such as TNO/VU and TRIALOG. However, none of the analysed solutions offers specifically support for security and privacy at the semantic level (which is actually offered by the underlying platforms). Therefore, the project will have to

actively include security and privacy by design as part of the recommended solution for the semantic interoperability layer.

- Most solutions are at least accessible by the consortium members, with two exceptions (i.e., TNO/VU and TRIALOG) which are open source and have the potential to grow even further and hopefully faster in an open ecosystem/community within and outside InterConnect.

Based on this analysis, the Knowledge Engine solution provided by TNO/VU is chosen by InterConnect as the recommended solution to implement the semantic interoperability layer, especially for its strength of being specifically developed to work with semantic technologies, and, therefore, providing the highest support for semantic reasoning and SAREF compliance, which are the main requirements for the semantic interoperability layer. Moreover, the Knowledge Engine solution provides by design the flexibility to work with various, distributed, heterogeneous devices, services and platforms by making use of mappings and adapters to, in principle, any data format, standard and protocol (although the mappings and adapters specifically needed in InterConnect will have to be developed during the project). In addition, because of the open-source nature of the Knowledge Engine initiative, its current deployment at TRL 5 has the potential to largely and quickly grow to higher TRLs within and outside the InterConnect ecosystem, in the open and inclusive manner foreseen by the semantic interoperability layer vision.

The choice of the Knowledge Engine is considered as the most suitable to be used as basis for the InterConnect semantic interoperability layer, but, at the same time, it does not exclude the other semantic solutions presented in this Section, which should rather be seen as complementary. The possible integration of the other available semantic solutions in Section 5.5 with the Knowledge Engine, is an ongoing work in the project.

The semantic solution proposed by KEO et al. (see Section 5.4.2) is based on the WoT architecture and its Things Description (TD), which became a W3C recommendation in April 2020[62], including also Security and Privacy Guidelines for the secure implementation and configuration of Things. The structure of the TD and its described formats can be transformed, just as any other format, into the semantic standards used by the Knowledge Engine using

[62] Web of Things (WoT) Architecture (w3.org)

smart connectors. An open question is that WoT is flexible with regards to the ontology that is being used, while the InterConnect project prescribes SAREF as the ontology of choice. Therefore, it is planned by KEO et. al to adapt to the InterConnect requirements by only using SAREF for thing descriptions of EEBUS devices. On the other hand, it is open to investigation in the future whether the Knowledge Engine could extend its reasoning mechanisms for orchestration of data exchange using the W3C WoT Things Description.

Concerning the S-LOR solution proposed by Trialog (see Section 5.4.4), its semantic reasoner can also be adapted to the requirement of SAREF compliancy of InterConnect, as it is based on an ontology that will be mapped to SAREF with explicit links such as `owl:equivalentClass`, `rdfs:subclassOf`, `rdfs:seeAlso` or using SAREF concepts or properties directly (saref:isMeasuredIn, saref:hasValue, etc.). The S-LOR semantic reasoner is mainly focused on unifying datasets in different formats for further processing, such as reasoning to infer new knowledge as described in Section 5.2.2, while the Knowledge Engine provides the additional functionality of reasoning for the orchestration of data exchange.

Other semantic solutions that scored relatively high in our analysis concerning SAREF compliance (level 2), like the ones proposed by GFI and SENSINOV, can be integrated into the recommended solution via the mappings and adapters offered by the Knowledge Engine, gaining, in this way, also the possibility to increase their reasoning support offered by the InterConnect semantic interoperability layer. The KNX solution based on the KNX IoT ontology, although it presents a relatively high level of semantic reasoning (level 2), is not considering in the immediate future to further work its mappings to SAREF. However, in principle, by working out these mappings via the adapters offered by the Knowledge Engine, it is possible to integrate also the KNX solution into the InterConnect semantic interoperability layer.

5.7 RECOMMENDED SOLUTION

The recommended solution for implementing the InterConnect semantic interoperability layer is based on the Knowledge Engine, as the main enabler for semantic interoperability adapters and reasoning for services running on digital platforms. The next sections present an overview of the recommended solution, a description of the components that this solution prescribes in

the semantic interoperable information architecture, a running example that shows how reasoning works, and additional information about the technology underlying the recommended solution.

5.7.1 OVERVIEW

Figure 55 shows the IC's interoperability framework as described in D5.1 [43]. Existing devices, services and platforms in the InterConnect ecosystem, but also newly built apps within the project, will be able to interact with each other in the IC's interoperability framework via adapters and connectors that give them access to the reasoning and discovery functionality of the semantic interoperability layer. The Knowledge Engine (KE) described in Section 5.4.1 is used as basis for implementing the semantic interoperability layer.

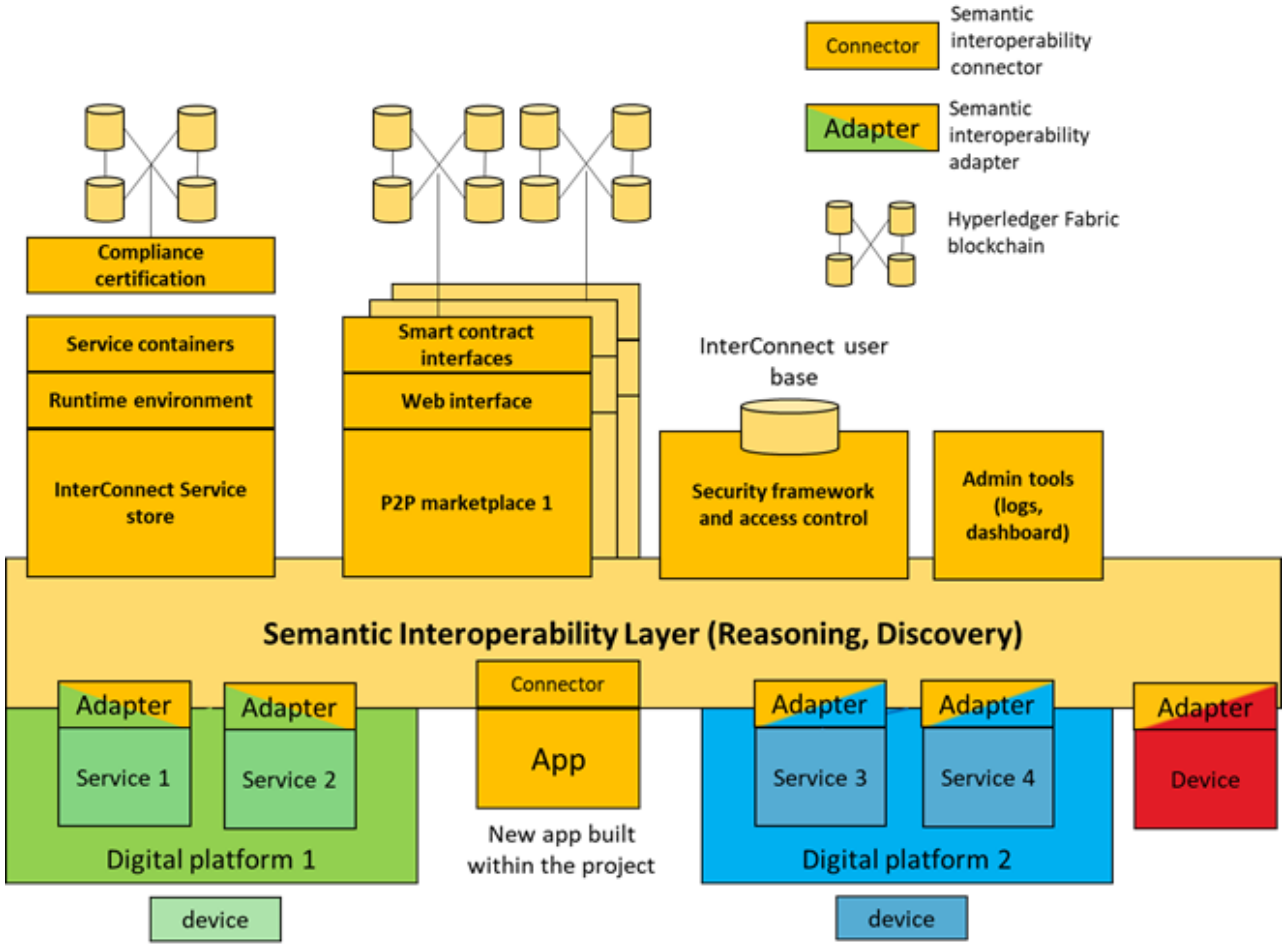


FIGURE 55 – INTERCONNECT'S INTEROPERABILITY FRAMEWORK

Figure 56 zooms into the specific KE components of the semantic interoperability layer.

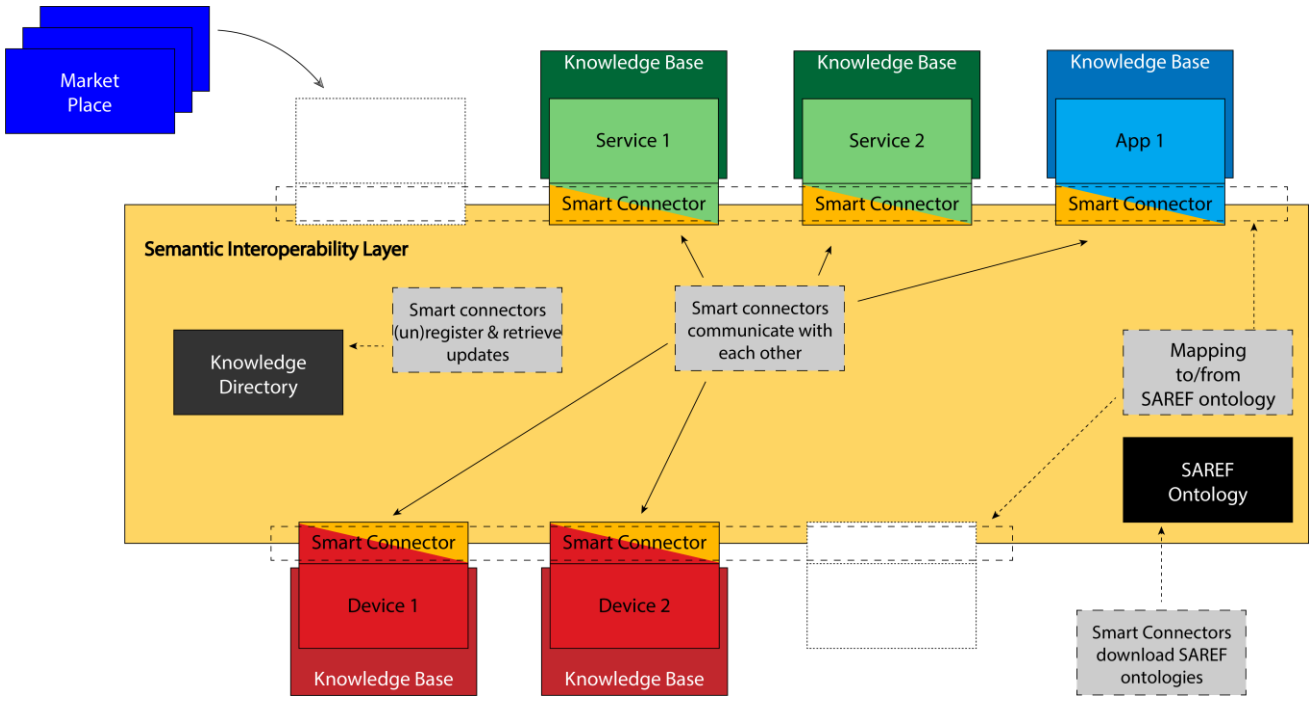


FIGURE 56 – SEMANTIC COMPONENTS

Existing devices, services, and platforms, as well as newly built apps, are called Knowledge Bases (KBs) in the KE terminology. KBs communicate with each other exclusively via so called Smart Connectors (SCs). Direct communication of KBs outside the InterConnect interoperability layer is less desirable[63]. SCs communicate using the SAREF suite of ontologies as shared reference model. Via an adapter, an SC maps the specific technology of a certain device, service, or platform (i.e., KBs) to concepts defined in SAREF. Each SC registers a description of its capabilities in a Knowledge Directory (KD). Capability descriptions are defined as Basic Graph Patterns (BGPs), to which we will simply refer to as graph patterns, which refer to concepts in SAREF. BGPs are part of the W3C SPARQL specification and are a set of triples consisting of subject, predicate and object (see Section 5.2.2 for an example of graph pattern). When a SC (and its corresponding KB) is no longer available, or when a new SC becomes available, the KD is dynamically updated. With this up-to-date information, the knowledge exchange amongst KBs (enabled by the SCs) can take place. The knowledge is

[63] InterConnect wants to *facilitate* interoperability, not force it. This is why using the InterConnect interoperability layer for discovery and data exchange is not mandatory but recommended. In some situations, it might be better, for practical reasons such as performance, to skip the interoperability layer altogether. Also, only using the interoperability layer for discovery only and not use it for actual data exchange is something that we would like to facilitate.

exchanged using a combination of SPARQL and RDF messages that refer to SAREF concepts.

5.7.2 SEMANTIC COMPONENTS

The following sections provide a summary of the different KE components that are part of the InterConnect semantically interoperable information architecture.

5.7.2.1 KNOWLEDGE BASE

A Knowledge Base (KB) is an independent producer or consumer of information to the IC semantic interoperability layer. Existing devices, services and platforms of the InterConnect ecosystem, as well as newly built apps, are considered as KBs.

Individually, each knowledge base is a component that provides useful functionality. However, the added value of using the KE technology in the IC semantic interoperability layer is that it provides the reasoning capability to orchestrate multiple knowledge bases that can discover and use each other (as required in Section 3.2.3). A knowledge base should be sufficiently described in terms of the knowledge that it processes. This means that we can describe what kind of knowledge can be extracted from this base and what kind of knowledge this base is interested in, and that we capture this well enough to provide synergy to the semantic interoperability layer.

Knowledge bases are not limited to being only producers or consumers of information; they could trigger actions, and thus play a role in control systems, such as heating systems or artificial cardiac pacemakers. Moreover, humans can play an essential role in a knowledge base. A knowledge base with humans in the loop could, for example, use a smartphone app that asks a human for input on a decision.

It is important to note that a KB does not interact directly with the semantic interoperability layer but uses a smart connector that acts on its behalf.

5.7.2.2 SMART CONNECTOR

A Smart Connector (SC) is an entity that acts on behalf of a KB. A SC allows a KB to register with the IC semantic interoperability layer and exchange knowledge. In the registration phase, a SC of a certain KB needs to specify:

- What knowledge it produces;
- What knowledge it publishes;
- What knowledge it wants to consumes;
- What knowledge it wants to subscribe to.

For example, an SC acting on behalf of a temperature sensor could publish its temperature measurements regularly and respond to requests for the current temperature. A thermostat app could subscribe to temperature measurements in a room or request the current temperature. A heating system could subscribe to both temperature preferences of a user and temperature measurements to be able to optimally control the temperature.

In the exchange phase, knowledge is consumed, produced, published or subscribed by the KB in the handlers that were configured during the registration phase.

The KE internally knows about the knowledge that is consumed, produced, published or subscribed in the IC semantic interoperability layer and can use reasoning to orchestrate the knowledge supply/demand on-demand. In other words, given a specification of knowledge that is requested, an SC can figure out for its KB where to get it. The developer of the KB does not have to know any specifics of the other KBs.

The main advantages of using smart connectors are:

- Knowledge orchestration removes the need to implement compatibility between all pairs of KBs in the network by hand;
- Changes in which KBs are connected to the interoperability layer are handled seamlessly. The SC synchronizes (via the Knowledge Directory) information about the knowledge that these KBs consume, produce, publish or subscribe;
- Based upon established open-source Semantic Web technologies which are leveraged to provide knowledge models and reasoning capabilities.

5.7.2.3 KNOWLEDGE DIRECTORY

The Knowledge Directory (KD) is a list of knowledge bases with associated capability descriptions that are available within a particular instance of the Knowledge Engine running in the IC semantic interoperability layer. Every KE instance has a single Knowledge Directory. Note that the Knowledge Directory is an internal component of the KE and developers using smart connectors do not need to know about it, since the communication and synchronization is handled by the smart connectors internally.

