Electronic Devices & Networks Annex EDNA

# Interoperability

OCTOBER 2022

Technology Collaboration Programme
by iea

# Interoperability

**Final Report**

**Report Prepared for IEA 4E EDNA by Viegand Maagøe**

**October 2022**

Electronic Devices & Networks Annex
EDNA

The Technology Collaboration Programme on Energy Efficient End-Use Equipment (4E TCP), has been supporting governments to co-ordinate effective energy efficiency policies since 2008.

Fifteen countries have joined together under the 4E TCP platform to exchange technical and policy information focused on increasing the production and trade in efficient end-use equipment. However, the 4E TCP is more than a forum for sharing information: it pools resources and expertise on a wide a range of projects designed to meet the policy needs of participating governments. Members of 4E find this an efficient use of scarce funds, which results in outcomes that are far more comprehensive and authoritative than can be achieved by individual jurisdictions.

The 4E TCP is established under the auspices of the International Energy Agency (IEA) as a functionally and legally autonomous body.

Current members of 4E TCP are: Australia, Austria, Canada, China, Denmark, the European Commission, France, Japan, Korea, Netherlands, New Zealand, Switzerland, Sweden, UK and USA.

Further information on the 4E TCP is available from: **www.iea-4e.org**

The EDNA Annex (Electronic Devices and Networks Annex) of the 4E TCP is focussed on a horizontal subset of energy using equipment and systems - those which are able to be connected via a communications network. The objective of EDNA is to provide technical analysis and policy guidance to members and other governments aimed at improving the energy efficiency of connected devices and the systems in which they operate.

EDNA is focussed on the energy consumption of network connected devices, on the increased energy consumption that results from devices becoming network connected, and on system energy efficiency: the optimal operation of systems of devices to save energy (aka intelligent efficiency) including providing other energy benefits such as demand response.

Further information on EDNA is available at: **edna.iea-4e.org**

This report was commissioned by the EDNA Annex of the 4E TCP. It was authored by Viegand Maagøe. The views, conclusions and recommendations are solely those of the authors and do not state or reflect those of EDNA, the 4E TCP or its member countries.

Views, findings and publications of EDNA and the 4E TCP do not necessarily represent the views or policies of the IEA Secretariat or its individual member countries.

The IEA, 4E, EDNA and the authors make no conclusions, endorsements or disendorsements in relation to the organisations and brands mentioned in this report.

# Table of Contents

# 1 Executive summary

The objective of this study is to gain a better understanding on the issue of (a lack of) device interoperability and the resultant impact of this on IE (Intelligent Efficiency) and DF (Demand Flexibility). To this purpose, the study follows a structure starting from a proposal of definition of interoperability, analysing causes and impacts of interoperability, to conclude with policy recommendations.

The proposed definitions are based on the technical literature that distinguishes the different interoperability layers: basic connectivity, network interoperability, syntactic interoperability, semantic interoperability and business context. The proposed definition of interoperability is linked to the specific needs of IE and DF, particularly in terms of semantic understanding.

The study analyses what specific features of the IoT market are behind the lack of interoperability, and their interlinkages. The IoT market has followed a rapid growth in a fragmented landscape where many businesses and developers coexist, delivering a wide range of applications. This has hindered the necessary standardisation to improve interoperability and has favoured the proliferation of closed ecosystems which places the interoperability issue in the realm of legacy and business strategy.

Among the impacts of this impaired interoperability, there is an untapped potential on energy savings derived from the inability of IoT systems to work co-ordinately and provide a full IE service. Besides, additional energy consumption stems from the need of hubs and bridges and apart from that, the lack of interoperability affects the user behaviour and discourage the users to install smart home systems and also to use them properly. The negative effects of interoperability in market development have spurred the efforts of technological companies to collaborate and be more open, though there may be the need for public intervention to incentivise these efforts.

The study also gathers the standardisation gaps from the relevant SDOs (Standards Developing Organizations) and specialised organisations, focusing on the most relevant ones: device connectivity, semantic interoperability and platform interoperability. This section highlights which standardisation efforts should be supported, and what solutions are under development.

The different options for policy makers to address the interoperability issues are put forward and analysed, taking into account the specific nature of each potential measure and the features of the IoT market. The study concludes with recommendation on different policy options that cover the most relevant areas to improve interoperability: support of open platforms and standards, stimulation of market uptake, information to end-users to support their purchase choice, support of standardisation for interoperability, organisational interoperability.

# 2 Introduction

The objective of this topic is to study the issue of (a lack of) device interoperability and the resultant impact of this on IE (Intelligent Efficiency) and DF (Demand Flexibility). The following questions are emphasised in the study:

1. What is a suitable definition for interoperability?
2. What is the scope of the problem? To what extend does lack of interoperability limit IE and DF (currently and potentially into the future)?
3. What are the causes of a lack of interoperability?
4. To what extent do “closed” proprietary device ecosystems limit interoperability? What are the commercial drivers for proprietary device ecosystems? What would be the commercial impacts if ecosystems were required to be “open”?
5. What standardisation efforts are underway and where are the gaps?
6. What are the implications for (government) policy makers?

# 3 Definition of Interoperability

**Subtask 1: What is a suitable definition for interoperability?**

With layman's words, interoperability is the ability for systems and devices to connect and communicate with each other. For the purpose of this study, interoperability is related to intelligent efficiency and demand flexibility, and these concepts will therefore be outlined as a first step.

