interconnect

interoperable solutions connecting smart homes, buildings and grids

WP2 – Interoperable IoT Smart Homes and Grid Reference Architecture

D2.1 Full Report

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 – Full Report Secure Interoperable IoT Smart Home/Building and Smart Energy System Reference Architecture
TYPE	Report
DISTRIBUTION LEVEL	Public
DUE DELIVERY DATE	30/09/2021
DATE OF DELIVERY	30/09/2021
VERSION	V2.0
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, E-REDES, 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, E-REDES, 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
1.1	Sensinov, TNO	15/09/2021	Edited version addressing EU reviewers' comments – ready for transformation to Executive Summary, Technical Summary and Full Report
1.7.5	TNO	22/09/2021	Full Report version – ready for internal review
1.8	INESC TEC, TNO	28/09/2021	Full Report version – internal review, feedback, and comments
2.0	Sensinov	30/09/2021	Full Report - 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	E-REDES
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
Fábio Coelho Filipe Ribeiro Ruben Queirós	INESC TEC
Thomas Fichedick	KEO
Joost Demarest	KNX
Stefaan Aelbrecht Chaim de Mulder	OpenMotics
Stefano Fava Fabrizio Tortonese	Planet Idea
Nour Sobh Maria Perez	RDGFi
Miguel Gonçalves	Schneider Electric Portugal
Eliana Valles Mahdi Ben Alaya	Sensinov
Amandio Ferreira	SONAE - ELERGONE

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:

ABSTRACT

This document is the first deliverable produced by WP2 – Domain Interoperable IoT Reference Architecture. D2.1 uses and develops the output and ongoing work of WP2 and other WPs. Hence, this Deliverable and its related tasks:

- Create **a common vision** for the InterConnect ecosystem from an architectural point of view that can be understood by all partners that come from highly different domains, each with their own standards, reference architectures and business models.

- Define the **Secure Interoperable IoT Smart home/building and smart energy system reference architecture (SHBERA)** for the technology-independent and device-agnostic InterConnect ecosystem, with its four viewpoints:
    a. the high-level organisationally oriented **Smart Energy Reference Architecture (SERA**) point of view, produced by task T2.2, from an Energy System perspective. It homogenizes the views of partners regarding relationships between devices and (commercial) services from different domains through InterConnect, the separation of concerns, and the relationship with the traditional (electrical) Energy System;
    b. a high-level technically oriented **Smart Home/Building IoT Reference Architecture (SHBIRA)** point of view**,** produced by task T2.1 from an Internet of Things (IoT) perspective. It homogenizes the views of partners regarding functional layers of abstraction in a system of Smart Homes, Buildings connected to a Smart Grid;
    c. a lower-level technically oriented **Interoperability Framework (IF)** point of view, based on the work in WP5. Through the use of technical adapters and connectors it adds significant constraints regarding the use of Internet and web technology for creating interoperability;
    d. a lower-level semantically oriented **Semantic Interoperability Layer (SIL)** point of view, produced by task T2.4. It provides a common understanding of semantical concepts (through ontologies) and adds significant constraints in the way Knowledge is exchanged between components of the InterConnect ecosystem on the basis of (the InterConnect set of) ontologies;
- 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, produced by T2.3;
- Contains the result of collaboration 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 four different **architectural viewpoints (i.e., SERA, SHBIRA, IF and the SIL)** that cover the full set of interactions between the different domain and actors specified in WP1;
- Providing a **high-level specification of what is needed create an ecosystem of semantically interoperable components**, 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.

KEY REPORT TAKEAWAYS

- This document introduces several relevant (reference) architectures that have already been introduced by key European Standardisation Organisations and other alliances in the domains of the Internet of Things (IoT) Smart Homes, Smart Buildings and Smart Grids. These **reference architectures are then categorised based on what is needed to create the system of interoperable solutions as foreseen by the InterConnect project**. It does so in three dimensions: interoperability, ontology, and Information and Communication Technology (ICT). Key findings can be summarized as follows:
  - Most **reviewed architectures score high across the three dimensions**, although not always equally throughout three subdimensions of interoperability: technical, syntactic, and semantic. **InterConnect aims at full interoperability across the board, implying that existing (reference) architectures did not provide enough support to achieve the desired impact of the H2020 InterConnect project.**
  - **Architectures that scored high regarding semantic interoperability also scored high in the ontology dimension**. Semantic reasoning and what it can convey to interoperability is one of the key exploitable results that InterConnect is expected to deliver.
  - Reference **architectures closer to the IoT ecosystem show significant relevance on the edge, fog, and cloud focus**. InterConnect also addresses the need to distribute processing between the edge devices and to include fog systems by delivering 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.
- Following both a top-down and a bottom-up approach, InterConnect's **Secure interoperable IoT smart Home/Building and smart Energy system Reference Architecture (SHBERA)** was derived from:
  - **The analysis of the SotA**: after analysis and consideration of each relevant reference architectures (RAs), it became clear no single RAs scores high enough in all dimensions when ranked by project stakeholders. The focus was then put on reusing and extending useful concepts while attempting to provide a bridge between different domains so that project stakeholders can understand each other in terms of the three dimensions interoperability, ontology, and ICT processing.
  - **The project's primary and derived requirements**, which are the high-level requirements that InterConnect's RA should always comply with. These principles were created to ensure that the resulting RA is a technology-independent and device-agnostic ecosystem.
  - **Multiple viewpoints:** each viewpoint shows the architecture of the system, but certain parts and/or components are abstracted from. This results in views on the architecture that are understood by the relevant domain experts and can still

be comprehended by the individual expert, thus allowing to build consensus on how to reach interoperability.

- The SHBERA contains the following viewpoints per domain:
  - **Energy (SERA):** the **Smart Energy Reference Architecture**. It is the InterConnect viewpoint from the Energy domain that focuses on devices, services, actors, business roles, and the Smart (electrical) Grid. It also emphasizes information exchange in the energy system from an InterConnect point of view
  - **Internet of Things (SHBIRA):** The perspective from the IoT domain that focuses on the interoperability and communication of services with each other and with devices, cloud, and local management systems at different layers (of abstraction).
  - **Technical integration for interoperability (IF):** InterConnect's Interoperability Framework takes the viewpoint of technical integration for interoperability**.** It looks at the InterConnect ecosystem as containing a platform with services, such as the service store for all interoperable services, P2P marketplace enablers, access control mechanisms, generic interoperability adapters, enabling communication, and others ; and
  - **Semantic engineering (SIL):** A viewpoint from the domain of semantic engineering and has even more focus on the language used in interoperability than the IF, causing it to be the visually smallest subset of *architectural* concepts in this visualization of the SHBERA.
- InterConnect aims to **achieve interoperability at the semantic level**. Thus, the project will **use semantic web technology supporting**:
  - The creation of the architecture for a large-scale distributed system of interconnected components that can exchange information using a shared understanding of complex concepts, documented in machine-parsable ontologies.
  - The integration of standardized and existing information models from different (industrial) domains. Instead of having to create a completely new standard, the relationship between these existing models is expressed in ontologies, enabling harmonisation at a higher level of abstraction.

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
IF	(InterConnect's) Interoperability Framework
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 Architectural 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

This deliverable document contains the **Full Report on the Secure Interoperable IoT Smart Home/Building and Smart Energy System Reference Architecture (SHBERA)**, which is a result of the work carried out within Work Package (WP) 2 of the H2020 InterConnect project. This chapter is an introduction to WP2, the relationship with other WPs, the objectives of D2.1 and provides an overview of the document structure.

1.1 WP2 - INTEROPERABLE IOT SMART HOMES AND GRID REFERENCE ARCHITECTURE

Within the InterConnect project WP2 oversees the following activities and objectives:

- Define **SHBERA** a technology-independent, device-agnostic system architecture for the Energy and IoT domains, **consisting of multiple (reference) architectural viewpoints** and frameworks as defined in different Tasks (T):
    - the **Smart Home/Building IoT Reference Architecture (SHBIRA)** as defined by T2.1;
    - the **Smart Energy Reference Architecture (SERA)**, as defined by T2.2; and
    - **InterConnect's Interoperability Framework (IF)**, as defined by T5.1; and
    - the **Semantic Interoperability Framework**, the result of the work in T2.4.
- Define the set of **privacy and security strategies and guidelines supporting a privacy-by-design approach** (in T2.3). WP5, and 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 Layer** (T2.4), supporting semantic interoperability among the different devices, services, and platforms available within the project's 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.
- 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 by WP1.

1.2 RELATIONSHIPS WITH OTHER WORK PACKAGES

As shown in Figure 1, the work of WP2 interacts with the work conducted by other (technology oriented) WPs, while at the same time providing architectural viewpoints as key enablers for those same WPs, namely:

- WP1, from which this WP utilized Use Cases to infer the architectural requirements for the project's reference architectural viewpoints.
- WP5, particularly T5.1, as it allowed for various iterations of the SHBERA and its viewpoints.

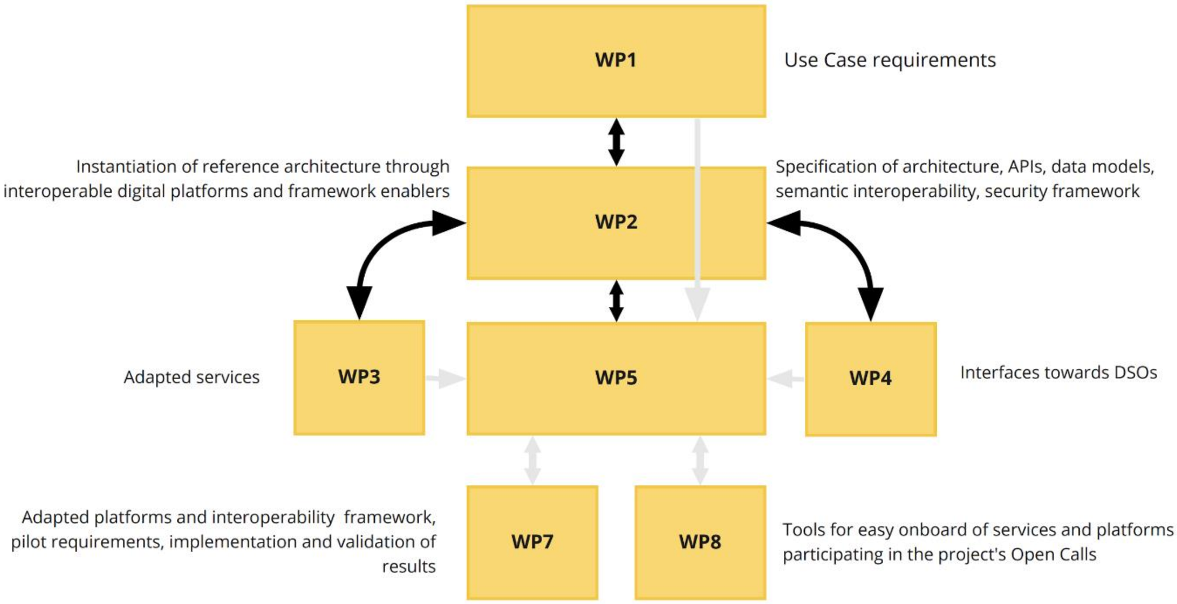

FIGURE 1 – RELATION BETWEEN WP2 AND OTHER WPS

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 InterConnect's Interoperability Framework[1] necessary for making their platforms and services interoperable with the interoperability framework and established pilots.

1.3 D2.1 OBJECTIVES

This deliverable provides the results of the work carried out within tasks T2.1, T2.2, T2.3 and T2.4. The main objectives at the time of delivery can be described as follows:

- Carry out a **detailed analysis of the project's use cases, roles, services, and digital platforms** as well as **their interoperability capabilities and requirements**;
- Introduce the project's Reference Architecture (**SHBERA**) and its **associated viewpoints**. Each (sub-) pilot's architectural implementation is mapped to the SHBERA in Annex VI.
- Contribute to the specification of **InterConnect's Interoperability Framework (IF)** and other interoperable resources and services.
- Contribute to the specification of the **Semantic Interoperability Layer (SIL)**, by identifying the set of connectors and adapters needed to integrate the benefits of ontologies and semantic technology into the InterConnect reference architecture.

To achieve these objectives, the present document introduces:

- An **overview and analysis of existing and relevant IoT, Smart Home, Smart Building, Smart Energy and industrial reference architectures**;
- A list of **requirements** for the Secure interoperable IoT smart Home/Building and smart Energy system Reference Architecture (**SHBERA**) and the methodology for deriving it;
- **A description of the SHBERA and its multiple points of view on the InterConnect ecosystem**, stemming from different domains like Energy and IoT. This includes a high-level description of considerations pertaining to security and privacy[2].
- **A high-level description of the Interoperability Framework in combination with the Semantic Interoperability Layer from an architectural point of view**, further developing the work already covered in WP5, which identified the set of connectors and

[1] **InterConnect's Interoperability Framework** can be defined as a set of tools and software components that will allow stakeholders to interconnect their semantically interoperable solutions into interoperable ecosystems. For more information, see D5.1 [14].

[2] More information on these two important aspects can be found in the InterConnect Deliverable D2.2 [15] which describes a Security and Privacy plan prOCeSs (SPOCS).

adapters required to convert frequently used data formats in InterConnect into Semantic Web standards, and map concepts like devices, services and platforms onto concepts already present in SAREF[3].

The content covered by this deliverable will be discussed and iterated until M36 (September 2022), the 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 have been able to build upon to work on the interoperability of the project's pilots.

1.4 DOCUMENT STRUCTURE

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

Section 2 summarizes our findings after reviewing and categorising existing **State of the Art** (SotA) reference architectures and models 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.

Section 3 describes **why and how a Reference Architecture** for a technology-independent and device-agnostic InterConnect ecosystem **had to be derived using the set of requirements** defined by project experts **and the results of the SotA analysis**.

In **Section 4, InterConnect's Secure Interoperable IoT Smart Home/Building and Smart Energy System Reference Architecture** (SHBERA) is described with its four different point of view on the InterConnect ecosystem, which together enable stakeholders to have a shared understanding of how to achieve interoperability across domains, roles, services, and devices.

Section 5 should be used as a guide for project participants (in other WPs and in the upcoming open call) that are active in constructing the ecosystem according to the SHBERA. This section provides a discussion of architectural support for business models and further describes relevant aspects of designing, constructing, and testing interfaces.

[3] Note that deliverable D2.3 (to be published at the end of December 2021) will cover in more detail the Interoperable and secure standards and ontologies of InterConnect.

In **Section 6** a short discussion is provided on the current status of the Secure interoperable IoT smart Home/Building and smart Energy system Reference Architecture (SHBERA) and its multiple viewpoints.

Finally, the document includes **five Annexes** with detailed information on the reviewed reference architectures introduced in the SotA, the project's ecosystem, the development of architectural viewpoints, ontology usage and reasoning support, and the semantic solution selection.

1.5 GLOSSARY AND TERMINOLOGY

The glossary table, presented below, will be maintained throughout the project. Please note that 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 based on 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 can offer 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 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 based on 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 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

This chapter provides a comparative overview of nine of the main reference architectures introduced by key European Standardisation Organisations and other alliances in the domains of IoT, Smart Homes, Smart Buildings, Smart Energy, and industry.

Table 1 provides a comparison regarding the surveyed reference architectures, categorising the latter 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 such as addressing SAREF[4] 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 analysis carried out in Table 1 was conducted by project stakeholders to position the InterConnect project effectively and quantitatively[5] in the IoT, smart home, building and energy ecosystem, further exploring the commonalities and divergences on the focus, goals and attained (or expected) results.

[4] The Smart Applications REFerence (SAREF) suite of ontologies created and maintained by ETSI. The SAREF ontology and its extensions (standard and custom, project defined) are used within the InterConnect project as the shared vocabulary for digital platforms, services and devices from both domains covered by the project.

[5] 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 1 into a heat map for visual guidance.

	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
HBAM	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 1 – COMPARISON OF KEY ARCHITECTURAL FEATURES

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

Below, a brief description of our key findings:

- 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 to support semantic interoperability, IEC and SGAM focus 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. **InterConnect aims at full interoperability, implying that these three interoperability levels**, but mainly the latter two, will have a deep commitment and impact on the results.
- **Architectures that scored high regarding semantic interoperability also scored high in the ontology 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[6]. **InterConnect establishes a close dependency on ontological developments, particularly to SAREF**. Semantic reasoning and what it can convey to interoperability is one of the key exploitable results that InterConnect is expected to deliver.

- Finally, regarding the ICT processing focus dimension, **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 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 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**.

This analysis is based on an in-depth analysis of the reference architectures mentioned above and partners' expertise and active participation in these initiatives. The groundwork carried out to achieve this result is briefly presented in the following subsections. Additional information can also be found in Annex I.

2.1 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.
- **AIOTI's HLA model offers a global, comprehensive, technological agnostic and highly evolutive model that can be deployed on large scale pilots.** Its three-layered model interprets the relations between users, virtual entities, and things. Each of the

[6] This might sound counter-intuitive, but in 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.

layers contains a set of functions and services that interact via the secure interfaces defined by the project.

- **AIOTI's HLA model 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 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 the foreground and considers and embeds complementary energy reference architectures into its core, exploring the SAREF ontology family.
- **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.

2.2 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'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. It also provides an open basic ontology model, describing the core classes, relations and properties found within compatible and non-compatible oneM2M systems and technologies.
- oneM2M focuses **on providing technical and syntactic interoperability**, allowing devices to establish data flows among them[7].
- ETSI's oneM2M standard offers a **robust reference architecture upon which the project can build and extend to develop a reference architecture for the building, home, and energy domain**s. However, since **oneM2M's core concepts do not provide a fine-grained model for interoperating energy flexibility management with home and building architectures**, additional work was needed 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

[7] A common data model introduces a first ontology mapping and step towards semantic interoperability.

capabilities as a 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).

2.3 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. Central to its design, smart data usage which enables specific APIs for data exchange while ensuring compliance with legacy applications via a set of harmonised data models.
- FIWARE's Reference Architecture is 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.
- **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 a groundwork to explore the **logic surrounding a generic adapter** that can attach to an already existing service and provide new interfaces with the ecosystem.

2.4 WORLD WIDE WEB CONSORTIUM (W3C)

- 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 [1]) 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.
- 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 allows for semantic annotation of

its structure and described contents and can be exchanged using multiple formats commonly used in the web.

- 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 if 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.

2.5 INTERNATIONAL DATA SPACES ASSOCIATION (IDSA)

- 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" [2], 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.
- 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 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.

- The **zero scoring** ('not relevant') with respect to the Interoperability dimension is because IDS is not about interoperability and semantics of devices and services in Smart Homes and Buildings, connected to a Smart Grid. It **is about interoperability in sharing data**. This does not mean that IDS cannot be used for interoperability regarding the sharing of datasets in a future version of the InterConnect Ecosystem between partners. It is not relevant at the current introduction of the architecture for the InterConnect Ecosystem.

2.6 DEUTSCHE KOMMISSION ELEKTROTECHNIK ELEKTRONIK INFORMATIONSTECHNIK IM DIN UND VDE (DKE)

- The Home and Building Architecture Model (HBAM) was developed by the German Commission for Electrical, Electronic & Information Technologies of DIN and VDE (DKE)[8], 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.
- The Home and Building Architecture Model (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.
- 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.

2.7 CENELEC

- CENELEC's Reference Architecture aims to achieve interoperability across devices or a 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.
- 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

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

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.

2.8 CEN-CENELEC-ETSI SMART GRID COORDINATION GROUP

- The Smart Grid Architectural Model (SGAM) defines a set of common concepts, across five distinct layers (i.e., business, functional, information, communication, and component). 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).
- **SGAM presents a good starting point for InterConnect, especially in the different layers and the energy domains**. It is also well suited to map (smart grid) use cases. We do not see the need to use the concept of zones in InterConnect directly since we only address the DSO level in the component layer**. The principles of the layering, the universality and scalability of SGAM have, nevertheless, served as the foundation for IC's reference architecture**.
- **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 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.

2.9 INTERNATIONAL ELECTROTECHNICAL COMMISSION (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 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.
- 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, but rather **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.

3. DERIVING INTERCONNECT'S REFERENCE ARCHITECTURE

This section discusses the need for an InterConnect Reference Architecture. It also provides an overview of the architectural requirements that have been derived from the project goals to create the architecture. This is followed by a discussion of the multiple viewpoints in the reference architectures. The chapter ends with describing the iterative approach of using different viewpoints in one Reference Architecture. After reading this chapter, the reader is equipped with everything needed to understand the background of the Reference Architecture presented in the next chapter.

3.1 ON THE NEED FOR A COMMON REFERENCE ARCHITECTURE

There is **no single existing reference architecture which can be used to create a common understanding between experts from different domains** (e.g., Energy, IoT) to create a technology-independent and device-agnostic (eco)system. Although existing reference architectures have their own merits and advantages, no single one scores high enough in all dimensions when ranked by project stakeholders (see Section 2). In other words: **the InterConnect project** should not reinvent existing reference architectures, but it does **need to provide a bridge between different domains so the experts involved can understand each other in terms of the three dimensions interoperability, ontology, and ICT processing.**

A common understanding is a key enabler[9] for successfully interworking between the 50 project partners from different (industrial) domains as well as connecting Smart Homes, Buildings and (electrical) Grids in seven European countries (Portugal, Greece, France, Netherlands, Germany, Belgium, Italy). These solutions should provide people from all over Europe with the **ability to interconnect devices** in their Smart Homes and Smart Buildings

[9] 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.

to a wide range of services from different providers, **using the Smart Grid as a means for efficient exchanging energy**.

The goal of the Reference Architecture is to provide a **way to describe 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.

3.2 PRIMARY AND DERIVED REQUIREMENTS

InterConnect discriminates between primary requirements and derived requirements. The primary requirements (introduced in Table 2) are **high-level requirements that the Reference Architecture should always comply with**. These requirements are the **end-results of discussions between experts from WPs 1, 2, 3 and 5**. The experts have looked at the Use Cases collected and described by WP1 from an architectural perspective. It was established what was required from the architecture to support the Use Cases as presented.

In the sections below each primary requirement is discussed and additional, more specific requirements are derived from the primaries.

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 2 – HIGH-LEVEL REQUIREMENTS FOR INTERCONNECT'S REFERENCE ARCHITECTURE

3.2.1 R1: BE TECHNOLOGY INDEPENDENT AND DEVICE AGNOSTIC

To create a large level playing field for a competitive market of IoT solutions and energy management services, the Reference Architecture MUST assume as little as possible regarding the technology used for implementing the InterConnect ecosystem. It should also assume as little as possible regarding devices' capabilities. By being 'device agnostic' the Reference Architecture should opt for an open system to which new devices can be added. Table 3 defines the set of derived requirements from R1, covering the InterConnect ecosystem and core principles:

Requirement #	Description
R1.1	IC Reference Architecture **SHOULD** be based on existing reference architectures in the Energy and IoT domains in order to make it relatively easy for domain experts to recognize concepts from their domain.
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

TABLE 3 – DERIVED REQUIREMENTS FROM R1

3.2.2 R2: EXPLOIT BENEFITS OF ONTOLOGIES AND SEMANTIC WEB TECHNOLOGY

Although the Reference Architecture must be as technology independent as possible according to R1, it **MUST** also allow for and even stimulate the integration of semantic technology. This will enable InterConnect to tap into the benefits of so called 'ontologies' for arriving at and using a shared understanding of the interrelated (complex) concepts within InterConnect.

3.2.3 R3: INCLUDE (NON-)ENERGY SERVICES & BUSINESS MODELS

The Reference Architecture MUST allow for the creation and offering of both energy (e.g., 'flexibility services') as well as non-energy services (e.g., 'remote lock operation'). It should do so in such a way there will be a mainstream uptake. That means that the Reference Architecture should be in line with major (established) architectures in the domain of energy (management) as well as the domain Internet of Things that has a broader range of related services than the energy domain. Table 4 provides a list of requirements derived from R3.

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 re-standardization 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

TABLE 4 – DERIVED REQUIREMENTS FROM R3

3.2.4 R4: USE INDUSTRY STANDARDS FOR SECURITY AND PRIVACY

As the InterConnect ecosystem of devices and services touches the (operation of) homes and people live and work in, there is a strong demand for security and the protection of privacy. 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. InterConnect has developed a specific process that makes use of the latest and most stable industry standards and insights for cybersecurity and data privacy protection industrial standards: the **Security and Privacy plan prOCeSs (SPOCS)**. The SPOCS framework and all related concepts can be found in InterConnect deliverable D2.2 [15].

The following sub-sections introduce the most relevant aspects related to this architectural requirement, so the reader is provided with a basic understanding from an architectural point of view.

3.2.4.1 SHARING OF INFORMATION AND/OR CONTROL

The correct provisioning of services using devices in Smart Homes and Smart Buildings, connected through the Smart Grid, requires sharing information and/or control. Sharing information differs from sharing control in several ways. It is important to be aware of this when implementing security and privacy protection measures:

- ***Information sharing***: in [3], 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). The InterConnect Interoperability Framework should provide users with the ability to set privacy levels while allowing them to accept (or decline) different provided services. This should also be enabled for services providers and platform operation who are managing consumer's data.
- ***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[10]. More can be found in [3], where the authors suggest a framework to examine sharing of control on Smart Grids in a structured way.

3.2.4.2 POTENTIAL CONFLICTS FROM DIFFERENT PERSPECTIVES

Within the InterConnect ecosystem, there are different parties, roles and/or different stakeholders (consumers, manufactures, service providers, DSOs, etc.). Depending on the role there might be a conflict of interest between these parties. For example, a flexibility service provider might want to have full access to all information regarding (planned) energy usage of a Smart Home, while the inhabitants might want otherwise (they only want to share aggregates). To be and remain aware of potential conflicts, InterConnect has created an overview of several stakeholder categories and their general perspective on security and privacy requirements. This overview is provided in Table 5.

Stakeholder	Perspective on security and privacy requirements
Service providers	Different kinds of service providers will have different requirements within different security groups. For example, a weather forecast service will not be interested in

[10] 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.

	investing heavily in secure communications. On the other hand, a DSO will need to invest heavily in secure (and reliable) communications because of the potential pervasive impact of the injection of wrong information (or a failure). Within the project, different service providers will have different/conflicting requirements. The ability to group service providers in different security demands to (depending on their specific perspective) will enable InterConnect to be attractive to all stakeholders. This should also help in identifying mutual security and privacy expectations between service providers that depend on each other[11].
DSOs & TSOs	DSOs and TSOs are expected to provide a reliable energy network ('Smart Grid'). Therefore, they require high-integrity measurement values. However, for the DSO and the TSO, conflicting requirements may arise. For some grid-related services, 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 people in Smart Homes and Buildings. 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.
Consumer / User	For most consumers, ease of usage is considered essential. For example, a consumer 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.

TABLE 5 – STAKEHOLDERS SECURITY AND PRIVACY REQUIREMENTS

1.1.1.1 SECURITY GROUPS

Not all devices and services will probably require the same amount of security to allow interaction (exchange of information or control signals). It depends on the impact of a security

[11] An example would be households that calculate 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.

breach. In the domain of the Energy there already is a standard that allows to classify in terms of security levels: ***ISO 62443 - Security levels (SGIS-SL)***. It is defined by the Smart Grid Information Security (SGIS) model[12], the security levels are specially described for the energy sector. Each security level describes an impact and varies from 1 (low) to 5 (highly critical)[13]. The InterConnect ecosystem can benefit from having support for different security levels at different parts and domains of the framework. This will reduce the amount of work to be carried out for integrating devices and services which require less security for interaction. The concept of having different levels of security of specific sets of ecosystem components is also known as having "security groups"[14]. Examples of such groups for InterConnect are:

- A Security Group for **devices** like **home appliances**, focusing on preserving the security of inhabitants of Smart Homes and/or Buildings;
- A Security Group for **devices** like home **sensors**, focusing on preserving the privacy of inhabitants of Smart Homes and/or Buildings;
- A Security Group for **energy system** related services, focussing on the integrity of the energy system.
- A Security Group for (on-line) **services** that carry out long term **accounting/logging** of end-user related activities, focusing on the privacy of end-users.