Since all smart connectors need to know about each other to exchange knowledge, they need a way to discover each other. This could be implemented as a centralized solution with only one KD, or several distributed KDs, for example, in InterConnect could be realized as one KD per smart building or per pilot. The Knowledge Directory is aware of all smart connectors and their knowledge Interactions.

5.7.2.4 KNOWLEDGE INTERACTION

Every Knowledge Base defines its capability description(s) in terms of Knowledge Interactions (KIs). One Knowledge Interaction can be seen as a single capability of the Knowledge Base. It consists of one or two graph patterns (i.e., the capability description) and a Communicative Act. The communicative act conveys the purpose of the data exchange described by this Knowledge Interaction. We distinguish four types of Knowledge Interactions:

1. **Ask**: a Knowledge Base asks its Smart Connector for certain data;
2. **Answer**: a Knowledge Base answers its Smart Connector with certain data;
3. **Post**: a Knowledge Base posts certain data (argument) to receive certain data (result). Both argument and result are optional but one of them should be present;
4. **React**: a Knowledge Base reacts with certain data (result) when it receives certain data (argument). Both argument and result are optional but one of them should be present.

The Ask and Answer knowledge interaction and the Post and React knowledge interaction are each other's counterparts. Therefore, when a Knowledge Base A has an Ask knowledge interaction for measurements of the temperature, and a Knowledge Base B has an Answer knowledge interaction for measurements of the temperature, then the Knowledge Engine will consult Knowledge Base B whenever Knowledge Base A asks its question.

5.7.2.5 COMMUNICATIVE ACT

Every Knowledge Interaction (i.e., a single capability of a Knowledge Base) also describes its Communicative Act. The communicative act is important because data can be exchanged for different purposes; sometimes it is being exchanged to inform, but sometimes it is also being exchanged to trigger some actions (i.e., a bid to the energy market or change the state of a device). The Knowledge Engine should be aware of any (different) communicative act of the Knowledge Interaction of two Knowledge Bases that are about to interact with each other. This prevents Knowledge Bases that, for example, post information to inform other Knowledge Bases to have accidental consequences such as changing the state of a device or placing a bid on the energy market. By default, this communicative act will be *to inform* or *be informed*, but the goal is to have an extendable ontology that contains all Communicative Acts that the Knowledge Engine distinguishes. This ontology is used by the Knowledge Engine and is not part of SAREF. It will be developed as part of the development of the Knowledge Engine.

5.7.3 EXAMPLE OF REASONING USING THE KNOWLEDGE ENGINE

As a running example to illustrate the different semantic components presented from Section 5.7.2.1 to Section 5.7.2.5, let us consider a scenario with three Knowledge Bases consisting of an App KB, a Measurements KB and a Temperature Converter KB. In this scenario, the App gives its user access to all available measurements in degrees Fahrenheit. However, the Measurements KB only stores measurements in degrees Celsius. The semantic interoperability layer is able to use the Temperature Converter KB to convert the available measurements in degrees Celsius into the requested measurements in degrees Fahrenheit. The Knowledge Interactions of the different Knowledge Bases look[64] as follows:

```
App Ask KnowledgeInteraction:
  pattern: ?meas rdf:type saref:Measurement .
      ?meas saref:tempInFahrenheit ?temp .

Measurements Answer KnowledgeInteraction:
```

[64] The patterns in the knowledge interactions are using syntax that is part of W3C's SPARQL 1.1 specification.

```
  pattern: ?m rdf:type saref:Measurement .
                ?m saref:tempInCelsius ?t .

Temperature Converter React KnowledgeInteraction:
  argument:  ?mm rdf:type saref:Measurement .
                ?mm saref:tempInFahrenheit ?tf .
  result:    ?mm rdf:type saref:Measurement .
                ?mm saref:tempInCelcius ?tc .
```

These KIs will result in the following backward rules in the App's Smart Connector:

```
if
    ?m rdf:type saref:Measurement .
    ?m saref:tempInCelsius ?t .
then
    retrieveDataFromKnowledgeBase(Measurements)
end

if
    ?mm rdf:type saref:Measurement .
    ?mm saref:tempInFahrenheit ?tf .
then
    ?mm rdf:type saref:Measurement .
    ?mm saref:tempInCelsius ?tc .
    retrieveDataFromKnowledgeBase(Temperature Converter)
end
```

The App asks its SmartConnector for measurements in degrees Fahrenheit, but the Measurements KB only contains measurements in degrees Celsius. The reasoner will therefore apply the backward rule of the Temperature Converter to every measurement that the Measurements KB returns. Therefore, the Measurements KB returns the following RDF:

```
:m1 rdf:type saref:Measurement .
:m1 saref:tempInCelsius "21" .
```

```
:m2 rdf:type saref:Measurement .
:m2 saref:tempInCelsius "18" .

:m3 rdf:type saref:measurement .
:m3 saref:tempInCelsius "24" .
```

The Temperature Converter KB is able to convert this into:

```
:m1 rdf:type saref:Measurement .
:m1 saref:tempInFahrenheit "69.8" .

:m2 rdf:type saref:Measurement .
:m2 saref:tempInFahrenheit "64.4" .

:m3 rdf:type saref:measurement .
:m3 saref:tempInFahrenheit "75.2" .
```

Which is the data that can be returned by the Smart Connector to the App KB as the answer to its query. But data exchange does not only involve asking questions and getting answers (i.e., pulling data), it often also entails publishing data to subscribers (i.e., pushing data). If we modify the Measurements KB of the above example into a Temperature sensor that periodically publishes the latest measurement in degrees Celsius. The Knowledge Interactions of the App and Temperature Converter KBs remain the same and the Temperature Sensor KB has the following KI:

```
Temperature Sensor Post KnowledgeInteraction:
  * argument:  ?m rdf:type saref:Measurement .
               ?m saref:tempInCelsius ?t .
  * result: <empty>
```

Note that the difference with the KI of the Measurements KB is that it has type Post instead of Answer. Therefore, the type of the KI indicates whether the output data of the KB can be pulled

by other KBs and/or whether it is automatically pushed to other KBs. In the case of the Temperature Sensor it is automatically pushed. This Temperature Sensor KI results in the following forward rule in the Smart Connector of the Temperature Sensor:

```
if
    ?m rdf:type saref:Measurement .
    ?m saref:tempInCelsius ?t .
then
    sendDataToOtherKnowledgeBases()
end
```

This means that whenever the Temperature Sensor publishes a new measurement, it will get pushed to subscribed KBs (in this case the App KB). The Smart Connector of the App KB will receive this measurement where its reasoner works with the following forward rules:

```
if
    ?mm rdf:type saref:Measurement .
    ?mm saref:tempInCelsius ?tc .
then
    retrieveDataFromKnowledgeBase(Temperature Converter)
    ?mm rdf:type saref:Measurement .
    ?mm saref:tempInFahrenheit ?tf .
end

if
    ?m rdf:type saref:Measurement .
    ?m saref:tempInFahrenheit ?t .
then
    sendDataToKnowledgeBase()
end
```

Upon receiving the new measurement, the rule for the Temperature Converter will trigger and convert the measurement into Fahrenheit. Once this is done, the new Measurement in degrees

Fahrenheit will be send to the App KB by the other rule. The App can now update its GUI with the latest measured temperature in degrees Fahrenheit.

5.7.4 CHALLEGES AND LIMITATIONS

The Knowledge Engine described in this section is conceptually derived from a Proof-of-Concept (PoC) version implemented by TNO. This version shows that in principle interoperable data exchange is possible with a smart connector that contains a reasoner and translates the internal language from a knowledge base into SAREF and capability descriptions based on SAREF. However, some limitations surfaced when we tried to apply it in certain real-world use cases (like the SPINE PoC with the help of EEBUS and KEO). These limitations can be divided into two categories: conceptual limitations and technical limitations. These limitations prevented the proof-of-concept implementation of the Knowledge Engine to be directly usable within the InterConnect project and the decision is made to address these limitations in a new version of the Knowledge Engine. The conceptual limitations were:

- Not being able to send data specifically to a particular recipient and allow the interoperability layer to be fully responsible for what Knowledge Base receives what data. We think this makes the Knowledge Engine too inflexible and might hinder the development in the Pilots. There, it was decided that optionally a single or multiple knowledge bases could be specified as the recipients, but the option of a wildcard has remained and still allows the previous behaviour;
- Not being able to communicate the purpose of data that is being exchanged (see explanation of the Communicative Act above). To prevent Knowledge Bases to accidently cause side-effects without their explicit goal, we introduced the concept of the Communicative Act. This allows the reason or purpose of the data exchange to be specified and the Knowledge Engine will take this into account when orchestrating;
- not being able to limit the connections between Knowledge Bases. Sometimes a device can only have a single controller and for the InterConnect project it is important that this limitation can be configured and is respected.

Apart from these conceptual limitations, the new version of the Knowledge Engine also needs to address some technical limitations that are mainly caused by using a traditional semantic reasoner for something it was not designed to do. Traditionally, semantic reasoners are built

to work on a single triple store which contains a predefined set of asserted triples. Using these asserted triples and a set of rules, a number of inferred triples are derived (in section 5.2.2, we call this ‘reasoning to infer new knowledge’). Apart from this goal of the reasoner, the Knowledge Engine uses a semantic reasoner to orchestrate data exchange, but for this purpose the assumption that all the asserted facts are available in a single triple store is no longer true. More specifically, data is distributed over multiple Knowledge Bases and the reasoner only has rules at its disposal to retrieve this data when necessary. In other words, where traditionally, the semantic rule reasoners used asserted triples and rules to generate inferred triples, the Knowledge Engine expects the reasoner to work in a situation where there are only inferred triples and no asserted triples, and it only has rules at its disposal. And although the reasoner can still be made to work, this has a consequence that is not acceptable for the InterConnect project; a single request for data from a Knowledge Base, should not result in more than one request for data to some other Knowledge Base. In the proof-of-concept version a single request for data results in ten (or more) requests of data from the Knowledge Engine to another Knowledge Base. Often these multiple requests are very similar and for the users of the Knowledge Engine it is unclear why these additional questions are necessary. An important reason why this happens, is because the rule reasoner does not support multi-headed backward rules.

As a result of the limitations mentioned above, there are also some challenges still to be tackled in InterConnect concerning the recommended solution. An important challenge concerns the SPARQL Basic Graph Patterns (BGP) that are being used by the Knowledge Engine to describe capabilities. They have a limited expressiveness because they only allow triple patterns connected by a logical AND operator. Other operators, like OR and NOT are supported within the SPARQL query language, but not in those Basic Graph Patterns. But why do not we just include the full SPARQL specification and increase the expressiveness? The short answer is that cause only the BGPs arrive at the reasoner-level while the other constructs like FILTER and UNION are handled by the SPARQL Query Engine instead of the reasoner. Since these constructs do not arrive at the reasoner-level, they cannot be included in the communication between the different Smart Connectors. Although handling it at the SPARQL engine level does not influence the answer to a SPARQL query, it can affect the performance. Since the reasoner of the Knowledge Engine needs to collect its inferred facts in a distributed manner, having no FILTER information means collecting all the measurements and only

filtering them at the very last moment. This means that all the measurements are transferred over the network and the filters are applied very late in the process. To allow filters to be applied as early as possible (ideally in the source Knowledge Base), the information about FILTERs needs to arrive at the reasoner-level and communicated to the distributed Knowledge Bases. The same holds for UNION information and other types of increased expressiveness like lists.

Another challenge with the Knowledge Engine will be bridging the gap between metadata and data. With metadata we mean the data about what Knowledge Bases are available and what their capabilities are. With data we mean the information that is actually being exchanged via Knowledge Interactions. We foresee use cases where we would like to combine graph patterns about the metadata with graph patterns about the data, but it is not entirely clear how to achieve this. For now, we introduced a special *hasData* property whose `xsd:string` value is a data graph pattern, but this is not entirely satisfying. The InterConnect project will provide information about whether and, if so, how this gap can be bridged.

5.8 GUIDELINES FOR OTHER WPS

In the previous sections we have described the recommended solution in the InterConnect project to achieve semantic interoperability. Although not everything is figured out yet, it is already possible to give some pointers to other WPs that need to work with the interoperability framework.

InterConnect will provide a set of generic adapters that should be used by other WPs that want to make their service, device or platform interoperable via the semantic interoperability layer. As part of the generic adapters, a Smart Connector focusses on providing interoperable data exchange using SAREF. The generic adapters have two functions. First, they wrap a Smart Connector and tailor it to a specific technology (i.e., REST, MQTT, SPINE, etc.) to increase the usability. Second, the adapters provide common functionalities of the Interoperability framework (related to, for example, the IC Service Store).

Section 5.8.1 elaborates on the Generic Adapters and the differences with the Smart Connector. Section 5.8.2 provides the steps that partners will need to take to implement the recommended solution for the semantic interoperability layer. Section 5.8.3 describes the InterConnect service store and how it is related to the Knowledge Engine. Finally, Section

5.8.4 provides a high-level overview of the automated compliance test as part of the service store.

5.8.1 SMART CONNECTOR VS GENERIC ADAPTERS

While the Smart Connector is the main component of the recommended semantic solution described in Section 5.7, it focusses solely on the task of providing partners with reasoning and interoperable data exchange using SAREF. The InterConnect Framework, however, consists of a lot more functionality (like security, privacy, the service store and more) to which partners need access. For this purpose and to lower the threshold to become interoperable, the InterConnect project will provide a set of generic adapters.

InterConnect's semantic interoperability layer will mainly reach out pilots and demonstrators via the adoption of one of the available generic adapters[65]. Generic adapters will be made available according to the software framework, namely: Java, Python; and according to the interaction protocol, namely: REST, MQTT or SPINE/SHIP. Generic Adapters will provide a base configuration and implementation where integration with common functionalities of the interoperability layer will be already available, namely connection to the Service Store or to the P2P marketplace enablers. Generic adapters will then become the gateway for already available software services to bridge with the InterConnect ecosystem. From the perspective of a service and/or digital platform owner, selecting the Generic Adapter will depend mainly on the available and underlying software framework and type of protocol in place. That is, a service that already considers, for instance a RESTful API, should consider the REST generic adapter. This does not preclude that given service or platform of opting for one of the other available adapters but opting for the closest technology available will ease the process.

Moreover, while the Generic Adapters are geared towards one specific software framework or protocol, providing a solution for easier integration, InterConnect will also develop Smart Connectors. These connectors will provide the same base gateway towards interoperable services as the generic adapter but will not be focused on facilitating the process of adaptation of an already existing API. On the other hand, the InterConnect connector will be the

[65] At the time of writing, 6 generic adapters are foreseen, which may increase or decrease according to pilot deployment needs.

suggested choice for new services, whose implementation is not yet available, or that do not yet have a mature external API.

Opting for the generic adapter or for the Smart Connector will have a direct impact in the integration. Mature services should opt for the generic adapter, requiring the service concept to be mapped according to the ontology (within the scope of WP3) where data requirements, format encoding and available capabilities are annotated to SAREF. The mapping process will enable the semantic reasoners to unlock data translation when pushing data between generic adapters.

5.8.2 STEPS TOWARDS INTEROPERABILITY

The following steps should be taken by partners for making their service/platform/device interoperable using the interoperability framework:

- Identify and map to SAREF the features/capabilities that are intended to be made interoperable (WP3);
- Accommodate the need to search service capabilities from within the InterConnect framework (e.g., from the service store) and include them in the business logic;
- Choose the candidate generic adapter to be considered;
- Expose the already existing API and annotate it according to the outcomes of bullet 1.

Considering the Smart Connector will be the preferred approach to link with new services that do not yet expose a mature interface, this means that such new services can directly build their representation and data encodings according to the ontology (i.e., SAREF compliant level 3 by design).

Task 5.2 will provide detailed guidelines on how to integrate an adapter or connector. However, Table 33 shows a preliminary version of such a guideline.