This can for example be based on the descriptions in the EDNA report "Harnessing IoT for Energy Benefits", where intelligent efficiency is described as the ability of connected products to "*use information collected by the device itself and relayed over the network to alter their operation" and to "save energy by using information to determine which services must be provided and strategically use low power states for components or functions that are not needed at any given time.*"

Intelligent efficiency is closely linked to Demand Flexibility, which is described in the same report as connected products' ability to "*utilize one or more load-shaping strategies to better match demand to electricity supply […] since "their connectivity can allow them to receive signals or information to alter their energy use, specifically by:*

- *Shedding load: reducing electricity use during a peak or emergency event, or*
- *Shifting load: shifting energy consumption from peaks or other periods of day when electricity is expensive or scarce to those when electricity is inexpensive and plentiful, such as during solar or wind generation peaks* (U.S. DOE 2019, EDNA 2020)."

Interoperability is a term used in many contexts related to digital communication. However, for the purpose of this study the definition will focus on interoperability in relation of intelligent efficiency and demand flexibility.

## 3.1 Technical definition

Several definitions were suggested by the various literature sources, some in text-based descriptions, such as:

- Two interoperable systems can understand one another and use the functionality of each other[1]
- The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units[2]
- The ability of two or more systems or components to exchange information and to use the information that has been exchanged[3]
- The ability of two systems to communicate and share services with each other[4]
- Interoperability is a property of a product or system, whose interfaces are completely understood, to work with other products or systems, present or future, without any restricted access or implementation[5]

[1] Mahda Noura, Mohammed Atiquzzaman, Martin Gaedke: Interoperability in Internet of Things: Taxonomies and Open Challenges, Published online: 21 July 2018 in Mobile Networks and Applications (2019) 24:796 – 809. Available: https://doi.org/10.1007/s11036-018-1089-9

[2] B ISO/IEC 2382-1:1993 Information Technology – Vocabulary Part 1: Fundamental terms. International Organization for Standardization (ISO). Available: http://www.iso.org/iso/catalogue_detail.htm?csnumber=7229

[3] Radatz J, Geraci A, Katki F (1990) IEEE standard glossary of software engineering terminology. IEEE Std 610121990(121990):3, Available: https://ieeexplore.ieee.org/document/159342

[4] Kiljander J, D ' Elia A, Morandi F, Hyttinen P, Takalo-Mattila J, Ylisaukko-Oja A, Soininen JP, Cinotti TS (2014) Semantic interoperability architecture for pervasive computing and internet of things. IEEE Access 2:856 – 873

[5] InterFuture – Future of Interoperability, for "ICT of the Future" programme by the Austrian Ministry for Transport, Innovation and Technology and the Austrian Research Promotion Agency (FFG). Authored by Mag. Kaltenbrunner Rainer – IDC, Mag. Neuschmid Julia – IDC, Dr. Bieber Ronald – OCG, DI Baumann Wilfried – OCG, Mag. Meir-Huber Mario.

- The ability of two or more devices from the same vendor, or different vendors, to exchange information and use that information for correct cooperation[6].

In other sources interoperability is presented as interoperability frameworks (IFs), which describe interoperability as a layered model, where each layer build upon each other. Some examples of IFs from the identified literature are provided in the following.

One of the simplest IFs is one used by the EU RESPOND project[7], which focuses on smart home and building management systems and on improving the energy efficiency. Their framework includes just three interoperability layers: technical (basic connectivity and network connectivity), syntactical (data exchange interoperability), and semantic (understanding in the meaning of the data):

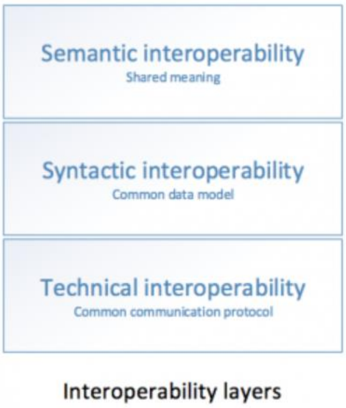


*Figure 3-1: The three interoperability layers as defined by the RESPOND project*

This model is expanded to a six-layer model in one of the literature sources[8], where these capability layers are coupled to the functional layers, see Figure 3-2.

[6] IEC61850-2010 https://joinup.ec.europa.eu/collection/ict-standards-procurement/solution/iec-61850-7-42010-communication-networks-and-systems-power-utility-automation-part-7-4-basic

[7] http://project-respond.eu/what-is-interoperability/

[8] Hannu Järvinen, Web Technology based Smart Home Interoperability, doctoral dissertation, Aalto University, School of Science, Department of Computer Science, Web Services Group. ISBN 978-952-60-6510-6 (pdf).

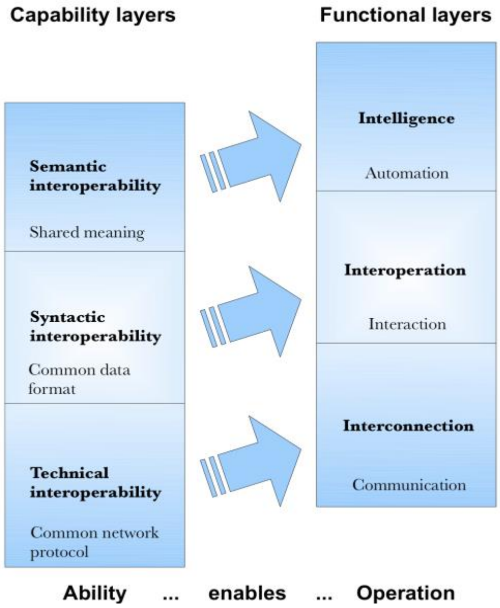


*Figure 3-2: In this expanded IF, the capability layers are connected to and enable operations on functional layers.*

The technical – syntactic – semantic IF has also been seen in a broader context and expanded to a seven-layer IF in Tolk et al.[9], where a layer below: no connection (no interoperability between systems) is added, as well as three layers above: pragmatic/dynamic (applicability of the information) and conceptual (shared view of the world).