1.1.1.2 EXAMPLE APPLICATION OF SECURITY AND PRIVACY PRINCIPLES

This section contains an example illustrating the application of security and privacy principles within the InterConnect ecosystem.

Situation: a manufacturer produces a particular model of a washing machine that can be part of the InterConnect ecosystem. This means an app on a smartphone from another ('3rd') party can be used to offer flexibility in consumption of electricity to the grid, in return for financial remuneration. A consumer buys this model and installs the 3rd party app on a smartphone to save money. The app can remotely start a washing machine program at an optimal point in time, based on consumer, grid and/or energy market demands. The consumer in this example

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

[13] 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.

[14] A security group is a set of security requirements, meant for a specified domain, with a specified security level.

is sharing part of the control of the washing machine, as it is the application that also decides the exact point in time when the washing machine program is started. In order not to completely invade the life of the consumer, there should be a level of participation in the decision-making process. The consumer should be able to set some boundaries (in time). In terms of security level this device is in this kilowatt range, connects to the water supply and could destroy valuable clothing (if washed repeatedly).

Given this situation, the following security and privacy aspects are important from the perspectives of the washing machine (device) manufacturer and the electrical flexibility service provider:

- **Identification:** how do washing machine and app identify each other? What kind of naming scheme they use for example?
- **Authentication**: who/what determines (how often) if the identities are those who they say they are?
- **Authorization:** who/what determines (how often) what an authenticated identity is allowed to do?
- **Accounting:** who/what stores exchange information and/or control signals? If there is a dispute afterwards regarding the activation of a washing program, what set of (logging) information is used to settle the dispute? This aspect is important for being able to 'bill for a service', where non-repudiation is important.
- **Transparency of communication:** to what extent can others see the communication between the washing machine and the app? What level of encryption is needed?
- **Trustworthiness of data:** what integrity measures on measurement data will be taken regarding exchanged information.

The aspects above also illustrate the benefits of having predefined types of security groups where there are general agreements on identification, the level of authentication, authorization, etc. A device manufacturer, a service provider and/or consumer can state which type of security group membership they want.

3.2.5 R5: ENABLE (FUTURE) DATA EXCHANGES BETWEEN COMPONENTS

Although it sounds obvious, an important requirement is that the Reference Architecture makes it relatively easy to allow data exchange between components. For example, there should be no congestion in the flow of information between components due to a 'central dispatcher'. The design should be decentralized, and no central parties should be in control of ending information. Also, it should be possible to exchange new types of data/information in the future without a redesign of the Reference Architecture. Table 6 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 6 – STAKEHOLDERS AND ENERGY PROVIDER INTEROPERABILITY REQUIREMENTS

3.3 MULTIPLE VIEWPOINTS

The InterConnect ecosystem is so complex and extensive, no single expert can fully comprehend all aspects of the system. This makes it difficult for experts to arrive at the necessary agreements for reaching interoperability. Different experts prefer to use different types of system modelling, depending on their field of expertise. Different technologies, different domains of application come with their own modelling style and people have been educated differently.

Trying to arrive at a Reference Architecture that forces experts to use the **same way of modelling** and **visual representation** of how they see the ecosystem turned **out to be time and energy demanding**. Instead of arriving at a concise, relatively easy to explain view, experts from different domains tend to add what is important to them, resulting in 'comprise' architectures that are not practical for use. This problem is not new, as society has been using ICT to build large scale distributed systems for many years now.

Therefore, the InterConnect project decided to follow the approach used for creating the **Reference Model for Open Distributed Processing** (RM-ODP[15]) and the **4+1 architectural view model**[16]. Instead of trying to create an architecture for the entire system that contains "*everything all different domain experts want"*, the project has developed **viewpoints**. In each viewpoint the architecture of the system is shown, but certain parts and/or components are abstracted from. This results in views on the architecture that are understood by the relevant domain experts and can still be comprehended by the individual expert.

Although InterConnect also uses viewpoints, the Reference Architecture should **not** be seen as a **replacement** of RM-ODP or the 4+1 model. The viewpoints in the InterConnect Reference Architecture are there **to enable different domain experts to collaborate on the same ecosystem from the perspective of their field of expertise**. These viewpoints are specific for dealing with the InterConnect ecosystem. The InterConnect Reference Architecture can also be seen as a **Rosetta Stone**[17]: the same ecosystem is described using different "languages". The difference between the Reference Architecture and the Rosetta Stone is that certain viewpoints/languages do not have 'words' for certain concepts and leave them out (abstraction).

Four different points of view have been identified during the project for four different domains of expertise and/or application of certain technology. It turns out that experts from these domains tend to focus on certain concepts/aspects while abstracting from other concepts. These are the:

- **Internet of Things (IoT) domain.** Focus is on separation of concerns in using and offering IoT services by layering in terms of communication, application, etc.
- **Energy domain**. Focus is on describing on how components (technological, business parties, etc.) interwork to manage balance and avoid congestion on the grid.
- **Technical integration for interoperability.** Focus is on describing on how different technological components interwork to achieve interoperability.
- **Semantic engineering.** Focus is on using semantic (web) technology for a common understanding and usage of InterConnect concepts.

[15] https://en.wikipedia.org/wiki/RM-ODP

[16] https://en.wikipedia.org/wiki/4%2B1_architectural_view_model

[17] https://en.wikipedia.org/wiki/Rosetta_Stone

These four different viewpoints on the same large and complex InterConnect ecosystem enable (business) architects, (software) engineers and/or (platform/system) designers to collaborate and still focus on specific directly related topics. It also uses the concept of modularity to keep information that is not needed outside a functional component inside and prescribes well-defined interfaces for the information that is required outside a component.

3.4 ITERATIVE APPROACH

The work in WP2 has been carried out iteratively where input and/or feedback from other WP perspectives (e.g., WP1, WP4, WP5) was integrated throughout time. This also enabled the project to include new information, methodologies and/or requirements. This iterative approach allowed for **collaborative and synergetic effort**, through cross-WP discussions, helping to synchronize and validate resulting viewpoints.

The successor to this deliverable is D2.4, due in M36. It will provide more details as more experience with implementing pilot architectures will have become available.

4. SECURE INTEROPERABLE IOT SMART HOME/BUILDING AND SMART ENERGY SYSTEM REFERENCE ARCHITECTURE

This chapter describes the resulting Reference Architecture, based on the requirements and methodology introduced in Section 3. InterConnect's Reference Architecture it's called **Secure interoperable IoT smart Home/Building and smart Energy system Reference Architecture (SHBERA).** After reading this chapter, the reader is equipped to understand the guidelines for the other WPs as provided in the next chapter.

4.1 VIEWPOINTS OVERVIEW

As discussed in Section 3.3, **InterConnect has created separate viewpoints for the domains of Energy, Internet of Things (IoT), technical integration for interoperability and semantic engineering**. Before describing these viewpoints in more detail, this section discusses the relations between the viewpoints. This description is also a discussion of the SHBERA, as it describes the relations between the parts (viewpoints) of a larger collection.

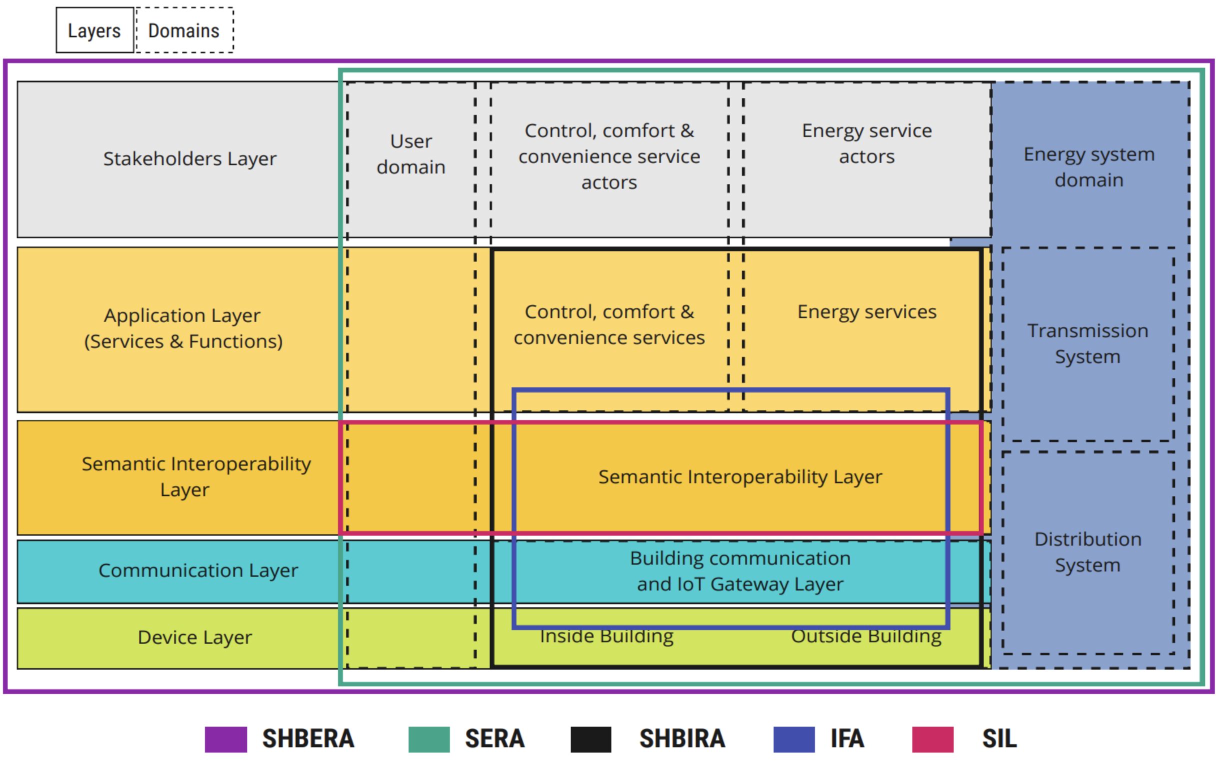

FIGURE 2 – THE SHBERA AND ITS DIFFERENT ARCHITECTURAL VIEWPOINTS

Figure 2 shows the logical relations between different viewpoints, by depicting the **viewpoints** as **sets of concepts**, also known as a 'Venn' diagram. Where sets **overlap**, they **share** the **relevancy** of concepts. There are five sets: the complete set called SHBERA and four subsets' SERA, SHBIRA, IF and SIL which will be shortly introduced below, after first explaining the underlying '**concept coordinate system**' for ordering concepts in a visual 2D space, providing a way to illustrate how the viewpoints relate to each other.

4.1.1 ORDERING INTERCONNECT'S CONCEPTS

Figure 2 contains **(horizontal) layers** for ordering concepts in InterConnect using the following categories: **devices**, **communication**, **semantic interoperability**, **applications** (for services that provide functionality) and **stakeholders** in the InterConnect (service) ecosystem. The use of these five layers, can be considered as a way of merging the Reference Architectural Model Industrie (RAMI) 4.0[18] and the Smart Grid Architecture Model (SGAM)[19]. The higher a layer in the InterConnect model, the less a concept relates to a physical device and the more it relates to services and the use/provisioning of a service (by consumers/organizations):

- **Device layer:** includes 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.
- **Communication layer**: includes 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. As within the SGAM model, emphasis is given to the description of 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.
- **Semantic Interoperability layer**: allows for 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 4.5.2) spanning across all four reference architecture layers.

[18] For more information on the RAMI 4.0, see https://www.plattform-i40.de/PI40/Navigation/EN/Home/home.html
[19] See Section 2.8.

- **Application layer**: 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's interoperability framework services also reside on this layer.
- **Stakeholder layer**: includes all project's stakeholders, end-users, and energy system actors/roles providing or benefiting from the Control, Comfort & Convenience (CCC) and Energy Services.

Then there are domains (depicted using dashed lines) for ordering concepts. The domains have been identified after processing the use cases in WP1. The following domains are present:

- The **User domain**, which expands over multiple layers to depict the set of roles found in use cases from WP1. This shows the diversity of roles, but also how they 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. Also sometimes called the 'non-energy services domain'.
- The **Energy services domain**, which covers key actors providing energy services and the services themselves.
- The **Semantic Interoperability Layer domain** comprises configured instances of interoperability adapters and smart connectors (see section 4.5.2) 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. It is the 'odd one out' in terms of the previous layering of concepts and denotes the 'smart energy domain' in terms of a distribution and transmission system that are present in (smart) electrical grids, including the organisations, markets, etc. needed to keep the energy system up and running. This domain is used to show the relationship of sets/viewpoints with the (classical) energy system.

4.1.2 MAPPING AND ORGANISATION OF VIEWPOINTS

With the use of a 'concept coordinate system' in terms of layers and domains it is possible to map the viewpoints from the SHBERA and organize the following viewpoints amongst themselves:

- **SERA (Smart Energy Reference Architecture)**. It is the InterConnect viewpoint from the Energy domain that focuses on devices, services, actors, business roles, and the Smart (electrical) Grid. It also emphasizes information exchange in the energy system from an InterConnect point of view. The SERA is **not** meant as a **replacement of SGAM**, but as a simplified version to **enable experts from IoT domains to bridge the gap with experts from the energy domain**. It reduces the amount of time and energy needed to understand the energy domain from an IoT perspective. The SERA is the largest subset as it refers to a large part of the concepts in the SHBERA, however it does not always contain the same level of detail as the sets that it overlaps with. The overlap is primarily in scoping with respect to the background of layers and columns.

- **SHBIRA (Smart Home/Building IoT Reference Architecture).** The SHBIRA takes the IoT domain perspective and **focuses on the interoperability and communication of services with each other and with devices, cloud, and local management systems** at different layers (of abstraction). Because the SHBIRA is a more IoT related viewpoint, it is a smaller subset than the SERA. This viewpoint provides more details on the IoT aspects, which are less relevant from an Energy domain perspective.

- **IF (Interoperability Framework).** It is a viewpoint from the domain of technical integration for interoperability**.** It looks at the **InterConnect ecosystem as containing a platform with services**, such as the service store for all interoperable services, P2P marketplace enablers, access control mechanisms, generic interoperability adapters, enabling communication, and others. It was introduced in deliverable D5.1 [14].

- **SIL (Semantic Interoperability Layer)**. A viewpoint from the domain of semantic engineering and has even more **focus on the language used in interoperability than the IF**, causing it to be the visually smallest subset of *architectural* concepts in this visualization of the SHBERA. Please note that it has the same name as the layer in the 'concept coordinate system' in the SHBERA, as it primarily provides a view from that layer. However, from the SIL point of view, all detailed information regarding all InterConnect's concepts relevant to users and providers (actors) of services can be seen. Zooming in once more brings us to the **Semantic Interoperability Layer (SIL)**, depicted in Figure 8. This is a logical concept within the IC Framework that enables semantic interoperability comprising ontologies, interoperability adapters and smart connectors with supporting orchestration enablers.

The following sections describe in more detail the architectural viewpoints. For each point of view there is a list of specific requirements, a description and then a discussion of several security and privacy considerations.

4.2 THE SMART ENERGY REFERENCE ARCHITECTURE

The **SERA** is an Energy System point of view on the InterConnect ecosystem and is its purpose is to serve as tool to help understanding the **interconnection** of **devices** in **Smart Homes**, and **Buildings** with (Internet-based) **services** and the (electrical) **Smart Grid** by the **exchange of information**. Key concept is the information object: a description of a particular set of information that is exchange through an interface between different actors, roles, and business parties from different (sub-)domains. The information objects can be used for establishing what concepts need to be present in the semantic interoperability layer as well. Figure 3 provides a visual description of the SERA[20].

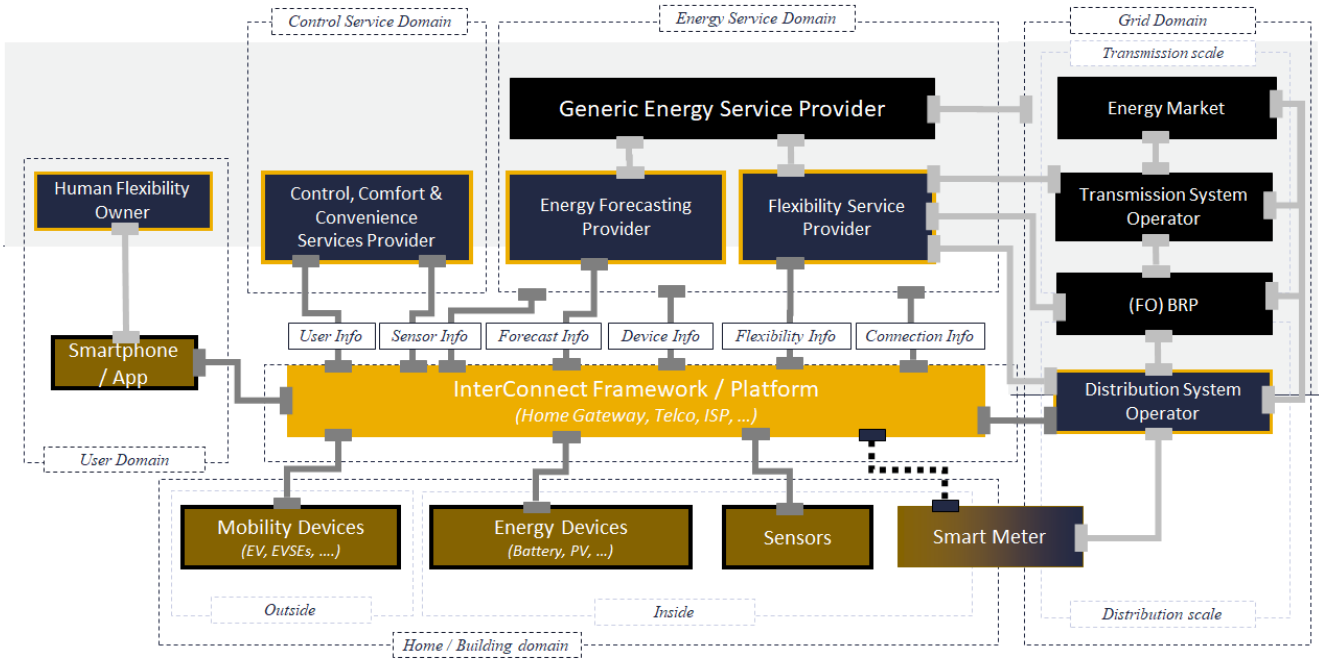

FIGURE 3 – SMART ENERGY REFERENCE ARCHITECTURE (SERA)

4.2.1 VIEWPOINT SPECIFIC REQUIREMENTS

To make this viewpoint also comprehensible for experts coming from other domains than the Energy System, InterConnect decided to let this viewpoint include fewer details than many of the existing reference architectures in the energy domain that have become commonplace in different subdomains of energy system expertise (e.g., smart grids, e-mobility, and energy flexibility markets with aggregators). However, to support a relatively easy comparison with other architectures, the SERA does show a close resemblance with *parts*[21] of existing

[20] The colour schema used helps denotate devices (brown fill colour) and roles (dark blue fill colour). The Smart Meter is depicted as both a Device and a Role since it is managed by an organisation that provides Smart Meter data. This can be a Distribution System Operator, but that does not always have to be the case. The InterConnect Framework has, by default, an orange fill colour.

[21] 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.

reference architectures in the smart grid domain. An example is the use of abstraction layers (like present in the SGAM). The simplification (in relation to other reference architectures) makes it easier for InterConnect to define new roles that emerge through interconnection.

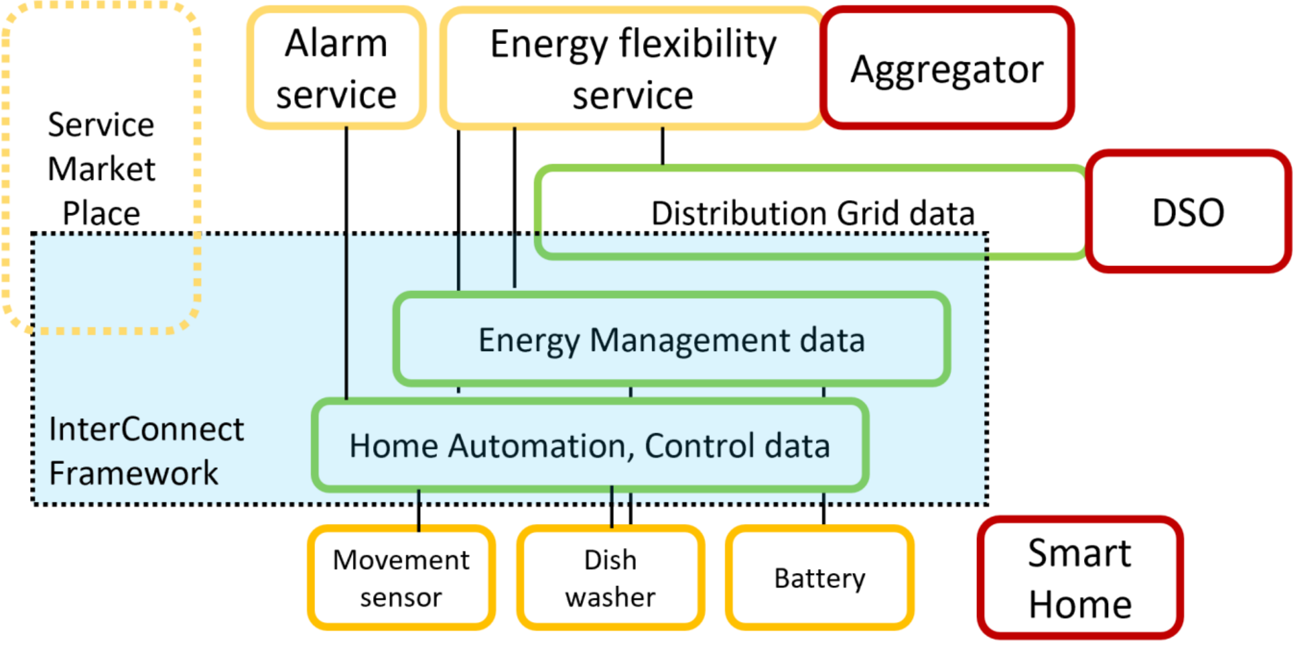

FIGURE 4 – SIMPLIFIED VIEW OF ABSTRACTION LAYERING AND SEPARATION OF CONCERNS

To be sure that the SERA would support the InterConnect pilots, it has also been derived from the use cases provided by the partners. The use cases contained a plethora of business actors, roles, and physical devices/components and have been ordered to different layers of abstraction and/or grouped based on separation of concerns. Figure 4 (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 the 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 [4]. Here, the InterConnect project determined that although lots of actors (TSO, BRP, and others) and markets (Balancing Market) were clearly defined, there are some differences in legislation across countries (and especially around energy flexibility) that introduce different views and possibilities on (local) flexibility markets, actors (technical, commercial aggregators).

4.2.2 SERA DESCRIPTION

The SERA introduces multiple domains that provide structure and overview. Components within one domain tend to share more things with each other (e.g., physical location, interests, a reference framework, etc.) than with components in other domains. Different domains can influence each other through relationships that span across domains[22]. Table 7 lists the architectural components per domain. Each domain and its components will be discussed in the subsections below, accompanied by a description of information objects that are relevant to this domain. Note that information objects can be exchanged between domains, but for reasons of readability are listed at a particular 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
Control Services Domain	• Control, Comfort & Convenience Services Provider
Energy Services Domain	• Generic Energy Service Provider • Flexibility Service Provider • Energy Forecasting Provider
Grid Domain	• Distribution System Operator (DSO) • Transmission System Operator (TSO) • Balance Responsible Party (BRP) • Energy Market
InterConnect Framework / Platform Domain	• InterConnect Framework / Platform

TABLE 7 – SUMMARY OF BASIC ROLES AND SYSTEM ELEMENTS PER DOMAIN

[22] 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 InterConnect Framework/Platform is a special logical concept and is depicted in the centre in its own domain. Components can be connected to the InterConnect Framework directly or indirectly. When directly connected, they will interface logically (and technically) with the InterConnect Framework/Platform[23] concept. As there are a wide range of information flows through this concept, different types of information have been grouped into the following themes to create structure and overview: **User**, **Sensor**, **Forecast**, **Device**, **Flexibility** and (grid) **Connection Info**.

4.2.2.1 USER DOMAIN

The User domain contains the following concepts and architectural components:

- **Human Flexibility Owne**r, a human that owns flexibility in the sense that the human can decide to let a device consume or produce less or more power at a certain point in time.
- **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).

The following Information Objects are part of the User domain:

- **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.

Table 8 contains examples of the generic domain concepts and specific instantiations from use cases as found in the InterConnect set of pilots, together with related information objects.

Generic Architectural Components and Specific Concepts	
Human Owner of Flexibility	**Use Case Information Producers and Receivers** ● End User ● Local community

[23] In Figure 3, components that have a direct connection with the InterConnect Framework have a differently coloured outline. Also, direct connections have a dark grey colour and indirect connections a lighter grey.

	• 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 8 – USER DOMAIN BASIC ROLES AND COMPONENTS

4.2.2.2 SMART HOME/BUILDING DOMAIN

The Smart Home / Building domain contains the following concepts and architectural components:

- **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.
- **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.

The following **Device and Sensor** related Information Objects are part of the Smart Home / Building Domain:

- **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.

Table 9 contains examples of the generic domain concepts and specific instantiations from use cases as found in the InterConnect set of pilots, together with related information objects.

Generic Architectural Components and Specific Concepts	
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 9 – SMART HOME/BUILDING DOMAIN BASIC ROLES AND COMPONENTS

4.2.2.3 ENERGY SERVICES DOMAIN

The Energy Services Domain contains the following concepts and architectural components[24]:

- **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.

Note that 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

[24] These definitions have been defined following USEF model definitions. For more information, see https://www.usef.energy/app/uploads/2016/12/USEF_TheFrameworkExplained-18nov15.pdf

Aggregator (CA). The following **Flexibility and Forecast** related Information Objects are part of the Energy Services Domain:

- **TA Aggregated flexibility**: An 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 (connected to a Building Energy Management System (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.
- **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).

Table 10 contains examples of the generic domain concepts and specific instantiations from use cases as found in the InterConnect set of pilots, together with related information objects.

<table>
<tr><th colspan="2">Generic Architectural Components and Specific Concepts</th></tr>
<tr><td rowspan="2">Flexibility Service Provider</td><td>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</td></tr>
<tr><td>Use Case Information Objects Exchanged</td></tr>
</table>

	• 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
Energy Forecasting Provider	**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 10 – ENERGY SERVICES DOMAIN BASIC ROLES AND COMPONENTS

4.2.2.4 GRID DOMAIN

The Grid Domain contains the following concepts and architectural components:

- **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 each 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.

The following Information Objects[25] are part of the Smart Grid domain:

- **DSO flex needs/request**: The request for flexibility from a DSO, often to reduce grid load 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.
- **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.

Table 11 contains examples of the generic domain concepts and specific instantiations from use cases as found in the InterConnect set of pilots, together with related information objects.

Generic Architectural Components and Specific Concepts	
Distribution System Operator (DSO)	**Use Case Information Producers and Receivers** • DSO DSO-Grid
	Use Case Information Objects Exchanged • DSO flex needs/request

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

	• 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 11 – SMART GRID DOMAIN BASIC ROLES AND COMPONENTS

IMPORTANT: as the DSO is an important stakeholder in the grid domain (e.g., due to the need to maintain power quality and avoid congestion), InterConnect has a dedicated work package for the studying the exchange of information and control signals between the DSO and other participants in the InterConnect ecosystem. In WP4's "DSO Interface" the InterConnect partners work on the functionality of this Interface and create an architectural approach for implementation of this DSO interfaces.