Step	Guidelines
Step 1	Select a component (service software application or client software application) that has to be made interoperable with the IC Interoperability framework. The component should be listed in the WP3 service catalogue and a related system use case should be available in task 1.4.
Step 2	In case of an existing component with a mature API:

	• Identify the features/capabilities that have to be made interoperable. This set of functions (or functionality) that will be made interoperable, is the actual IC service. • Check the IC SAREF ontology (see step 2b for further details) • Map the API to the IC SAREF ontology (see step 2c for further details) • Determine the platform that will host the adapter. • Determine how the adapter will be integrated in the digital platform IT/technology architecture. • Select the appropriate implementation technology of this IC adapter. An adapter will be provided in a python and Java based version that can be wrapped in a software container (e.g., docker).
Step 2b	Detailed steps to check the IC SAREF ontology: • If the SAREF Ontology does not provide a similar concept in the ontology, then the service cannot be made interoperable (this should not take place for the services required by the pilots in InterConnect because the outcomes of WP1 and WP3 define the requirements for the definition of the ontology in task 2.4); • If the implementation of the service/concept defined in the SAREF ontology requires functionality or data model mappings not provided by the existing component, then the business logic of the component should be enhanced. The definition of a IC SAREF ontology service/concept will be based upon many existing service implementations. The outcome of the ontology creation process may not be a concept/service that allows a one-to-one mapping for each existing implementation of such a service; • If the existing component and its API requires more information or interaction than provided by the service/concept in the IC SAREF ontology, then at this stage the business logic for the component should be adapted to make it interoperable. At the same time the requirements of the existing component can be handed over to the ontology expert team so they can investigate if this missing functionality should be part of the ontology.
Step 2c	Detailed steps to map the API to the IC SAREF ontology: • Select a generic adapter that provides a protocol endpoint (REST HTTP, MQTT, SPINE, …) corresponding to the protocol used by the API; • Provide the necessary configuration of the adapter (for instance an URL to link with the API endpoint of the existing component) and map the API to the generic interface of the smart connector (part of the IC adapter).
Step 2e	Detailed steps to determine how the adapter will be integrated in the digital platform IT/technology architecture. For instance, the adapter may need: • To be placed as a software process in front of an API manager/gateway or API endpoint; • To be integrated in the API manager/gateway; • To be integrated as a software component (for instance to communicate with a IC container service on the same platform);

	• To be set up as a standalone process to act as the remote IC adapter to a service on a device (the device may not be capable to host the IC adapter); • …
Step 3	In case of a new component: • Start from the IC SAREF ontology. Select the concepts needed; • Determine if you want to use the IC Smart Connector or the IC Generic Adapter approach (see step 3b for further details); • Determine the platform that will host the connector; • Determine how the connector will be integrated in the digital platform IT/technology architecture (see step 3d for further details); • Select the appropriate implementation technology of this IC connector. A short description of the Java Developer API can be found in section; • Make the integration in the business logic.
Step 3b	Detailed steps when determining if you want to use the IC Smart Connector or the IC Generic Adapter approach: • In case of the IC Generic Adapter approach, proceed with step 2.c and next; • In case of the IC Smart Connector approach, proceed with step 3.c and next.
Step 3d	Detailed steps when determining how the connector will be integrated in the digital platform IT/technology architecture. For instance, the connector may be: • Integrated directly with the business logic as a software component (library, package); • Integrated as a software process;

TABLE 33 – STEPS FOR WPS TOWARDS INTEROPERABILITY

Further details from a technical standpoint are provided in Sections 5.5 and section 6 of D5.1 [43]

5.8.3 SERVICE STORE

The Service Store will provide a common reference point to catalogue all services made available via the interoperability framework. As one of the main IC interoperability framework tools, the IC service store will provide a single stop for all providers and adopters of interoperable services from energy and non-energy domains. The service store is conceptualized as a web service with its front-end and back-end modules and processes. The main objective is to enable building of the InterConnect ecosystem of service providers and adopters by allowing them to register new interoperable services and browse existing ones to

identify services best suited for the challenge at hand and get all necessary information for accessing and properly utilizing selected services.

As mentioned in [31], a service (software) component is a software component offering a service via a (digital) interface. A software component can be regarded as an application or part of an application, and it has or represents some functionality. A service in the real world is realized by performing some of this functionality to accomplish a goal with an impact in the real world. A software component is hosted on a digital platform. A digital platform can host a service component or not. A device is or can incorporate a digital platform. A device hosting some service components (via its digital platform) and offering or using a service via a digital interface is called a smart device. A device with a digital interface is called a connected device. Via one digital interface one or more services can be offered or requested, depending on the implementation.

In the context of the project, an InterConnect Service is a software that offers an IC service via one of the available digital platforms (or in a standalone approach like SaaS – Software As A Service) exporting an IC (digital) interface. An IC service stands for the functionality offered via this digital interface by the IC service component. An IC service is compliant with the (or a set of) requirements imposed by the IC Interoperability Framework regarding the functionality provided by the service as well as the features and functioning of the digital interface.

A service by itself is a class or category. An Energy Service is a service of which the main goal is to accomplish an objective in the domain of energy. The scope of an Energy Service can vary for example from improving the energy efficiency at device level, self-consumption at building level (covered in WP3) up to balancing an energy grid or an energy portfolio (covered in WP4). A PV forecasting service is an energy service because it contributes to the above-mentioned goals. Services of which the main goal is not related to the energy domain, such as comfort, convenience and control (CCC), or non-energy services. The outcome of a non-energy service may result in some energy consumption as a side effect. In fact, depending on the context an IC service can be regarded as a energy service or as a non-energy service, or even as both.

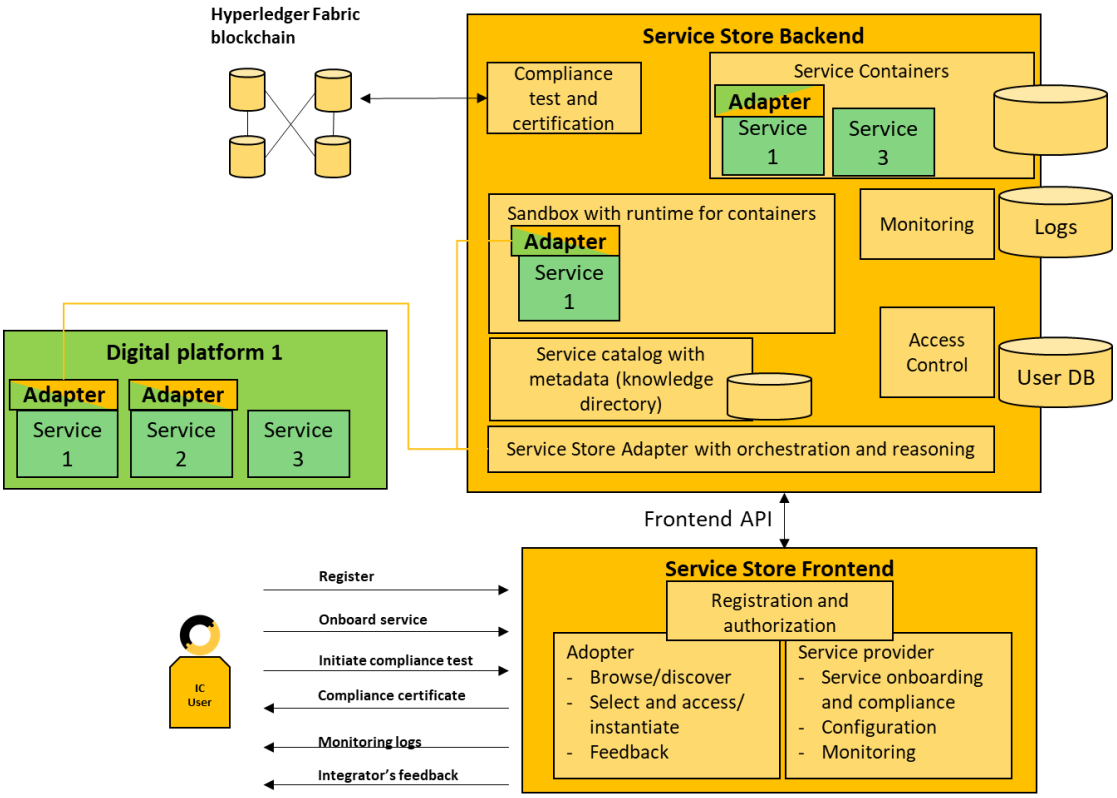


FIGURE 57 – IC'S SERVICE STORE ARCHITECTURE

For instance, a washing machine is a device. The washing machine is not regarded as a digital platform, but it usually contains a controller. The controller is a digital platform and can potentially host a service software component[66]. To a user the main service provided by the washing machine is washing the laundry. In IC the main service provided by the washing machine is the ability to remotely (and digitally) start or delay the start of a washing machine program. Depending on the context this service can be regarded as a comfort service (non-energy) or/and as an energy service. More details are covered in D5.1 [43].

The Service Store will be a gateway to register interoperable services and make them (and their capabilities) available for other projects and third parties. We expect there to be a single instance of the Service Store for the whole of InterConnect available to all Pilots and future partners. This is a different scope than the Knowledge Engine and its Knowledge Directory, of which we expect there will be multiple instances (probably a single instance of the Knowledge Engine per building), that works together with the Service Store.

[66] The IC service software component could also be hosted in the cloud and not on the device itself. In this case the IC service software component communicates via a proprietary or standard interface with the controller. Via the IC interface it is connected to the IC interoperability framework. IC service represents the service offered by the device.

The exact relation between the Service Store and a Knowledge Engine instance is yet to be clarified in future deliverables. However, there are some correspondences that can already be outlined. The semantically interoperable capability descriptions of the Knowledge Engine (with graph patterns) can be used in the Service Store as well. They can be used to find and compare services with each other and might even allow a reasoner to automatically suggest services to the user. The Knowledge Engine Administrator interface should allow the searching/finding/installing of new services into that particular Knowledge Engine instance.

The Service Store will become one of the key front-end interfaces of the Interoperability framework, holding a series of dashboards for monitoring assurance and identity provisioning and security and cybersecurity provisioning. The availability of the actual service capabilities and digital interfaces will be kept at their original location, but it will be made available to the InterConnect ecosystem by means of the InterConnect Generic Adapter. Finally, the Service Store will also provide a repository of software images, where interoperable software services can be uploaded and later on downloaded by interested parties for deployment at their own infrastructures.

5.8.4 AUTOMATED TESTS FOR COMPLIANCE

The InterConnect project will provide service providers and digital platform operators a set of tools for making their services and platform resources semantically interoperable in line with the InterConnect interoperability framework. The main interoperability enablers will be generic interoperability adapters which WP5 will provide for most pervasive interfacing technologies in the project pilots: REST, MQTT and SPINE/SHIP. Section 5.8.2 provides a high-level overview of the service adaptation process by instantiating corresponding generic interoperability adapters. Services can also be made interoperable by directly integrating the Knowledge Engine Java API.

Once a service is made interoperable with the InterConnect semantic interoperability layer (based on the Knowledge Engine), it needs to be registered into the knowledge directories. The InterConnect Service Store (see D5.1 [43] and section 5.8.3 for more information) will provide a catalogue of all interoperable services and their capabilities accompanied with achieved compliance level certificate (compliance levels are discussed in section 5.3). In order to get the InterConnect semantic interoperability compliance certificate, each service needs to

pass an automated compliance test. This compliance testing is an integral part of the InterConnect Service Store and it is performed during the service registration process and with every service update and could also be considered during updates in the InterConnect semantic interoperability layer. Figure 58 provides a high-level overview of the automated compliance test as part of the service store.

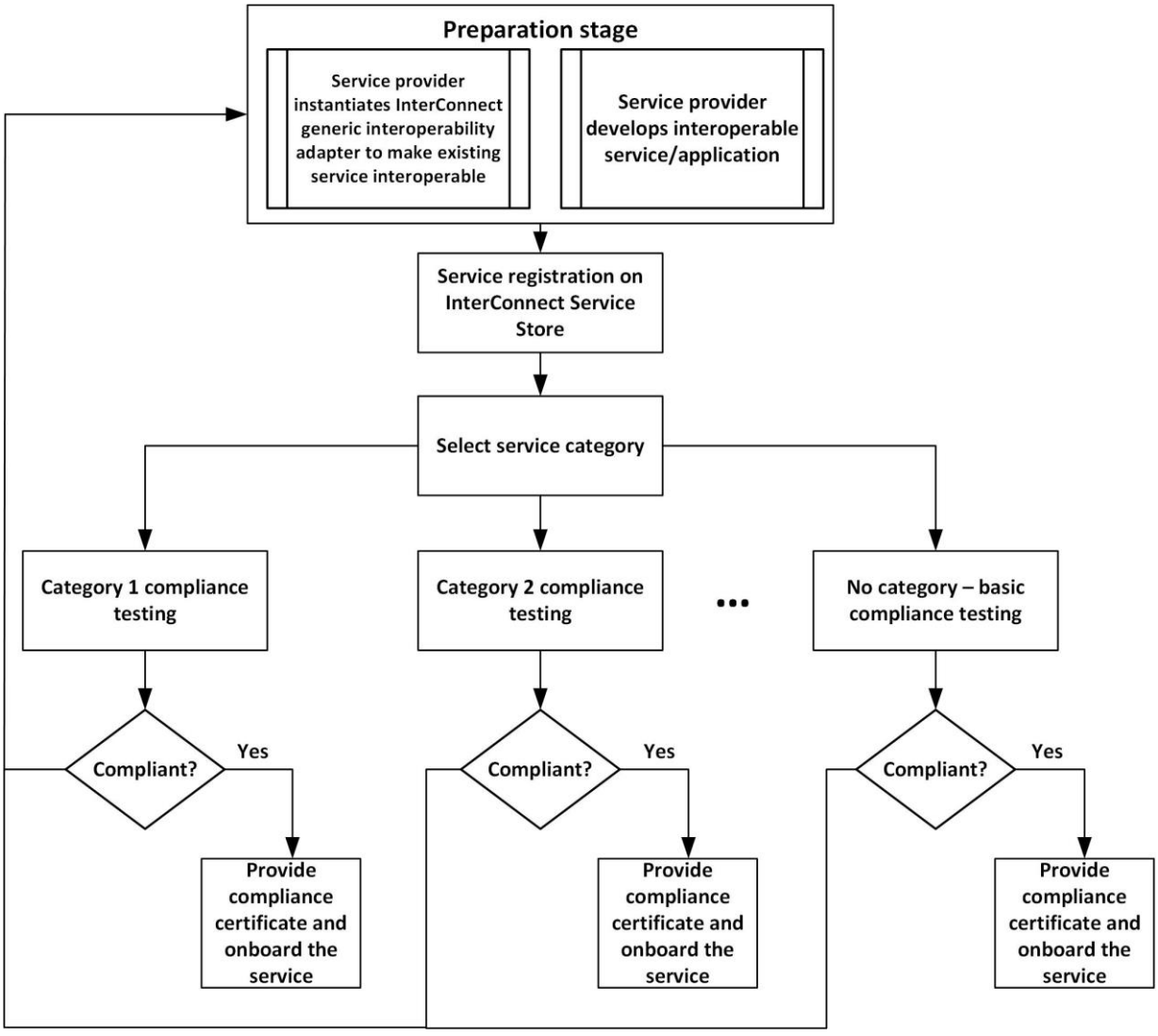


FIGURE 58 – AUTOMATED SEMANTIC INTEROEPRABILITY COMPLIANCE TEST

The InterConnect project is in process of defining the main service categories in the scope of WP3. Example service categories: forecasting services, flexibility services, remote device control services etc. Each service category will include a minimum set of semantic interoperability indicators as specified by the semantic interoperability layer/Knowledge Engine and SAREF ontology. These semantic interoperability indicators will include:

- Base set of SAREF and Knowledge Engine semantic interoperability compliance indicators;
- Set of semantic interoperability compliance indicators specific for each service category.

The basic and service category specific set of semantic interoperability indicators will be defined in the scope of WP2 and reported in future deliverables.