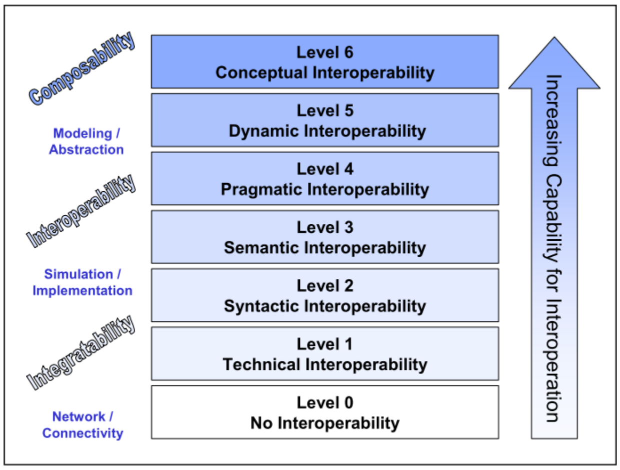


*Figure 3-3: Levels of Conceptual interoperability*

A similar six level model is proposed in other sources, such as the one shown below, in which the six layers are equivalent to layer 1 through 6 in in the above.

[9]Tolk A (2004) Composable mission spaces and M&S repositories – applicability of open standards. In Spring simulation interoperability workshop, Arlington (VA)

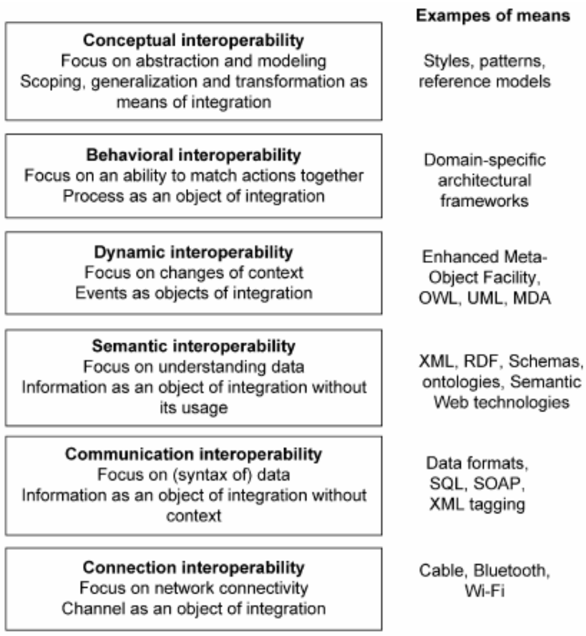


*Figure 3-4: Six-layer IF similar to that in figure 4, but with different taxonomy*[10]

Even though all of these frameworks seek to explain the same subject, they differ in both taxonomy and delimitation between the layers, because interoperability is seen from different perspectives.

The above models focus on interoperability in the view of Internet of Things in general, whereas the third interoperability framework, developed by CEN/CENELEC and IEC[11] is focused explicitly on smart grid and is also named Smart Grid Architecture Model (SGAM), which highlights the complexity and a smart grid system in terms of both organizational and technological aspects. See Figure 3-5.

[10] Pantsar-Syväniemi S, Purhonen A, Ovaska E, Kuusijärvi J, Evesti A (2012) Situation-based and self-adaptive applications for the smart environment. J. Ambient Intell. Smart Environ. 4(6):491 – 516. https://www.researchgate.net/figure/Interoperability-levels-of-smart-environments_fig1_236131773

[11]CEN-CENELEC-ETSI Smart Grid Coordination Group , Smart Grid Reference Architecture , 2012 and Covrig, C.F., Munoz Diaz, M.A., Georgiopoulos S. and Marinopoulous, A., Smart Grid Interoperability Laboratory: A toolkit for smart energy management, EUR 30211 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-18820-9, doi:10.2760/822668, JRC120540, EUR 30211 EN.

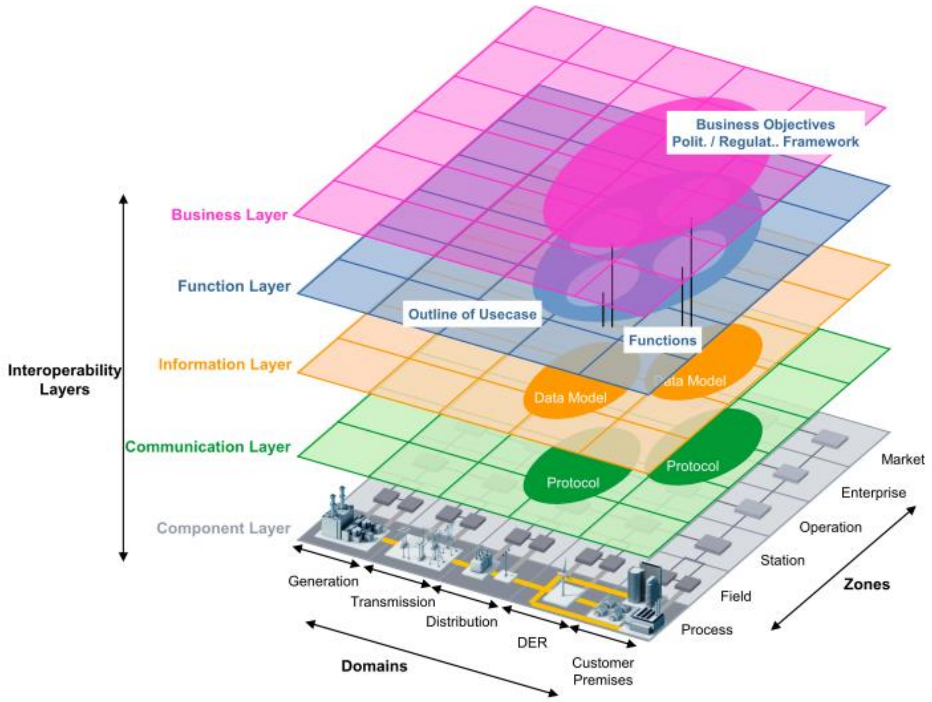


*Figure 3-5: The Smart Grid Architecture Model (SGAM) also includes the organisational layers (such as the business layer) of a smart grid system.*

SGAM is inspired in the model developed by GridWise Architecture Council, aggregating its layers in five interoperability layers: Business, Function, Information, Communication and Component. Figure 3-6 shows the correspondence between both models.