4.2.2.5 CONTROL SERVICES DOMAIN

The Control Services Domain contains the following concepts and architectural components:

- **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.)

Table 12 contains examples of the generic domain concepts and specific instantiations from use cases as found in the InterConnect set of pilots, together with related information objects.

Generic Architectural Components and Specific Concepts	
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 12 – CONTROL SERVICES DOMAIN BASIC ROLES AND COMPONENTS

4.2.2.6 INTERCONNECT PLATFORM

The InterConnect Platform Domain contains the following concepts and architectural components:

- **InterConnect Platform**: 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.)

Table 13 contains examples of the generic domain concepts and specific instantiations from use cases as found in the InterConnect set of pilots, together with related information objects.

Generic Architectural Components and Specific Concepts	
InterConnect 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 13 – INTERCONNECT PLATFORM DOMAIN BASIC ROLES AND COMPONENTS

4.2.3 SECURITY AND PRIVACY CONSIDERATIONS

The InterConnect platform in the SERA is a logical concept that acts as an intermediary between devices and services. During construction of the InterConnect ecosystem the engineers should be aware of the *man-in-the-middle* 'attack' where a fourth party acts as the InterConnect platform and intercepts data (containing information and/or control signals) between devices and the InterConnect platform or the platform and services (and vice versa). A way to counteract this is using signatures to prove the integrity of data ('no tampering').

Another important aspect to take into consideration is the fact that the InterConnect platform should in general not weaken existing secure relationship between devices and services. If it does, there will be less reasons for device manufacturers and service providers to use the InterConnect ecosystem.

4.3 THE SMART HOME AND BUILDING IOT REFERENCE ARCHITECTURE (SHBIRA)

This section describes the IoT point of view, known as the **Smart Home/Building IoT Reference Architecture (SHBIRA)**. It is the result from an extensive analysis of the state of the art including nine key reference architectures and models, developed by other European initiatives for these domains (e.g., SGAM, AIOTI). It aims to build on and extend existing work 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.

The SHBIRA views the InterConnect ecosystems in terms of layers and interfaces with specific functionalities. It provides a flexible, device and technology-agnostic high-level architectural point of view, while focusing on interoperability based on communication of services with each other and with the devices and considers (physical) concepts with a location like the 'cloud' and (local) management systems in homes and buildings. In comparison: the SERA in section **Erreur ! Source du renvoi introuvable.** abstracts from concepts like the cloud and local management systems. The SHBIRA is depicted in Figure 5.

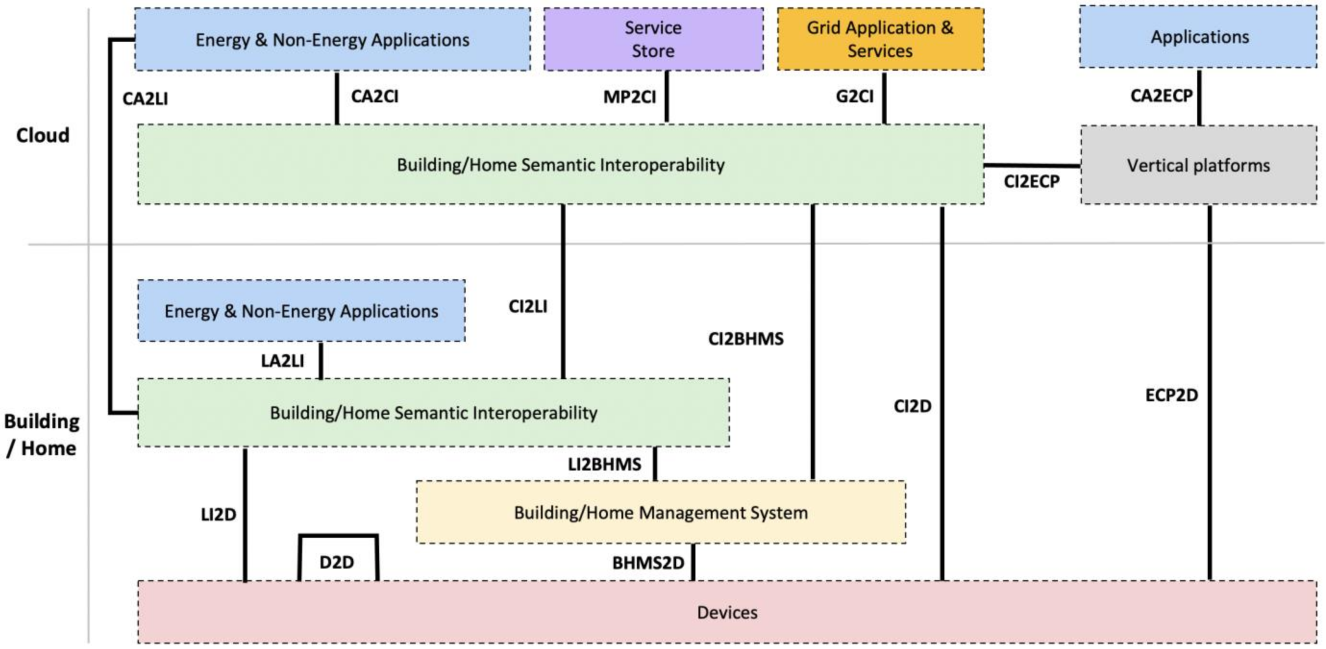

FIGURE 5 – SMART HOME AND BUILDING IOT REFERENCE ARCHITECTURE (SHBIRA)

4.3.1 VIEWPOINT SPECIFIC REQUIREMENTS

Although there are no specific requirements from the SHBIRA point of view, it is important to mention that the SHBIRA provides a viewpoint that enables project partners to see the relationship of the (existing) digital/IoT platforms provided by them for the realization of the pilots and use cases[26] since their platform architectures often have a same ordering of components using the same type of layering. By complying it to the SHBIRA it is possible to add interoperability in a general and unified way instead of specifically per-interface/service. This means different pilots can produce a different 'instantiation' of the SHBIRA, using the service components from WP3 and the interoperability framework as implement in WP5.

[26] Especially in platforms which provide 'vertical market' solutions for individual or multiple smart buildings.

4.3.2 SHBIRA DESCRIPTION

The SHBIRA has a fundamental categorization in two domains:

- 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. Robust security measures are expected to protect sensitive (including personal) data and combat cyber-attacks.
- The **cloud domain**, which groups cloud-based systems such as IoT platforms and applications offering 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 the flexibility and adaptability needs of each user.

Within this decomposition, the SHBIRA provides a layered view on its main architectural components, containing:

- a layer for **Devices**, 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);
- a layer for **Building/Home Management Systems (BHMS),** which supervise, and control appliances and smart devices present in homes and buildings. BHMSs may interact with the cloud, e.g., for getting tariffs pertaining to flexibility management and may also include energy management functions. Being compliant with the SHBIRA does not require this component to be present. However, if it exists, it should provide the required interfaces (e.g., APIs, documentation, and credentials) to connect with the following layer:
- a layer for **Building/Home Semantic Interoperability**, containing all the required functions needed to enable semantic interoperability between devices, applications, and services[27]. This layer is an abstraction and generalization of the functional

[27] InterConnect defines 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 these 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.

components that can be found in the Interoperability Framework Architecture (IF, see section **Erreur ! Source du renvoi introuvable.**) point of view and the Semantic Interoperability Layer (SIL, see section 4.5) point of view. As visualized the software and hardware components for this layer can be present locally (i.e., at a home or building), or in the cloud or even 'in between', like the fog or edge cloud. It depends on the implementation requirements and specifications of a specific device and/or service. For example, the more sensitive data about a building is, the less chance the data is allowed to "leave the premises".

- a layer for **(non-)Energy Application**s, containing the functional components for services that use the functionality in the Building/Home Semantic Interoperability Layer for the exchange of information and/or control signals with devices. Functional components in the Applications layer, such as those for home automation or energy efficiency services, can be instantiated either locally (i.e., at a home or building) or remotely within the cloud domain. It depends on needs of end-users and service provider preferences.

Next to the layers, to be in accordance with requirements to the reference architecture, the SHBIRA point of view contains the following architectural concepts:

- **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**[28], which provides a catalogue of all services in the InterConnect. It will enable all interoperable digital platforms, services, and applications to navigate the collection of available services and find the connection to interoperate with these services (as delivered by WP3).
- **Grid applications** for providing (corresponding) **services**. Examples are applications collecting information for observing past, current, and future load on the grid from the perspective of Homes and Buildings. This kind of information can be beneficial to distribution / transmission systems operators, market agents and consumers. To support an economy of scale, these applications need agnostic data exchange mechanisms that respect access, control, and comply to GDPR and different NRA guidelines.

4.3.3 SECURITY AND PRIVACY CONSIDERATIONS

As described in the security and privacy considerations regarding the SERA (see section 4.2.3) it is important to be aware of a man-in-the-middle attack when separating devices and services by intermediate components in a line of communication. In the case of the SHBIRA

[28] The service marketplace/store was specified within InterConnect Deliverable D5.1 [14] and will be implemented in WP5.

there are multiple layers with potentially multiple components, located in two domains: the Building/Home domain and the Cloud domain.

The presence of potentially shared responsibility for security and privacy across both domains causes a risk of assuming “the other domain” takes care of security and privacy. Therefore, device manufacturers and service providers need to be aware of these three different architectural approaches:

- **Most security and privacy related tasks are executed in the Building/Home domain.** Service specific devices do not connect directly to the cloud domain, but first communicate with a specific gateway at the local premises that limits what information and control signals can be exchanged with the cloud domain. From the perspective of an end-user / consumer at home trust is ‘laid anchor’ at home or in a building. The cloud domain still must take care of providing the following security and privacy related functionality:
    a. **validating applications**. End-users in the home domain use (a service in) the cloud domain to determine if an application (for offering a certain service) is trustworthy. This is comparable with a Certificate Authority (CA) in Transport Layer Security (TLS) in communication across the Internet. End-users trust a CA to determine if the certificate provided by a party on the Internet is valid;
    b. **connecting services** (including those with a smartphone user interface) to devices;
- **All security and privacy related tasks are executed in the cloud domain.** Service specific devices connect directly to the cloud domain; This will also cause components in the home domain to be highly dependent on an internet connection for security and privacy. From the perspective of an end-user / consumer at home trust is ‘laid anchor’ in the cloud domain.
- A **hybrid system, where some security and privacy related tasks are executed in the cloud domain and others in the Building/Home domain.**

4.4 THE INTEROPERABILITY FRAMEWORK (IF)

The Interoperability Framework (IF) point of view shows what is needed for enabling interoperability across all participating digital platforms, services, applications - providing energy and non-energy services (control, comfort, and convenience) - and devices. Contrary to the SERA (see section 4.2) it does not look at domains like energy services and the grid. Contrary to the SHBIRA (see section 4.3) it does not look at a separation of concerns in terms of physical domains and layers of abstraction. The Interoperability Framework viewpoint focusses on interoperability in communication.

IMPORTANT: The IF is so essential to the functioning of the InterConnect Ecosystem and has so many aspects that it has its own InterConnect Deliverable D5.1 [14]. In this deliverable, only the main aspects and the relationship to other viewpoints are described.

4.4.1 VIEWPOINT SPECIFIC REQUIREMENTS

Table 14 further specifies the requirements derived from **R1**, specific to the interoperability framework.

Requirement #	Description
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

TABLE 14 – IF VIEWPOINT SPECIFIC DERIVED REQUIREMENTS FROM REQUIREMENT R1

Table 15 further specifies the requirements derived from **R2**, specific to the interoperability framework.

Requirement #	Description
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

TABLE 15 – IF VIEWPOINT SPECIFIC DERIVED REQUIREMENTS FROM REQUIREMENT R2

Table 16 further specifies the requirements derived from **R3**, specific to the interoperability framework.

Requirement #	Description
R3.4	IC Interoperability Framework **SHOULD** implement a mechanism for interoperability compliance test and certification

TABLE 16 – IF VIEWPOINT SPECIFIC DERIVED REQUIREMENTS FROM REQUIREMENT R3

Table 17 further specifies the requirements derived from **R4**, specific to the project's system security and privacy.

Requirement #	Description
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 17 – IF VIEWPOINT SPECIFIC DERIVED REQUIREMENTS FROM REQUIREMENT R4

4.4.2 IF DESCRIPTION

The overall functional architecture of the is visualized in Figure 7. The main functional components are:

- a **Device**. A physical apparatus comparable to a device in the SERA and SHBIRA viewpoints.
- a **Digital platform**. An (IoT) hardware/software platform to which a device is connected, and which can also provide the foundations for running
- a **Service**, which is a (software) component comparable to the components in the Applications and Grid-Services layers of the SHBIRA. It uses
- an **Adapter**, which is a (software) component that adapts (existing) services on a digital platform to connect to
- the **Semantic Interoperability Layer (SIL)** which interconnects existing digital platforms, and services they offer, among themselves and with so called "interoperability framework services". Example services that support the design, construction and operation of services (through application components as visible in the SHBIRA) are the 'service store', 'P2P marketplaces', 'compliance certification', 'data protection' and 'access control'. The Semantic Interoperability Layer in the IF is an abstraction and generalization of the set of components that are visible in the Semantic Interoperability Layer viewpoint (see section 4.4.3).

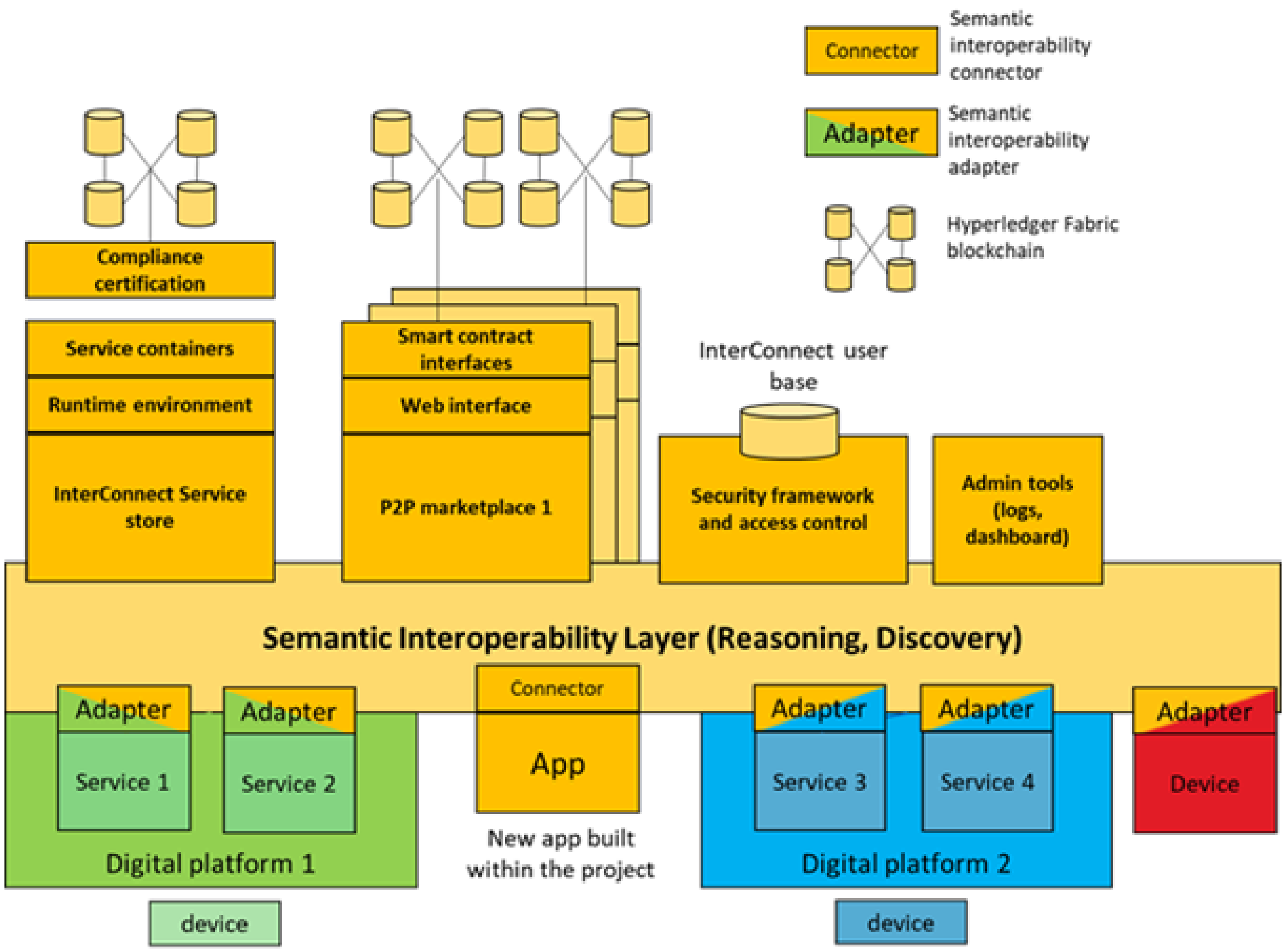

FIGURE 6 – INTEROPERABILITY FRAMEWORK (IF)

IMPORTANT: a digital platform can have many kinds of technical instantiations. For instance, a washing machine can be considered as a device. The washing machine itself is not regarded as a digital platform, but it when it contains a controller, that controller can be considered as a digital platform. Potentially it hosts a service software component[29]. From the perspective from an end-user the main service provided by the washing machine is washing the laundry. From an IF point of view 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) and/or as an energy service.

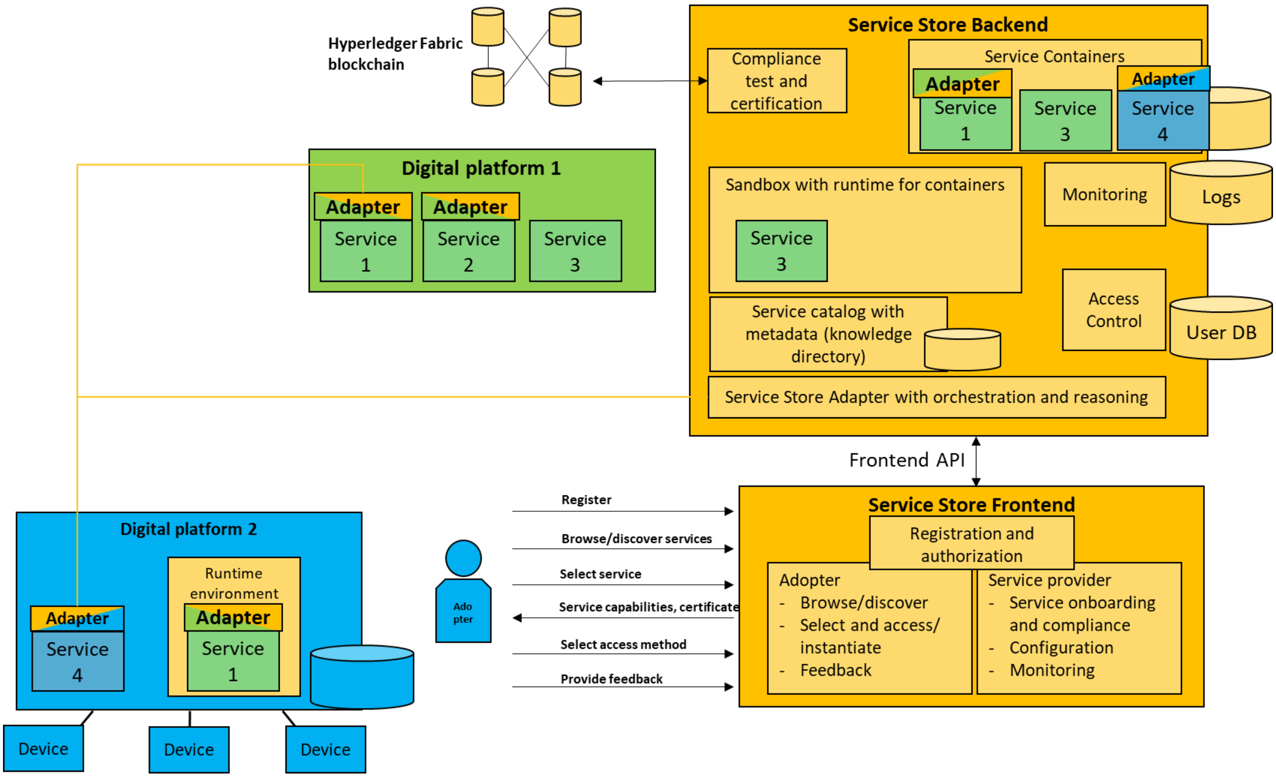

FIGURE 7 – IC SERVICE STORE FUNCTIONAL ARCHITECTURE AND FUNCTIONALITIES

IC's Interoperability Framework also introduces the concept of the **Service Store** (depicted in Figure 7), which is specific to InterConnect. It provides a comprehensive catalogue of all interoperable services from the smart home/building and energy domains. The service store provides a set of generic services (e.g., for data analysis, weather forecast). To be featured in the service catalogue, a service needs to have an interface (e.g., an adapter) which allows for

[29] 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 connection to the SIL. The service store will be specified and implemented in WP5, specifically in T5.1 responsible for specification and T5.2 responsible for implementation.

4.4.3 SECURITY AND PRIVACY CONSIDERATIONS

The Service Store is a place where the identification, authentication, authorization of using a particular service could take place in a uniform manner. That does not mean it is the only place where it could take place. For example, the interfaces of components can always demand extra identification and authentication information to be exchanged increasing the level of security. Also, the authorization to use certain functionality of a component by other components in the architecture can be done inside components as well, if the particular components have a means to identify and authenticate on the other components want to use that functionality (on behalf of a certain identity).

The Service Store is also a place that could provide certain guarantees on the authenticity and/or reputation of a service by 'signing' it. When end-user might not be able to research a certain service, the Service Store could serve as a trust anchor. This is comparable to the concept of 'app stores' on digital device platforms. The Service Store can also check if a service complies to demands from a particular security group. If an end-user trusts the Service Store, the end-user must carry out less research into the way a service is offered or who offers a service.

4.5 SEMANTIC INTEROPERABILITY LAYER (SIL)

The Semantic Interoperability Layer (SIL) point of view brings into focus what is needed to have interoperable exchange of information with explicit encoding of semantics. It abstracts from concepts like (non-)energy services and business roles (as visible in the SERA viewpoint in section 4.2), IoT layering (as visible in the SHBIRA viewpoint in section 4.3) and a service store (as visible in the IF in section 4.4).

4.5.1 VIEWPOINT SPECIFIC REQUIREMENTS

Table 18 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
R2.3	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 18 – SIL VIEWPOINT SPECIFIC DERIVED REQUIREMENTS FROM REQUIREMENT R2

Table 19 further specifies the requirements derived from **R4**, specific to the Semantic Interoperability Layer.

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

TABLE 19 – SIL VIEWPOINT SPECIFIC DERIVED REQUIREMENTS FROM REQUIREMENT R4

4.5.2 SIL DESCRIPTION

The SIL and the relationship to the Smart Applications REFerence (SAREF) will both be covered at length in the upcoming InterConnect Deliverable D2.3 (due in December 2021). This deliverable only contains a description of the key architectural concepts of the SIL. In section 5.2.1, pilot participants can find (high-level) guidelines on making the information models of devices, service and/or digital (IoT) platforms compatible with the SIL.

The architectural components of the SIL can be visualized in Figure 8. It partially resembles Figure 6 in terms of the central position of the layer and the appearance of blocks which connect to that layer. For example, the IF has ‘adapters’, the SIL has ‘Smart Connectors’, which are conceptually closely related. The SIL has 'Knowledge Bases' and the IF has 'Digital Platforms', which are conceptually not closely related because they are at different layers of abstraction and only visible from each viewpoint separately.

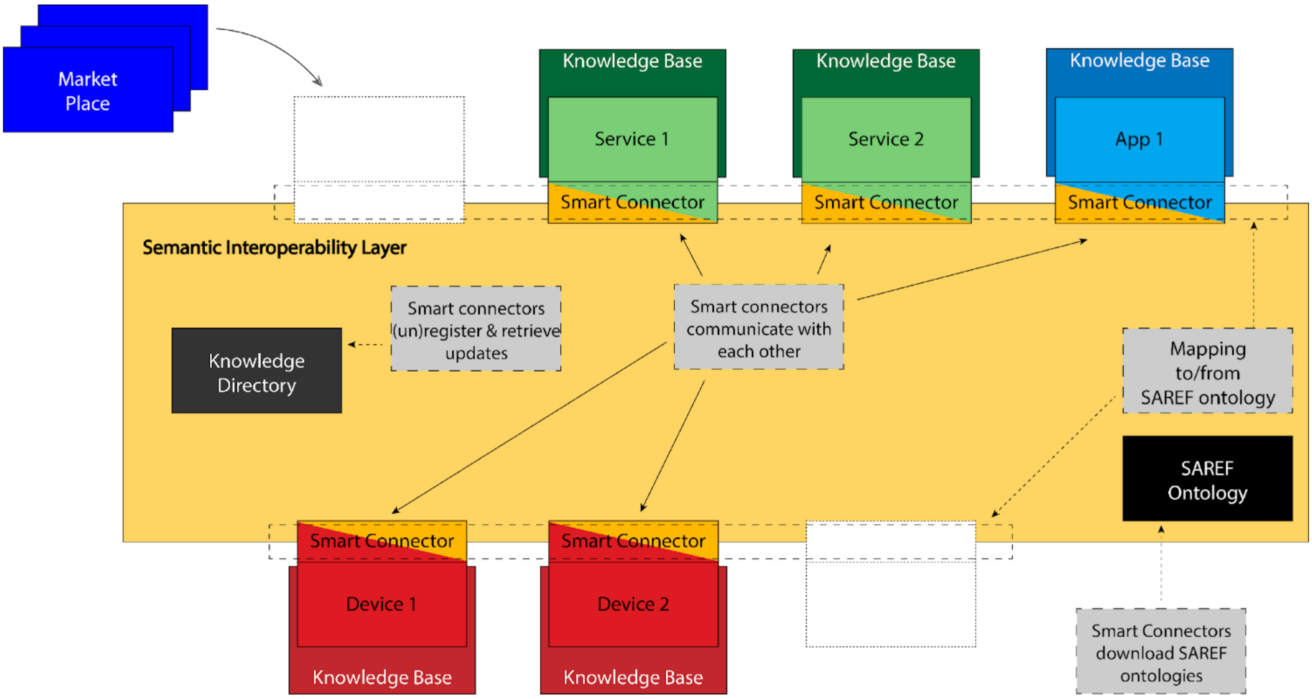

FIGURE 8 – COMPONENTS IN THE SIL

Before describing the components in Figure 8 it is important to realize that the SIL assumes the usage of the Knowledge Engine (KE) technology to exchange and reason about semantically encoded information between architectural components. See Annex IV for more information about the concept of reasoning. The choice for using the KE was based on the generic and specific requirements and on the results of the analysis of existing solutions for the exchange of information with explicit encoding of semantics (see Annex V). With that in mind the following architectural components and concepts are present in the SIL:

- **Knowledge Base (KB)**: an independent producer or consumer (component) of information to the IC semantic interoperability layer[30]. Individually, each knowledge base is a component that provides certain functionality and has a list with descriptions of its capabilities. Multiple knowledge bases can discover and exchange information with each other. Existing devices, services, and platforms of the InterConnect ecosystem, as well as newly built apps, are KBs. It is important to note that a KB does not interact directly with the semantic interoperability layer but uses a Smart Connector.

[30] KBs can also trigger actions, and thus play a role in control systems, such as heating systems or artificial cardiac pacemakers.