After the service provider registers an interoperable service and selects appropriate service category, the automated compliance test mechanism of the InterConnect Service Store will be initiated. During the compliance test, the Service Store backend process will test semantic reasoning compliance and SAREF compliance of the interoperable service (service runs on a hosting digital platform operated by the service provider or a 3rd party). Multiple messages of specific format and content will be sent to the interoperable service which will provide reply in line with its core functionality. The compliance test backend procedure of the Service Store will analyse received replies and derive compliance results indicating achieved interoperability compliance level (see section 5.4). Every interoperable service needs to satisfy the basic set of compliance indicators. Services mapped to a specific InterConnect service category will have to satisfy the base set and category specific set of interoperability compliance indicators. Service provider will receive a compliance test report which can be used for improving the service interoperability.

After successful completion of the compliance test, the service provider will receive a digital certificate of compliance. This certificate will be written on a project wide immutable database (based on private permissioned blockchain) and it will be displayed in the InterConnect Service Store catalogue in human and machine-readable formats. Services with compliance certificates will finalize the onboarding process and be included into the InterConnect service store catalogue and into the semantic interoperability layer (be part of the reasoning procedures).

In this section we focused on compliance testing of interoperable services. Similar logic applies for interoperable digital platforms, applications and devices. InterConnect WP3 and WP5 will work on specification of the interoperability compliance tests for these platforms and resources. Functional Architecture Implementation in Pilots

The InterConnect project plans to instantiate the reference architectures in seven7 large scale pilots in seven countries (Belgium, France, Greece, Germany, Italy, Portugal and The Netherlands). Some of the pilots are organized into multiple sub-pilots while our and also partner cyberGRID partner is working on the implementation of a cross pilot use case related to energy flexibility management.

The first step was the specification of high-level use cases for each (sub-)pilot in the scope of WP1 (see D1.1 [39]). Next, within WP5, pilot teams worked on the specification of overall system architecture focusing on digital platforms participating in the realization of the pilots/use cases and interfaces through which platforms communicate. The goal of this exercise was to identify the first set of pilots requirements for semantic interoperability, which was used in the specification of the InterConnect Interoperability Framework (see D5.1 [43]).

When the initial HLA (based on the SHBIRA), the SERA and the architecture of the InterConnect Interoperability Framework were defined, the next step was to organize a workshop with all pilot teams and work with them on mapping each pilot's architecture, key services and resources onto the InterConnect reference architecture viewpoints.

Mapping of each (sub-)pilots' architectures and available/planned resources onto the initial HLA was based on the template presented in Figure 59. Pilot teams performed the following tasks:

- **Map all key services** behind the use cases onto the gateway and application layer;
- **Map all devices** which will be used for use case realization onto the device layer;
- **Indicate which services which are required by the (sub-)pilot**, but are not provided by any of the participating partners. This might lead to pilots using services from other pilots (platform providers from other pilots) either directly, from a hosting platform, or by instantiating them in runtime (i.e., Docker container) established in one of the digital platforms available in the (sub)-pilot's ecosystem;
- **Depict interfaces between the system layers/resources that bypass the semantic interoperability layer** – communication-based on legacy interfacing technology.

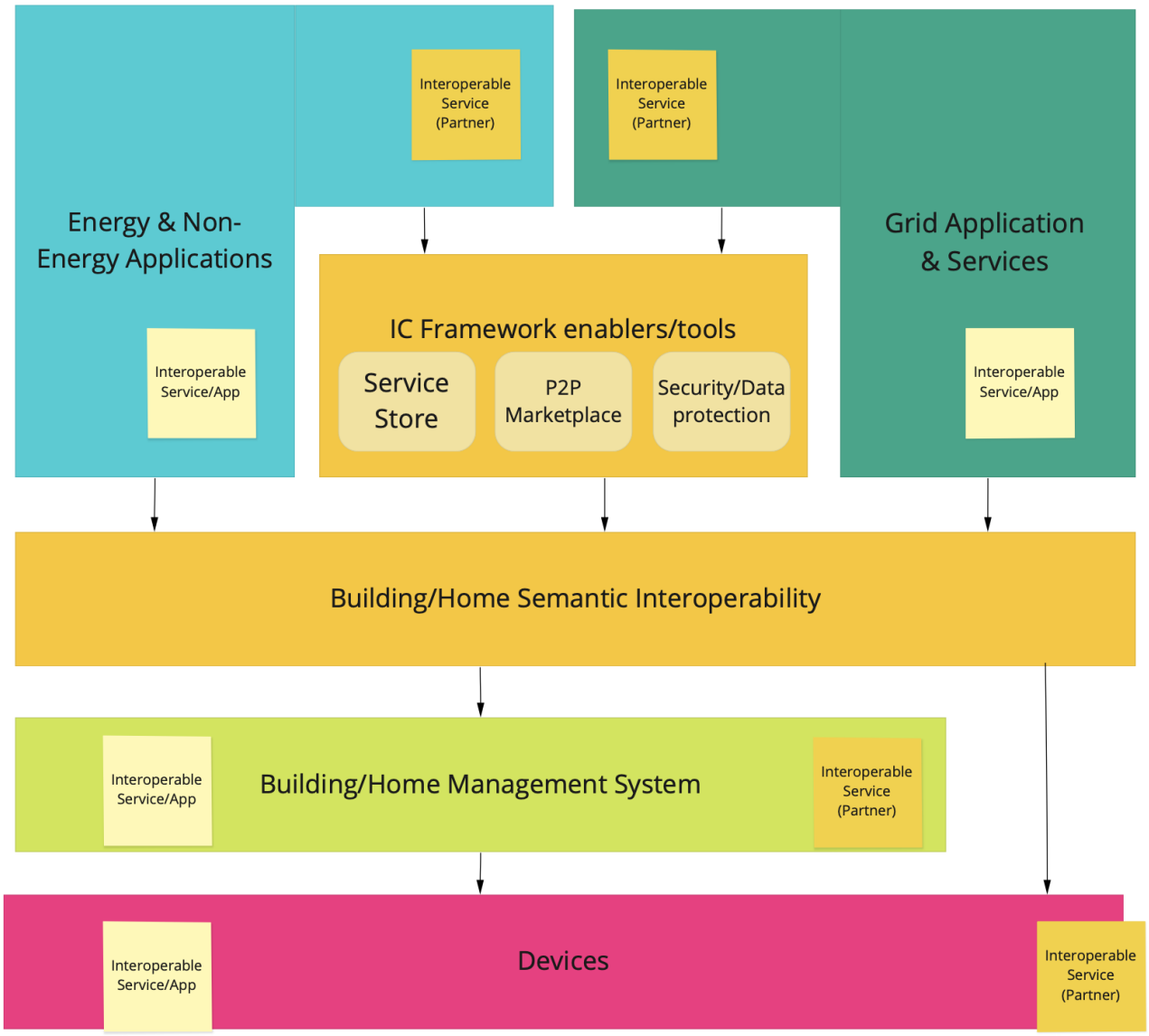


FIGURE 59 – INITIAL HLA TEMPLATE FOR THE WORKSHOP

The Mapping of (sub-)pilots' architectures and available/planned resources to SERA was done using the template presented in Figure 60. Pilot teams performed the following tasks:

- Map resources/devices to the bottom layer of SERA;
- Indicate the main actors and their roles onto their within corresponding domains comprising the SERA;
- Indicate the main services that actors perform on the resources/devices;
- If available, indicate the information objects needed for service and devices;
- Identify missing links and relationships within the SERA.

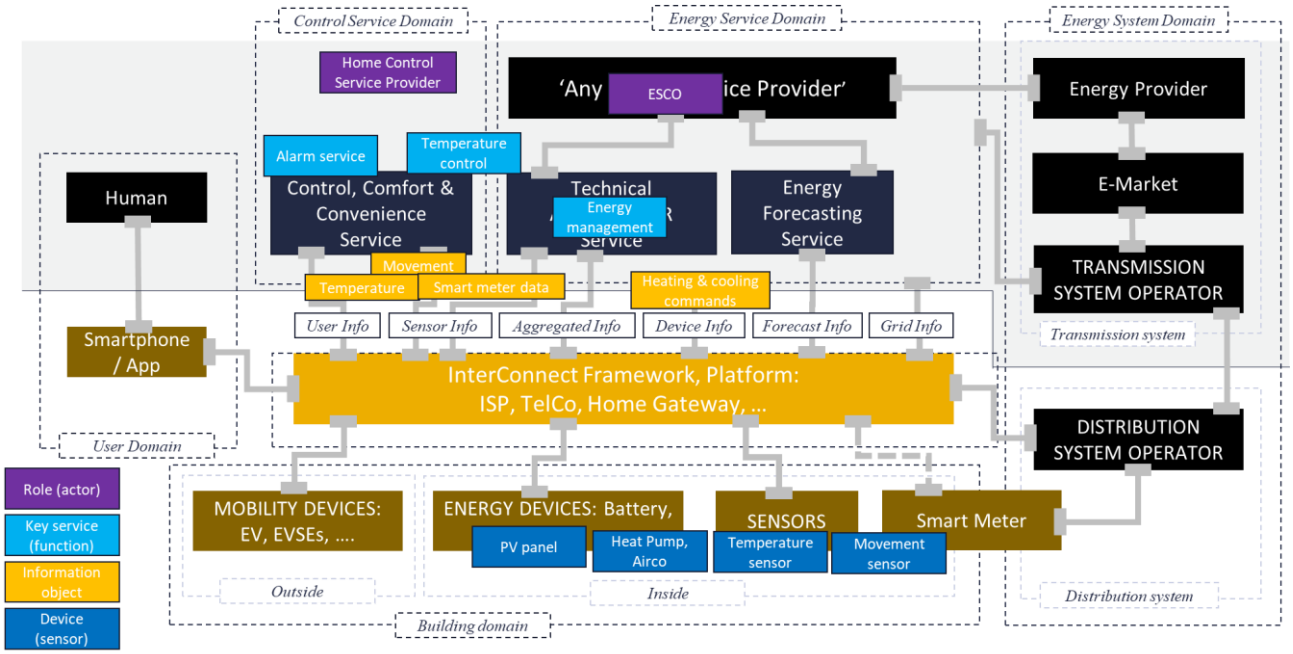


FIGURE 60 – SERA TEMPLATE FOR THE WORKSHOP

Mapping of (sub-)pilots' interoperable services and other interoperable resources onto the InterConnect Interoperability Framework Architecture utilized template presented in Figure 61. Pilot teams performed the following tasks:

- **Identify each (sub-)pilot services (available or to be developed) to be made semantically interoperable** (in the scope of WP3). Furthermore, the goal was to indicate what are the current communication interfacing technologies used by these services to interoperate with other endpoints and what are specific access control rules defined for these services;
- **Map interoperable services onto the different digital platforms** that host them;
- **Identify devices to be made semantically interoperable** by adapting the semantic interoperability adapter provided by WP5;
- Decide if the **(sub-)pilot will utilize p2p marketplaces** for the realization of its use cases;
- Decide if the **(sub-)pilot requires the instantiation of the InterConnect service store** at the level of the pilot, or can and will utilize service store instance on the level of the project;
- Decide **which of the mapped interoperable services can be provided as a downloadable container** (i.e., Docker).

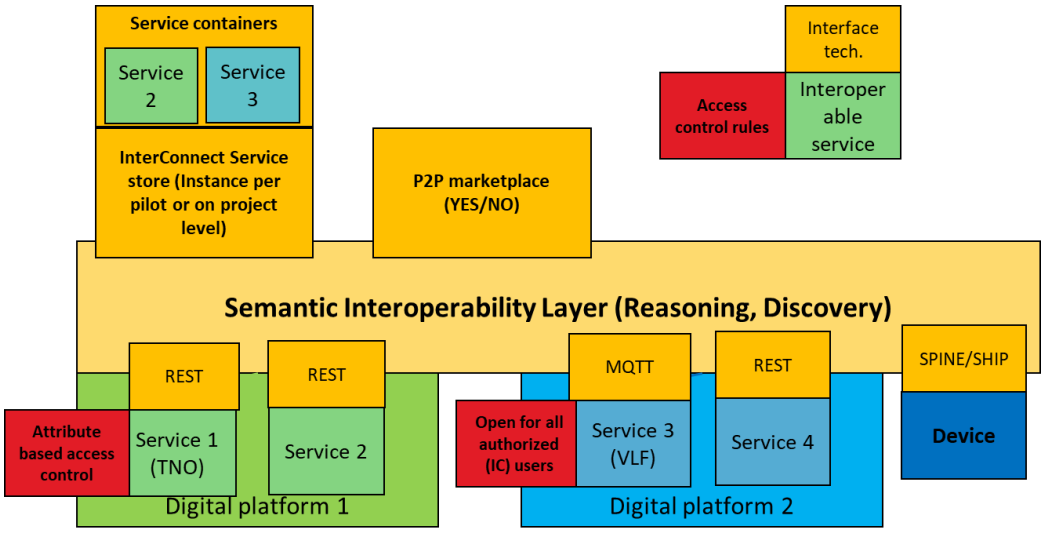


FIGURE 61 – INTEROPERABILITY FRAMEWORK ARCHITECTURE TEMPLATE FOR THE WORKSHOP

The online collaborative tool "Miro"[67] was used for collecting inputs from the (sub-)pilot teams for all three architectural viewpoint mappings. Collected inputs were then analysed and discussed with each of the (sub-)pilot teams. Finally, these inputs were mapped onto the overall SHBERA view in the form of a table representing the key architectural system layers and domains.

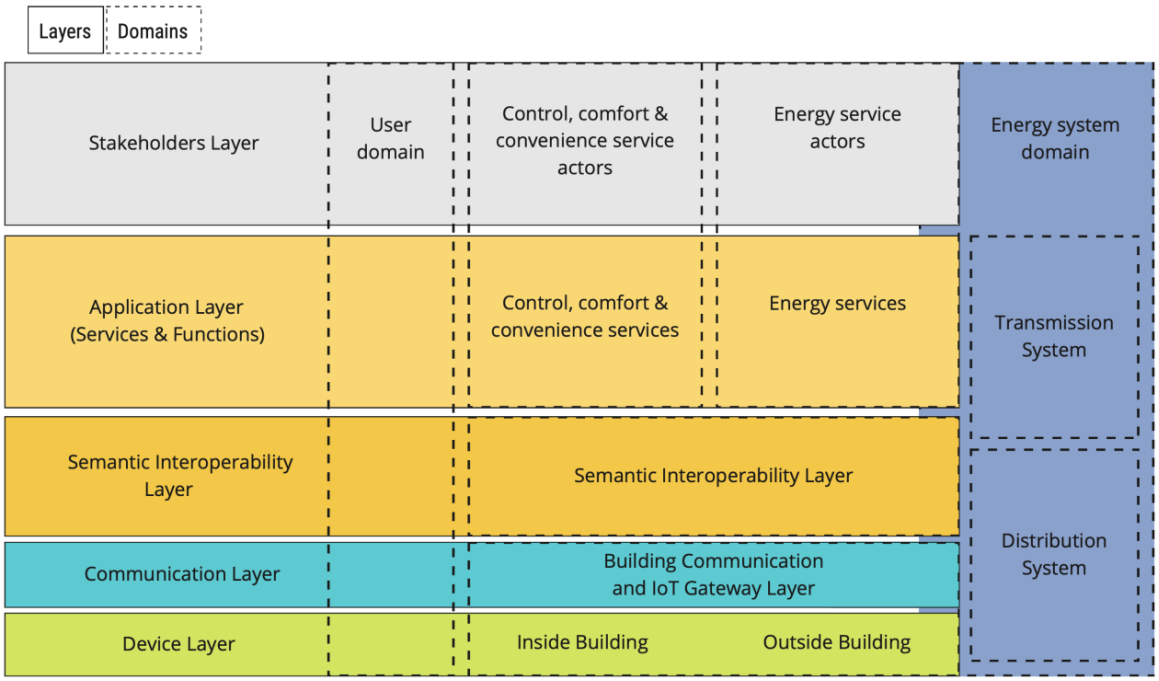


FIGURE 62 –INTERCONNECT'S SECURE INTEROPERABLE IOT SMART HOME/BUILDING AND SMART ENERGY SYSTEM REFERENCE ARCHITECTURE (SHBERA)

[67] https://miro.com/

After the workshops, the different architectural viewpoints for each of the pilots were consolidated using the SHBERA (introduced in Section 4 and shown in Figure 62). For this purpose, the SHBERA was converted into a table format (detailed in Table 34).