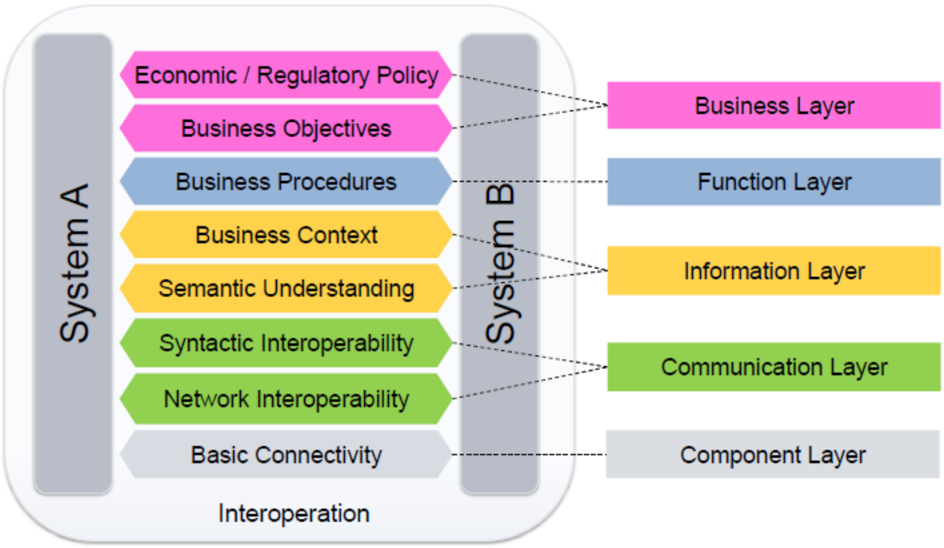


*Figure 3-6: GridWise Architecture IF categories and Smart Grid Architecture Model (SGAM)*

GridWise Interoperability Framework Categories are extensively explained in GridWise® Interoperability Context Setting Framework (2008)[12], which are summarised below:

[12] GridWise® (2008) Interoperability Context-Setting Framework v 1.1

- The Basic Connectivity category focuses on the digital exchange of data between two systems and the establishment of a reliable communications path. This is achieved by agreeing to conform to specifications describing the data transmission medium, the associated low-level data encoding, and the transmission rules for accessing the medium. Examples of common physical interoperability standards include Ethernet and Wi-Fi.
- Network Interoperability refers to the issues arising from transporting information between interacting parties across multiple communication networks. The protocols agreed upon in this category are independent of the information transferred. Examples of common Protocol Interoperability standards include:
    - FTP—File Transfer Protocol
    - TCP—Transport Control Protocol
    - UDP—User Datagram Protocol
    - IP/IPv6—Internet Protocol (version 6)
    - ARP—Address Resolution Protocol
    - IPSec—Internet Protocol Security
- Syntactic Interoperability refers to agreement on the rules governing the format and structure for encoding information exchanged between transacting parties. Proper syntax enables decomposition of content into a common scheme or “grammar”, but it does not entail a meaning of the content. Examples of common Syntactic Interoperability standards include:
    - HTML—Hypertext Markup Language
    - XML—Extensible Markup Language
    - ASN.1—Abstract Syntax Notation One
    - SOAP—Simple Object Access Protocol
    - SNMP—Simple Network Management Protocol
- Semantic Understanding is about understanding of the concepts contained in the message. Therefore, semantic understanding includes rules governing the definition of things, concepts, and their relationship to each other, i.e. a informational model. A model is usually domain-specific, i.e., pertaining to one area of expertise, such as a car, a building, or a power system. Groups have come together to establish shared semantic understanding within an area of interest or business domain. Examples include:
    - Common Information Model (CIM) power model - (International Electrotechnical Commission [IEC] 61970 CIM - based on Resource Description Framework [RDF])
    - tModels based on universal description, discovery, and integration (UDDI)
    - Object models based on XML schema definition (XSD)
    - Object models based on OPC Unified Architecture (a manufacturing automation standard).
    - Object models based on the IEC 61850 substation automation standard.
- Business Context refers to restricting and refining the aspects of an information model relevant to the specific business process in question. These restrictions may include the roles of the players involved in the interaction as well as specific rules and constraints on the information exchanged. A business context may draw upon information models from different domains (e.g., electric distribution and factory automation systems) as it aggregates the appropriate knowledge to support a business process application.
- Business Procedures: Effective information interoperability between business organizations requires that the involved organizations have compatible processes and procedures across their interface boundaries. The rules of engagement consistent with the relevant business process must be agreed upon and aligned for organizations to participate in distributed business transactions.

Finally, the organisational categories Business Objectives and Economic and Regulatory Policy involve the procedures to align the objectives of the different stakeholders, among private businesses and with public authorities.

The taxonomy proposed by Noura et al (2018)[1] provides a framework to identify the main issues derived from interoperability failures and to analyse the solutions currently adopted and under research:

- Device interoperability, comprising the exchange of information between heterogeneous devices and heterogenous communication protocols and the ability to integrate new devices into any IoT platform

- Network interoperability deals with mechanisms to enable seamless message exchange between systems through different networks (networks of networks) for end-to-end communication
- Syntactic interoperability refers to interoperation of the format as well as the data structure used in any exchanged information or service between heterogeneous IoT system entities
- Semantic interoperability enabling different agents, services, and applications to exchange information, data and knowledge in a meaningful way, on and off the Web.
- Platform interoperability: the cross-platform interoperability between things and data enables interoperability across separate IoT platforms specific to one vertical domain such as smart home, smart healthcare, smart garden, etc.