- **Smart Connector (SC):** a component that acts on behalf of a KB. A SC allows a KB to register with the IC semantic interoperability layer and exchange knowledge. In an initial registration phase (where a KB is added to the ecosystem), a SC of a certain KB needs to specify what knowledge it produces, publishes, wants to consume, and subscribes to. In the exchange phase, knowledge is consumed, produced, published, or subscribed by the KB as configured during the registration phase.
- **Knowledge Directory (KD):** The KD component contains a list of knowledge bases with associated capability descriptions that are available within a particular instance of the KE running in the semantic interoperability layer. Every KE instance has a single KD[31]. 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 this could be realized as one KD per smart building or per pilot. The KD is aware of all smart connectors and their Knowledge Interactions.
- **Knowledge Interactions (KIs):** the concept of interaction between KBs in terms of knowledge (exchange). Knowledge is exchanged using so-called '*graph patterns*' which are collections of statements in predicate logic. The statements make use of a set of ontologies that define (the relationship) of concepts in terms of predicate logic, and which have been especially created for InterConnect. This set is labelled 'SAREF ontology' in the visualization, but consists of multiple ontologies, where SAREF is one of them, together with ontologies that describe other concepts that do relate to InterConnect (but are not directly part of SAREF). There are four types of KIs:
    a. **Ask:** a KB asks its SC for certain data. Certain parts of the graph pattern can be left 'empty' using special notation, showing the KE what is desired.
    b. **Answer[32]:** a KB answers its SC by providing certain data,
    c. **Post:** a KB posts certain data (a.k.a. the 'argument') to receive certain data (a.k.a. the 'result'). Both argument and result are optional but one of them should be present,
    d. **React:** a KB reacts to receiving certain data (argument) by providing certain data (result). Both argument and result are optional but one of them should be present.
- **Communicative Act (CA):** a concept to express which type of interaction is intended by a component. Every KI describes its CA. This is necessary 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). KEs involved should be aware of the intent of

[31] Note that the latter 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.

[32] 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.

the KB, as it this cannot be inferred from the information itself[33]. The CA is used by the KE and can be encoded using a specific CA ontology. The goal of the designers of the SIL was to create an extensible ontology for describing CAs, that could contain all potential CAs that a KE might be able to handle in the future. Note that the CA ontology is not the same as the SAREF ontology and is meant to describe concepts at a different layer of communication. SAREF is about communicating knowledge regarding an ecosystem containing Energy and IoT concepts. The CA is about intent of communication.

4.5.3 SECURITY AND PRIVACY CONSIDERATIONS

The concept of a local Knowledge Base in the SIL acts as a passive defense against a breach of privacy. Knowledge is not sent to a central database by default but is only shared when needed. Using the capabilities of the built-in reasoner in the Knowledge Engine a Knowledge Base can determine where to discover information. A Knowledge Base receiving a request to be information (through a particular type of Knowledge Interaction) can decide whether to share that information.

In the IF point of view in section 4.4 there is already support for security and privacy (specifically described in 4.4.3), but as mentioned there that does not mean there cannot be extra attention to security and privacy from the viewpoint of a Knowledge Base in the SIL. Service providers can have specific and extra demands regarding identification, authentication, and authorization[34] which go beyond the level which is provided by the Service Store. Security and privacy at the abstraction level of the Service Store in the IF is oriented at who is allowed to use a certain interface for a service. From a knowledge perspective there can also be authorization on which authenticated identity is allowed to access what part of available information. Access control could be encoded into Knowledge Interactions semantically. An example of such an approach is Ontology-Based Access Control (OBAC) [5]. At the time of writing of this deliverable D2.1 work is still going on in WP2 and WP5.

[33] Knowing the intent prevents Knowledge Bases from, for example, posting 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.

[34] In InterConnect Deliverable D2.2 [15], several examples of authorization control are mentioned in other (comparable) projects (especially RBAC and ABAC). These are taken into consideration in the realization of the InterConnect ecosystem.

5. BUILDING THE INTERCONNECT ECOSYSTEM

The previous section provided a description of the Secure interoperable IoT smart Home/Building and smart Energy system Reference Architecture (SHBERA). By iterating over the four different architectural points of view the reader has been equipped with the shared understanding of aspects of the InterConnect ecosystem. This chapter is a guide for project participants (in other WPs and in the upcoming open call) that are active in constructing the ecosystem according to the SHBERA.

This chapter starts with a discussion of architectural support for business models. It then describes relevant aspects of designing, constructing, and testing interfaces. Finally, as the SHBERA will be updated in D2.4, there will be a special section on providing feedback to WP2 based on implementation of pilots.

5.1 BUSINESS MODEL AND SERVICE SUPPORT

This section contains guidance with respect to the support of the SHBERA for business models and services.

5.1.1 REUSE OF EXISTING SERVICES

It seems obvious – in theory – that InterConnect participants would make use of already existing services. In terms of the Interoperability Framework point of view, users of services can connect to adapters from services are through to the Semantic Interoperability Layer. During the analysis in WP2 of Use Cases from partner pilots' similarity in provided services was noticed. They can an opportunity to demonstrate interoperability by reusing these services between pilots.

However, in practice, it seems wiser to carry out 're-use of services' in two steps since this project is about demonstrating interoperability by creating a common understanding of (semantic) concepts involved for the first time. It is only logical that during initial pilot implementations there will be misunderstandings at first. This can seriously hinder the progress of implementation of a pilot if there is a 'spaghetti' bundle of interdependent services that do not entirely agree on definitions. WP2 suggests to first implement each pilot based on the common understanding (as documented in the set of ontologies) and after a first implementation of a pilot has been delivered, a re-use of similar services available elsewhere in the InterConnect will be attempted. From these attempts feedback can be provided to the set of ontologies. An example of similarity in services can be found in the domain of energy flexibility and forecasting.

5.1.2 FLEXIBILITY SERVICES

Although the designers of the SHBERA tried to avoid prescribing a certain business model as much as possible, there is an exception to this rule, and this can be found in the area of flexibility services. The reason for this is InterConnect's goal to democratize energy management. This can only be done in an economy of scale, which can never be realized if different stakeholders all have their own business model of flexibility services. In this section this is briefly discussed to push service providers towards interoperability in flexibility services.

IMPORTANT: *As the concept of flexibility on the electrical grid is discussed at length in the deliverables of WP4 ("DSO Interface") and semantical concepts related to flexibility will be part of deliverable D2.3, this section will only discuss what is relevant to the prescription of business model at the architectural level.*

In the SERA point of view (section 4.2) of the SHBERA multiple business roles and/or architectural components can be identified that are involved in the production, trading, transmission, distribution, and consumption of electricity. Flexibility in the consumption or production of devices (e.g., washing machine, home battery) can be used by multiple parties for different goals. A Distribution System Operator might want to use flexibility to avoid congestion on the grid, a Building (with PV panels) owner might want to use the flexibility to reduce the need for buying electricity from other parties in the energy system. Due to the immediate nature of the flow of electricity, the actions of one party in this system influence others. They ALL need to agree on who has what kind of responsibility and how the market is organized. In WP4 different kinds of agreements / models of interaction are discussed (e.g., the Universal Smart Energy Framework (USEF) with its USEF Flexibility Trading Protocol).

Mixing these agreements is not possible and not even the Semantic Interoperability Layer will be capable of 'harmonizing' business models. The ability to reason using semantical concepts from the set of InterConnect ontologies does not take care of that. This can easily be seen in terms of a 'chess and checkers' analogy. It is theoretically possible to describe the generic concept of a boardgame on a rectangular even sized grid, consisting of white and black squares, with black and white game pieces that can make moves in terms of moving from one square to another square in a certain direction. Both games can be described as specializations of this general concept. Checkers has one game piece (a disc), with a relatively limited set of allowed moves and a board of 10x10 squares. Chess has 6 pieces, each with a relatively large set of allowed moves and a board of 8x8 squares. However, it is impossible to describe how a valid move of a checkers player should be interpreted by a chess player. Both players use different boards, have different game pieces and different valid moves per game piece.

Flexibility services can also be seen as a 'game' where players (clients and servers) make moves according to certain 'rules of engagement'. A move in one set of agreements on flexibility (market organization) cannot be interpreted in another set of agreements. An example is trying to mix 'incentive-based' and 'control model-based' business models for flexibility services. In an incentive-based flexibility services business model, a device owner is incentivized to consume or produce less or more power (often by financial remuneration). What a device owner will do remains unknown to the user of the flexibility in advance, contrary to a control model-based business model, where device owners and users of the flexibility have an agreement in advance. They are mutually exclusive.

Each addition of an extra flexibility services business model to the set of allowed business models for flexibility will reduce the amount of interoperable flexibility services and the potential economy of scale. This is why the designers of InterConnect have created a limited set of flexibility concepts, which – somewhat paradoxically – does include both a incentive-based model and a control-model based business model. Although they reduce the economy of scale, both business models have collected so much critical mass in terms of pilots and acceptance of standards that excluding either of them would result in less industrial support of InterConnect. The SIL deals with this difference by making the type of business model explicit in terms of semantic concepts. Devices and services can state which business model they assume. This also enables the designers of InterConnect to add another flexibility business model if it turns out to be necessary for wider acceptance or if there is an evolution in flexibility business models. Future developments will determine what happens. In the meantime, the designers try to keep the amount of different (non-interoperable) flexibility business models as small as possible.

5.2 INTERFACES

This section serves as a guide for project participants involved in the design, creation, and operation of interfaces between architectural components.

5.2.1 'SAREFIZATION'

Services in the InterConnect ecosystem are offered through (digital) interfaces using semantic (web) technology, using architectural components that are visible in the SIL viewpoint (see section 4.5). From that point of view, the use and provisioning of services is implemented as the exchange of knowledge between Knowledge Bases. This knowledge is encoded in a set of predicate logic statements (a.k.a. graph patterns). This differs from the traditional REST[35] Application Programming Interface (API), where Uniform Resource Locators (URLs) and/or the Secure Hypertext Transfer Protocol (HTTPS) are used to exchange (requests for) information.

IMPORTANT: *it requires a certain level of skill and knowhow to translate traditional client-server interaction using REST APIs to the exchange of knowledge between InterConnect Knowledge Bases. One of the important skills is being versed in predicate logic and semantic web technology. An explanation attaining those skills is beyond the scope of deliverable D2.1.*

In the InterConnect project the process of transforming the interfaces of pre-InterConnect existing software components is called 'SAREFization'. This means something along the lines of 'translation to the SAREF ontology', which is a bit too simplistic. The SAREF ontology is one of the main ontologies in the InterConnect set of ontologies for encoding the semantics of knowledge does contain (parts of) the SAREF ontology, but there are more ontologies that are used. However, at one point the verb 'SAREFizing' got used for transformation of an existing API to one that is InterConnect compatible and it 'stuck'. SAREFization has been part of the

[35] https://en.wikipedia.org/wiki/Representational_state_transfer

tasks in InterConnect WP3 that develops 'semantic service components' that can be connected to the Service Store that is being developed in WP5 and that is visible in the IF point of view (see section 4.4).

The remainder of this section describes the two major steps and minor steps involved in SAREFization so the reader can grasp the basics of it from the SIL architectural point of view.

5.2.1.1 STEP 1 – SEPARATION OF CONCERNS IN SERVICE PROVISIONING

The first step in SAREFization of a service is getting a clear picture of 'what has to go where' in terms of logical (and later technical) components for providing a service. This can be done using the following minor steps:

1. Use the SERA viewpoint to determine what business roles and actors are involved in the provisioning of a particular service and how they relate to each other. Identify which other parties are (also) needed for providing a service. In case of a flexibility related service: make sure which kind of business model is used, so you will know what semantic concepts you must choose later (also see section 5.1.2).
2. Create a logical decomposition of functional components, based on responsibilities of business roles and actors involved; including criteria related to security and privacy (e.g., 'who has the right to own information').
3. Use the SHBIRA viewpoint to determine where) these logical components could and/or should be located and/or implemented in terms of location and abstraction layers of IoT platforms.
4. Now determine if these logical components can be implemented 1) completely or 2) partially using existing software components, or 3) not at all and a completely new component must be built 'from scratch'.

Note that in the InterConnect project a list of services has been made in WP3, also based on the collected use cases in T1.4 of WP1. For each logical component a next step can be made. Which step (2a or 2b) depends on the availability of existing software components (with interfaces).

5.2.1.2 STEP 2A – INTEGRATING EXISTING SOFTWARE COMPONENTS

This step is taken in case of an existing pre-InterConnect component with a non SIL compatible API:

1. Consider this component with 'business logic' to be a (partial) Knowledge Basis from a SIL point of view.

2. Determine what Knowledge it needs to function or possesses/generates to (potentially) share. The InterConnect set of ontologies (final version to be published in D2.3) can be used to describe Knowledge in the InterConnect way.
3. Determine what data/information processing to take place in an adapter, to create meaningful Knowledge Interactions using an existing API of a software component to store/retrieve information from a component (and transform it to KIs).
4. Using the logical decomposition from the SHBIRA point of view in step 1.3 to determine on what digital platform the adapter needs to be implemented.
5. Code the data/information processing for the digital platform from step 4.
6. Select the appropriate implementation technology for connecting to the InterConnect Service Store (visible in the IF point of view, see section **Erreur ! Source du renvoi introuvable.**). It is planned to have adapter technology provided in a Python and Java based version that can be wrapped in a software container (e.g., Docker).
7. Integrate the data/information processing code from step 5 with the implementation technology for the adapter from step 6 and 'build' the software component.

5.2.1.3 STEP 2B – ADDING A NEW COMPONENT

This step is taken in case of a not yet implemented logical component. It somewhat resembles the step 2a, but it requires less coding for adaptation and more code for data/information processing.

1. Determine what Knowledge the component needs to function or possesses/generates to (potentially) share. The InterConnect set of ontologies (final version to be published in D2.3) can be used to describe Knowledge in the InterConnect way.
2. Using the logical decomposition from the SHBIRA point of view in step 1.3 to determine on what digital platform the component needs to be implemented.
3. Code the data/information processing (a.k.a. 'business logic') needed to implement the desired functionality, considering input/output as the exchange of Knowledge between Knowledge Bases. Do this on the digital platform from step 2.
4. Select the appropriate implementation technology for connecting to the InterConnect Service Store (visible in the IF point of view, see section 4.4.
5. Integrate the data/information processing code from step 3 with the implementation technology for the adapter from step 4 and 'build' the software component.

5.2.2 AUTOMATIC COMPLIANCE TESTING

Once (the interface of) a service is made interoperable through SAREFization, it needs to be known within the InterConnect ecosystem. From the Semantic Interoperability Layer point of view this means registration with the Knowledge Directories (see section 4.5.2). The InterConnect Service Store, visible from the Interoperability Framework point (see 4.4.2 section is planned to require an achieved compliance level certificate. This enables end-users to use the Service Store as a trust anchor (see section 4.4.3).

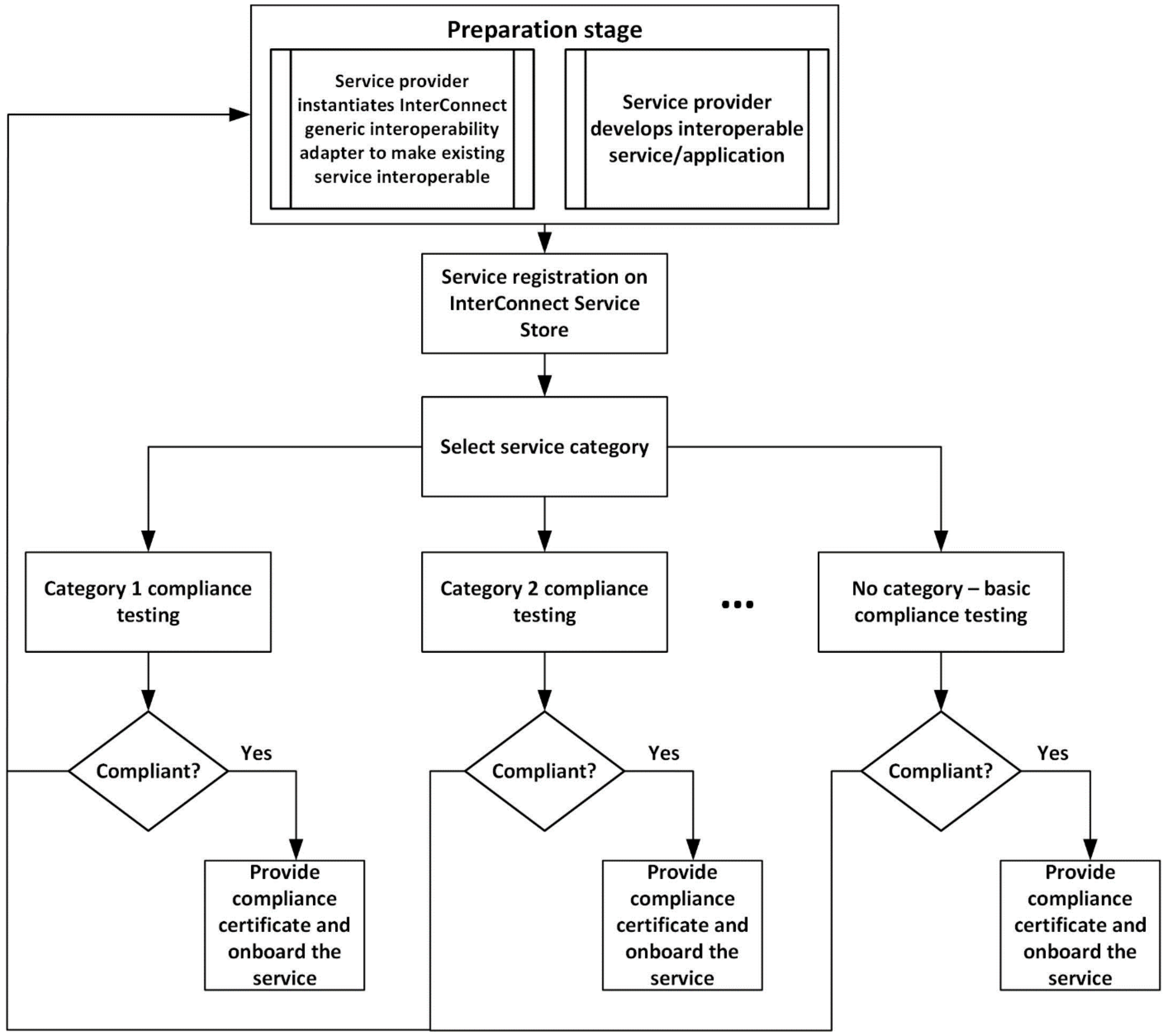

FIGURE 9 – AUTOMATED SEMANTIC INTEROPERABILITY COMPLIANCE TEST PROCESS FLOW

To get an InterConnect interoperability compliance certificate, it is planned to have each service need to pass an automated compliance test. It should be performed during the service registration process and with every service update and could also be considered during updates in the InterConnect semantic interoperability layer (see section 5.2.3). Figure 9 provides a high-level overview of the automated compliance test as part of the service store.

After the service provider registers an interoperable service and selects an 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 compliance with the semantic technology of InterConnect, including the correct use of the InterConnect semantic technology and the set of ontologies. Multiple messages of specific format and content will be sent to the (interface of the) service that is tested. There should be a reply in line with agreements as made within the InterConnect project. A compliance test backend procedure of the Service Store will analyse received replies and derive compliance results indicating achieved if interoperability has been achieved. After successful completion of the compliance test, a 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. From that point on they are connected to the Semantic Interoperability Layer and can be included in reasoning across Knowledge Bases.

Note that this is a high-level description of automatic compliance testing and that details need to be fleshed out during realization of the Service Store in WP5.

5.2.2.1 SERVICE DIMENSIONS AND LEVELS OF COMPLIANCE

Instead of just carrying out ‘binary’ checking for interoperability in terms of the correct usage of semantic InterConnect technology, it might also be possible to agree on certain dimensions of services and levels of interoperability. Some examples (described at a relatively high level of abstraction):

1. Version of the InterConnect set of ontologies. As described in section 5.2.3, the InterConnect set of ontologies is relatively young and further evolutions are to be expected.
2. Category of service: forecasting services, use of flexibility, remote device control, etc.
3. Ability to use and discriminate on self-defined security groups.

4. Suited for inclusion in cross knowledge base reasoning. If the response-time of a knowledge base (after a request) is bigger than a certain amount, it is no longer suited for reasoning as it will slow down overall performance of a service.

Once service dimensions and levels of interoperability compliance are agreed upon, then they can be used as criteria to score on. A minimal level of scores on a minimal set of criteria would need to be defined as "basic compliance". All services in the Service Store would need to have 'basic compliance' to get a certificate. Given the different criteria and levels it would become possible to let the Service Store send a compliance test report to a service provider that could be used for improving the service interoperability ("score higher").

Currently the InterConnect project is focussed on realizing a first working version of the Interoperability Framework, including the Semantic Interoperability Layer. Once that has been achieved, the project can start working on testing for levels of compliance.

5.2.3 INTERCONNECT ONTOLOGIES EVOLUTION

At the time of writing this Deliverable, the set of InterConnect ontologies has not been finalized for usage in pilots. The final set will be published in D2.3, but even after that experience gathered during the pilots will probably lead to new insights into how to semantically model the InterConnect ecosystem. It is therefore important that interface designers and implementers create adapters that can be relatively easily modified and replaced in case of new releases of the InterConnect ontology set. It is expected that the set will stabilize in 2022, but even then, changes might be introduced to align with industrial standards in the domain of Energy and IoT. Keeping the amount of software and driver updates as low as possible while supporting evolution of the ontologies will be an important part of the implementation of the Semantic Interoperability Layer.

6. CURRENT STATUS AND NEXT STEPS

In the previous chapter 'building the InterConnect ecosystem' was discussed from an architectural point of view. In this final chapter, a short discussion is provided on the status of the Secure interoperable IoT smart Home/Building and smart Energy system Reference Architecture (SHBERA) and its multiple viewpoints (see section 4.1). Finally, the most important next steps from an architectural point of view are presented.

6.1 CURRENT STATUS

The SHBERA is a necessary (see section **Erreur ! Source du renvoi introuvable.**) derivation of state of the art reference architectures/models (see section 2) and InterConnect ecosystem requirements (see section 3.2). Currently, is that it has largely been applied in a theoretical way. Only after implementing the plans for the different pilots the InterConnect project can collect enough feedback to determine to which extent, it actually provides what is needed for creating the desired interoperable ecosystem at a European scale of millions of devices and hundreds of services.

6.1.1 RELATIONSHIP WITH PLANNED PILOT ARCHITECTURES

The current version of the SHBERA has been used for a so called 'mapping' of specific pilot architectures. When the first versions of the SHBERA viewpoints were presented many of the pilots already had a description of plans at the architectural level. Different styles and different points of view had been used by participants. This enabled the designers of the SHBERA in WP2 to include certain wishes and demands coming from different project partners in several iterations of the SHBERA viewpoints.

After the SHBERA viewpoints had stabilized (i.e., no more major changes) workshops were held where the most recent planned pilot architectures were analysed in terms of the SERA (section 4.2), SHBIRA (section 4.3) and IF (section 4.4) points of view present in the SHBERA. A detailed description of the mapping and its analysis can be found in Annex VI of this document. One conclusion was that a significant number of project pilot partners could work with the mentioned viewpoints of the SHBERA and could create pilot architectures that were compatible with the SHBERA and its requirements. This was probably partially because these three viewpoints use a relatively high level of abstraction, while the non-included SIL point of view (section 4.5) does not. The SIL point of view was not included at the time the workshops because not enough (descriptions of the) related technology and InterConnect ontologies involved were available yet.

6.1.2 THE INTERCONNECT ONTOLOGIES

Although the set of InterConnect ontologies (a product of T2.4) can be considered as not being part of the architecture, it is so closely related to application of the architecture it must be mentioned here. Without having access to the InterConnect set of ontologies it is impossible for device manufacturers, service providers and other parties involved in the democratization of energy management to determine if their view on the world can be somehow mapped to the shared understanding as created in InterConnect. This is especially important due to the limitation of the number of allowed business roles/actors/components in providing/using flexibility on the electrical gird. As stated in section 5.1.2, this limit exists because of the need for an economy of scale and the wish to have broad industrial support for the InterConnect ecosystem. Deciding to become interoperable with the ecosystem requires parties to compare their own demands with respect to (semantical) business concepts to what InterConnect prescribes in the ontologies.

The status of the set of InterConnect ontologies is that the set has not been finished yet although a significant number of semantical concepts have been discussed and been made part of the current (preliminary) set. This was done during and after specific T2.4 workshops in which semantic engineers and ontologists discussed needs and requirements from pilot partners that presented a selection of typical use cases. Also, in T2.5, significant efforts were made in discovering the similarities and differences in semantical concepts relating to the concept of flexibility (on the electrical grid). The outcomes of these discussions and analyses were used to iterate across the preliminary set. The work in WP3 on the creation of Semantic Service Components and the graph patterns (see section 5.2.1 on SAREFization) – demonstrated that understanding of several concepts – especially flexibility – was not shared across all project partners.

6.2 NEXT STEPS

WP2 has not finished its work yet and will continue to be active until M36. There will be a new and improvised version of the architecture and a finalized InterConnect set of ontologies. This section provides a description of the planned next steps.

6.2.1 ARCHITECTURAL COMPLIANCE FROM A SIL POINT OF VIEW

As stated in section 6.1.1, there has been no comparison of planned pilot architectures from a SIL point of view (section 4.5), so no actions can be taken to assure there is compliance from that point of view as well to achieve interoperability. However, at the time of writing of this Deliverable D2.1 there has been a significant advance in the delivery of InterConnect specific semantic technology in WP5 and a set of ontologies incorporating all required semantic concepts will be delivered in D2.3 at the end of December 2021. This is done based on feedback from several pilot implementing partners (also active in WP3 for creating Semantical Service Components), automatically resulting the mapping of pilot architectures and their implementation from a SIL point of view.

6.2.2 FINALIZING THE ONTOLOGIES

As stated in section 6.1.2 the InterConnect set of ontology has not been finished but needs to be soon. The experiences, wishes and demands from WP3 are and will also be used by semantic engineers and ontologists in T2.4 to complete the set of ontologies, which should result in the availability of a first set that is applicable by all pilot partners involved. The results will be published in D2.3 at the end of December 2021.

6.2.3 PUBLISHING THE ARCHITECTURE

In M36, an updated version of the SHBERA and its viewpoints will be published in InterConnect deliverable D2.4. The pilot architectures will have been compared to the SHBERA and where necessary changes will be made to increase a unified way of architecting the InterConnect ecosystem.

REFERENCES

EXTERNAL DOCUMENTS

[1] W3.org , «Web of Things (WoT) Architecture,» 2020.

[2] Deutsches Institut für Normung (DIN), «DIN SPEC 27070 Requirements and reference architecture of a security gateway for the exchange of industry data and services,» 2020.

[3] K. Helmholt et G. Broenink, «Degrees of Freedom in Information Sharing on a Greener and Smarter Grid,» chez *in ENERGY 2011 : The First International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies*, Italy, 2011.

[4] Smart Grids Task Force, «EG3 REPORT - Regulatory Recommendations for the Deployment of Flexibility,» 2015.

[5] C. Brewster, B. Nouwt, S. Raaijmakers et J. Verhoosel, «Ontology-based access control for FAIR data,» *Data Intelligence,* n° %101, pp. 66-77, 2020.

[6] AIOTI, «High Level Architecture (HLA),» 2018.

[7] oneM2M, «Functional Architecture».

[8] FIWARE, «FIWARE NGSI v2 specification,» 2018.

[9] IEC, «Communication networks and systems for power utility automation,» 2020.

[10] AIOTI, «Semantic Interoperability,» 2015.

[11] ETSI TS: 103 264, «SmartM2M; Smart Appliances; Reference Ontology and oneM2M Mapping,» 2017.