Layer (HLA)	Domains (SERA)			
Stakeholders	**User** This segment of the mapping depicts key categories of users as stakeholders in the pilot	**Control, comfort & convenience (CCC) services (actors)** Key actors and toles providing and benefiting from the control, comfort & convenience services	**Energy services (actors)** Key actors and roles providing energy services or involved in providing them	**Energy System** Key actors and roles from energy system domain
Application	Users of provided applications and services	**Control, comfort & convenience (CCC) services** Non-energy control, comfort & convenience and other services comprising/ enabling the pilot. Services to be provided by external partner are underlined	**Energy services** Energy services comprising/enabling the pilot. Services to be provided by external partners are underlined	**Transmission System** Key resources and services from TSO domain
Semantic Interoperability		**InterConnect Interoperability Layer** List of services to be made semantically interoperable with their interface technology. Which service to be provided as a downloadable container. Digital platforms hosting interoperable services. (Sub-)Pilot plans to utilize p2p marketplaces (Y/N)		
Communication (gateway)		**Building Communication and IoT Gateway Layer** Services and enablers on fog/edge/gateway level interconnecting resources and services within a building and between in-building systems with services and stakeholders outside a building		**Distribution System** Key resources and services from DSO domain
Device	Users/owners of devices	**Inside Building** Devices/appliances/ resources available inside home/building	**Outside Building** Resources/devices residing outside of a building or towards DSO	

TABLE 34 – OVERVIEW OF THE SHBERA TEMPLATE FOR MAPPING (SUB-)PILOT'S ARCHITECTURES

Each pilot's output was then mapped onto this uniform table for further analysis and discussions. This section discusses the output of this work. Additional details about the pilot use cases can be found in deliverable report D1.1 [39], while more details about the pilot's architecture and interoperability requirements can be found in deliverable report D5.1 [43].

The following subsections contain some information on the digital platforms and the solutions (represented with their official names) offered on the market by the project partners who operate them. All digital platforms are described in detail in D5.1 [43].

Please note that some changes and updates to the presented mappings are possible until the pilots start their execution, since most of the InterConnect pilots are still being specified and negotiated for most parts.

5.9 FRANCE (YNCRÉA)

This pilot aims to maximize the use of renewable energy, reduce the environmental impact of energy consumption, and, ultimately, reduce the bill of end-customers. More details about the pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

Layer (HLA)	Domains (SERA)			
Stakeholders	**User**	**CCC services (actors)** • Service provider	**Energy services (actors)** • Orchestrator • Flexibility manager	**Energy System** • Energy retailer • DSO
Application	**Stakeholders**	**CCC services** • User preferences management (ENGIE, ThermoVault, Trialog, Inetum, Yncréa) • Generate advices (Yncréa, Inetum) • User comfort (ENGIE, ThermoVault, Trialog) • Decide appliance control (ENGIE, ThermoVault, manufacturers) • Remote control of devices (ENGIE, ThermoVault, manufacturers) • GUI user interface (user management interfaces and hypervision - ENGIE, Inetum, Trialog, ThermoVault, Yncréa, manufacturers)	**Energy services** • Flexibility management (ENGIE, ThermoVault) • Flexibility monetized on markets (ENGIE, ThermoVault) • Aggregation service (ENGIE, ThermoVault) • Dynamic tariffs (ENGIE, ThermoVault) • Consumption forecasts (Enedis, ENGIE, ThermoVault) • Cost/bill analysis (ENGIE, ThermoVault) • Smart meter & adapter services - real time data (max capacity, instantaneous consumption) (ENEDIS) • Energy limitation management at home level (Linky, Inetum, Yncréa, ENGIE, ThermoVault, Trialog) • Consumption optimization (ENGIE, Inetum, ThermoVault, Trialog, Yncréa) • EV Charging platform (Trialog)	**Transmission System** • Flexibility used as ancillary for TSO (ENGIE, ThermoVault)

<table>
<tr><td>Semantic Interoperability</td><td></td><td colspan="2">InterConnect interoperability layer
Semantically interoperable services/platforms: ENEDIS data metering platform (metering data platform interface), ThermoVault aggregation platform (ThermoVault), manufacturer backend service (SPINE), EV charging platform (REST), ENGIE aggregation platform (ENGIE interface), Flexibility manager (REST), Orchestrator (REST).
P2P marketplace enablers - NO
Services available as downloadable containers - TBD.</td><td></td></tr>
<tr><td>Communication (gateway)</td><td></td><td colspan="2">Building Communication and IoT Gateway Layer
ENGIE EMS
ThermoVault EMS
Metering data platform
Remote control of appliances</td><td rowspan="2">Distribution System
Smart meter & adapter services (ENEDIS)
Linky</td></tr>
<tr><td>Device</td><td></td><td>Inside Building
PV
Whitegoods
Control devices
Heaters
Hot water tank
Heat pump
ThermoVault endpoint
ENGIE endpoint</td><td>Outside Building
Electric Vehicles
EV Charging Point
Linky and sensors</td></tr>
</table>

TABLE 35 – FRENCH PILOT ARCHITECTURAL MAPPING TO THE SHBERA

The French pilot is not planning on using services from other pilots. Details about access control mechanisms for interoperable services will be decided later, during pilot preparations. Many of the listed services are either provided or will be developed and managed by multiple participating partners.

5.10 BELGIUM

The Belgian pilot has eight sub-pilots; each has with its lead partner, participating digital platforms and interoperability requirements:

- Cordium Hasselt – led by VITO;
- Thor park Genk – led by VITO;
- Student housing Antwerp – led by IMEC;
- Smart District Nieuwe Dokken Gent – led by Ducoop and OpenMotics;
- Zellik Green Energy Park Brussels – led by VUB;
- Nanogrid Leuven – led by TH!NK-E;
- Oud-Heverlee public buildings – led by 3E;
- Genk apartments - led by Thermovault.

5.10.1CORDIUM HASSELT AND THOR PARK GENK (VITO)

These pilots aim to reduce the environmental impact of energy consumption and reduce overall energy costs for site owners. From VITO's perspective, these sub-pilots will allow exploring new concepts related to interoperability and energy management. More details about each (sub-)pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

<table>
<tr><th>Layer (HLA)</th><th colspan="4">Domains (SERA)</th></tr>
<tr><td>Stakeholders</td><td>User
DHN/HP/ Turbine owner (Cordium)
Social housing company (Cordium)</td><td>CCC services (actors)
Site operator (Imtech)</td><td>Energy services (actors)
Energy service provider (VITO)
Technical aggregator (VITO)</td><td>Energy System
Energy retailers</td></tr>
<tr><td>Application</td><td>Apartment tenant</td><td>CCC services
BEMS application</td><td>Energy services
Flexibility Service (provided by smart whitegoods via SPINE)
Flexibility service
PV & Wind Forecasting
Day ahead/Intraday Energy price forecaster
Heat demand forecasting
Carbon intensity estimator
Carbon intensity forecaster
DEMS application / technical aggregation & optimization with local objectives
Heat Demand forecaster</td><td rowspan="3">Transmission System</td></tr>
<tr><td>Semantic Interoperability</td><td></td><td colspan="2">InterConnect interoperability layer
Semantically interoperable services: Flexibility service (REST), PV (-T) Forecaster (REST), Wind turbine forecaster (REST), Day ahead intraday energy price forecaster (REST), flexibility service provided by whitegoods (SPINE)
P2P Marketplace - TBD
Services provided as containers: potentially all semantically interoperable services.
Access control - token based.</td></tr>
<tr><td>Communication (gateway)</td><td></td><td colspan="2">Building Communication and IoT Gateway
Heating Substations Management System
BMS (Metasys)
IoT Gateway / PLC
BEMS / IoT Gateway</td><td rowspan="2">Distribution System</td></tr>
<tr><td>Device</td><td></td><td>Inside Building
Heating sub-stations
Electric heaters
Smart washing machine
Smart dryer
Apartment meter
Apartment sensors</td><td>Outside Building
District Heating Network
Rooftop wind turbine
PV(-T) inverter
Borehole Thermal Energy Storage
Heatpumps
Large water buffers</td></tr>
</table>

TABLE 36 – CORDIUM HASSELT PILOT ARCHITECTURAL MAPPING TO THE SHBERA

VITO, the pilot leader, envisions using three semantically interoperable services provided by other partners (underlined in Table 36). Pilot leader of Thor park site (VITO) and pilot leader of the Genk site (Thermovault) are looking into the possibility of virtually connecting the Thor park pilot and the Genk site pilot. This would mean that flexibility could be exchanged between the two pilots and even aggregated.

<table>
<tr><th>Layer (HLA)</th><th colspan="4">Domains (SERA)</th></tr>
<tr><td>Stakeholders</td><td>User
Public EVSE operator
Building Manager EnergyVille1
Building Manager Incubator</td><td>CCC services (actors)
BMS operator</td><td>Energy services (actors)
Energy service provider (VITO)
Technical aggregator (VITO)</td><td>Energy System
Energy retailers</td></tr>
<tr><td>Application</td><td></td><td>CCC services</td><td>Energy services
Flexibility Service
PV Forecasting
Day ahead/Intraday Energy price forecaster
EV charging demand forecasting
Carbon intensity forecaster
DEMS application / technical aggregation & optimization with local objectives
Cooling demand forecast</td><td rowspan="3">Transmission System</td></tr>
<tr><td>Semantic Interoperability</td><td></td><td colspan="2">InterConnect interoperability layer
Semantically interoperable services: Flexibility service (REST), PV Forecaster (REST),) Day ahead intraday energy price forecaster (REST) P2P Marketplace - TBD
Services provided as containers: potentially all semantically interoperable services.
Access control - token based.</td></tr>
<tr><td>Communication (gateway)</td><td></td><td colspan="2">Building Communication and IoT Gateway Layer
EVSE management system
BMS Incubator
BMS EnergyVille1</td></tr>
<tr><td>Device</td><td></td><td>Inside Building
PV and PV submeter EnergyVille1
EnergyVille1 grid connection meter
Cooling HVAC Thor Central
EVSEs EnergyVille1</td><td>Outside Building
EVSEs Thorpark</td><td>Distribution System</td></tr>
</table>

TABLE 37 – THORPARK PILOT ARCHITECTURAL MAPPING TO THE SHBERA

The Pilot leader is planning to use a envisions carbon intensity forecasting service as a semantically interoperable service, which pilot could use if provided by other partners/pilots.

5.10.2STUDENT ROOMS ANTWERP (IMEC)

This pilot's main objective is to test smart grid solutions within a smart student dormitory building context, and ultimately, to evidence the advantages of having such solutions to improve the efficiency of the building energy consumption and the balance of the grid. In order to do this, IMEC will perform energy consumption monitoring and will explore the gamification of the use of common appliances. More details about (sub-)pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

<table>
<tr><th>Layer (HLA)</th><th colspan="3">Domains (SERA)</th><th></th></tr>
<tr><td>Stakeholders</td><td>User
Students
Building inhabitants</td><td>CCC services (actors)
Building operator
Building owner</td><td>Energy services (actors)
Game provider</td><td>Energy System
Energy provider</td></tr>
<tr><td>Application</td><td></td><td>CCC services
DYAMAND Application
Game Controller Service
Community-driven
application (SpaceFlow)
Building Digital Twin (OpenMotics)</td><td>Energy services
Flexibility Service
Gamification Application (SpaceFlow)
Grid Forecast (external partner)</td><td rowspan="2">Transmission System</td></tr>
<tr><td>Semantic Interoperability</td><td></td><td colspan="2">InterConnect interoperability layer
Semantically Interoperable services: DYAMAND application (REST), Gamification Application (REST), Grid Forecast (external partner)
P2P marketplace - NO
Services provided as containers - TBD
Access control for interoperable services - device type constraints, user category constraints and geographical constraints</td></tr>
<tr><td>Communication (gateway)</td><td></td><td colspan="2">Building Communication and IoT Gateway Layer
DYAMAND client</td><td rowspan="2">Distribution System
Smart meter</td></tr>
<tr><td>Device</td><td></td><td>Inside Building
Dryer
Washing Machine
Dishwasher</td><td>Outside Building
Smart meter</td></tr>
</table>

TABLE 38 – STUDENT ROOMS ANTWERP PILOT ARCHITECTURAL MAPPING TO THE SHBERA

5.10.3SMART DISTRICT NIEUWE DOKKEN GENT (DUCOOP & OPENMOTICS)

This sub-pilot aims to manage and operate a large, primarily residential, Local Energy Community in Ghent. The goal is to, bringing smart Energy IoT-appliances into practice in a real-life environment. Furthermore, it wishes to improve the partner's alignment with STORM and Farys Solar, allowing them to ultimately match the energy consumption with the excess wind energy and a local large PV set-up. More details about the (sub-)pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

<table>
<tr><th>Layer (HLA)</th><th colspan="3">Domains (SERA)</th><th></th></tr>
<tr><td>Stakeholders</td><td>User
Building owner
EV driver
Resident</td><td>CCC services (actors)</td><td>Energy services (actors)
ESCO</td><td>Energy System</td></tr>
<tr><td>Application</td><td></td><td>CCC services (OpenMotics)
Heatpump control
Battery control
Charging station control
District heating control</td><td>Energy services
Flexibility Service
Thermal Energy Flexibility
PV self-consumption (OpenMotics)
Electricity & heat demand forecast (OpenMotics)
Maximize use of wind power over fossil (OpenMotics)
Peak shaving (OpenMotics)
Energy efficiency management (OpenMotics)
Belpex price predictions (ENTSOE)
Weather predictions (Meteobleu)</td><td rowspan="3">Transmission System</td></tr>
<tr><td>Semantic Interoperability</td><td></td><td colspan="2">InterConnect interoperability layer
Semantically interoperable services: OpenMotics EMS (services use REST: maximize use of wind-power over fossil, PV self-consumption, Electricity and heat demand forecast, peak shaving), potentially interoperable services: Belpex price predictions (REST), Wind-power parameters (REST), Weather predictions (REST).
P2P marketplace - NO
Services available as containers - TBD</td></tr>
<tr><td>Communication (gateway)</td><td></td><td colspan="2">Building Communication and IoT Gateway Layer
EMS (OpenMotics) allowing for heat pump, battery, charging station, district heating and solar inverters control, i.e., sending/receiving signals over IoT gateway (OpenMotics)</td><td>Distribution System
Digital meters</td></tr>
<tr><td>Device</td><td></td><td>Inside Building
Heat pump (BlueHeat)
Battery (Battery Supplier)
District heating (Callens)
Whitegoods</td><td>Outside Building
EV Charging Station(s) (Powerdale)
Digital heat/calory meter
Digital Meters
Weather station (Davis Instruments)
Solar panels (Linea Trovata)</td><td></td></tr>
</table>

TABLE 39 – SMART DISTRICT NIEUWE DOKKEN GENT PILOT ARCHITECTURAL MAPPING TO THE SHBERA

5.10.4ZELLIK GREEN ENERGY PARK BRUSSELS (VUB)

The main objective of this pilot is to integrate energy and non-energy services (e.g., mobility) at the Green Energy Park living lab site and evaluate the added value for the stakeholder's integration of SAREF-compliant household appliances and bidirectional charging sites. More details about (sub)pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

<table>
<tr><th>Layer (HLA)</th><th colspan="4">Domains (SERA)</th></tr>
<tr><td>Stakeholders</td><td>User
EV user</td><td>CCC services (actors)
Home control service provider</td><td>Energy services (actors)
Aggregator</td><td>Energy System
Grid manager</td></tr>
<tr><td>Application</td><td></td><td>CCC services
Prosumer preferences
Automatization of assets
Optimal use of devices in house
Mobility forecasting</td><td>Energy services
Flexibility Service
Flexibility trading
Aggregation Service
Energy forecasting
Energy monitoring</td><td rowspan="2">Transmission System</td></tr>
<tr><td>Semantic Interoperability</td><td></td><td colspan="2">InterConnect interoperability layer
Semantically interoperable services - TBD
P2P marketplace - YES
Access control mechanisms - TBD
Services provided as downloadable containers - TBD</td></tr>
<tr><td>Communication (gateway)</td><td></td><td colspan="2">Building Communication and IoT Gateway Layer
BMS (to be specified)</td><td rowspan="2">Distribution System
Smart meter</td></tr>
<tr><td>Device</td><td></td><td>Inside Building
Battery storage (neighbourhood, house)
Whitegoods
PV
Sensors (temperature, movement)</td><td>Outside Building
EV Charging station (individual, collective), fast charging stations
Smart meter</td></tr>
</table>

TABLE 40 – ZELLIK GREEN ENERGY PARK PILOT ARCHITECTURAL MAPPING TO THE SHBERA

This (sub-)pilot is in an early stage of specification. More detailed mapping (especially to the interoperability framework architecture) will be provided as the pilot team progresses with definitions.