Interoperability definition needs to be aligned with its ultimate energy purposes in terms of IE and DF, and extended to smart grids. Previous EDNA reports[13] provide suitable definitions for IE and DF, as follows:

- Intelligent Efficiency: the deployment of network-connected ICT technologies to facilitate efficient operation of energy-using equipment, leading to energy savings.
- Demand flexibility: the capability of an electricity system to respond to upward or downward changes in the supply/demand balance in a cost-effective manner over a timescale ranging from a few minutes to several hours

Demand flexibility is a subset of the broader concept of smart grids, which have been also defined in technical and scientific literature. Some examples from different institutions are gathered below:

- A smart grid is an electricity network that can intelligently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to efficiently ensure sustainable, economic and secure electricity supply (Smart Grid European Technology Platform)
- A smart grid uses digital technology to improve reliability, security, and efficiency (both economic and energy) of the electric system from large generation, through the delivery systems to electricity consumers and a growing number of distributed-generation and storage resources (DOE 2009)
- A smart grid is an electricity network that uses digital and other advanced technologies to monitor and manage the transport of electricity from all generation sources to meet the varying electricity demands of end-users. (IEA 2011)

However, smart grids are complex systems which spans transmission and distribution, energy storage, distributed generation, etc. that go beyond the scope of this report.

The definitions of IE and DF already hint the crucial role of IoT interoperability. Both IE and DF require semantic interoperability, while DF business context and procedures, due to the interaction between smart home systems and electricity systems.

## 3.2 Conclusion and recommended definition

Interoperability in the framework of IE and DF is a paramount element to ensure that the multiple systems and stakeholders involved deliver the expected results. The basic connectivity, network, syntactic and semantic interoperability can be considered as minimum requirements, business layers of interoperability needs may depend on the complexity of context i.e. if business layers are an integral part of the required interoperability to reach the goals of the IE, DF and smart grids.

Based on the previous analysis, a first proposal for a definition of interoperability within the framework of IE and DF could be formulated *as the capability of a product or system within the smart home landscape, to interact with other products or systems, by means of exchange of the necessary information and its common understanding, in order to maximise energy savings and to enable electricity system to respond to upward or downward changes in the supply/demand balance in a cost-effective manner.*

[13] intelligent efficiency - A case study of barriers & solutions - Smart homes

For the purpose of this study, the technical interoperability layers defined by GrideWise will be used to complement the definition of interoperability and to structure and address its evaluation along the study:

- Basic connectivity
- Network interoperability
- Syntactic
- Semantic
- Business context
- Business procedures

In many studies and papers, the IoT platform constitutes the upper layer of interoperability above semantic interoperability. As defined by UNIFY-IoT[14], *a IoT platform is an intelligent layer that connects the things to the network and that abstracts applications from the things with the goal to enable the development of services. IoT platforms achieve several main objectives such as flexibility (being able to deploy things in different contexts), usability (being able to make the user experience easy) and productivity (enabling service creation in order to improve efficiency, but also enabling new service development). An IoT platform facilitates communication, data flow, device management, and the functionality of applications. The goal is to build IoT applications within an IoT platform framework. An IoT platform allows applications to connect machines, devices, applications, and people to data and control centres.* The term platform will be also used in this study to ensure the coherence with the original reference.

A Smart Home system with DF is a good example to illustrate the different levels of interoperability, and better understand the abstract definitions within a real context:

- Basic connectivity: the different household appliances (lighting, HVAC, dishwasher, etc.) are connected to the smart home central control through ZigBee, for example, which connects to internet through the Wi-Fi access point, where the ZigBee gateway is connected to.
- Network interoperability: the smart home central control and internet create a network that interoperate through IP or similar protocols.
- Syntactic interoperability: the smart home central control interacts with the electricity supplier (or an aggregator having a contract with the smart home owner and with the DSO (Distribution System Operator) or TSO (Transmission System Operator) by means of SOAP XML messages over IP.
- Semantic understanding: BACnet committee (the ASHRAE Building Automation and Control Networking Protocol) and IEC TC57 (power systems management and associated information exchange) committee agree on information exchange and on BACnet objects for addressing load reduction applications.
- Business context: smart home system and the electricity supply system agree on the type of messages (real time price, share of renewable, peak loads, customer identification, type of DF program)
- Business procedures: the smart home system and the electricity supplier agree on:
  - A contract that specifies: account IDs, passwords/keys, rate class, web server address, etc.
  - Data which is distributed using a web service interface with encryption.
  - Message data which includes hourly information about prices, renewable share, etc.

Intelligent efficiency also provides good examples of the need of interoperability. This could be the case of a smart air conditioning system from a manufacturer that interacts with the occupancy detectors of a smart lighting system from another manufacturer. Basic connectivity and network interoperability would be similar, which would enable the integration into a smart home central control or a smart home platform. The central control or the platform would provide the syntactic and semantic interoperability of the different devices, and the interface with the user. If the devices to be connected are not part of the same ecosystem, the smart air conditioning system and the smart lighting system will have their own user interfaces, and will need to develop a way to access the smart home platform. This access and the issues around it are addressed in this report as platform interoperability, i.e. the interaction between smart devices and platforms.