[12] A. Gyrard, C. Bonnet et K. Boudaoud, «Enrich Machine-to-Machine Data with Semantic Web Technologies for Cross-Domain Applications,» chez *IEEE World Forum on Internet of Things WF-IoT)*, Seoul, Korea, 2014.

INTERCONNECT DOCUMENTS

[13] InterConnect project. "D1.1 Services and use cases for smart buildings and grids". 2021.

[14] InterConnect project. "D5.1 Concept, design and architecture of the interoperable marketplace toolbox", 2020.

[15] InterConnect project. “D2.2 Privacy and security design principles and implementation guidelines”. 2021.

Annex I. STATE OF THE ART: COMPLEMENTARY INFORMATION

1. AIOTI's Reference Architecture

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) [6], 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). AIOTI's functional model 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.

Additional layers are also present to interface between planes. 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. 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 allow access to services exposed by an IoT Entity. The data plane interface supports sending/receiving 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, through exposing/requesting services.

AIOTI includes propositions for unlocking semantic interoperability features in large-scale pilots 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. oneM2M's Reference Architecture

oneM2M architecture comprehends three layers: 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 [7]. Each layer contains a common services entity (CSE), an application entity (AE), or both.

An AE provides application logic (e.g., remote power monitoring), while a CSE comprises a set of service functions (also called common services functions or 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 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.

3. FIWARE's Reference Architecture

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 semantic expansion of the data models, there is yet no direct semantic reasoning capabilities [8] 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.

4. W3C'S WORLD OF THINGS (WOT)

The W3C's reference architecture is built around the concept of things. A thing is an abstraction of any uniquely identified physical or virtual entity. 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 [1]. 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" [1].

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.

5. IDSA'S Reference Architecture

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-premises 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 contains an elaborate stack of security functionality. Moreover, it should be noted that the complete IDS architecture is highly flexible. 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 can also be used to log a full copy or a subset of the original data and can be hashed or encrypted.

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.

6. DKE's Home and Building Architecture Model (HBAM)

In 2019 the HBAM model was presented in IEC SEG9-WG3 and updated according to the discussions which took place. The HBAM 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[36]. 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 20 – HBAM MODEL LAYER DESCRIPTION

7. CENELEC's Reference Architecture

CENELEC provides standards for interoperability touching the energy domain. With the European Mandate M490, the Smart Grid Coordination Group (SG CG) developed a High-

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

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 (Smart Premises Interoperable Neutral message Exchange) [37], which defines a neutral layer which helps to connect different communication technologies to build an energy ecosystem from grid to device level.

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 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 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 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.

8. SMART GRID ARCHITECTURAL MODEL (SGAM)

Within SGAM, interoperability is the focus, and it 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 [9].

This mechanism encompasses a three-dimensional model, that merges the five interoperability layers enumerated above (Business, Functional, Information, Communication

[37] For more information, please visit: https://www.eebus.org/technology/.

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 highlighting 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.

9. IEC's REFERENCE ARCHITECTURE

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[38] regarding a 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 using 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.

[38] 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)

Annex II. INTERCONNECT'S ECOSYSTEM OF SYSTEMS

This annex provides a description of the InterConnect ecosystem as it has been envisioned.

1. Ecosystem of systems

The InterConnect ecosystem will be a complex system of systems that can be divided into two categories: systems (a.k.a. components) that **already existed** before the InterConnect ecosystem was developed and those that did not. This distinction is important, as InterConnect is not about a replacement of what is already there. In fact, its creation is based on a 'need-to-add' concept instead of 'replacement'.

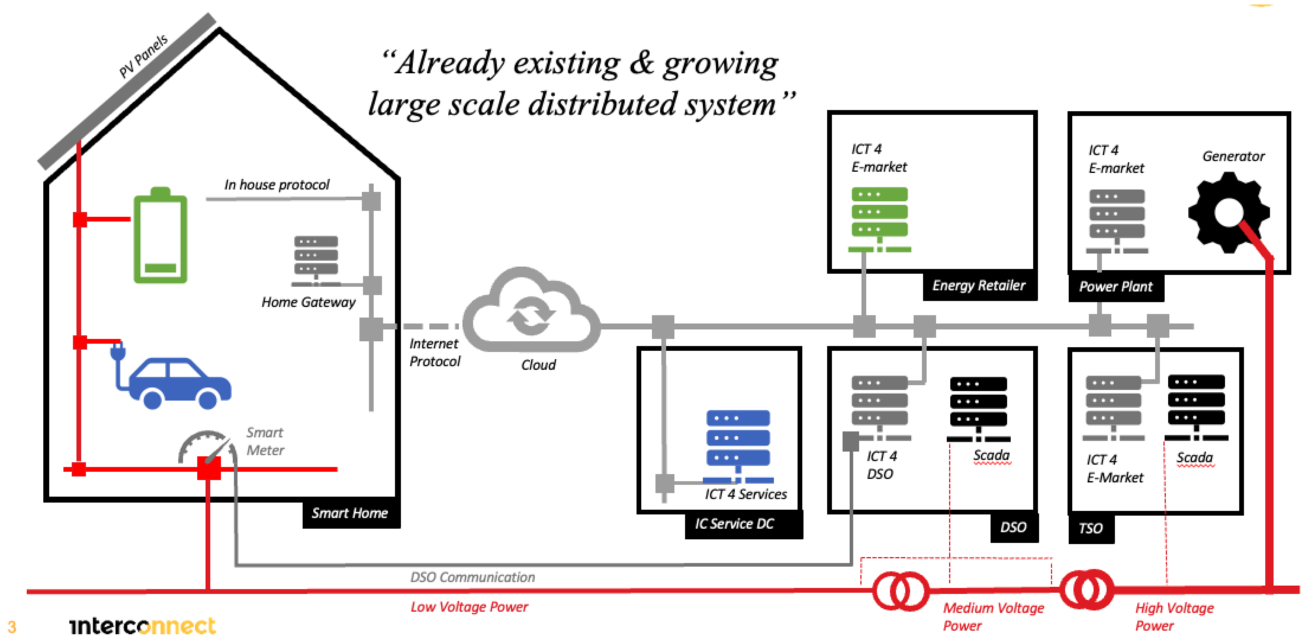

FIGURE 10 – INTERCONNECT HIGH LEVEL VIEW ON THE ECOSYSTEM OF SYSTEMS

From a high-level point of view, the following components (in bold) can be identified, that were already there before InterConnect came to see the light of day:

1. **Smart Homes** and **Smart Buildings**, connected to a **Smart Grid**.
2. **Devices** in Smart Homes and Smart Buildings.
3. **Services** offered to **Customers** by **Service Providers**.

A more detailed InterConnect definition of some of these components will provided later in this annex.

1.1 Illustration of the ecosystem's components

Figure 10 contains an illustration of some of these already existing components. On the left side there is a Smart Home with several devices: PhotoVoltaic (PV) panels, an Electric Vehicle (EV), a home battery and a Home Gateway that provides a connect to the Internet and/or Cloud. The Smart Home has a connection (in red) to the Smart Grid which has a low voltage, medium voltage, and high voltage power networks. On the right side there are several service providers. A Distribution System Operator (DSO) operates the low and medium voltage power network, the Transmission System Operator takes care of the high voltage power network. There is a traditional Power Plant generating electricity and an Energy Retailer that takes care of selling the power. All service providers use Information and Communication Technology (ICT) systems for providing their services. In Figure one of these is ICT systems explicitly mentioned: ICT for trading on the E(lectricity)-markets. Finally, there is a 'InterConnect' (IC) Service (Provider) DC, which serves as a generic placeholder for service providers that offer a particular service. Just like the Smart Homes, the Service Providers are all connected to the Internet and/or Cloud.

These components (or subsystems) are connected through interfaces, and through those they can use other components to carry out their tasks. There are many kinds of interfaces. Some interfaces are mostly physical, like for example a low voltage wall outlet: metal connectors with 230 Volts of AC voltage at 50Hz. This interface is not meant for communication but for the transmission of power (although there are devices today that can transmit data across in house powerlines). Other interfaces are more sophisticated like an Internet point connection from a cable operator, which are meant for the transmission of data. These include metal wires like wall outlets, but also include computers to encode data into transmissible signals across the metal wires. But optical cables can also be used and then the computers encode data into light pulses. Finally, there are even more highly sophisticated interfaces that primarily exist on an abstract level in the form of the exchange of information between software components that are distributed across the Internet and/or Cloud. In short: there is a spectrum of interfaces between system components engineered for specific purposes. **InterConnect is not replacing all these kinds of interfaces.**

1.1.1 Ease of use for all stakeholders involved

A lot of the innovation InterConnect brings in agreement on interfaces between components at different levels of abstraction. But the most visible innovation is what InterConnect could look from an end-user point of view, especially from the perspective of democratizing energy management.

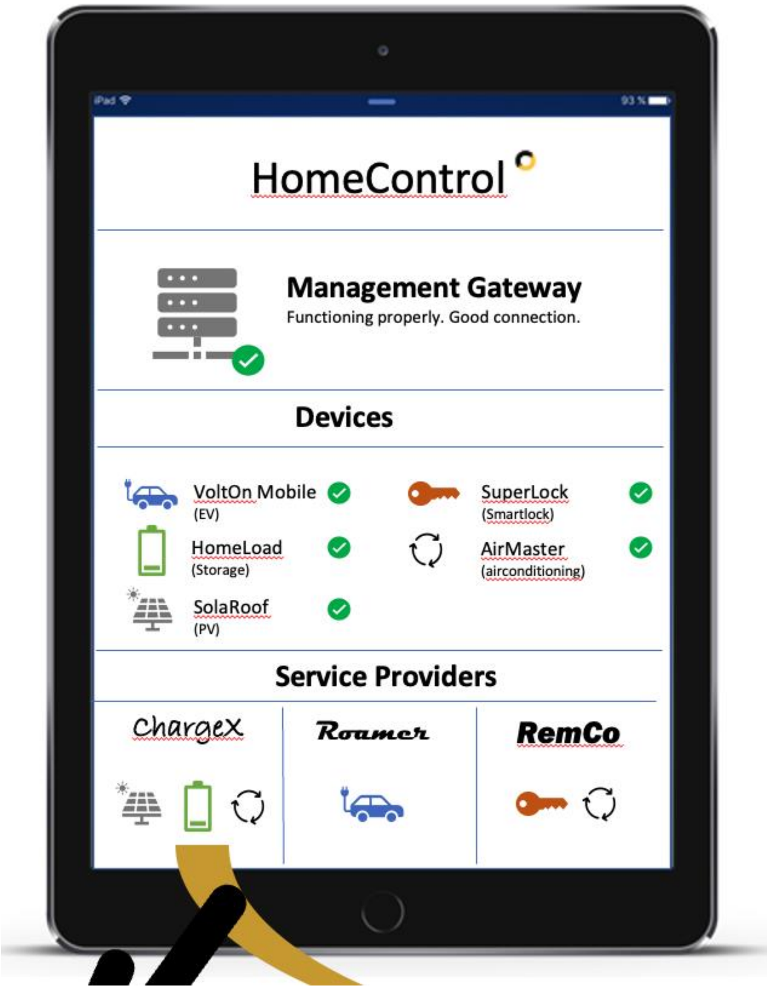

FIGURE 11 SMART HOME END-USER EXAMPLE VIEW OF DEVICES AND SERVICES

In Figure 11 there is an artistic and simplified rendering of what an end-user in a Smart Home might see on a tablet using an imaginary app – called ‘HomeControl’ that provides the ability to interact with the configuration of devices and services in a Smart Home. The app has the InterConnect ‘circle logo’ to show that it is InterConnect compatible.

At the top of the view is a field with information of the status of the ‘Management Gateway’. This is an imaginary component in a Smart Home – for the sake of this example - which provides a communication connection to the outside world (using the Internet). The app tells the End-User that the gateway is functioning properly and that there is a good connection. If this component fails, then all other services that need an outside connection might fail as well, depending how often they need to communicate using the Internet.

Then there is a list of devices in the Smart Home from (imaginary[39]) brands:

1. an Electric Vehicle **(EV)** from 'VoltOn Mobile',
2. a home battery for **storage** of electrical energy from 'HomeLoad',
3. PhotoVoltaic (**PV**) panels from 'SolaRoof',
4. a remotely operated lock (a.k.a. **Smartlock**) from 'SuperLock'. It has a camera attached to it, so people can see who is at the door from a distance,
5. an **air conditioning** system from 'AirMaster'.

All devices are in full operation and functioning properly. The devices are used by services from three providers:

1. **ChargeX** that (also) offers smart 'charging' services for home storage (in a broad sense). The service ensures the air inside the house is fresh ('charged with cool air') and the home storage is charged in the most optimal way in terms of energy prices, potential low voltage grid overload, battery lifetime conditions and air quality (depending on the preferences of the homeowner). It uses the following devices:
    a. **PV** panels, as an electricity sink.
    b. **Storage**, as an electricity source and sink
    c. **Air conditioning**, as an electricity sink.
2. **Roamer** that offers charging for electric vehicles. The customer of Roamer has low charging costs and is ensured it can charge across Europe at different providers of (smart) charging. Charges an Electric Vehicle **(EV)** from 'VoltOn Mobile'. It uses the following devices:
    a. **EV**, as an electricity sink, but also as a source ('vehicle to grid') if necessary.
3. **RemCo** that offers remote control capabilities for devices in a Smart Home. It is a trusted service provider that has proven to be resilient against hacker attacks. It uses the following devices:
    a. **Smartlock,** to control access to the house remotely
    b. **Air conditioning,** to control the indoor comfort away from home.

In this example the **air conditioning** device is used by two different services. One service is targeted at energy management, while the other is target at home comfort. InterConnect

[39] The InterConnect WP2 teams wants to avoid the impression of favouring a certain brand, vendor and/or enterprise.

enables devices to communicate their monitoring and control options in such a way that this is possible. The end-user can configure master settings and provide 'operating bands' for different services. The priority is also set by the user of the HomeControl app. The screens for doing this are not rendered, neither are the information models and the communication between devices and services using the interoperability layer. This is beyond the scope of this introductory chapter. Now to show what InterConnect interoperability means, the user of the HomeControl app will now reconfigure the usage of devices.

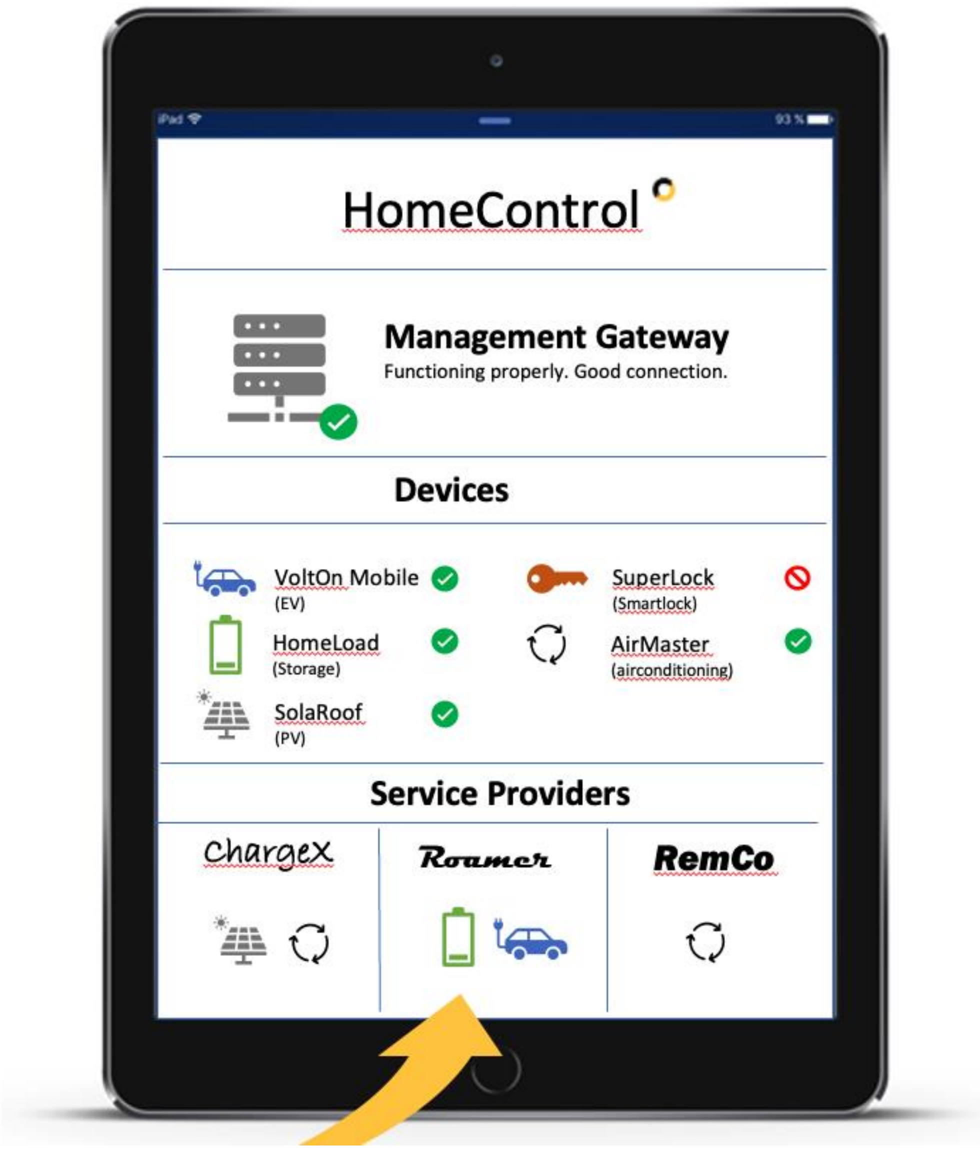

FIGURE 12 SMART HOME END-USER EXAMPLE VIEW OF INTEROPERABILITY

In Figure 12 the user has 'swiped' the **storage** device (icon) from ChargeX to Roamer. This means the following:

1. **ChargeX** can no longer use the **storage** device as an electricity source and sink. It can still use the **PV** panels as a source and can still 'charge' the house with fresh air using the air conditioner in an optimal way in terms of energy prices and potential low voltage grid overload, battery lifetime conditions and air quality (depending on the preferences of the homeowner).
2. **Roamer** can now use the **storage** device as an electricity source and sink of the Smart Home for providing the best price/performance in electrical mobility (depending on the preferences of the homeowner and/or guests).

Also, the Smartlock device is out of operation. This was done by the homeowner – in this example illustration – because there was a news item that talked about a failure in certain older devices from the SuperLock brand. As a precaution the homeowner used the HomeControl app to temporarily stop this device from functioning. As a result, RemCo can no longer use the SmartLock for its services as well.

The configuration screens for moving the storage device from ChargeX to Roamer and switching of the Smartlock are not rendered, neither are the information models and the communication between devices and services using the interoperability layer. This is beyond the scope of this introductory chapter. What is important to realize is that InterConnect offers device manufacturers/vendors and service providers to add technology (hard/software) to their existing devices/equipment that enables end-users to make use of interoperability.

1.1.2 Interoperability through wrapping components

InterConnect has been developed to increase the level of **interoperability** of components in the ecosystem of Smart Homes, Buildings and Grids that already existed. More interoperability means less restrictions for systems or components to work together (if authorized to do so of course).

The basic approach of increasing interoperability is proven. It is done by **wrapping** (**existing) components** with a so called '**Interoperability Layer**', as visualized in Figure 13. Instead of letting components communicate across interfaces using vendor/brand specific communication protocols the InterConnect ecosystem offers the ability to communicate at a high level of abstraction using standardized concepts. The less proven part of increasing interoperability (as InterConnect does it) is by using **web services** and especially **semantic web technology**. This means that in InterConnect components (also) have interfaces that can send and receive data with meaning (i.e., 'semantics') encoded into them. This makes it easier for the sending component to express the meaning of the data and for the receiving component to understand the meaning. It is easier because the use of semantic web technology enables the senders and receivers to refer to a dictionary of concepts where the relationship between concepts is described in such a way that a computer can parse data/information using this dictionary, which is known in the world of the semantic web as an '**ontology**'. This reduces the design and engineering load of (software) engineers if they are versed in using semantic web technology of course. The load is reduced because much of the work on agreeing how to communicate information regarding concepts across an interface has already been carried out by the ontology designers. Note that InterConnect has tried and still tries to stay close to existing industrial standards where interaction between components through certain interfaces already has taken place. Examples are the technical specifications and/or standards from EEBUS and CEN/CENELEC in the domain of using flexibility in power consumption and production of devices. If there already is a widely accepted agreement that has result in interoperability, InterConnect tries to increase that by applying semantic web technology to a standardized (and existing) data/information model, instead of reinventing the (interoperability) wheel in a certain domain and/or industry. **For example, if everyone creates their own systems of using flexibility, then there is no interoperability at all in the field of energy management.**

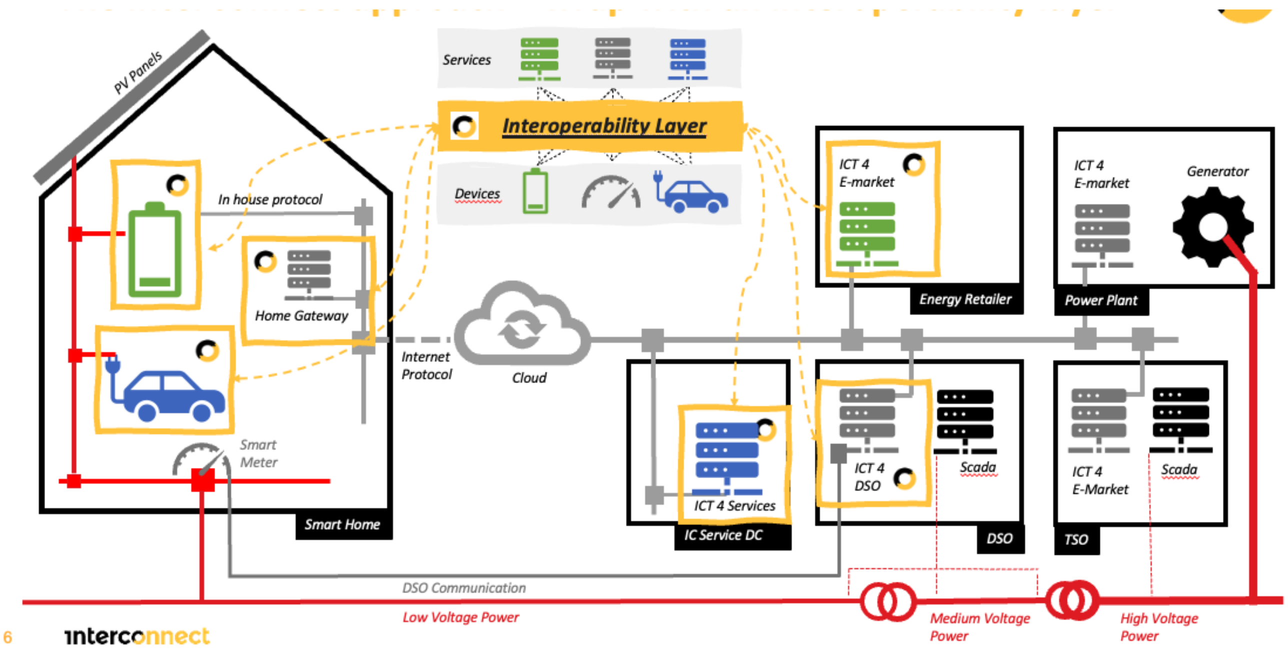

FIGURE 13 VISUALIZATION OF WRAPPING OF COMPONENTS

For those readers that want to get an idea of the abstraction level at which InterConnect lets components communicate: the semantically encoded data is communicated using the existing Hypertext Transfer Protocol Secure (**HTTPS**), which itself makes use of the existing underlying Transmission Control Protocol (**TCP**), which is on top of the existing Internet Protocol (**IP**). The IP can be and (already is) 'rolled out' on top off specific types of physical carriers (radio waves, metal, glass, and avian[40]). By exchanging data and/or information at such a high abstraction level there is much freedom in design and engineering the way components are physically connected. It does however require a certain level of computational power at both the sending and receiving end for encoding and decoding. Given the combination of reduction of costs and size and the increase of computational power the designers and engineers of InterConnect thinks the costs of less interoperability outweigh the need for extra computation. **In short: to achieve more interoperability InterConnect is following the traditional approach of higher-level abstraction on the Internet (and the Web).**

InterConnect adds innovative elements to an existing (complex) ecosystem using a proven Internet-based approach. It thus stimulates business competition on a commercially level playing field, without requiring participants (customers, manufacturers, and service providers) to rebuild an entire infrastructure.

1.2 Devices and services connected to the grid

In the previous section a high-level view of the InterConnect Ecosystem was provided. An illustration was provided of what InterConnect could mean for the end-user and it was discussed how wrapping (existing) components with an 'Interoperability Layer' can help in creating system wide interoperability of components. The remainder of the Annex 1 looks at the important concepts of devices and services, largely from the perspective of the (electrical) grid which is the primary means in InterConnect to share energy.

1.2.1 Devices

From the InterConnect ecosystem point of view **devices** are defined as physical objects that are in/or nearby a home or a building and are (in)directly **connected** to the **electrical grid**.

[40] https://datatracker.ietf.org/doc/html/rfc1149

They can be fixed into place and permanently connected to the grid, but also moveable and intermittently (e.g., an electric vehicle). Devices are also (in)directly connected to the **Internet**. This does **not** necessarily mean that a device needs to have a **computer built in**. It does mean that the device must have some physical means of communication with a computer that is (in)directly connect to the Internet.

This InterConnect definition of a device allows for many physical objects to be considered as a device which can be used by services. Here are some examples:

1. A **washing machine** with WiFi built in, that allows it to be operated remotely across the Internet using an WiFi access point.
2. A **pool heater** with a Modbus communication interface, which can be connected to a computer with both a Modbus interface as well as Internet access.
3. An **electric vehicle** connected to a charger with WiFi built in, allowing remote control of the charging.
4. A **lamp** with wireless 433MHz frequency built in for communication to a nearby computer.
5. An **electromechanical lock** which can (also) communicate to a nearby computer with Internet access.
6. A **PhotoVoltaic (PV) panel**, connected to a converter with the ability to communicate with a nearby computer with Internet access.
7. A **home battery**, with a built-in computer that has access to the Internet.

According to the InterConnect definition a device can both consume and produce electrical power.

1.2.2 Challenges for the Grid

In the world of InterConnect, a house or building that uses some kind of automation to remotely monitor and/or control (I.e., operate) devices is often called a ‘Smart Home’ or ‘Smart Building. These types of homes and buildings can be used to deal with challenges for the (smart) electrical grids of today and tomorrow. InterConnect sees a Smart Grid as a grid that uses automated remote monitoring and control to deal with the challenges of intermittent electricity production and congestion.

Automated control is useful in the field of grid management because of the rise **of intermittent electricity production**. For example, devices like PV panels can suddenly ramp up/down quickly in power production after clouds (dis)appear. As physical laws dictate that supply and demand on the electrical grid always need to be balanced, the rise of intermittent electricity production requires a rise in controlling the demand. In case of a sudden increase in electricity production decisions must be made whether to store it in home batteries, to use it for charging EVs, heating the pool, decouple PVs, etc. The same goes for a sudden drop. By making use of the electrical grid connecting homes and buildings, there are more ways to ‘solve the supply and demand puzzle’. Remote monitoring and control of devices also seems a way of dealing with **increasing congestion** on the electrical grid. This is – to a large part – caused by using the electrical grid for other things than powering household appliances. The power for electric mobility often flows through the grid, and in countries where natural gas networks are (partially) decommissioned the power for heating also must flow through the grid. Unless people want to be on the mobile phone on a 24/7 basis with other people, while running around to operate devices, automation is the way to go forward.