5.10.5NANOGRID LEUVEN (TH!NK-E)

This sub-pilot aims to provide a holistic, collaborative approach to advance the way we look at buildings and neighbourhoods. More details about this (sub-)pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

<table>
<tr><th>Layer (HLA)</th><th colspan="4">Domains (SERA)</th></tr>
<tr><td>Stakeholders</td><td>User
Energy community member
(Volunteers) participating in the Energy Community</td><td>CCC services (actors)
Energy Community Service Provider</td><td>Energy services (actors)
Project-level Service Provider
i.Leco as technical aggregator
Energy community service provider</td><td>Energy System
DSO/TSO (organizer of flex market)</td></tr>
<tr><td>Application</td><td></td><td>CCC services
User application with configuration parameters and preferences</td><td>Energy services
Flexibility service
Grid Energy Forecasting
Local Flexibility Market
Local energy forecasting
Derive available (aggregated) flexibility
Weather forecasting</td><td rowspan="3">Transmission System</td></tr>
<tr><td>Semantic Interoperability</td><td></td><td colspan="2">InterConnect interoperability layer
Semantically interoperable services - Aggregator of local flexibility (TBD)
Access control mechanisms and service containers - TBD
P2P Marketplace - YES</td></tr>
<tr><td>Communication (gateway)</td><td></td><td colspan="2">Building Communication and IoT Gateway Layer
BMS (i.Leco, outside of Consortium)</td></tr>
<tr><td>Device</td><td></td><td>Inside Building
Energy devices (PV, heatpump, whitegoods, energy storage, hydrogen fuel cell, hydrogen boiler)
Sensors (temperature, humidity and motion)</td><td>Outside Building
EV (V2G)
Local Electricity Grid on DC voltage
Energy meter</td><td>Distribution System
Local Electricity Grid on DC voltage
Energy meter</td></tr>
</table>

TABLE 41 – NANOGRID LEUVEN PILOT ARCHITECTURAL MAPPING TO THE SHBERA

This (sub-)pilot is in an early stage of specification. More detailed mapping (especially to the interoperability framework architecture) will be provided as the pilot team progresses with definitions.

5.10.6OUD-HEVERLEE PUBLIC BUILDINGS (3E)

This sub-pilot's objective is to steer the HVAC system, EV charger, and battery of a cluster of non-residential buildings (e.g., standard offices, such as city hall) to limit the impact on the low-voltage grid (220V), minimize the electricity bill and unlock the available flexibility to an aggregator. More details about the (sub-)pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

Layer (HLA)	Domains (SERA)			
Stakeholders	**User**	**CCC services (actors)** • DeltaQ (3rd party) • 3E SQPower	**Energy services (actors)** • Aggregator • Energy Service Provider	**Energy System** Supplier DSO
Application		**CCC services** • Platform as a service - user interface - User's settings, intervention, preferences, Power & Flexibility schedules, Setpoints, Acknowledgements, measurements & direct control	**Energy services** • Flexibility Service • Peak shaving • Weather, load, EV, PV, and price forecasts • ToU (DR) scheme • Self-consumption • EV & demand charge management • Monitoring • DSO signal following • Flexibility provision • (Energy) data and measurements (historical & real time)	**Transmission System**
Semantic Interoperability		**InterConnect interoperability layer** • Semantically interoperable services/platforms - SQPower platform with listed services (REST), DeltaQ (TBD). • P2P Marketplace - TBD • Services available as containers - TBD • Access control rules - TBD		
Communication (gateway)		**Building Communication and IoT Gateway Layer** • DeltaQ system • Field Automation Gateway • Infrastructure as a Service • On-site controllers		**Distribution System** Smart meter
Device		**Inside Building** • PV system • Battery (ABB) • HVAC (sensors & actuators) • Split unit (DAIKIN)	**Outside Building** • EV Charger (ABB) • Smart meter	

TABLE 42 – OUD-HEVERLEE PUBLIC BUILDINGS PILOT ARCHITECTURAL MAPPING TO THE SHBERA

This sub-pilot is currently developing the following services using SynaptiQ: REST API supports customer services from forecasting to optimization, control and monitoring. At the

same time, devices like battery and EV charger by ABB and Split by DAIKIN will be interfaced via interconnect interoperability framework. EV, price, and load forecast and EV charge management plus monitoring and UI as mentioned in the HLA are currently developed in SynaptiQ power for the sub-pilot. Details about mapping onto the interoperability framework architecture will be provided as the pilot progresses in specifications.

5.10.7GENK (THERMOVAULT)

This sub-pilot aims to prove the potential benefits of community self-consumption and peak shaving energy services by retrofitting and controlling legacy thermal loads, like electric water heaters, and interacting with whitegoods and electric vehicles. Moreover, partners participating in this sub-pilot wish to prove these services improve convenience, when combined with existing services like energy efficiency, energy comfort maximization and frequency response. More details about the (sub-)pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

<table>
<tr><th>Layer (HLA)</th><th colspan="4">Domains (SERA)</th></tr>
<tr><td>Stakeholders</td><td>User
Residential consumers and members of the local energy community</td><td>CCC services (actors)</td><td>Energy services (actors)
Energy management orchestrator (TBD)
EV aggregator (TBD)
Whitegoods aggregator (TBD)
PV forecaster (TBD)
Water heater aggregator (ThermoVault)</td><td>Energy System
Real time pricing provider</td></tr>
<tr><td>Application</td><td></td><td>CCC services
Thermal loads energy efficiency periodic reports
Comfort maximization</td><td>Energy services
PV forecasting (Vito?)
Water heater forecast and flexibility (ThermoVault)
EV forecast, flexibility (Vito, VUB?)
Whitegoods flexibility (?)
Energy management orchestrator
Peak shaving
Real time pricing
Self-consumption
Frequency response (TV)</td><td rowspan="3">Transmission System
Frequency
TSO API</td></tr>
<tr><td>Semantic Interoperability</td><td></td><td colspan="2">InterConnect interoperability layer
Semantically interoperable services - Water heater forecast and flexibility (REST)
P2P marketplace - NO
Services available as downloadable containers - NO</td></tr>
<tr><td>Communication (gateway)</td><td></td><td colspan="2">Building Communication and IoT Gateway Layer
Remote control of appliances</td></tr>
</table>

Device		**Inside Building** • Water heater • PV • Whitegoods • ThermoVault IoT modules	**Outside Building** • EV Charger • Smart meter	

TABLE 43 – GENK PILOT ARCHITECTURAL MAPPING TO THE SHBERA

In this pilot, the Device layer communicates directly with upper-layer services – (no BMS is envisioned). Services (underlined) are requested from other partners from other pilots.

5.11 PORTUGAL (EDP D)

This pilot's objective is to test how a Smart Grid infrastructure can enable new business demand to integrate DSF in e-markets. More details about the pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

Layer (HLA)	Domains (SERA)			
Stakeholders	**User** • Residential household consumer, prosumer • Commercial building manager (supermarket)	**CCC services (actors)** • Smart building system manager	**Energy services (actors)** • Technical integrator (INESC, SONAE, SENSI) • Incentive service provider	**Energy System** • DSO
Application		**CCC services** • Continente app (SONAE) • Energy monitoring app • HEMS device automation • ThermoVault controller • Data sharing with focus on privacy protection	**Energy services** • Flexibility service • Flexibility optimizer • Grid optimizer • Forecasting service • Metering data service • Energy monitoring service • EV forecasting and charging • Reduce energy fees • Incentives service	**Transmission System**
Semantic Interoperability		**InterConnect interoperability layer** • Semantically interoperable services/platforms: EV Forecast (SONAE/INESC, REST), Continente application (SONAE, REST), Energy monitoring application (SENSINOV/SONAE/INESC, REST), Data sharing service (INESC, REST), Grid optimizer (EDPD, interface TBD), Forecasting service (SONAE/INESC/EDPD, interface TBD), Metering data service (EDPD, metering data interface), DSO interface (interface tech TBD in WP4) • Services provided as downloadable containers: YES, TBD • P2P marketplace: YES • Access control mechanisms for services: TBD		

Communication (gateway)		**Building Communication and IoT Gateway Layer** • HEMS • BEMS • Flexibility service (HEMS) • ThermoVault controller		**Distribution System** • Smart meter • DSO interface
Device		**Inside Building** • HEMS device controller • ThermoVault controller	**Outside Building** • EV Charging • Smart meter	

TABLE 44 – PORTUGUESE PILOT ARCHITECTURAL MAPPING TO THE SHBERA

The Portuguese pilot will validate InterConnect's reference architecture and interoperability framework in residential and commercial buildings (supermarkets). The DSO interface will be developed within WP4 and will be used in other pilots as well (detailed mapping to other pilots will be decided as WP4 progresses).

5.12 GREECE (GRIDNET)

The goal of this pilot is to demonstrate the implementation of energy services (e.g., monitoring, control, Demand-Response), as well as Home control and comfort services in a residential set-up. More details about the pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

Layer (HLA)	Domains (SERA)			
Stakeholders	**User** • Home Owners/ Residents	**CCC services (actors)** • Smart home/building service providers (COSMOTE, GRIDNET, HERON) • Cloud providers (COSMOTE, GRIDNET, HERON) • Mobile app provider (AUEB)	**Energy services (actors)** • Smart home/building service providers (COSMOTE, GRIDNET, HERON) • Cloud providers (COSMOTE, GRIDNET, HERON) • Mobile app provider (AUEB) • Flexibility service provider (GFI) • Data analytics service provider (WINGS)	**Energy System** • DSO (Virtual)
Application		**CCC services** • Local/Remote Home Comfort services (monitoring, control and automations) - (COSMOTE, GRIDNET, HERON) • Cloud data storage and provisioning service (COSMOTE, GRIDNET, HERON)	**Energy services** • Local/Remote Home Comfort services (monitoring, control and automations) - (COSMOTE, GRIDNET, HERON) • Cloud data storage and provisioning service (COSMOTE, GRIDNET, HERON)	**Transmission System**

		• Mobile app for end users (AUEB)	• Mobile app for end users (AUEB) • Flexibility service (GFI) • Forecasting service (WINGS) • Recommendation service (WINGS)	
Semantic Interoperability		**InterConnect interoperability layer** • Semantically interoperable services/platforms: energy monitoring & control (COSMOTE/GRIDNET/HERON, REST, MQTT), home comfort monitoring & control (COSMOTE/GRIDNET/HERON, REST, MQTT), flexibility service (GFI, interface TBD), Forecasting & recommendation (WINGS, REST), mobile application for end users (AUEB, to integrate semantic interoperability during development). • P2P marketplaces: NO • Services provided as downloadable containers: NO • Access control mechanisms for services: pilot based and project-based access control		
Communication (gateway)		**Building Communication and IoT Gateway Layer** • IoT Gateway (COSMOTE, GRIDNET) • User's WiFi Network (HERON)		**Distribution System**
Device		**Inside Building** • Smart meter (Fuse Box) • Sensors (temperature, humidity, pressure, motion, luminosity, door/window, fire/gas) • Whitegoods (washing machine, dryer, dish washer) • A/C and water heaters • Comfort IoT (smart plugs, Google home speaker, light switches, IP cameras, TV sets, IR controller) • Alarm sirens.	**Outside Building** • EV charging station • Smart meter (For EV charging station)	

TABLE 45 – GREEK PILOT ARCHITECTURAL MAPPING TO THE SHBERA

Three of the pilot partners (GRIDNET, COSMOTE and HERON) will provide services and digital platforms for energy monitoring & control and home comfort monitoring & control. These services/platforms provide similar functionalities, but with different technology stacks. Achieving semantic interoperability between these three digital platforms and sets of services will be one of the main goals of the pilot. End-user mobile application (developed by partner AUEB) will utilize the achieved semantic interoperability to enable monitoring and control functionalities across all three digital platforms. Additional services, including flexibility service developed by GFI and data analytics service provided by WINGS will rely on the interoperability layer in order to gather data and provide the required services.

5.13 NETHERLANDS (HYRDE - ICITY)

The pilot's objective is to implement a set of devices, appliances, and sensors to increase the level of comfort and convenience while offering extra energy and non-energy services through the platform. Therefore, this pilot will explore and define the possibilities for demand-side flexibility and develop new business models for these services. More details about the pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

<table>
<tr><th>Layer (HLA)</th><th colspan="4">Domains (SERA)</th></tr>
<tr><td>Stakeholders</td><td>User
End user</td><td>CCC services (actors)
Building automation provider</td><td>Energy services (actors)
Flexibility service provider
Energy insights service provider</td><td>Energy System
Energy tariff provider</td></tr>
<tr><td>Application</td><td>End user’s application</td><td colspan="2">CCC services
Ekco portal, dashboard, workflow & automation/rules (Hyrde)
Ekco Marketplace & digital transaction switch (Hyrde)
Ekco installer app (Hyrde)
Ekco Fiware context broker (Hyrde)
UI for services & access management (Hyrde)
Net2grid (3rd party)
SmartThings app (Hyrde)
Homies (3rd party)
Energy services
Forecasting service
Weather forecast
Achmea service
Contract management
ReFlex - flexibility aggregation and optimization (TNO)
Energy insights (Net2Grid)</td><td rowspan="3">Transmission System</td></tr>
<tr><td>Semantic Interoperability</td><td></td><td colspan="2">InterConnect interoperability layer
Semantically interoperable services and platforms: Ekco services for smart homes/buildings (Hyrde, interfaces: REST, mDNS, SPINE/SHIP), ReFlex services for flexibility aggregation and optimization (TNO, interfaces: REST, SPINE/SHIP)
P2P marketplace: TBD - integrated with Ekco digital transaction solution
Services provided as downloadable containers: TBD
Access control mechanisms: InterConnect user base and access management API, Ekco codes/vaults (DTS)</td></tr>
<tr><td>Communication (gateway)</td><td></td><td colspan="2">Building Communication and IoT Gateway Layer
Edge IoT agents (Hyrde)
Edge device (Hyrde)
ReFlex resource manager (Hyrde, TNO)
Samsung SmartThings</td><td>Distribution System
Smart meter</td></tr>
</table>

Device		**Inside Building** • PV panels • Whitegoods (dishwasher, dryer, washing machine) • Samsung SmartThings & supported sensors, devices • VAV - ventilation • Sensors and smart home (ST motion, ST contact, Awair omni climate, Hue smart lights, ST camera, dim/switch, ST buttons, iLOq/Bold lock)	**Outside Building** • Batteries • EV Chargers • Smart meter (net2grid, p1port, dongle)	

TABLE 46 – DUTCH PILOT ARCHITECTURAL MAPPING TO THE SHBERA

The Dutch pilot integrates two main digital platforms: Hyrde Ekco for home automation and other IoT related functionalities, and TNO's ReFlex solution for energy flexibility management. Additional platforms and services are envisioned but are in negotiations with third parties and other project partners. The Dutch pilot is currently looking for a project partner providing forecasting services.

5.14 GERMANY (EEBUS)

The German pilot has two sub-pilots:

- The Commercial Pilot in Hamburg;
- The Residential Pilot in Norderstedt.