# 4 Causes of lack of interoperability

The aim of the subtask is to dive into the causes of lack of interoperability with the focus on intelligent efficiency and demand flexibility. The causes have been categorised attending to multiple facets: market, standardisation, end-user behaviour. This has led to the following subsections assessing the causes of the lack of interoperability:

- Rapid development of the market
- Wide and varied range of applications, devices, manufacturers and developers
- Lack of universal standardisation
- Closed ecosystems
- Market penetration

## 4.1 Rapid development of the market

The smart-home ecosystem shows a rapid expansion, reaching households penetrations of 12% worldwide, 16% in EU27 and 40% in US, in 2021 (Statista). Considering the current moderate user penetration, long product replacement cycles and increasing device connectivity, adoption will steadily grow in the next years. The estimated penetration in 2026 will be 25%, 39% and 63%, worldwide, EU27 and US respectively (Statista).

The evolution of IoT platforms in the market is a good indicator of this trend. The IoT platform market boomed in 2013 driving business opportunities for potentially 25 billion things connected to the Internet in less than five years, according to the report on IoT platform activities from UNIFY-IoT project. The number of IoT platforms launched per year is shown in Figure 4-1[14]:

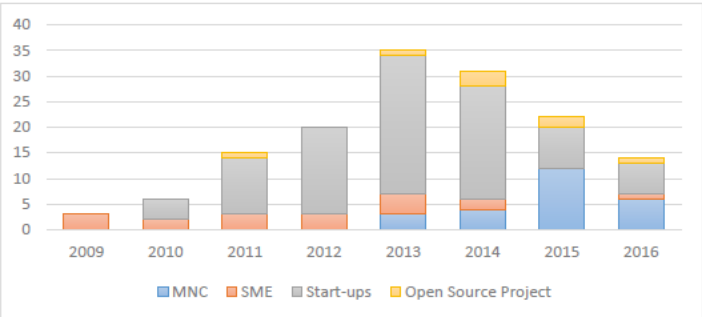


*Figure 4-1: Number of IoT platforms launched on the market per year worldwide (Source: UNIFY-IoT, IoT Analytics)*

According to IoT Analytics, from 2015 to 2019, the number of publicly known IoT platforms more than doubled from 260 to 620. However, since 2019, that number has decreased slightly to 613, showing signs of stagnation (Figure 4-2).

[14] UNIFY-IoT (2016) Report on IoT platforms

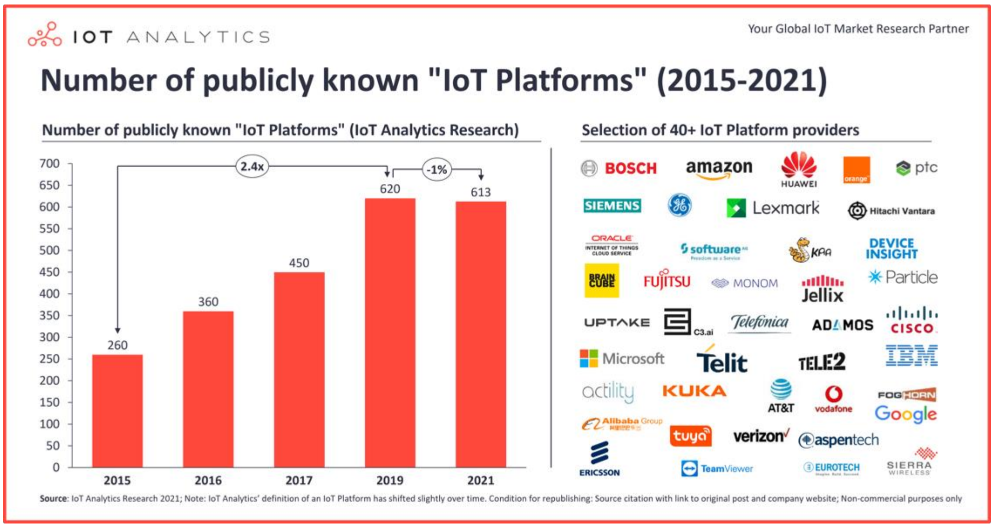


*Figure 4-2: Number of publicly known IoT platforms worldwide (Source: IoT Analytics)*

The number of IoT platforms might have stopped growing, but the size of the market has still increased substantially. In 2020, $5 billion were spent on IoT platforms. The market is expected to grow to $28 billion in 2026. That constitutes a 33% compound annual growth rate (CAGR) for 2020 to 2026. The growth is fuelled by the rapid adoption of cloud-based IoT platforms and the increasing number of customers choosing to buy (not make) IoT platforms[15].

## 4.2 Wide and varied range of applications, devices, manufacturers and developers

**Business context / platforms**

IoT devices are designed by manufacturers in many different industries such as electricity, electronics, home appliances, telecoms, and internet. There is a wide range of applications where smart connected devices and platforms have been integrated in, such as commerce, healthcare, agriculture, utilities, energy, transportation, industrial control and buildings, etc. There are also a multitude of platforms available on the market in support of IoT developments. Most of these platforms are proprietary and try to offer the broadest possible set of features and services in a relatively closed ecosystem.

European project UNIFY-IoT identified more than 300 IoT platforms in the current market, the most popular ones in the field of smart home services are Apple, Google Cloud, Cisco IoT Cloud Connect, IBM Watson IoT, Amazon AWS IoT Core, which are proprietary. However, there are also smart home platforms like Eclipse IoT and Smart Data Platform, which are open source. A list of the platforms used in the IoT-EPI projects their characteristics can be found in UNIFY-IoT report on IoT platform activities[14].

As explained previously, IoT platform is an intelligent layer that connects the things to the network and that abstracts applications from the things to enable the provision of services. Each of these platforms develops and promotes its own IoT infrastructure, protocols and interfaces, in standards, formats and semantics. Proprietary platforms create closed ecosystems (sometimes called stove pipes or silos), which hinder the interoperability of smart home systems. In these IoT ecosystems, the various devices and applications are installed and operate in their own platforms, but without adequate compatibility with products from different brands. This may lead to a broad range of interoperability difficulties, ranging from total impossibility of exchanging data, up to not being able to assign the correct meaning to data that has been exchanged[21].