1.2.3 Distributed decision making using interworking EMS

When the remote monitoring and control of devices is automated, it becomes particularly important **who** or **what** is **making decisions** (and executes them). For example, there is the lesser issue of *comfort*, where a house is not heated as much as someone would like. There is the bigger issue of someone suffering from the cold, but there might arise a *safety* issue when (e.g.) four EV owners in a street near simultaneously decide it is time to charge their EV as fast as the EV allows for and the local part of the grid cannot deal with that amount of simultaneous use. Best case the local grid will partially shut down to protect itself from an overload. Worst case a physical overload takes place that locally damages the grid. The loss of the electrical grid in a world that uses the grid for driving appliances, heating and mobility can have a massive impact.

Given the consequences of device behaviour, remote monitoring and control is interesting for organizations that operate grids and/or complete energy systems, like a Distribution System/Network Operator (DSO, DNO for low and medium voltage networks) or a Transmission System Operator (TSO, for high voltage networks). If they are provided with the ability to remotely monitor and control devices, they could theoretically protect their networks against all kinds of dangers and keep them up and running. However, in practice this would mean that electricity grid operators would have to manage several millions of devices, depending on how many homes and buildings are connect to the part of the grid they operate.

This is not what these operators are used to do. In the last decades operators have evolved to support the flow of electrical power across the grid in a reliable and affordable way. **Electricity markets** have been used to balance demand and supply, where trading parties like retailers **aggregate** smaller demand and supply volumes into larger ones. Grid operators had no knowledge of specific electrical devices, apart from exceptional outlier 'devices' like an aluminium smelter plant that has a gigantic 'footprint' on the grid.

Apart from the fact that remote monitoring and control of grid-connected devices in homes and buildings would mean a **fundamental change** for **network operators**, the inhabitants of homes, offices and/or facility managers of buildings would probably not be amused if they would experience a take-over of devices. They have their own requirements and since they pay for the devices and the electricity used, it would be not considered fair if other people completely decide for them when to use the devices. Also, on what grounds would a DSO for example be allowed to deny a specific consumer to charge its EV at a certain point in time? Or who decides on disconnecting the PV panels of a particular building from the grid in case of congestion? This would stop building owners from selling the power they do not need, thus reducing the Return on Investment (RoI). Would it not be the responsibility of the network operator just to upgrade the local grid, so it has more bandwidth for power? But who is going to pay for that upgrade? Why should people that do not have massive PV installations pay for the people that congest the electrical grid? Why not let the PV owners pay for their own storage?

Making decisions that are both **experienced as fair** and **stimulates the use of renewable energy** resources at a societal level is an extraordinarily complex thing to do. Especially while keeping the electrical grid **reliable** and **affordable**.

Because of the complexity involved, a lot of research, development and pilots have been carried out in the field of automated energy management. This has resulted in a wide range of approaches and there is no universal standard yet. The world is still searching for a common approach. Many of the approaches do apply **separation of concerns**, where the network operator and/or electrical energy retailers are shielded from the remote monitoring and control of **individual** devices. A so-called Energy Management System (**EMS**) is added to a home, a building or a set of buildings (e.g., 'campus'). The EMS has specific knowledge on the current and potential future state of devices and can also make estimations on energy consumption and production given the local situation. The EMS is the automated point of contact for outside automated systems that want to request, suggest, or enforce certain electrical behaviour of the home, building or campus. An EMS is sometimes also known as a Home Energy Management System (**HEMS**), Building Energy Management System (**BEMS**), or Central Energy Management System (**CEMS**). By grouping and organizing the EMSs of different homes and buildings in a certain way and applying various **levels of (geographical / network topological) abstraction**, it becomes theoretically possible to distribute the decision-making process regarding devices in such a way that the complexity becomes more manageable in terms of fairness, reliability, affordability, and increase the use of renewable energy sources.

What type of grouping and organization is optimal from a societal point of view also depends on political views, so it is quintessential that the technology that is used for this type of distributed decision making supports different 'societal settings', enabling citizens to collectively decide on the type of decision making, grouping and organizations of EMSs. If societal views change, it should be possible to **reconfigure** instead of having to rebuild the **distributed system** of **EMSs.** An example is the difference between **financially incentivizing** an EMS to behave in a certain way, or to manage production and consumption of electricity according to (financially binding) **contracts** between the EMS and outside systems. When incentivizing an EMS, it is not clear on beforehand what the outcome of the management process will be. When adhering to contracts it mostly is.

Apart from the fact that the remote monitoring and control shields the network operators from having to know about the state and behaviour of **specific devices**, an EMS can also help in keeping things **private**. Why should a network operator, an energy retailer or anyone else have knowledge about devices in a home or building? Knowing about the usage of devices provides insight into the life of the people using them. Although there might be people that have no issues in sharing all information with everyone, there are also people that want to share information on a need-to-know basis, which is the current situation in many countries. Only the **accumulated (or aggregated) amount** of electrical power usage is used in trading with consumers. It used to be 'per year', but with the arrival of smart meters – that provide remote monitoring - it is possible to do this per month.

Finally: when the remote control of devices can have significant physical consequences and financial implications, the **access** to **devices** becomes quintessential to societal acceptation. What if for example hackers inject ransomware in EMSs on a mass scale and take over the control of energy flow in a part of the grid? They could threaten a network operator to take down parts of the grid by letting homes and buildings behave erratically. A less dramatic scenario is where a homeowner wants only some inhabitants of the home to be able to control the heating of the pool.

Next to the ability to control who is given access, it is also important to be able to revoke permission to remotely monitor and control devices. Trust relationships between consumers and service providers might change.

1.2.4 Services

From the InterConnect ecosystem point of view a **service** is defined as the offering of certain functionality from one component in the ecosystem to another (authorized) component. The InterConnect ecosystem is not a revolution in doing business on the Internet. It uses the same proven concepts; however, it is important to understand how InterConnect sees services from a commercial perspective to avoid misunderstandings by the reader.

A service (from a commercial point of view) is a component in the concept of **Value Networks** as defined by Fjeldstad and Stabell[41]. They see the following components:

1. **Customers**
2. An **Organization** to provide the service.
3. A **Service** that enables interaction between customers and an organization
4. **Contracts** that enable access to the service

In InterConnect ecosystem the 'interaction' between customers and an organization is the offering of functionality. Also, an organization is sometimes also known as a **business**, a **company** or a **service provider**. As an organization can be a customer from another organization that provides a service, it is possible to create chains and even networks.

Business services are the driving force behind the **flow of value** in the InterConnect ecosystem. As the functionality offered by a service provider is of value to a customer, there is a flow of value from the service provider to the customer. If the customer pays for the service, there is a monetary flow from the customer to the service provider. If the customer does not pay money, but – for example – sees ads, then there is also a flow of value from the customer to the service provider, but not a monetary one. In this example the service provider could

[41] https://en.wikipedia.org/wiki/Value_network#Value_configuration

transform this value into money by asking payment from customers that want to advertise something through the contact the service provider has with customer.

To get an idea of what services there can be in the InterConnect ecosystem here are some examples:

1. A '**Home Electricity Trading Service'** (for the electrical grid), where a customer is offered the functionality of automated trading of the electricity their home can produce using certain *devices* (e.g., PV panels or a home battery). Customers can configure the conditions (e.g., 'have the EV always charged to 80% first') under which they want to sell electricity. This type of service also includes optimization of electrical power usage in homes, to optimize return on investments for the homeowner.
2. A '**Certified Green Resource First**', where a customer is offered the functionality of only using electricity generated with renewables, within certain financial boundaries as configured by the customer. The customer receives bills with the ability to check the certification.
3. A '**Building Access Control'** service, where a customer is offered the functionality of remote monitoring and control of locks of a building. Customers can configure which persons have access to the building.
4. A '**Economical Electrical Pool Heating'** service, where a customer is offered the functionality of getting their pool heated for a relatively low amount of money. The customer accepts that it can take a while sometimes before the pool is heated to the desired temperature. This allows organizations like DSOs, and TSOs to optimize the flow of electricity on the grid in time.
5. A '**Green and Healthy Air**' service, where a customer is offered the functionality of conditioning the air in a building in such a way that it is in a desired temperature range, while at the same time it is ensured that build-up of pathogens (e.g., fine dust, COVID19, etc.) is stopped.

Annex III. DERIVING ARCHITECTURAL VIEWPOINTS

This Annex provides a high-level description of how the Smart Energy Reference Architecture (SERA, see section 4.2) and Smart Home/Building IoT Reference Architecture (SHBIRA, see section 4.3) viewpoints in the Secure interoperable IoT smart Home/Building and smart Energy system Reference Architecture (SHBERA, see section 4.1) were derived from requirements and existing state of the art reference architectures and models.

1. Deriving the SERA

This section describes the method 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:

1. Collect Use Cases and analyse.
2. Create time sequences of information exchange.
3. Generalize of architecture components
4. Validate results with use case analysis
5. Create a structure by separation of concerns

1.1 Step 1: Collect use cases and analysis

This first step includes the compilation of the 'Lisbon Use Cases' (WP1) focusing on smart grids[42]. 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

[42] 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.

1.2 Step 2: Create time sequences of information exchange

Collecting WP1 use cases allowed for identifying a set of actors, their actions and time sequences of their interactions. The IEC standard IEC 62559-2 served as a starting point for defining the structure of a standardised use case template[43], 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 14 depicts an example of the description of a step in a sequence diagram step table.

3.1 Steps – Normal Sequence

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

FIGURE 14 – 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 15, depicting a possible market design interaction scheme. Another example is from the Portuguese pilot, shown in Figure 16.

43 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.

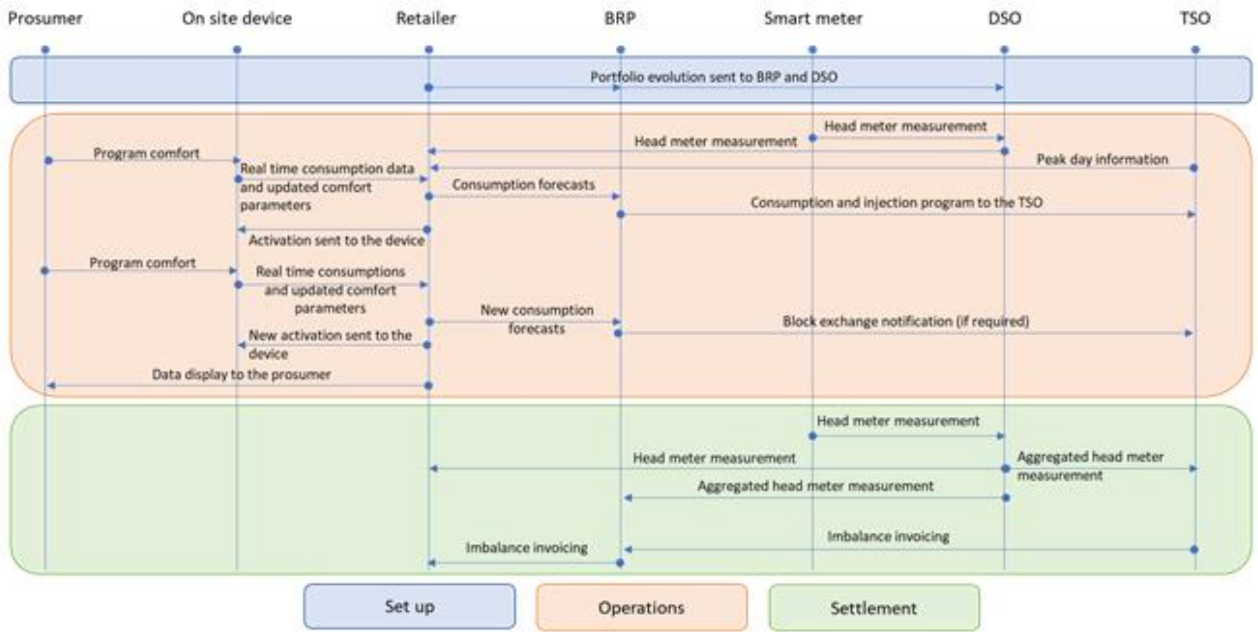

FIGURE 15 – USE CASE SEQUENCE DIAGRAM FROM THE FRENCH PILOT

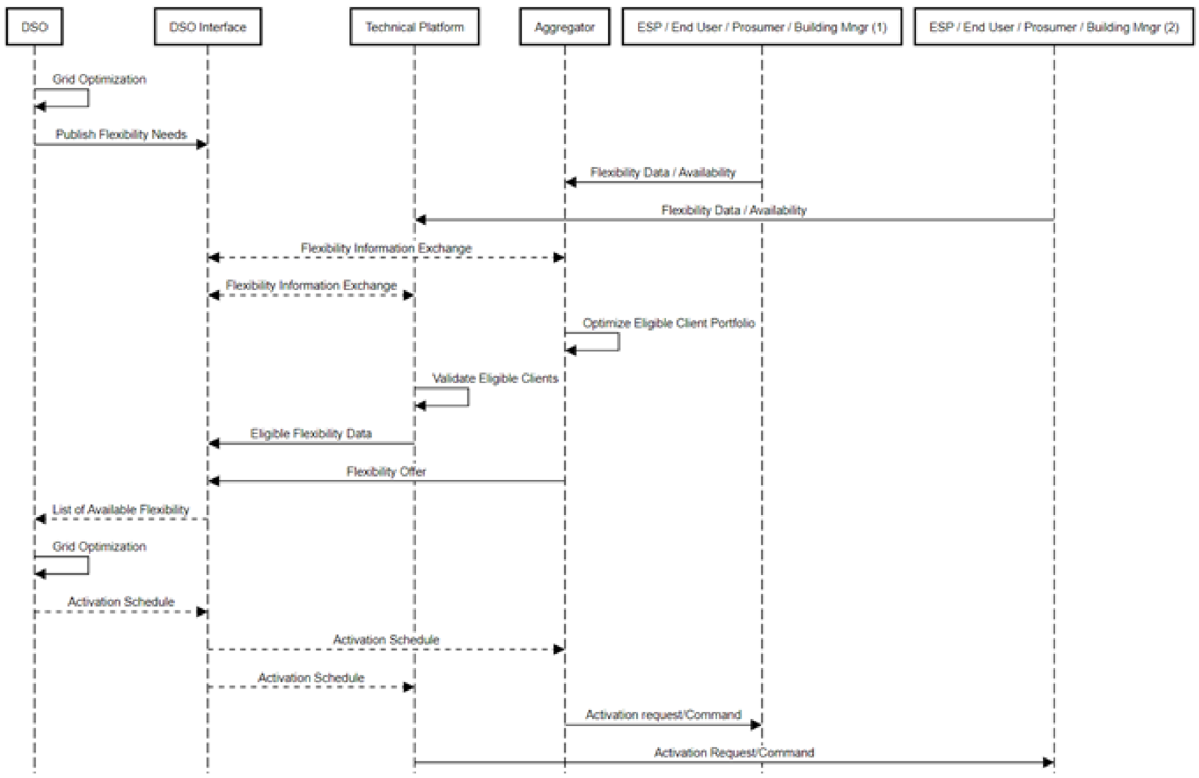

FIGURE 16 – USE CASE SEQUENCE DIAGRAM FROM THE PORTUGESE PILOT

Use Cases from all seven pilots were analysed by looking at different aspects, and textual descriptions were modelled into time sequences. An example of such an analysis ‘table’ is shown in Figure 17. The structure of that table, based on the IEC standard, was extended to include the following aspects/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 measu	Unlikely	TSO etc	DSO	DSO Smart Meter data
20	Settlement	DSO	BRP	Aggregated head meter measu	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 17 – EXAMPLE TABLE OF USE CASES WITH ASPECTS FOR ARCHITECTURAL 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 have been presented in tables in section 4.2.2.

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 18) into components of an architecture 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).

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 18 – EXAMPLE OF DEVICE INFORMATION SUBTYPE INFORMATION EXCHANGE

1.4 Step 4: Validate results with 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). See Figure 19 for a visual overview of the analysis.

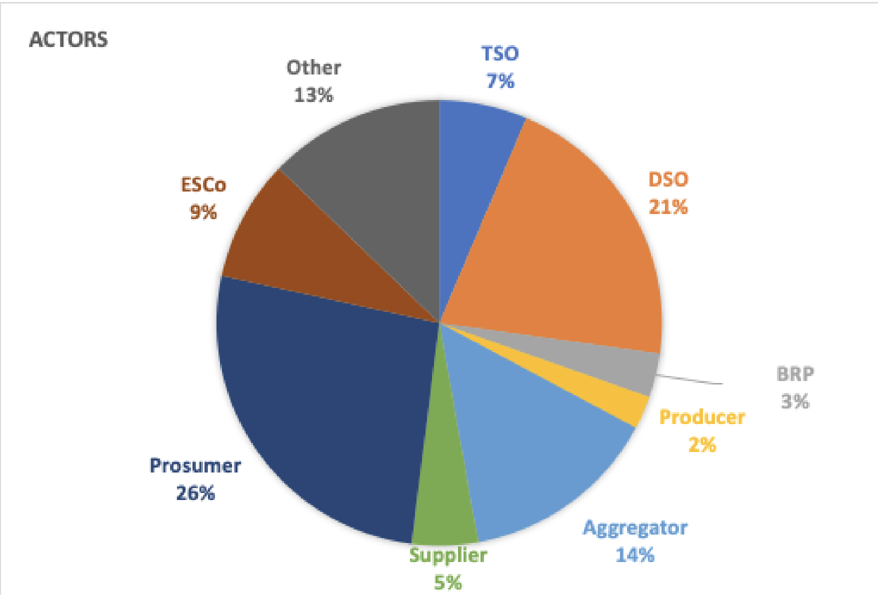

FIGURE 19 – ACTOR REPARTITION ANALYSIS (BASED ON WP1 USE CASES)

1.5 Step 5: Create a structure by separation of concerns

In step 5 the generalized architectural components from step 3 were spatially ordered and grouped in domains for providing structure and overview. An important ordering principle for the placing of components in a domain was the separation of concerns. Components within one domain tend to share more things with each other (e.g., physical location, interests, a reference framework, etc.) than with components in other domains. This also pertains to the exchange of information.

2 Deriving the SERA

This section describes the method that was used for deriving Smart Home/Building IoT Reference Architecture (SHBIRA). It consists of five steps:

1. Collect Use Cases and analyse.
2. Compare with an overview of existing IoT architectures.
3. Identify key functionality in layers
4. Identify the flow of information
5. Distribute physical components

This method can to a certain extent also be associated with the layers of the Smart Grid Architectural Model (SGAM, see section 2.8) from the **Erreur ! Source du renvoi introuvable.**. It therefore not only is based on existing IoT architectures, but also tries to align with the domain of Energy as much as possible. Where relevant the association will be mentioned in describing the steps below.

2.1 Step 1: Collect use cases and analysis

As the SBHIRA should provide a point of view on the same ecosystem as the SERA does, Use Cases were collected in the same way as for the SERA. See section 2.1.1 above in this annex. This step – where information from project stakeholders was collected - can be associated with the Business Layer of SGAM: the architecture should support their business.

2.2 Step 2: Compare with an overview of existing IoT architectures

To avoid reinventing the proverbial wheel, the collected information and Use Cases in step 1 were compared to what was described in existing IoT architectures (see section 2). This step can also be associated with the Business Layer of SGAM: the architecture should support their business.

2.3 Step 3: Identify key functionality in layers

With the Use Cases and information from stakeholders in mind and after the comparison with existing IoT architectures, key functionality of components was inferred and identified.

This step can be associated with the Function Layer in SGAM, 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.

2.4 Step 4: Identify flow of information

After key functionality was identified the flow of information between components could be determined in step 5, by looking at the nature of the information exchanges between the different architectural components, functions, and services.

This step can be associated with the overall objective and representation of the Information Layer in SGAM and with the Communication Layer.

2.5 Step 5: Distribute physical components

As the SHBIRA is a point of view from the Internet of Things perspective, the physical distribution of components is important: are they located in a home or building or are they 'in the cloud'. This determines their relative position to the Internet (infrastructure). Two domains were added to the layered functionality, and the physical distribution of all participating components was inspected, including the key services, actors and applications that need to be made interoperable within the large-scale pilot demonstrators.

This step can be associated with the Component Layer in SGAM.

Annex IV. ONTOLOGY USAGE AND REASONING SUPPORT

This annex discusses the usage of ontologies and the closely related support for reasoning. It serves as a backdrop for sections 4 and 5.

1. Ontology usage level

In the InterConnect ecosystem components exchange of information and/or knowledge using a shared understanding of (semantic) concepts which are documented in the InterConnect set of ontologies. The full (initial) set will be published in D2.3 at the end of December 2021. The Smart Applications REFerence (SAREF) suite of ontologies created and maintained by ETSI[44] since 2015 will be such a quintessential part of that set that transforming existing interface of service providing components has been named 'SAREFization' (also see 5.2.1). In the remainder of this section, the abbreviation ICSO for the InterConnect Set of Ontologies (ICSO) is used to explicitly show that not all semantic concepts in InterConnect are part of SAREF.

When analysing an ecosystem of information exchanging components, multiple levels of usage of ontologies can be discerned. Below is a ladder of compliance with respect to the usage of the ICSO:

1. **Level 0: no ICSO compliance.** That is, the ISCO is not used at all.
2. **Level 1: basic ICSO compliance.** That is, the ICSO is considered and an explicit mapping of component internal information models to ICSO exists via a document, such as a textual file, a table, or a spreadsheet[45]. Note that this type of mapping, however, is not automated nor directly machine processable, but requires manual human interpretation.

[44] 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.

[45] See for example the mappings in the form of a look-up table elaborated during the first Smart appliances study for the European Commission [10], also available as a more detailed mapping spreadsheet at https://sites.google.com/site/smartappliancesproject/documents

3. **Level 2: intermediate ICSO compliance.** That is, not only is the ICSO considered, but machine interpretation is also carried out. For example, data that is already encoded in a certain format (e.g., XML or JSON) can be annotated (labelled) using concepts (from the ICSO) in RDF/OWL. In this way, the mapping to the ICSO becomes machine processable, as an automated script, for example, can be used to convert the original data format into ICSO compliant RDF/OWL triples.

4. **Level 3: full ICSO compliance.** That is, direct use of ICSO concepts in RDF/OWL. A SAREF-compliant file in RDF/OWL exists and it is fully machine interpretable so a reasoner can be used, as described in the next section.

InterConnect targets at level 3 ICSO compliance for reasoner support and to be able to connect to systems having level 2.

1.1 Reasoning support

Part of the functionality of the Semantic Interoperability Layer (SIL, see section 4.5) in the SHBERA is the ability to automatically reason. In InterConnect two types of reasoning can be identified:

1. **To infer new knowledge:** making knowledge explicit (in terms of stored predicate logic statements) that was implicitly there already, using ontologies and semantic web technologies, such as RDF, OWL and SPARQL. When talking about (semantic) reasoning in the context of the Semantic Web, often this refers to inferring knowledge. Detailed information on this type of reasoning can be found in the white paper on semantic interoperability by AIOTI [10]. A concrete example of inference:

    a. general rule: Electric Vehicles (EV) need to charge if empty

    b. statement: a specific EV called 'Elom' is empty.

    c. Inferred knowledge: the EV called 'Elom' needs to charge

2. **Reasoning for orchestration:** determining which knowledge from which components needs to be exchanged according to the rules and logic stored in (a part of) the InterConnect SIL. This is – at the level of ICT - about the orchestration of data exchange in a distributed environment where data 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[46].

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 SIL. 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.

As with the levels of usage of the ICSO in the previous section, it is also possible to determine the level of reasoning support:

1. **Level 0: no reasoning support.** With reasoning support, we mean reasoning based on.
2. **Level 1: basic reasoning to infer new knowledge**. 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.
3. **Level 2: advanced reasoning to infer new knowledge**. 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.
4. **Level 3: additional reasoning to orchestrate data exchange** 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 knowledge bases (i.e., distributed data sources), which can be associated with devices, services or IoT 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.

[46] 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.

Level 3 in OCSI 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 ICSO.

Annex V. SEMANTIC SOLUTION SELECTION

This annex provides a description of the selection process of semantic solutions that was needed to determine which components should be in the Semantic Interoperability Layer (SIL, see section 4.5 and 5.

Different semantic solutions from different parties have different levels of support of the usage of ontologies and reasoning (also see Annex III). This required the InterConnect project to make an informed choice by means of a comparative analysis.

1. Request for information template

This section presents the template that has been used to collect information on the available semantic solutions among InterConnect partners. As this was still relatively early in the project the abbreviation SAREF was used as a 'pars pro toto' for the InterConnect Set of Ontologies (ICSO) which construction was carried out later in the project.

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 considered and an explicit mapping to SAREF exist via a document, such as a textual file, a table or a spreadsheet[47]. 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 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.?*

[47] See for example the mappings in the form of a look-up table elaborated during the first Smart appliances study for the European Commission [11], also available as a more detailed mapping spreadsheet at https://sites.google.com/site/smartappliancesproject/documents

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 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.*

TABLE 21 – AVAILABLE SEMANTIC SOLUTIONS TEMPLATE

1.1 Information collected

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 implemented and tested. We analyse these solutions based on the high-level requirements specified in Section 3.2 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 presented above.

1.2 The knowledge engine (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 can interconnect different Knowledge Bases (KB), which are depicted in Figure 20 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[48] 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 20. The knowledge is exchanged using a combination of SPARQL[49] and RDF messages that refer to SAREF concepts.
Semantic Components Description	• **Smart Connectors:** Figure 8 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). It further shows that the mapping to/from SAREF occurs within the interoperability framework. This mapping is realized by the SCs,

[48] Basic Graph Pattern (BGP), see https://www.w3.org/TR/sparql11-query/#BasicGraphPatterns
[49] Basic Graph Patterns (see above) and SPARQL Result Set in JSON (https://www.w3.org/TR/sparql11-results-json/).

	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[50] 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.
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[51] and RDF[52]).
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[53], Java Messaging Service (JMS[54]), SPARQL[55] and RDF[56].
Security and Privacy	The Knowledge Engine uses Ontology-Based Access Control (OBAC) [5] 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).