The following sections provide detailed descriptions of each sub-pilot's objectives, defined use cases, and architectural implementation.

5.14.1HAMBURG PILOT AND BEEDIP ARCHITECTURES (KEO)

This pilot aims to demonstrate how the Smart Grid infrastructure can act as an enabler of new business demand to integrate DSF in e-markets. More details about the (sub-)pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

Layer (HLA)	Domains (SERA)			
Stakeholders	**User** • Hotel manager • Hotel receptionist • Hotel guest/ EV driver	**CCC services (actors)** • Charge point operator	**Energy services (actors)** • Technical aggregator	**Energy System** • Energy supplier • DSO

Application		**CCC services** • Hotel guest application • Hotel manager application	**Energy services** • Flexibility service • DSO service (Fraunhofer/Uni. Kassel) • Aggregator service (Fraunhofer/Uni. Kassel) • Grid protection service (Fraunhofer/Uni. Kassel) • Grid calculation service • Hotel metering service • Local fuse protection service • Price optimized operation service • Forecasting	**Transmission System**
Semantic Interoperability		**InterConnect interoperability layer** • Semantically interoperable services/platforms: EMS (EEBUS, interface SPINE), mobile app for hotel guests (REST), Beedip platform services (SPINE, Web of Things with SAREF via MQTT). • P2P marketplace: YES • Services provided as downloadable containers: YES/TBD • Access control mechanism for services: certified Smart Meter Gateways and the necessary secure Infrastructure by German law (BSI)		
Communication (gateway)		**Building Communication and IoT Gateway Layer** • EMS (KEO, EEBus) • Smart Gateway (Theben)		**Distribution System** • Smart meter (Theben) • Hotel metering service
Device		**Inside Building** • Local EMS	**Outside Building** • Smart meter (Theben) • EV supply equipment (Wirelane) • EV ISO/PWM	

TABLE 47 – HAMBURG AND BEEDIP PILOT ARCHITECTURAL MAPPING TO THE SHBERA

P2P marketplace enablers will be utilized in this pilot's use cases: Grid stabilization; flexible tariffs; power consumption limitation; energy forecast services; monitoring of power consumption.

5.14.2RESIDENTIAL PILOT AT NORDERSTEDT (EEBUS)

This pilot aims to demonstrate how the Smart Grid infrastructure can act as an enabler of new business demand to integrate DSF in e-markets. More details about the (sub-)pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

<table>
<tr><th>Layer (HLA)</th><th colspan="4">Domains (SERA)</th></tr>
<tr><td>Stakeholders</td><td>User
Prosumer/ house owner</td><td>CCC services (actors)</td><td>Energy services (actors)
Technical aggregator (SWN)</td><td>Energy System
Energy supplier (SWN)
DSO (SWN)</td></tr>
<tr><td>Application</td><td></td><td>CCC services
Info service over CLS (SWN)</td><td>Energy services
Flexibility service
DSO service
Aggregator service
Grid protection service
Grid calculation service
Tariff service
Local fuse protection service
Tariff optimized operation service
Charging plan for EV</td><td rowspan="3">Transmission System</td></tr>
<tr><td>Semantic Interoperability</td><td></td><td colspan="2">InterConnect interoperability layer
Semantically interoperable services and platforms: EMS (EEBUS, interface SPINE/SHIP), SWN info service application (REST), SWN platform grid services (WoT with SAREF over MQTT, SHIP/SPINE).
P2P marketplace: TBD
Services provided as downloadable containers: TBD
Access control mechanism for services: certified Smart Meter Gateways and the necessary secure Infrastructure by German law (BSI)</td></tr>
<tr><td>Communication (gateway)</td><td></td><td colspan="2">Building Communication and IoT Gateway Layer
EMS (KEO, EEBus)
Smart Meter Gateway (Theben)</td></tr>
<tr><td>Device</td><td></td><td>Inside Building
Whitegoods (BSH, Miele, Whirlpool)
Heatpump (Vaillant, Dalkin)
PV (Open)</td><td>Outside Building
Smart meter (Theben)
EV supply equipment (Wirelane)
EV ISO/PWM</td><td>Distribution System
Smart meter</td></tr>
</table>

TABLE 48 – RESIDENTIAL NORDERSTEDT PILOT ARCHITECTURAL MAPPING TO THE SHBERA

The utilization of P2P marketplaces and the decision on who will be providing the interoperable services as downloadable containers are still in discussion with partner SWN.

5.15 ITALY (PLANET IDEA)

This pilot has three main objectives, which can be detailed as follows:

- Test and demonstrate an interoperable energy management system for residential dwellings, leveraging on different home appliances (type and manufacturer) and systems;

- Guarantee a seamless interoperability and data exchange between systems and devices within the Planet App;
- Exploit energy and non-energy services, including flexibility services for grid support.

More details about the pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

<table>
<tr><th>Layer (HLA)</th><th colspan="4">Domains (SERA)</th></tr>
<tr><td>Stakeholders</td><td>User
Smart home/building owner/ manager</td><td>CCC services (actors)
Living services provider (Planet Idea)</td><td>Energy services (actors)
Consumption optimization aggregator (RSE)
Energy manager (Planet Idea)</td><td>Energy System</td></tr>
<tr><td>Application</td><td>Application user
Device provider cloud</td><td>CCC services
Living manager aggregator (Planet Idea)
Remote control application
Whirlpool cloud services</td><td>Energy services
Energy forecast & consumption analysis (WD)
Energy optimization
Tariff schema for energy flexibility & optimization (RSE)
Energy forecast (WD)
Energy constraints validator (WD)</td><td rowspan="3">Transmission System</td></tr>
<tr><td>Semantic Interoperability</td><td></td><td colspan="2">InterConnect interoperability layer
Semantically interoperable services/platforms: Whirlpool digital platform (REST), Planet application (new app developed during project - interoperable), Planet Idea digital platform (REST, MQTT).
P2P marketplace: NO
Services available as downloadable containers: NO
Access control mechanisms: role-based access control, authorized access to devices (OAuth).</td></tr>
<tr><td>Communication (gateway)</td><td></td><td colspan="2">Building Communication and IoT Gateway Layer
Planet Energy Manager (Planet Idea)</td></tr>
<tr><td>Device</td><td>Device manufacturer (Whirlpool)</td><td>Inside Building
Whirlpool smart washing machine</td><td>Outside Building
Smart meter
Water meter
Heating/cooling meters</td><td>Distribution System
Smart meter</td></tr>
</table>

TABLE 49 – ITALIAN PILOT ARCHITECTURAL MAPPING TO THE SHBERA

The details about the integration of RSE and WD services are still in negotiation within the pilot team. The pilot's leader is looking into the possibility to integrate a monitoring and control capability of electric heat pumps to enrich load flexibility portfolio.

5.16 CROSS-PILOT (CYBERGRID)

This use case will demonstrate the interoperability advantages of interoperability between the digital platforms operating in several of the national pilots by creating an overarching demonstration. The focus is on showcasing the functionality that will be done using a service that enables exchanging flexibility information cross-border. It aims to aggregate different energy assets across various project pilots into the flexibility pool, providing a Pan-European cross border balancing services to the TSO. More details about the pilot's functional architecture, goals and high-level use cases can be found in deliverable reports D5.1 [43] and D1.1 [39].

<table>
<tr><th>Layer (HLA)</th><th colspan="4">Domains (SERA)</th></tr>
<tr><td>Stakeholders</td><td>User
Energy asset owner</td><td>CCC services (actors)
Energy asset controller</td><td>Energy services (actors)
Flexibility service provider
Flexibility service aggregator (cyberGRID)
Energy community manager</td><td>Energy System
BRP (out of scope)
TSO (out of scope)
DSO (out of scope)</td></tr>
<tr><td>Application</td><td></td><td>CCC services
Flexibility management platform (cyberGRID) - control signals</td><td>Energy services
Flexibility service
Flexibility management platform (cyberGRID) - management and aggregation</td><td rowspan="3">Transmission System
(Group) Balancing - simulated</td></tr>
<tr><td>Semantic Interoperability</td><td></td><td colspan="2">InterConnect interoperability layer
Semantically interoperable services and platforms: CyberNOC platform with flexibility management services (REST and MQTT)
P2P marketplace: TBD
Services available as downloadable containers: NO
Access control mechanism for services: consent for flexibility access - provided by energy asset owner.</td></tr>
<tr><td>Communication (gateway)</td><td></td><td colspan="2">Building Communication and IoT Gateway Layer
Generic energy assets - enable flexibility service on different levels (device, edge/BMS)</td></tr>
<tr><td>Device</td><td></td><td>Inside Building
Generic energy assets</td><td>Outside Building
Generic energy assets</td><td>Distribution System</td></tr>
</table>

TABLE 50 – CROSS-PILOT ARCHITECTURAL MAPPING TO THE SHBERA

The overarching use case for flexibility management will showcase interoperability between project pilots and their architectures through flexibility aggregation and management services

provided by CyberNOC platform. The following (sub-)pilots are expected to will provide flexibility services for this overarching use case:

- Belgium - Oud Heverlee – led by 3E;
- Belgium - Nieuwe Dokken Gent – led by OpenMotics;
- Belgium - Nanogrid – led by Think E!;
- Belgium - Cordium and Thorpark – led by VITO;
- Belgium - Antwerp – led by IMEC.
- Portugal – led by EDPD;
- Greece – led by GRIDNET (more information needed before deciding).
- German sub-pilots – led by EEBUS.
- The Netherlands – led by VolkerWessels Telecom/Hyrde.

The other (sub-)pilots (France and Italy) are continuing to review their possible flexibility service provision. Task 7.8 leader, cyberGRID, is working with these pilots to help them decide how they might participate in the overarching demonstration.

5.17 CONCLUDING REMARKS

This section mapped architectures and key resources (digital platforms, services, devices) and stakeholders of the project (sub-)pilots onto SHBERA. The mapping is done based on the workshop organized in the scope of WP2 and WP5 with all project (sub-)pilots. It is important to note that most of the project (sub-)pilots are working internally on detailed specifications of architectures, roles and implementation tasks. Specific updates to the presented mappings to SHBERA are possible as the(sub-)pilots progress with their specifications and implementations.

The main conclusions of the SHBERA mappings are:

- All pilots include both CCC and energy domain services;
- All pilots include devices residing inside and outside of a building;
- (Sub-)pilot partners cover the key stakeholders' roles identified for their pilots;
- DSO stakeholder is present in Portuguese, German and French pilots. In some of the (sub-)pilots, DSO stakeholders and key functions will be emulated;
- DSO interface (to be specified and implemented in WP4) will play an essential role for all pilots seeking to demonstrate integration with this type of stakeholder;

- All (sub-)pilots require some flexibility management and forecasting services. Enabling semantic interoperability of these services will significantly increase their reusability between pilots and provide opportunities for validation of service semantic interoperability between pilots;
- The overarching pilot/use case led by cyberGRID will provide an opportunity for validating interoperability between pilots and between regulatory domains from the perspective of flexibility management services;
- Most of the services and digital platforms, which will be made semantically interoperable, expose RESTful communication APIs while some utilize MQTT protocol. Additionally, SPINE/SHIP protocol stack is represented in resources (e.g. devices and digital platforms) which will be made semantically interoperable. Based on this, WP5 will focus on implementing generic interoperability adapters for REST, MQTT and SPINE/SHIP;
- P2P marketplace enablers will be validated in at least 5 (sub-)pilots (confirmed). More pilots will decide on the need/plans for implementation of P2P marketplaces before the pilots' kick-off;
- Four (sub-)pilots indicated that they plan to provide their interoperable services as downloadable containers that can be instantiated on third party digital platforms with properly configured runtime environments. Other (sub-)pilots are still deciding on this. The InterConnect Service Store will be developed with this functionality as one of the minimal requirements.

6 CONCLUDING REMARKS

This document reports the current progress and results of the WP2 activities within the InterConnect project.

This document is the first version of InterConnect's Secure interoperable IoT smart home/building and smart energy system reference architecture (SHBERA), the second version is D2.4, due in M36.

The goal of this deliverable, and its related tasks, was multifold:

- Define, along with the project stakeholders, all of the guiding principles and requirements that InterConnect's Reference Architecture needed to aby by, at all times. In total, 5 High-Level Requirements, pertaining to all core components (e.g., Security & privacy, Semantic Interoperability Layer, Service Store, and others) were defined. These requirements are detailed in Section 3.4;
- Produce a technology-independent and device agnostic system architecture, based from WP1 Use Cases and other European initiatives, for the Smart Home, Smart Building and Smart (Grid) Energy domain. This work was carried out in tasks T2.1 and T2.2, which produced the SHBERA and its two composing viewpoints: the Smart Energy Reference Architecture (SERA), and the Smart Home and Smart Building IoT Reference Architecture (SHBIRA). All of these viewpoints were covered in Section 4;
- Define an approach for achieving project-wide interoperability, via semantic reasoning mechanisms that can exploit the benefits of ontologies. This work was carried out mostly in T2.4 and its result are discussed in Section 5;
- Provide initial guidelines and recommendations for embedding security and privacy policies into the resulting reference architecture, defined in Sections 3.3 and 4.5;
- Align and converge on Energy Flexibility and Demand Response interfaces and data models for system services, including functions for congestion management (with DSOs) or flexibility activation validation.

These objectives can be structured into 'areas' for structuring this deliverable's key take-aways and observations, as well as gaps and expected actions to be addressed in D2.4. The following areas were considered: Reference Architecture, Security, Services, InterConnect Framework, Semantic Interoperability and Energy Flexibility.

Area	Key take-away/observation	Gaps & Expected actions for V2
Reference Architecture	• The layered SHBERA and the different architecture viewpoints it defines different type of partners and people to engage with the InterConnect Reference Architecture. It can be used by energy actors, energy or in-home service providers, use case creators, platform developers, etc. • Establishing a consolidated common energy actor and role definition was not possible due to different future visions/options and different legislations in the energy domain. • But establishing an architecture with basic roles and system elements was feasible, due to similarity in use cases and the related information objects exchanged between the basic roles and system elements. • IoT and the energy system (Smart Home and Smart Grid) have very different backgrounds and were not easy to converge in one vision/approach. We have made first steps, but are not completely there yet. In and with WP4 next steps on integrating the DSO better in the architecture can be made.	• Next steps in pilot architectures need to be compared with the reference architecture. Differences should be explained (deviations for specific purpose, legacy, etc.), and will lead to an update of the reference architecture and other lessons learned in a next version of this document. • In and with WP4 next steps on fully embedding of the DSO and DSO related interfaces in the Smart Energy Reference Architecture needs to be made.
Security	• The InterConnect Architecture and Framework should be able to facilitate different security groups. Each security group will define a specific domain and security level.	• Security, and ways to put this in the architecture and system is another area that needs more attention in the next period of the project. Especially specify the different security groups, the security requirements for each security group and specify for each device/service which security group applies. • Pilots need to follow privacy by design principles when instantiating the reference architecture. • Integration of access control and privacy protection procedures with semantic interoperability layer and its main functions - reasoning and orchestration needs to be performed.
Services	• Having several implementations of the same service by different partners provides the opportunity to test interoperability and even interchangeability by switching from one service instance to another instance of the same service. • Most project pilots require energy flexibility and forecasting services - this is opportunity to demonstrate interoperability by reusing these services between pilots.	• Specification of minimum interoperability requirements/indicators per service category, digital platforms and device types. • Specification of interoperability compliance tests for services (per category) and devices. • Service providers need to assess added value of semantic reasoning.