[15] https://iot-analytics.com/iot-platform-companies-landscape/

These interoperability issues are directly related to the closeness of platforms and are not accidental, but usually part of the legacy companies to protect their market share. This is further developed in sections 4.4 and 5.2.

**Basic connectivity**

The variety is not limited to the IoT platforms, but also to basic connectivity. Some examples are described by Noura et al: IoT devices such as Smart TV, printers, air conditioners support traditional Wi-Fi technologies and 3G/4G cellular communications, while wearable devices mostly support Bluetooth SMART and NFC, and finally sensors use ZigBee based on IEEE 802.15.4 standard[1], among other protocols. Recently, Thread has also joined the wireless solutions for connecting IoT devices. Besides, different standard communication protocols are used for smart devices and sensors: Z-Wave, ZigBee, KNX, and there are also non-standard proprietary solutions such as LoRa and SIGFOX.

## 4.3 Lack of universal standardisation

Interoperability failures are caused by the combination of a rapid development of the market of IoT devices and the wide and varied range of applications, devices, manufacturers, developers and rest of stakeholders. These two characteristics of the IoT market hinder the process to come up with appropriate standards, i.e., recognised and applicable by all the players, since they usually require time and resources for reaching wide consensus.

As no standardisation has succeeded in paving the way for a common language for connected devices, many devices and companies have created their own diverse protocols[16], with their own network types and use of semantics. While some open industry protocols are widely used, they might be customised by some companies, creating a gap in interoperability with devices using other versions of the same protocol, or requiring a bridge from both brands to communicate with devices of other brands, thus adding a device (the bridge) to the network and increasing the energy consumption and sometimes the complexity in interconnecting the devices.

The interoperability solutions mostly focused on the connection of technology and selection of protocols, but limited focus on semantics has created a new set of issues to be resolved[17]. Even if devices manage to communicate with each other, they might not understand and interpret the commands they receive due to the different semantics. For example, if a central device manage sends a command to a device to switch off, it might be interpreted as a different request[18].

**Basic connectivity**

As mentioned previously, there are several technologies and standards commonly used for basic connectivity. In those cases where devices to be connected use different standards, the most common solution are adapters or gateways (also known as bridges or hubs). Figure 4-3 shows how the connectivity is achieved when different standards protocols co-exist, being Internet Protocol (IP) and cloud platforms as de facto intermediate “standards” in the communication link between appliances and the smart phone[19].

[16] EDNA (2021), Retrofitting Connectivity for Energy Benefits

[17] Daniele, Solanki, den Hartog, Roes (2016), Interoperability for Smart Appliances in the IoT World

[18] Guidehouse Inc. (2020), Policy Guidance for Smart, Energy-Saving Consumer Devices

[19] VITO, Viegand Maagøe, Universität Bonn, Armines, Wuppertal Institut (2018) Preparatory study on Smart Appliances

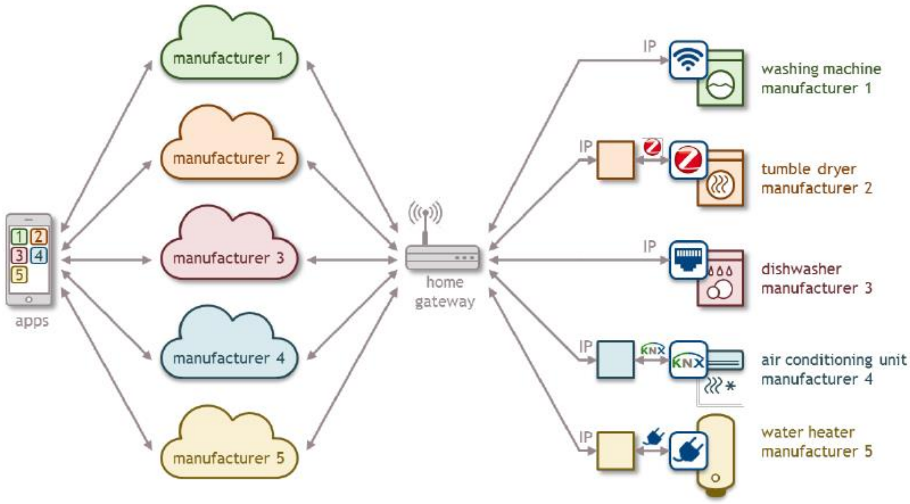


*Figure 4-3: Connectivity of different appliances with different technologies and standard protocols (Source: Preparatory study on Smart Appliances )*

However, some authors as Noura et al stressed these bridges are limited in scalability in device-to-device connection and the additional energy consumption it may entail[1]. Therefore, it is essential to develop a standard protocol for all devices. According to news from IT specialised media[20], big tech companies have been working on Project Connected Home over IP (Project CHIP), now rebranded as Matter. This open-sourced IP-based connectivity standard is being developed by Amazon, Apple, Google / Nest, and Samsung, alongside many other smart home and smart home-adjacent companies, including Wyze, iRobot, Signify (Philips Hue), Ecobee, and more (over 200 companies). The Connectivity Standards Alliance (formerly the Zigbee Alliance) is in charge of its organisation. Matter is a communication protocol compatible with existing technologies — Thread, Wi-Fi, Bluetooth, and ethernet — allowing all devices to communicate with each other locally, without the need for a cloud.

Figure 4-4 shows Matter network map where devices will connect to each other, to the internet, and to other protocols using Wi-Fi, Thread, and Matter controllers.