[50] Apache Jena GenericRuleReasoner, https://jena.apache.org/documentation/inference/#rules
[51] https://www.w3.org/TR/sparql11-query/
[52] https://www.w3.org/TR/rdf11-concepts/
[53] https://en.wikipedia.org/wiki/HTTPS
[54] https://en.wikipedia.org/wiki/Java_Message_Service
[55] https://www.w3.org/TR/sparql11-query/
[56] https://www.w3.org/TR/rdf11-concepts/

Accessibility and License	The KE is freely available and open source.
Strengths	• **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
Weaknesses	• **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 22 – SEMANTIC SOLUTION: TNO/VU'S KNOWLEDGE ENGINE

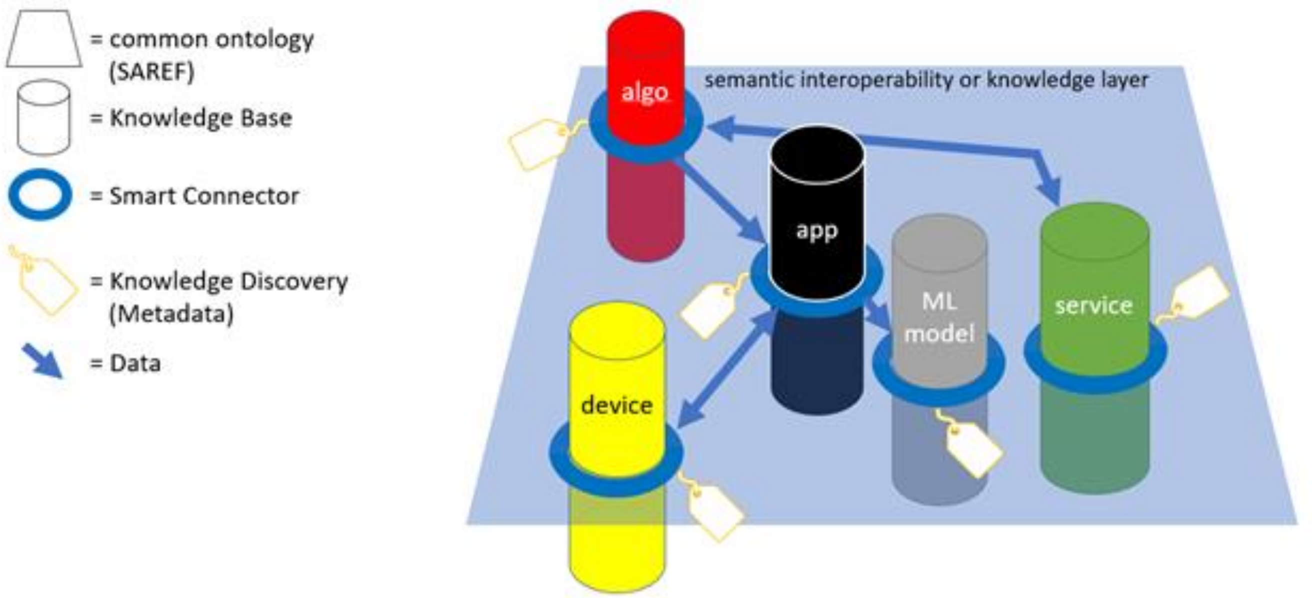

FIGURE 20 – VISUAL OVERVIEW OF THE KNOWLEDGE ENGINE

1.3 WOT Framework (KEO, DFKI, DORTMUND, 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 21). 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 22 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 23 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 require 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.
Security and Privacy	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.

Accessibility and License	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/.
Strengths	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 23 – SEMANTIC SOLUTION: WOT FRAMEWORK

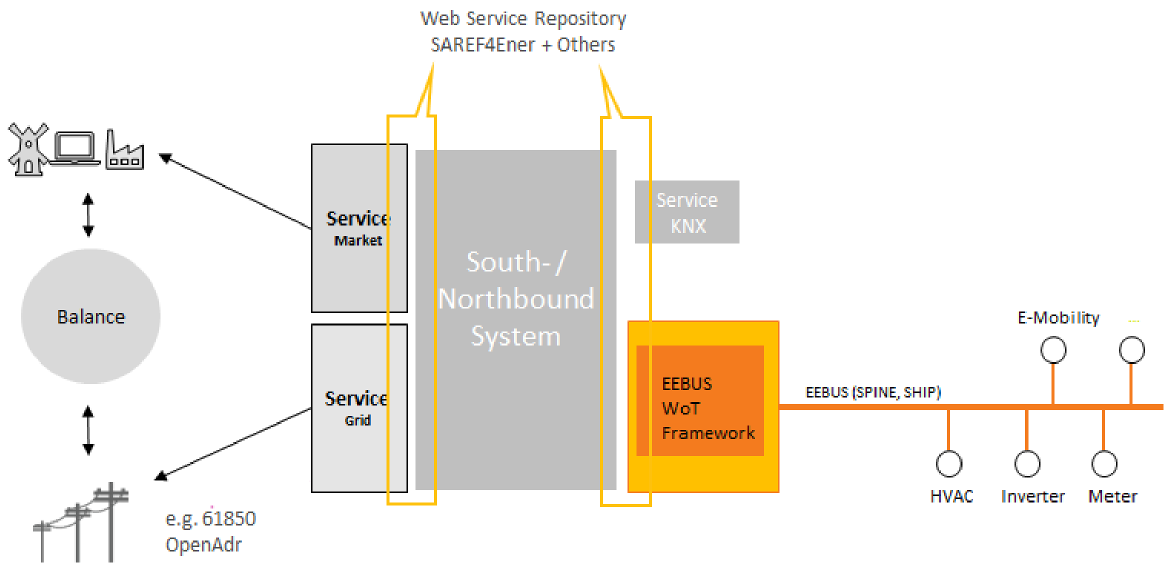

FIGURE 21 – VISUAL LOGICAL OVERVIEW OF THE WOT FRAMEWORK

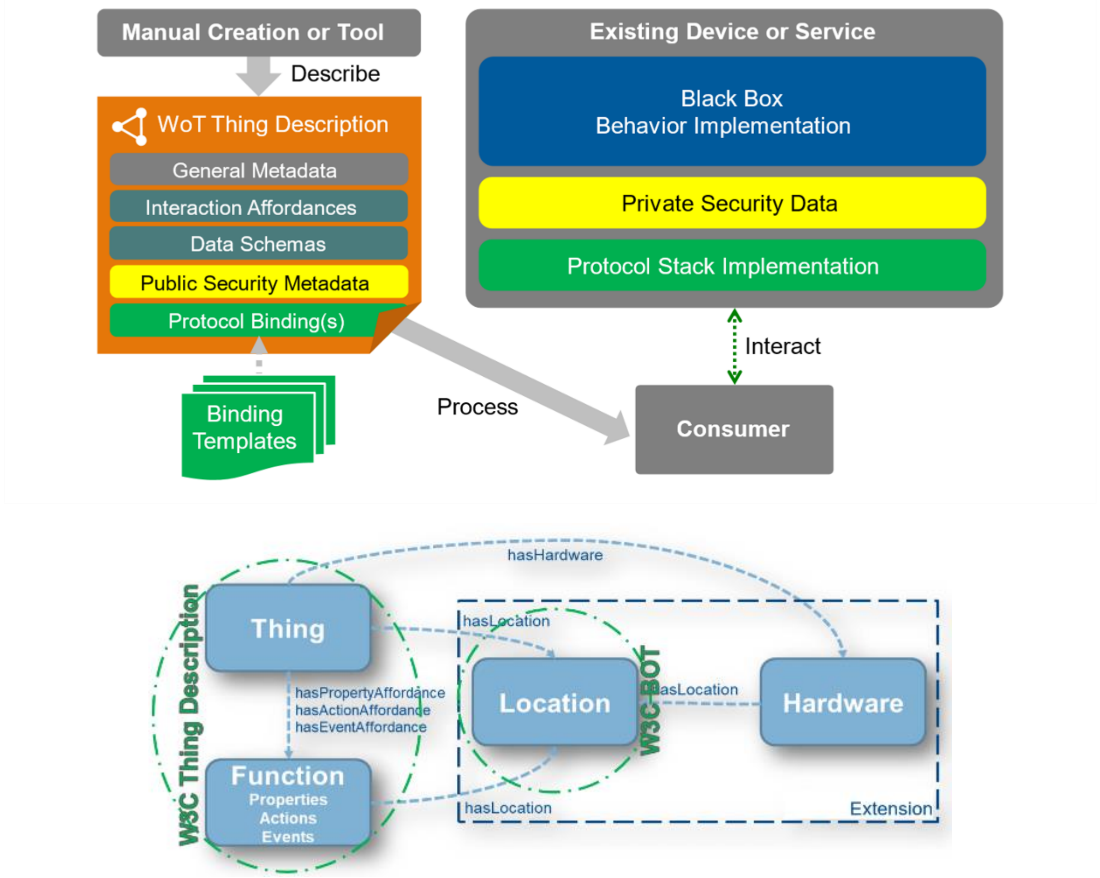

FIGURE 22 – VISUAL DATA ORIENTED OVERVIEW OF THE WOT FRAMEWORK

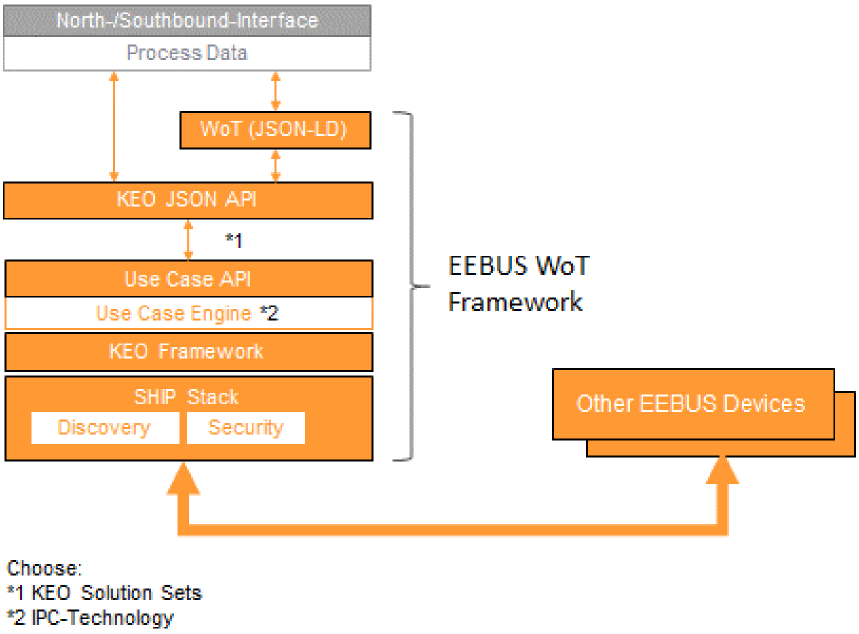

FIGURE 23 – VISUAL API STACK OVERVIEW OF THE WOT FRAMEWORK

1.4 IoT ontology (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 24 and reflected by an individual "model" for Location, Devices, Applications as well as the Communication for exchange of control information (depicted in Figure 25). All individual model parts together form the entire KNX IoT Information Model as a single ontology. Figure 25 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 24 – SEMANTIC SOLUTION: IOT ONTOLOGY FROM KNX

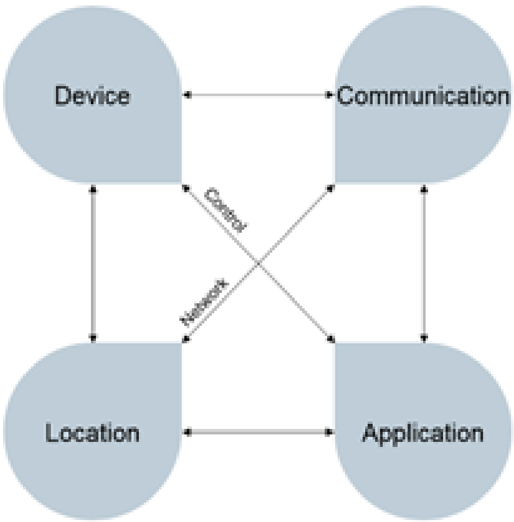

FIGURE 24 – VISUAL OVERVIEW OF IOT ONTOLOGY CONCEPTS

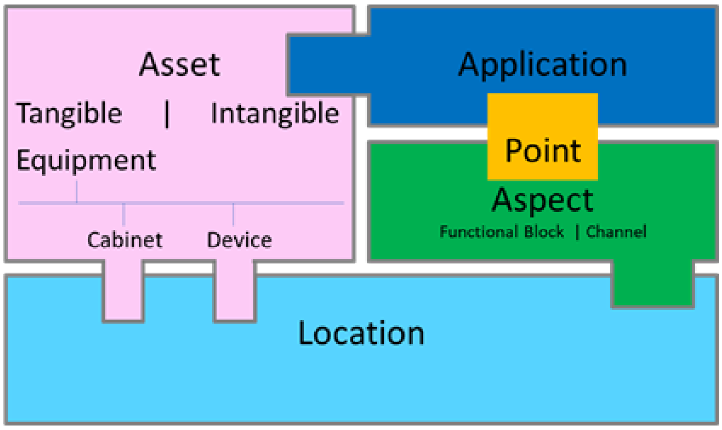

FIGURE 25 – VISUAL OVERVIEW OF THE HBES INFORMATION MOD

1.5 Sensor-based linked open rule (S-LOR) (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[57] (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

[57] See 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.

	reasoning/inference engine to interpret IoT data. The rule-based reasoning engine is compatible with the M3/M3-lite ontologies[58].
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 the figure 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[59] 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.

[58] More information can be found in: (1) 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. (2) 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.

[59] See (1) 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. (2) 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. (3) 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. (4) 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. (5) 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.

Semantic Components Description	The reasoning engine for IoT devices to infer meaningful information[60]. We can contribute as follows[61]: 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)[62] 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 26 explains each step of the Figure 27 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 considered, but machine interpretation is enabled).

[60] Derived from (1) 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. (2) 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. (3) 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. (4) 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.

[61] Also explained within the semantic interoperability for IoT white papers (1) 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. (2) 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.

[62] See (1) 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. (2) A. Gyrard and A. Sheth, "IAMHAPPY: Towards an IoT knowledge-based cross-domain well-being recommendation system for everyday happiness," Smart Health Journal, 2019.

<table>
<tr><td></td><td>The M3 ontology[63] can be considered as a SAREF extension with a focus on the concepts describing data generated by devices (saref:Device):
● 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</td></tr>
<tr><td>Supported data formats</td><td>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.</td></tr>
<tr><td>Supported standards and protocols</td><td>● 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.</td></tr>
<tr><td>Security and Privacy</td><td>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)[64] 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.</td></tr>
<tr><td>Accessibility and License</td><td>We have online demos[65]. S-LOR is under GNU GPLv3 license, a component of the M3 (Machine-to-Machine Measurement) framework. The are numerous publications describing the project[66]. In the INESC TEC presentation, they highlight the issues regarding Intellectual Property when a project is refined with several projects.</td></tr>
</table>

[63] http://sensormeasurement.appspot.com/?p=m3
[64] http://securitytoolbox.appspot.com/
[65] http://linkedopenreasoning.appspot.com/?p=slorv2
[66] http://linkedopenreasoning.appspot.com/?p=publication

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; ● 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 25 – SEMANTIC SOLUTION: S-LOR FROM TRIALOG

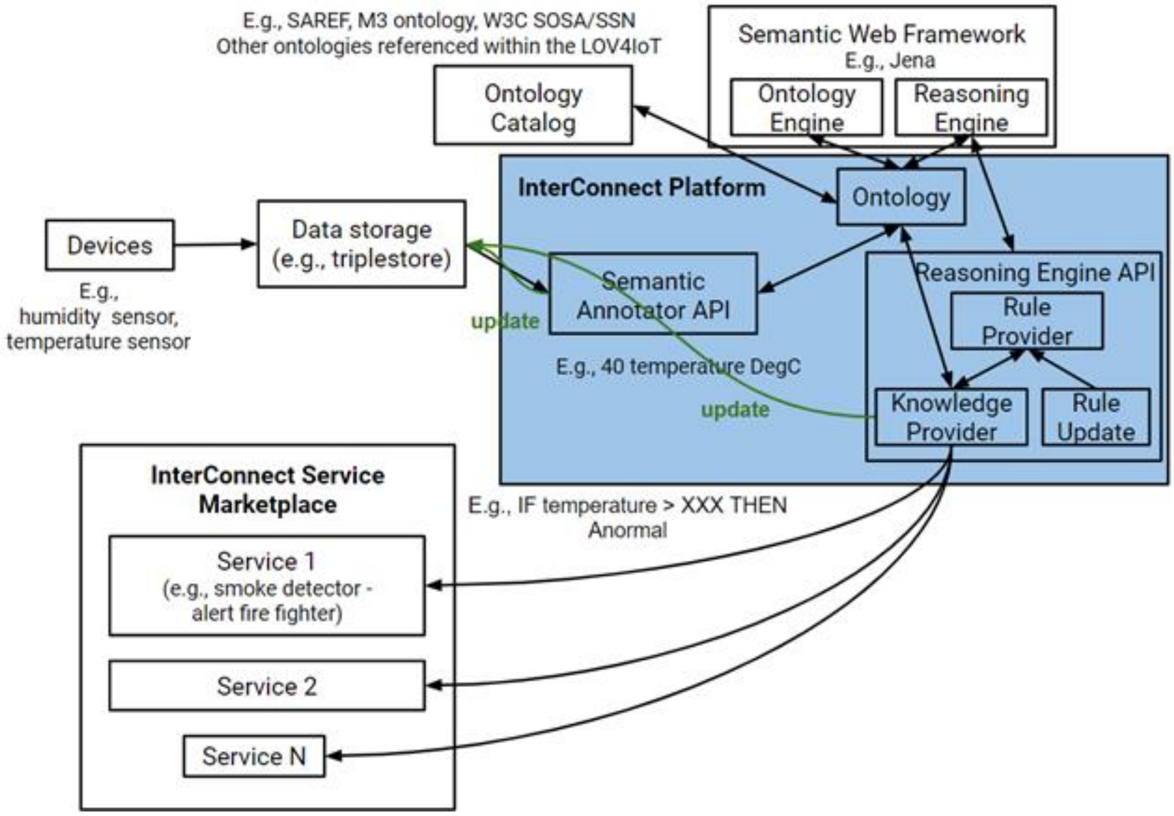

FIGURE 26 – ONTOLOGY-BASED REASONING IN S-LOR FROM SENSOR-DATA TO END-USERS

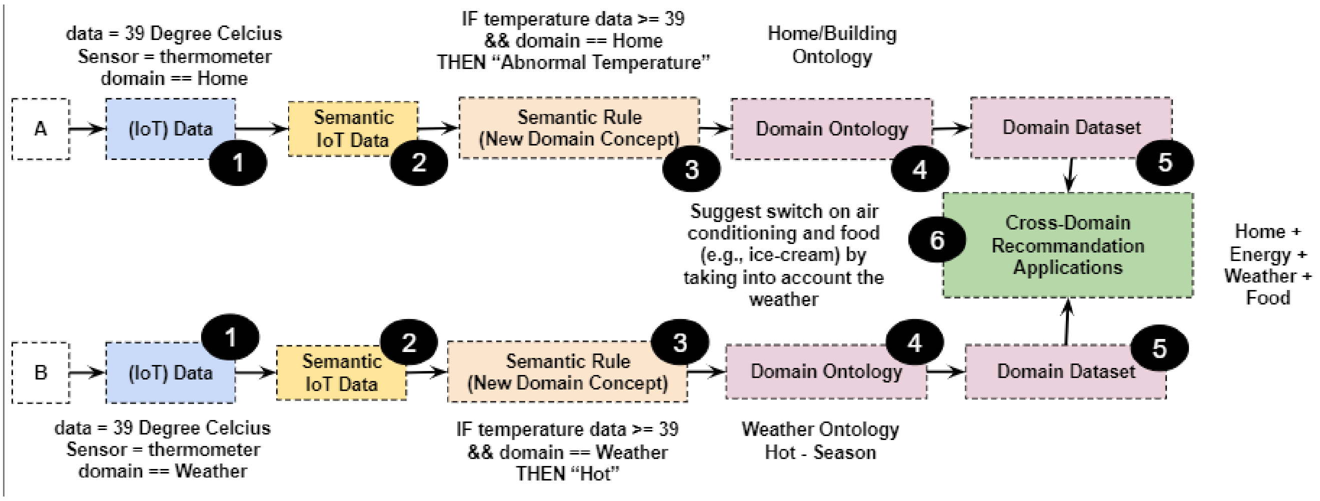

FIGURE 27 – CROSS-DOMAIN KNOWLEDGE/RULE-BASED REASONING ENGINE & DATA WORKFLOW IN S-LOR[67]

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

[67] See (1) A. Gyrard and A. Sheth, "IAMHAPPY: Towards an IoT knowledge-based cross-domain well-being recommendation system for everyday happiness," Smart Health Journal, 2019.

	conditions. The recommendations can be acted upon both by end-users and intelligent machines.

TABLE 26 – STEPS IN CROSS-DOMAIN KNOWLEDGE/RULE-BASED REASONING[68]

1.6 The Semantic Layer (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 28. 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. 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 using many different communication networks and protocols, provides storage facilities next to visualization and reporting functionalities. Whereas the IoT layer may provide syntactical

[68] Idem.

	interoperability between the physical world and the IT systems using 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 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 29. 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 27 – SEMANTIC SOLUTION: THE SEMANTIC LAYER FROM GFI

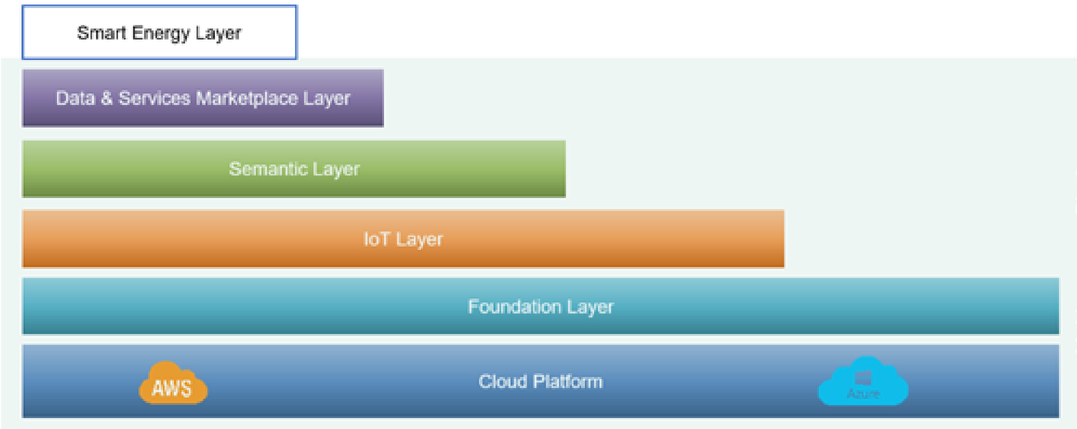

FIGURE 28 – GFI'S LAYERING FOR DATA SHARING

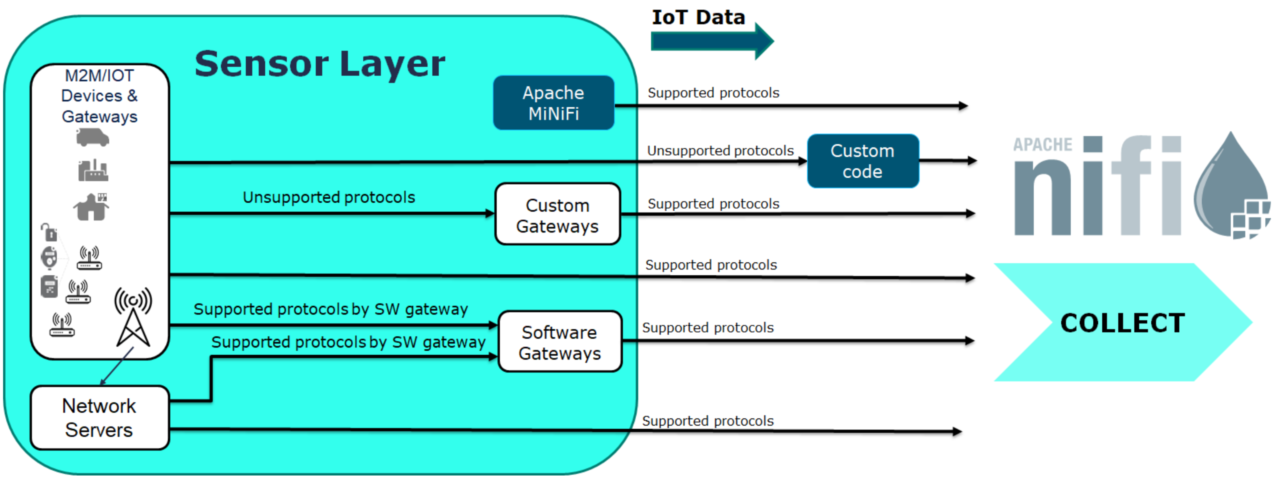

FIGURE 29 – INTERFACES IN GFI'S DATA SHARING SOLUTION

1.7 Building Operating System (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 30 and Figure 31: • 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 considered, 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 28 – SEMANTIC SOLUTION: BUILDING OPERATING SYSTEM FROM SENSINOV

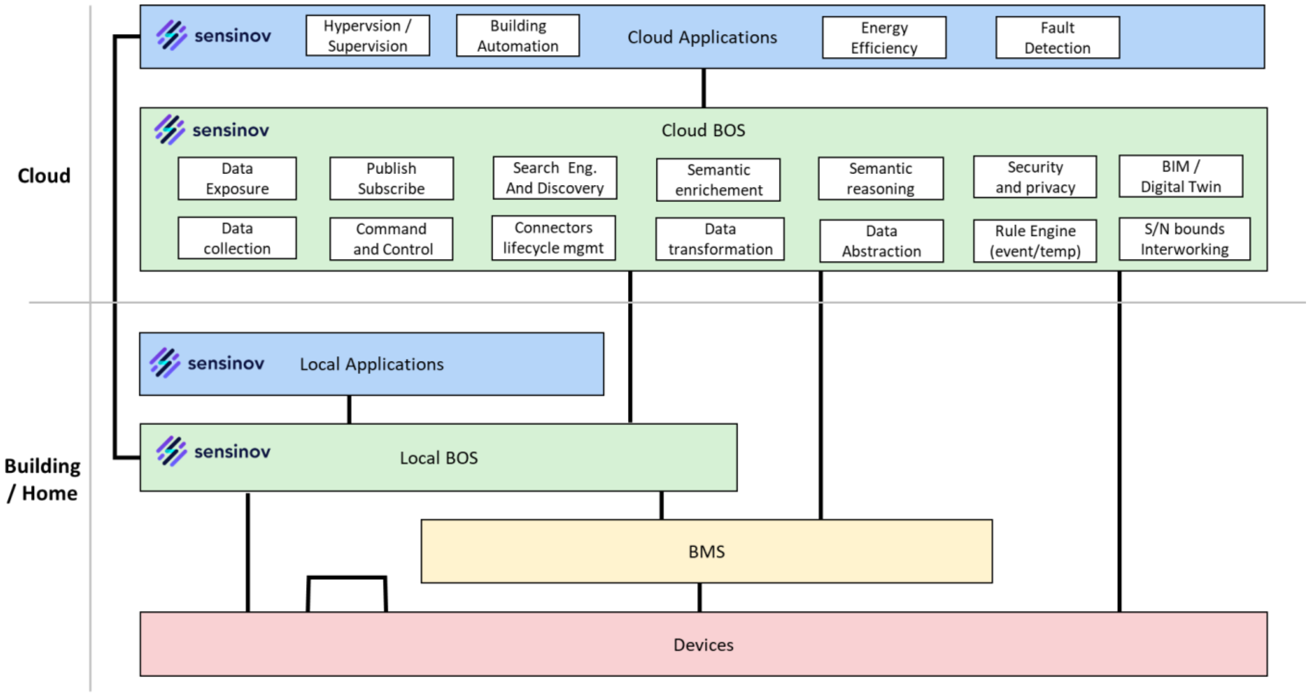

FIGURE 30 – FUNCTIONAL COMPONENTS IN THE BOS FROM SENSINOV

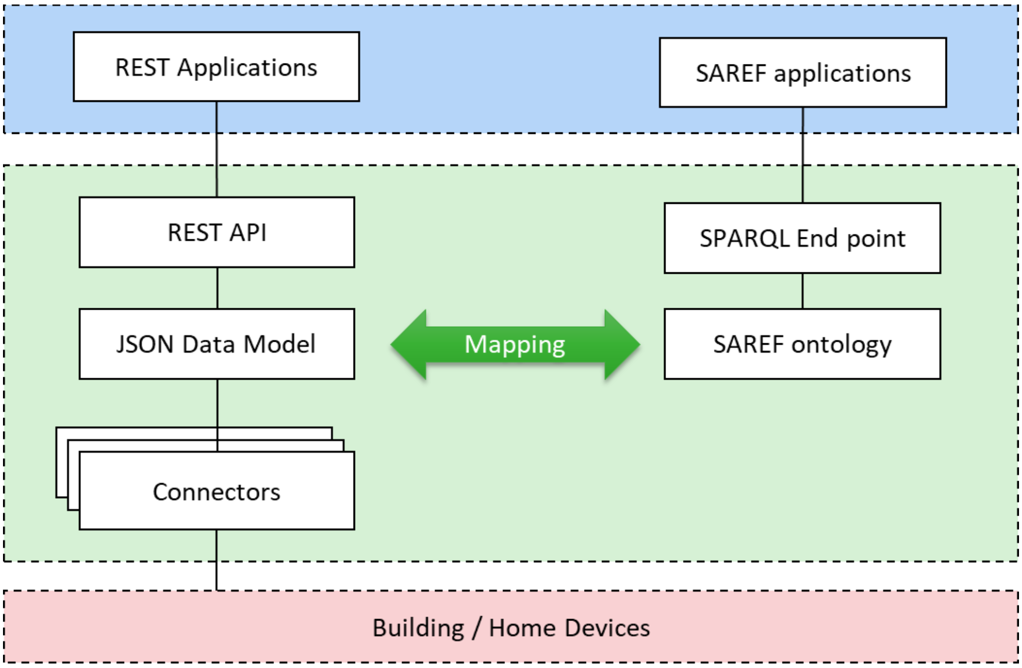

FIGURE 31 – BOS DATA MODEL AND MAPPING TO INTERCONNECT

1.8 Comparative analysis

After receiving information regarding the semantic solutions from different parties a comparative analysis was carried out. The characteristics of the solutions detailed in the previous section are summarized in Table 29.