	• Flexibility services need to be better defined and scoped to enable using the same services.	• Pilots should reuse interoperable services from other pilots instead of developing their own.
InterConnect Framework	• WP5 needs to develop InterConnect Interoperability Framework as enabler for instantiation of reference architectures within project pilots. • Most services and digital platforms utilize REST and MQTT communication interfaces/APIs - WP5 should therefor focus on producing generic interoperability adapters for REST, MQTT and SPINE/SHIP.	• When the InterConnect Framework is further specified and mature enough to demonstrate, next steps in promotion and ecosystem building needs to take place.
Semantic Interoperability	• Semantic interoperability enables instantiation of the reference architectures in the project pilots across available digital platforms and other key resources comprising these pilots. • The Semantic Interoperability Layer needs to integrate best practices and functionalities from presented solutions provided by partners. • Although we still need to figure out several details regarding the interoperability layer, we have found a good compromise between innovative, flexible and practical.	• Semantic Interoperability and ontologies is a promising technology but are for many partners and people a quite complex technology. Examples that show the benefits can help to increase the understanding and adoption rate. • Focus on getting a minimum viable product as soon as possible and then start extending/changing it in an iterative way. Do not expect the first version to already cover everything. • Specification of unifying interoperability protocol - SPARQL+. • Impact of reasoning on different service categories and realization of use cases. • Applicable SAREF ontologies need to be further defined and brought into standardisation organisations.
Energy Flexibility	• Energy Flexibility is used but also expressed in different ways and different abstraction levels. For full interoperability this is currently not good enough.	• Next steps towards a ‘universal’ way to express and exchange energy flexibility needs to be made. Starting from the mentioned energy flexibility pattern is currently the best way forward. When available this needs to be brought into the ontologies and into standardisation organisations. • Energy flexibility (and forecasting) data/information model need to be created.

TABLE 51 – KEY TAKE-AWAYS AND GAPS TO BE ADDRESSED IN D2.4

ANNEX 1 – TEMPLATE FOR SEMANTIC SOLUTIONS

This section presents the template that has been used to collect the available semantic solutions among InterConnect partners that are described and analyzed in Section 5.4.

Category	Objectives
Title and Proposer(s)	*Short title to summarize the underlying concept and the InterConnect partners proposing the solution.* ***Please describe your semantic solution in max 2 pages***
Context and Project(s)	*In which context and projects the solution has been (or is being) developed (including pointers/URLs)*
Maturity	*An evaluation of the maturity of the solution using the Technology Readiness Level (TRL):* *TRL 1 – basic principles observed* *TRL 2 – technology concept formulated* *TRL 3 – experimental proof of concept* *TRL 4 – technology validated in lab* *TRL 5 – technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)* *TRL 6 – technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)* *TRL 7 – system prototype demonstration in operational environment* *TRL 8 – system complete and qualified* *TRL 9 – actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)*
Overview (max 200 words)	*A general description* ***in max 200 words*** *of the proposed solution and its main components that also shows how the semantic interoperability mechanism is embedded in the more general InterConnect reference architecture (which is still under development, so it is fine if there are implicit suggestions here also for the reference architecture). Please provide an overall picture (we encourage architecture images) and a high level explanation.*
Semantic Components Description (max 300 words)	*A detailed description in* ***max 300 words*** *of the semantic components (with pictures, if needed, otherwise refer to the picture provided in the Overview section above). In particular, please explain the following (clearly and briefly):* • *How does your solution realize the translation/mapping mechanism from devices to SAREF (or other ontologies) and vice-versa? (Southbound interface)*

	• *Does your solution include a mechanism/repository to semantically publish and discover services to support the InterConnect marketplace and how does it work? (Northbound interface)*
Reasoning support	*How does your solution guarantee reasoning support? Which of the following levels of SAREF compliance does your solution provide? (Note that the aim of InterConnect is to start at least from level 2):* • *Level 0: no reasoning support. With reasoning support, we mean reasoning based on ontologies using semantic web technologies, such as RDF, OWL and SPARQL (as described in Section 5.3);* • *Level 1: basic reasoning to infer new knowledge (according to section 5.3.1). That is, the use of a reasoner for consistency checking to validate that there are not violations in RDF/OWL. For example, if two classes are declared as disjoint (e.g., black and white), but a certain instance (e.g., snow) is declared as rdf:type of both these classes (therefore, meaning that snow is both white and black), then the reasoner will throw a violation.* • *Level 2: advanced reasoning to infer new knowledge (according to section 5.3.1). That is, the use of a reasoner for deriving new knowledge via, for example, subclassing, axioms and rules. This is the most powerful feature of ontologies and semantic web technology, and sometimes it can lead to unexpected results, even for the ontology developers themselves. Therefore, it must always be checked with a reasoner what are the implications of the relations, axioms and rules linking the concepts defined in an ontology.* • *Level 3: additional reasoning to orchestrate data exchange (according to section 5.3.2), on top of the advanced reasoning to infer new knowledge at level 2. That is, the use of a reasoner for the composition of knowledge coming from various, distributed data sources (which can be devices, services or platforms in the InterConnect ecosystem) to meaningfully orchestrate their data exchange. This orchestration is not simply based on an exact matching of explicitly defined RDF/OWL triples but makes use of a reasoner for an advanced matching of these triples.*
Compliance with SAREF	*How does your solution guarantee compliance with SAREF? Which of the following levels of SAREF compliance does your solution provide? (Note that the aim of InterConnect is to start at least from level 2):* • *Level 0: no SAREF compliance. That is, SAREF is not used at all. Note that this is decoupled from the reasoning support mentioned above (in other words, level 0 in SAREF compliance does not automatically imply level 0 in reasoning support. In fact, reasoning support can be guaranteed using other ontologies than SAREF).* • *Level 1: basic SAREF compliance. That is, SAREF is taken into account and an explicit mapping to SAREF exist via a document, such as a textual file, a table or a spreadsheet[68]. Note that this type of mapping, however, is not automated nor directly machine processable, but requires manual human interpretation.* • *Level 2: intermediate SAREF compliance. That is, not only SAREF is taken into account, but machine interpretation is enabled. For example, data that is already encoded in a certain format (e.g., XML or JSON) can be annotated (labelled) using SAREF concepts in a semantic web language like for instance*

[68] See for example the mappings in the form of a look-up table elaborated during the first Smart appliances study for the European Commission [6], also available as a more detailed mapping spreadsheet at https://sites.google.com/site/smartappliancesproject/documents

	RDF/OWL. In this way, the mapping to SAREF becomes machine processable, as an automated script, for example, can be used to convert the original data format into SAREF compliant RDF/OWL triples. • *Level 3: full SAREF compliance. That is, direct use of SAREF concepts in RDF/OWL. A SAREF compliant file in RDF/OWL exists and it is fully machine interpretable, also using a reasoner. Note that this level has a relation with the reasoning support mentioned above, as level 3 in SAREF compliance enables levels 1, 2 and 3 of reasoning support (but not vice-versa, as reasoning support can be guaranteed using other ontologies rather than SAREF).*
Supported data formats	*What data format is originally used to structure the exchanged data among devices? E.g., JSON, XML, CSV, etc.?*
Supported standards and protocols	*What standard(s) and protocol(s) does the proposed solution support for the communication among devices (southbound interface)? E.g., SPINE, KNX, ZigBee, etc. What standard(s) and protocol(s) are supported for the interoperability among services (northbound interface)?*
Security and Privacy	*Are security and privacy taken into account into the proposed solution? If so, how? Has a risk analysis been done? Is there an authentication and access-control mechanism?*
Accessibility and License	*Does the solution provide a license specification? Is it open source or freely available for InterConnect partners and/or outside InterConnect? See INESC TEC presentation on Intellectual Property Management (link): take your time and think carefully about this.*
Strengths	*A generic description of the current strengths. What are the main advantages of this solution?*
Weaknesses	*A generic description of the current weaknesses. What are the disadvantages of this solution and weak spots? Are there measures and solutions already foreseen or available to overcome these weaknesses?*
References	*List here your references, if any.*

REFERENCES

EXTERNAL DOCUMENTS

[1] AIOTI, "High Level Architecture (HLA)," 2018. [Online]. Available: https://aioti.eu/wp-content/uploads/2018/06/AIOTI-HLA-R4.0.7.1-Final.pdf.

[2] oneM2M.org, “Functional Architecture,” [Online]. Available: https://www.onem2m.org/getting-started/onem2m-overview/introduction/functional-architecture. [Accessed 2020].

[3] FIWARE, “FIWARE NGSI v2 specification,” 2018. [Online]. Available: http://fiware.github.io/specifications/ngsiv2/stable/ . [Accessed 2020].

[4] E. a. B. M. a. K. J. a. Y. J. a. L. G. F. a. Z. M. Kovacs, “Standards-Based Worldwide Semantic Interoperability for IoT,” *IEEE Communications Magazine,* vol. 54, pp. 40-46, 2016.

[5] W3.org, "Web of Things (WoT) Architecture," 2020. [Online]. Available: https://www.w3.org/TR/wot-architecture/. [Accessed 2020].

[6] IEC, “Communication networks and systems for power utility automation,” 2020.

[7] Deutsches Institut für Normung (DIN), “DIN SPEC 27070 Requirements and reference architecture of a security gateway for the exchange of industry data and services,” 03 2020. [Online]. Available: https://www.din.de/en/wdc-beuth:din21:319111044. [Accessed 2020].

[8] K. Helmholt and G. Broenink, "Degrees of Freedom in Information Sharing on a Greener and Smarter Grid," in *ENERGY 2011 : The First International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies*, Venice/Mestre, Italy, 2011.

[9] K. Helmholt and G. Broenink, “Degrees of Freedom in Sharing Control of Smart Grid Connected Devices; A framework for comparison of cross-organizational control sharing mechanisms for balancing supply & demand,” in *ENERGY 2012: The Second International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies*, St. Maarten, Netherlands Antilles, 2012.

[10] M. J. Konsman, W. E. Wijbrandi and G. B. Huitema, "Unlocking residential Energy Flexibility on a large scale through a newly standardized interface," in *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2020.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant agreement No 857237

[11] T. Nuytten, B. Claessens, K. Paredis, J. Bael and D. Six, "Flexibility of a combined heat and power system with thermal energy storage for district heating," *Applied Energy,* vol. 04, p. 583–591, 2013.

[12] Smart Grids Task Force , “EG3 REPORT - Regulatory Recommendations for the Deployment of Flexibility,” 01 2015. [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/EG3%20Final%20-%20January%202015.pdf. [Accessed 2020].

[13] ETSI TS: 103 375, “SmartM2M; IoT Standards landscape and future evolutions,” 2016. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf. [Accessed 2020].

[14] AIOTI, "Semantic Interoperability," 2015. [Online]. Available: https://www.iab.org/wp-content/IAB-uploads/2016/03/AIOTIWG03Report2015-SemanticInteroperability.pdf.

[15] S. Widergren, D. Hardin, R. Ambrosio, R. Drummond, E. Gunther, G. Gilchrist and D. Cohen, “GridWise Interoperability Context-Setting Framework,” 2008.

[16] ETSI TS: 103 264, “SmartM2M; Smart Appliances; Reference Ontology and oneM2M Mapping,” 2017.

[17] R. v. d. Weerdt, V. d. Boer, L. Daniele and B. Nouwt, “Validating SAREF in a Smart Home Environment,” in *Research Conference on Metadata and Semantics Research*, 2021.

[18] M. Bauer, H. Baqa, S. Bilbao, A. Corchero, L. Daniele, I. Esnaola-Gonzalez, I. Fernandez, Ö. Frånberg, R. G. Castro, M. Girod-Genet, P. Guillemin, A. Gyrard, C. E. Kaed and A. Kung, "Semantic IoT Solutions - A Developer Perspective," 2019.

[19] C. Brewster, B. Nouwt, S. Raaijmakers and J. Verhoosel, “Ontology-based access control for FAIR data,” *Data Intelligence,* pp. 66-77, 01 2020.

[20] A. Gyrard, M. Serrano, S. K. Datta, J. B. Jares and M. I. Ali, "Sensor-based Linked Open Rules (S-LOR): An Automated Rule Discovery Approach for IoT Applications and its use in Smart Cities," in *3rd International ACM Smart City Workshop (AW4city) in conjunction with 26th International World Wide Web Conference (WWW 2017)*, Perth, Australia, 2017.

[21] A. Gyrard, C. Bonnet and K. Boudaoud, “Enrich Machine-to-Machine Data with Semantic Web Technologies for Cross-Domain Applications,” in *IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, Korea, 2014.

[22] M. Serrano and A. Gyrard, “A Review of Tools for IoT Semantics and Data Streaming Analytics,” in *The Building Blocks of IoT Analytics - Internet-of-Things Analytics*.

[23] A. Gyrard, C. Bonnet and K. Boudaoud, “Helping IoT application developers with Sensor-based Linked Open Rules,” in *7th International Workshop on Semantic Sensor Networks, in conjunction with the 13th International Semantic Web Conference (ISWC)*, Riva del Garda, Trentino, Italy, 2014.

[24] M. Bauer, H. Baqa, S. Bilbao, A. Corchero, L. Daniele, I. Esnaola-Gonzalez, I. Fernandez, O. Franberg, R. G. Castro, M. Girod-Gene, P. Guillemin and A. Gyrard, "Towards Semantic Interoperability Standards based on Ontologies," 2019.

[25] P. Murdock, L. Bassbouss, A. Kraft, M. Bauer, O. Logvinov, M. B. Alaya, T. Longstreth, R. Bhowmik, P. Martigne, P. Brett, C. Mladin and R. Chakraborty, "Semantic Interoperability for the Web of Things," 2016.

[26] A. Gyrard and A. Sheth, "IAMHAPPY: Towards an IoT knowledge-based cross-domain well-being recommendation system for everyday happiness," *Smart Health Journal,* 2019.

[27] DKE Deutsche Kommission ElektrotechnikElektronik Informationstechnik in DIN und VDE, “German Standardization Roadmap: Smart Home + Building,” 2015. [Online]. Available: https://www.dke.de/resource/blob/1741662/45ca0b869b3c199349c472d8a008f93e/german-standardization-roadmap-smart-home---building--version-2-0-data.pdf.

[28] Industrial Internet Consortium, "The Industrial Internet of Things Volume G1: Reference Architecture," 2019. [Online]. Available: https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf. [Accessed 2010].

[29] International Data Spaces, “Reference Architecture Model,” 04 2019. [Online]. Available: https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf. [Accessed 2020].

[30] Nsl, Data Intelligence, “Ontology-based access control for FAIR data,” pp. 66-77, 01 2020.

[31] E. Kovacs, M. Bauer, J. Kim, J. Yun, F. L. Gall and M. Zhao, “Standards-Based Worldwide Semantic Interoperability for IoT,” *EEE Communications Magazine,* vol. 54, no. 12, pp. 40-46, 2016.

[32] S. Vandael, B. Claessens, M. Hommelberg, T. Holvoet and G. Deconinck, “A Scalable Three-Step Approach for Demand Side Management of Plug-in Hybrid Vehicles,” *IEEE Transactions on Smart Grid,* vol. PP, pp. 1-9, 2012.

[33] L. Daniele, F. d. Hartog and J. Roes, “Study on Semantic Assets for Smart Appliances Interoperability,” 2015.

[34] ETSI TS: 103 376, “SmartM2M; IoT LSP Use Caes and Standards Gaps,” 2016.

[35] L. Daniele, W. Strabbing, B. Roelofsen, A. Aalberts and P. Stapersma, “Study on ensuring interoperability for enabling Demand Side Flexibility,” 2018.

[36] J. Moreira, L. Daniele, L. P. Ferreira, K. Wasielewska, P. Szmeja, W. Pawlowski, M. Ganzha and M. Paprzycki, “Towards IoT platforms’ integration: Semantic Translations between W3C SSN and ETSI SAREF,” 2017.

[37] A. Gyrard, “Designing cross-domain semantic Web of things applications,” 2015.

INTERCONNECT DOCUMENTS

[38] InterConnect Grant Agreement number 857237.

[39] InterConnect project. “D1.1 Services and use cases for smart buildings and grids”. 2020.

[40] InterConnect project. “D1.2 Mapping between se cases and large-scale pilots”, unpublished report. 2020.

[41] InterConnect project. “D1.3 System use cases for smart buildings and grids”, unpublished report. 2021.

[42] InterConnect project. “D2.2 Privacy and security design principles and implementation guidelines”, unpublished report. 2021.

[43] InterConnect project. “D5.1 Concept, design and architecture of the interoperable marketplace toolbox”. 2020.

[44] InterConnect project. “D5.2 Data flow management”. 2020.