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)[69]	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

[69] Note that the value between brackets denotes the maturity of the full commercial solution, while the maturity of the semantic aspects is featured with no brackets.

KNX	TRL4 (TRL9)[70]	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)[71]	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 commercialization 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 29 – COMPARISON OF SEMANTIC SOLUTION CHARACTERISTICS

In the following subsections observations can be made based on the previously received information and the table.

1.8.1 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 various Use Cases. 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, the maturity of the semantic solutions that the various consortium partners bring to InterConnect starts at TRL 4 to 5. A higher TRL level is required to use the solutions as a basis for (distributed) operational environments that go across vertical domains (silos) and are deployed

[70] Idem.
[71] Idem.

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).

1.8.2 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. 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 exchange of data.

1.8.3 ICSO/SAREF compliance

Compliance with SAREF is one of the requirements specified in InterConnect, 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. 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).

1.8.4 Data formats

As can be seen in Table 29, most of the solutions support JSON and often RDF and/or JSON-LD. Therefore, a mapping of these formats to RDF/OWL via adapters should be fairly straightforward. For an extensive analysis of the platforms available in InterConnect and their supported data formats, refer to D5.1 [14].

1.8.5 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, see InterConnect Deliverable D5.1 [14].

1.8.6 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 the semantic solutions are required to be 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.

1.8.7 Accessibility and License

If the specifications of the interoperability layer, the vocabularies, schemas, 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.

1.9 Conclusions

From the comparative analysis in the previous the following can be concluded:

1. The maturity of the semantic solutions that the various consortium partners bring to InterConnect starts at TRL 4 to 5. At the end of the InterConnect project this should have been brought to a higher TRL level, as the projects recommended semantic solution needs to be deployed in into a large-scale operational environment containing various InterConnect pilots.
2. 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.
3. Concerning ICSO compliance, the Knowledge Engine solution provided by TNO/VU is the only one to present the highest level (level 3), namely the potential direct use of ICSO (currently primarily SAREF) concepts expressed in Sematic Web standards such as RDF/OWL.
4. Most of the solutions support the use of the JSON data format; some solutions provide support also for Semantic Web standards such as RDF and/or JSON-LD; only the

Knowledge Engine solution by TNO/VU, in addition to Semantic Web support, provides (in theory) the flexibility to work with any data format via mappings.

5. 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 the use of adapters.
6. Commercially available solutions, such as those from KEO/EEBUS, KNX, GFI and SENSINOV, have a stronger security and privacy level than prototype solutions in small-scale demonstrators, such as those from TNO/VU and TRIALOG. However, none of the analysed solutions offers specifically support for security and privacy at the semantic level (which is offered by the underlying platforms). Therefore, the InterConnect project will have to actively include security and privacy by design as part of the recommended solution for the semantic interoperability layer.
7. 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.

1.10 Outcome

Based on this analysis, **the Knowledge Engine solution provided by TNO/VU has been selected by InterConnect as the recommended solution to implement the Semantic Interoperability Layer**, especially because it has been 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 grow to higher TRLs within and outside the InterConnect ecosystem, in an open and inclusive manner with respect to other technologies (from other parties).

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 above. They could be seen as complementary. For example, the WoT Framework from KEO et. al. could be adapted to the InterConnect requirements by only using SAREF for thing descriptions of EEBUS devices. The semantic solution proposed by KEO et al. is based on the WoT architecture and its Things Description (TD), which became a W3C recommendation in April 2020[72], also including 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 smart connectors. Another possibility is to let the Knowledge Engine 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 could also be adapted to fit he requirement of SAREF/ICSO compliancy, 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, while the Knowledge Engine provides the additional functionality of reasoning for the orchestration of data exchange.

Other semantic solutions that scored relatively high in the comparative 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.

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

Annex VI. THE SHBERA AND PILOT'S ARCHITECTURES

This annex describes the results of workshops (see 6.1.1) planned pilot architectures were analysed in terms of the SERA (section 4.2), SHBIRA (section 4.3) and IF (section 4.4) points of view present in the Secure interoperable IoT smart Home/Building and smart Energy system Reference Architecture (SHBERA, see section 4.1).

1. Method of mapping

The online collaborative tool "Miro"[73] 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. The remainder of this section describes these steps in more detail.

1.1 Collecting pilot architectures

Before the pilot architectures could be collected, high-level Use Cases for each (sub-)pilot in the scope of WP1 (see D1.1 [13]) had to described, so within WP5, pilot teams could work on the specification of overall system architecture. They would focus on digital platforms participating in the realization of the pilots/use cases and interfaces through which platforms communicate. This exercise also helped identify the first set of pilots' requirements for (semantic) interoperability, which was also used in the specification of the InterConnect Interoperability Framework (see D5.1 [14]).

1.2 Mapping to the SHBIRA

The collected (sub-)pilot architectures and available/planned resources were then mapped onto a so called 'High Level Architecture' (HLA) template based on the layering in the SHBIRA.

[73] https://miro.com/

The naming of the layers differed slightly in the sense that the Building/Home Management Systems (BHMS) layer in the SHBIRA was generalized into a broader concept of 'Communication' (gateway). This made it easier to map pilots that did not work with a BHMS. During the workshops pilot teams performed the following tasks:

1. **Map all key services in a Use Case** onto the corresponding Communication (gateway) and Application layers.
2. **Map all devices which will be used in the pilot** realization of Use Cases onto the Device layer.
3. **Indicate which services are required by the (sub-)pilots but are not provided by any of the participating pilot partners.** This could be an opportunity for pilots to use services from other pilots (e.g., 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.
4. **Identify interfaces between the system layers/resources that bypass the Semantic Interoperability layer** and what communication will be based on legacy interfacing technology.

1.3 Mapping to the SERA

After mapping pilot architectures to the SHBIRA point of view, the collected (sub-)pilot architectures and available/planned resources were mapped onto to the SERA. Pilot teams performed the following tasks:

1. **Map resources/devices to the area of Devices** in the domain of Smart Home/Buildings.
2. Indicate where main **actors** and **business roles** within the pilots should be in terms of SERA domains.
3. Indicate the main **services** that actors offer related to the usage of devices/resources.
4. If available, indicate the **information objects** that are exchanged (e.g., between service and devices).
5. Identify missing links and relationships within the SERA from a pilot architecture Energy system perspective.

1.4 Mapping to the IF

After mapping pilot architectures to the SERA point of view, the collected (sub-)pilot architectures and available/planned resources were mapped onto to the IF. Pilot teams performed the following tasks:

1. **Identify each (sub-)pilot service (available or to be developed) to be made semantically interoperable (in the scope of WP3).** Also determine what current communication interfacing technologies are used by these services to interoperate with other endpoints/components and what specific access control rules have already been defined for these services;

2. **Map interoperable services onto the different digital platforms** that host them.

3. **Identify devices to be made semantically interoperable** by adapting the semantic interoperability adapter provided by WP5.

4. Decide if the **(sub-)pilot will utilize p2p marketplaces** for the realization of its use cases.

5. Decide if the **(sub-)pilot requires the instantiation of the InterConnect service store** at the level of the pilot or can and will utilize a service store instance on the level of the project.

6. Decide **which of the mapped interoperable services can be provided as a downloadable container** (i.e., Docker).

1.5 Consolidation using the SHBERA

After the workshops, the different architectural viewpoints for each of the pilots were consolidated using the SHBERA. using a table template based on the SHBERA as shown in Table 30. Each pilot's output was mapped onto this uniform table for further analysis and discussions.

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

<table>
<tr><td>Application</td><td>Users of provided applications and services</td><td>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</td><td>Energy services
Energy services comprising/enabling the pilot.
Services to be provided by external partners are underlined</td><td rowspan="2">Transmission System
Key resources and services from TSO domain</td></tr>
<tr><td>Semantic Interoperability</td><td></td><td colspan="2">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)</td></tr>
<tr><td>Communication (gateway)</td><td></td><td colspan="2">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</td><td rowspan="2">Distribution System
Key resources and services from DSO domain</td></tr>
<tr><td>Device</td><td>Users/owners of devices</td><td>Inside Building
Devices/appliances/ resources available inside home/building</td><td>Outside Building
Resources/devices residing outside of a building or towards DSO</td></tr>
</table>

TABLE 30 – TABLE TEMPLATE FOR CONSOLIDATING PILOT ARCHTECTURE SHBERA MAPPINGS

2 Mapping results

In the next sections tables are presented which contain the consolidated information from the steps described in the previous sections. Additional details about the pilot Use Cases can be found in InterConnect Deliverable D1.1 [13], while more details about the pilot's architecture and interoperability requirements can be found in InterConnect Deliverable D5.1 [14].

Please note that some changes and updates to the presented mappings are possible until the pilots start their execution, since some of the InterConnect pilots are still being specified and negotiated due to new insights that appear during collaboration

2.1 France

This pilot – led by YNCRÉA - 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 InterConnect Deliverables D5.1 [14] and D1.1 [13].

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 advice** (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)
Semantic Interoperability		**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.		
Communication (gateway)		**Building Communication and IoT Gateway Layer** • ENGIE EMS • ThermoVault EMS • Metering data platform • Remote control of appliances		**Distribution System** • Smart meter & adapter services (ENEDIS) • Linky
Device		**Inside Building** • PV • Whitegoods • Control devices • Heaters • Hot water tank • Heat pump • ThermoVault endpoint	**Outside Building** • Electric Vehicles • EV Charging Point • Linky and sensors	

		• ENGIE endpoint		

TABLE 31 – SHBERA MAPPING FOR THE FRENCH PILOT

The French pilot is not planning on using services from other pilots. Details about access control mechanisms for interoperable services would be decided later, during pilot preparations. Many of the listed services are either provided or will be developed and managed by multiple participating partners.

2.2 Belgium

The Belgian pilot has eight sub-pilots; each has with its lead partner, participating digital platforms and interoperability requirements:

1. Cordium Hasselt and Thor Park Genk – led by VITO.
2. Student Rooms Antwerp – led by IMEC.
3. Smart District Nieuwe Dokken Gent – led by Ducoop and OpenMotics.
4. Zellik Green Energy Park Brussels – led by VUB.
5. Nanogrid Leuven – led by TH!NK-E.
6. Oud-Heverlee public buildings – led by 3E.
7. Genk apartments - led by Thermovault.

2.2.1 Cordium Hasselt and Thor Park Genk

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 InterConnect Deliverables D5.1 [14] and D1.1 [13].

Layer (HLA)	Domains (SERA)			
Stakeholders	**User** • DHN/HP/ Turbine owner (Cordium) • Social housing company (Cordium)	**CCC services (actors)** • Site operator (Imtech)	**Energy services (actors)** • Energy service provider (VITO) • Technical aggregator (VITO)	**Energy System** • Energy retailers
Application	• Apartment tenant	**CCC services** • BEMS application	**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	**Transmission System**
Semantic Interoperability		**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.		
Communication (gateway)		**Building Communication and IoT Gateway** • Heating Substations Management System • BMS (Metasys) • IoT Gateway / PLC • BEMS / IoT Gateway		**Distribution System**
Device		**Inside Building** Heating sub-stations • Electric heaters • Smart washing machine • Smart dryer • Apartment meter • Apartment sensors	**Outside Building** • District Heating Network • Rooftop wind turbine • PV(-T) inverter • Borehole Thermal Energy Storage • Heatpumps • Large water buffers	

TABLE 32 – SHBERA MAPPING FOR THE BELGIUM CORDIUM HASSELT BELGIUM SUBPILOT

VITO, the pilot leader, envisions using three semantically interoperable services provided by other partners (underlined in Table 32). 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.

Layer (HLA)	Domains (SERA)			
Stakeholders	**User** • Public EVSE operator • Building Manager EnergyVille1 • Building Manager Incubator	**CCC services (actors)** • BMS operator	**Energy services (actors)** • Energy service provider (VITO) • Technical aggregator (VITO)	**Energy System** • Energy retailers
Application		**CCC services**	**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	**Transmission System**
Semantic Interoperability		**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.		
Communication (gateway)		**Building Communication and IoT Gateway Layer** • EVSE management system • BMS Incubator • BMS EnergyVille1		**Distribution System**
Device		**Inside Building** • PV and PV submeter EnergyVille1 • EnergyVille1 grid connection meter • Cooling HVAC Thor Central • EVSEs EnergyVille1	**Outside Building** • EVSEs Thorpark	

TABLE 33 – SHBERA MAPPING FOR THE BELGIUM THORPARK BELGIUM SUBPILOT

The Pilot leader is planning to use a carbon intensity forecasting service as a semantically interoperable service, which the pilot could use if provided by other partners/pilots.

2.2.2 Student Rooms Antwerp

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. 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 InterConnect Deliverables D5.1 [14] and D1.1 [13].

<table>
<tr><th>Layer (HLA)</th><th colspan="4">Domains (SERA)</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 34 – SHBERA MAPPING FOR THE BELGIUM STUDENT ROOMS ANTWERP BELGIUM SUBPILOT

2.2.3 Smart District Nieuwe Dokken Gent

This sub-pilot aims to manage and operate a large, primarily residential, Local Energy Community in Ghent. The goal is to bring 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 InterConnect Deliverables D5.1 [14] and D1.1 [13].

Layer (HLA)	Domains (SERA)			
Stakeholders	**User** • Building owner • EV driver • Resident	**CCC services (actors)**	**Energy services (actors)** • ESCO	**Energy System**
Application		**CCC services (OpenMotics)** • Heatpump control • Battery control • Charging station control • District heating control	**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)	**Transmission System**
Semantic Interoperability		**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		
Communication (gateway)		**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)		**Distribution System** • Digital meters
Device		**Inside Building** • Heat pump (BlueHeat) • Battery (Battery Supplier) • District heating (Callens) • Whitegoods	**Outside Building** • EV Charging Station(s) (Powerdale) • Digital heat/calory meter • Digital Meters • Weather station (Davis Instruments) • Solar panels (Linea Trovata)	

TABLE 35 – SHBERA MAPPING FOR THE NIEUWE DOKKEN GENT BELGIUM SUBPILOT

2.2.4 Zellik Green Eenrgy Park Brussels

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 the (sub)pilot's functional architecture, goals and high-level use cases can be found in InterConnect Deliverables D5.1 [14] and D1.1 [13].

<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 36 – SHBERA MAPPING FOR THE ZELLIK GREEN ENERGY PARK BELGIUM SUBPILOT

This (sub-)pilot was in an early stage of specification. More detailed mapping (especially to the interoperability framework architecture) would be provided as the pilot team would progress with definitions.

2.2.5 Nanogrid Leuven

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 InterConnect Deliverables D5.1 [14] and D1.1 [13].

Layer (HLA)	Domains (SERA)			
Stakeholders	**User** • Energy community member • (Volunteers) participating in the Energy Community	**CCC services (actors)** • Energy Community Service Provider	**Energy services (actors)** • Project-level Service Provider • i.Leco as technical aggregator • Energy community service provider	**Energy System** • DSO/TSO (organizer of flex market)
Application		**CCC services** • User application with configuration parameters and preferences	**Energy services** • Flexibility service • Grid Energy Forecasting • Local Flexibility Market • Local energy forecasting • Derive available (aggregated) flexibility • Weather forecasting	**Transmission System**
Semantic Interoperability		**InterConnect interoperability layer** • Semantically interoperable services - Aggregator of local flexibility (TBD) • Access control mechanisms and service containers - TBD • P2P Marketplace - YES		
Communication (gateway)		**Building Communication and IoT Gateway Layer** • BMS (i.Leco, outside of Consortium)		**Distribution System** • Local Electricity Grid on DC voltage • Energy meter
Device		**Inside Building** • Energy devices (PV, heat pump , whitegoods, energy storage, hydrogen fuel cell, hydrogen boiler) • Sensors (temperature, humidity and motion)	**Outside Building** • EV (V2G) • Local Electricity Grid on DC voltage • Energy meter	

TABLE 37 – SHBERA MAPPING FOR THE NANOGRID LEUVEN PARK BELGIUM SUBPILOT

This (sub-)pilot was in an early stage of specification. More detailed mapping (especially to the interoperability framework architecture) would be provided as the pilot team would progress with definitions.

2.2.6 Oud-Heverlee Public Buildings

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 InterConnect Deliverables D5.1 [14] and D1.1 [13].

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 38 – SHBERA MAPPING FOR THE OUD-HEVERLEE PUBLIC BUILDINGS BELGIUM SUBPILOT

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.

2.2.7 Genk

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 InterConnect Deliverables D5.1 [14] and D1.1 [13].

Layer (HLA)	Domains (SERA)			
Stakeholders	**User** • Residential consumers and members of the local energy community	**CCC services (actors)**	**Energy services (actors)** • Energy management orchestrator (TBD) • EV aggregator (TBD) • Whitegoods aggregator (TBD) • PV forecaster (TBD) • Water heater aggregator (ThermoVault)	**Energy System** • Real time pricing provider
Application		**CCC services** • Thermal loads energy efficiency periodic reports • Comfort maximization	**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)	**Transmission System** • Frequency • TSO API
Semantic Interoperability		**InterConnect interoperability layer** • Semantically interoperable services - Water heater forecast and flexibility (REST) • P2P marketplace - NO • Services available as downloadable containers - NO		
Communication (gateway)		**Building Communication and IoT Gateway Layer** • Remote control of appliances		**Distribution System**
Device		**Inside Building** • Water heater • PV • Whitegoods • ThermoVault IoT modules	**Outside Building** • EV Charger • Smart meter	

TABLE 39 – SHBERA MAPPING FOR THE GENK BELGIUM SUBPILOT

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.

2.3 Portugal

The objective of this pilot – led by E-REDES – 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 InterConnect Deliverables D5.1 [14] and D1.1 [13].

<table>
<tr><th>Layer (HLA)</th><th colspan="4">Domains (SERA)</th></tr>
<tr><td>Stakeholders</td><td>User
• Residential household consumer, prosumer
• Commercial building manager (supermarket)</td><td>CCC services (actors)
• Smart building system manager</td><td>Energy services (actors)
• Technical integrator (INESC, SONAE, SENSI)
• Incentive service provider</td><td>Energy System
• DSO</td></tr>
<tr><td>Application</td><td></td><td>CCC services
• Continente app (SONAE)
• Energy monitoring app
• HEMS device automation
• ThermoVault controller
• Data sharing with focus on privacy protection</td><td>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</td><td rowspan="2">Transmission System</td></tr>
<tr><td>Semantic Interoperability</td><td></td><td colspan="2">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 (E-REDES, interface TBD), Forecasting service (SONAE/INESC/E-REDES, interface TBD), Metering data service (E-REDES, 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</td></tr>
<tr><td>Communication (gateway)</td><td></td><td colspan="2">Building Communication and IoT Gateway Layer
• HEMS
• BEMS
• Flexibility service (HEMS)
• ThermoVault controller</td><td rowspan="2">Distribution System
• Smart meter
• DSO interface</td></tr>
<tr><td>Device</td><td></td><td>Inside Building
• HEMS device controller
• ThermoVault controller</td><td>Outside Building
• EV Charging
• Smart meter</td></tr>
</table>

TABLE 40 – SHBERA MAPPING FOR THE PORTUGESE PILOT

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).

2.4 Greece

The goal of this pilot – led by GridNet - 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 InterConnect Deliverables D5.1 [14] and D1.1 [13].

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) • Mobile app for end users (AUEB)	**Energy services** • Local/Remote Home Comfort services (monitoring, control and automations) - (COSMOTE, GRIDNET, HERON) • Cloud data storage and provisioning service (COSMOTE, GRIDNET, HERON) • Mobile app for end users (AUEB) • Flexibility service (GFI) • Forecasting service (WINGS) • Recommendation service (WINGS)	**Transmission System**

<table>
<tr>
<td>Semantic Interoperability</td>
<td></td>
<td colspan="2">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</td>
<td></td>
</tr>
<tr>
<td>Communication (gateway)</td>
<td></td>
<td colspan="2">Building Communication and IoT Gateway Layer
• IoT Gateway (COSMOTE, GRIDNET)
• User's WiFi Network (HERON)</td>
<td rowspan="2">Distribution System</td>
</tr>
<tr>
<td>Device</td>
<td></td>
<td>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.</td>
<td>Outside Building
• EV charging station
• Smart meter (For EV charging station)</td>
</tr>
</table>

TABLE 41 – SHBERA MAPPING FOR THE GREEK PILOT

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 to gather data and provide the required services.

2.5 The Netherlands

The objective of this pilot – led by HYRDE - ICITY 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 InterConnect Deliverables D5.1 [14] and D1.1 [13].

<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>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)</td><td>Energy services
• <u>Forecasting service</u>
• Weather forecast
• Achmea service
• Contract management
• ReFlex - flexibility aggregation and optimization (TNO)
• Energy insights (Net2Grid)</td><td rowspan="2">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 rowspan="2">Distribution System
• Smart meter</td></tr>
<tr><td>Device</td><td></td><td>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)</td><td>Outside Building
• Batteries
• EV Chargers
• Smart meter (net2grid, p1port, dongle)</td></tr>
</table>

TABLE 42 – SHBERA MAPPING FOR THE DUTCH PILOT

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. At the time of the workshops the Dutch pilot was looking for a project partner providing forecasting services.

2.6 Germany

The German pilot has two sub-pilots:

1. The Commercial Pilot in Hamburg, led by KEO.
2. The Residential Pilot in Norderstedt, led by EEBUS.

The following sections provide descriptions of the mapping of these sub-pilots to the SHBERA architecture.

2.6.1 Commercial Hamburg pilot

This sub-pilot – led by KEO - 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 InterConnect Deliverables D5.1 [14] and D1.1 [13].

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 43 – SHBERA MAPPING FOR THE COMMERCIAL HAMBURG GERMAN SUB-PILOT

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.

2.6.2 Residential Norderstedt pilot

This sub-pilot – led by KEO - 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 InterConnect Deliverables D5.1 [14] and D1.1 [13].

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 44 – SHBERA MAPPING FOR THE COMMERCIAL HAMBURG GERMAN SUB-PILOT

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.

2.7 Italy

This pilot – led by Planet IDEA - 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 InterConnect Deliverables D5.1 [14] and D1.1 [13].

Layer (HLA)	Domains (SERA)			
Stakeholders	**User** • Smart home/building owner/ manager	**CCC services (actors)** • Living services provider (Planet Idea)	**Energy services (actors)** • Consumption optimization aggregator (RSE) • Energy manager (Planet Idea)	**Energy System**
Application	• Application user • Device provider cloud	**CCC services** • Living manager aggregator (Planet Idea) • Remote control application • Whirlpool cloud services	**Energy services** • Energy forecast & consumption analysis (WD) • Energy optimization • Tariff schema for energy flexibility & optimization (RSE) • Energy forecast (WD) • Energy constraints validator (WD)	**Transmission System**
Semantic Interoperability		**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).		
Communication (gateway)		**Building Communication and IoT Gateway Layer** • Planet Energy Manager (Planet Idea)		**Distribution System** • Smart meter
Device	• Device manufacturer (Whirlpool)	**Inside Building** • Whirlpool smart washing machine	**Outside Building** • Smart meter • Water meter • Heating/cooling meters	

TABLE 45 – SHBERA MAPPING FOR THE ITALIAN PILOT

At the time of the workshops the details about the integration of RSE and WD services were still in negotiation within the pilot team. The pilot's leader was looking into the possibility of integrating a monitoring and control capability of electric heat pumps to enrich the load flexibility portfolio.

2.8 Cross-European pilot

This pilot – led by CYBERgrid – has a 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 service to the TSO. More details about the pilot's functional architecture, goals and high-level use cases can be found in in InterConnect Deliverables D5.1 [14] and D1.1 [13].

Layer (HLA)	Domains (SERA)			
Stakeholders	**User** • Energy asset owner	**CCC services (actors)** • Energy asset controller	**Energy services (actors)** • Flexibility service provider • Flexibility service aggregator (cyberGRID) • Energy community manager	**Energy System** • BRP (out of scope) • TSO (out of scope) • DSO (out of scope)
Application		**CCC services** • Flexibility management platform (cyberGRID) - control signals	**Energy services** • Flexibility service • Flexibility management platform (cyberGRID) - management and aggregation	**Transmission System** • (Group) Balancing - simulated
Semantic Interoperability		**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.		
Communication (gateway)		**Building Communication and IoT Gateway Layer** • Generic energy assets - enable flexibility service on different levels (device, edge/BMS)		**Distribution System**
Device		**Inside Building** • Generic energy assets	**Outside Building** • Generic energy assets	

TABLE 46 – SHBERA MAPPING FOR THE EUROPEAN CROSS-PILOT

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 provide flexibility services for this overarching use case:

1. Belgium - Oud Heverlee – led by 3E.
2. Belgium - Nieuwe Dokken Gent – led by OpenMotics.
3. Belgium - Nanogrid – led by Think E!.

4. Belgium - Cordium and Thorpark – led by VITO.
5. Belgium - Antwerp – led by IMEC.
6. Portugal – led by E-REDES.
7. Greece – led by GRIDNET (more information needed before deciding).
8. German sub-pilots – led by EEBUS.
9. The Netherlands – led by iCity/Hyrde.

At the time of the workshops the other pilots (France and Italy) were continuing to review their possible flexibility service provisioning. Task 7.8 leader, cyberGRID, was working with these pilots to help them decide how they might participate in the overarching demonstration.

3 Conclusions

After the mapping results were presented, the following conclusions could be drawn:

1. All pilots include Control, Comfort and Convenience (CCC) and Energy Services.
2. All pilots include devices residing inside and outside of a building.
3. (Sub-)pilot partners cover the key stakeholders' roles identified for their pilots.
4. DSO stakeholders are present in Portuguese, German and French pilots. In some of the (sub-)pilots, DSO stakeholders and key functions will be emulated.
5. 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.
6. All (sub-)pilots require some management services for flexibility (in terms of consumption and production) 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.
7. 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.
8. Most of the services and digital platforms, which will be made semantically interoperable, expose RESTful communication APIs while some utilize MQTT protocol. Additionally, the SPINE/SHIP protocol stack is represented in resources (e.g., devices and digital platforms) which can be made semantically interoperable. Based on this, WP5 will try to implement generic interoperability adapters for REST, MQTT and SPINE/SHIP as well.
9. P2P marketplace enablers will be validated in at least 5 (sub-)pilots (confirmed). More pilots would decide on the need/plans for implementation of P2P marketplaces before the pilots' kick-off.
10. 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 were still deciding on this during the workshops. The InterConnect Service Store will be developed with this functionality as one of the minimal requirements.