[20] https://www.theverge.com/22787729/matter-smart-home-standard-apple-amazon-google

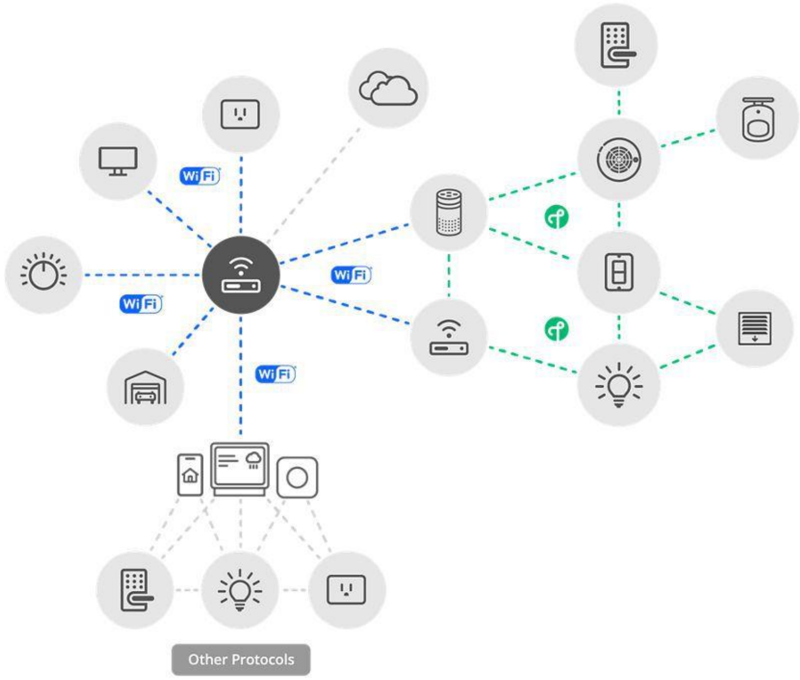


*Figure 4-4: Matter network map. (Source: Image: Z-Wave Alliance, The Verge)*

Thread is paramount for Matter, as it is a low-power IP-based mesh networking protocol, which does not require hubs or bridges to communicate with internet. This will turn IP as the de facto standard of the Internet, providing a single open standard interface for a billion things. However, the drawback is that direct access to these devices may lead to security related issues like authentication[1].

**Semantic interoperability**

Semantic Interoperability is a key issue and a key enabler to open platform adoption, for which ontologies are developed. Ontologies in IoT *are a set of objects and relationships used to define and represent an area of concern. They represent an abstraction technology which aims to hide heterogeneity of IoT entities, acting as a mediator between IoT application provider and consumers, and to support their semantic matchmaking*[1]

Several standards address the need for semantic interoperability to unlock the real potential of IoT, such as ETSI SAREF, ETSI NGSI-LD, OPC UA, W3C SSN, schema.org or oneM2M base ontology. However, gaps remain and these multiple approaches may increase the fragmentation. The wide scope of vertical applications domains prevents the design of a unique standard data models for cross-domain semantic interoperability. Metamodels such as oneM2M base ontology can be considered as a meta-model that may be extended for vertical domain ontology design and implementation[1,19].

**Business context and business procedures / platform interoperability**

The current platform landscape is very fragmented, and also shows certain lack of maturity with a lot of solutions developed ad-hoc point for a very specific question. This hinders the interoperability among platforms, which could be improved by an “standardize approach”, i.e. using solutions from standardisation organisations. ETSI report ETSI TR 103 536 V1.1.2[21] reflects on how this "standardized approach" to platforms is getting traction. This approach would need a choice of a reference (technical) architecture with a layered model, an information and interoperability strategy, a selection of Reference Points and APIs. These solutions are based on standards developed openly with clear and

[21] ETSI (2019) SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms

fair IPR rules, and typically are not controlled by any specific company or group of companies. In the IoT domain, oneM2M is the most prominent example.

Noura et al[1] points at standard APIs for platform interoperability. Application Programming Interface (API) exposes data or functions to an application written in a high-level language, enabling developers streamlined access to functionalities and services. Although public APIs are available for cross-platform interoperability, the majority of IoT platform providers develop and deploy APIs that are platform-specific and proprietary. For example, a mobile application may offer to control an internet-connected dishwasher. Without a standard API, if the mobile application wants to integrate more than one dishwasher vendor, it must write custom code to use another platform-specific API, while a standard API enables cross-platform interoperability between the existing solutions with minimal change in the application. Some examples of projects aimed to resolve this issue are the symbIoTe and Big-IoT which are working on a generic interworking API to provide uniform access to resources of all existing and future IoT platforms to address syntactic and cross-platform interoperability.

## 4.4 Closed ecosystems

**Business context and procedures / platforms**

As explained previously, the proliferation of IoT platforms and their fragmentation is at the core of interoperability issues. There is a plethora of vertically oriented and mostly closed systems: the share of open source platforms is below 5% and the majority dominated by commercial offerings, according to UNIFY-IoT Project.

Closed proprietary platforms provide increased functionality and consistency between their existing devices, to establish a market advantage over their competitors[22]. For small manufacturers, supporting different protocols and interfaces for all platforms can be very costly[1]. Other reasons why manufacturers chose to keep a protocol closed includes security and encryption concerns, and the intellectual property related to the benefits of their closed protocol[23]. Data collection and management is also defined by proprietary systems: Commercial IoT platforms are designed to provide users with a very complete offer of services that go from connectivity up to data visualization, analytics, processing and rule-based actions. When dedicated APIs are developed to enable access from third party applications and systems, the device sending data needs to apply the data format that is inherent to the platform, and the platform will be collecting and managing the data generated by the device[21].

Closed platforms provide means to allow for interoperability, such as public APIs to assist developers access their services. Developers require extensive knowledge of the platform specific APIs and information models of each different platform to be able to adapt their applications from one platform to another. Since many platforms do not offer standard API, as explained in the previous section, developers must write custom code to use each platform-specific API. Apart from standard APIs, other solutions such open standards are considered a significant way to achieve this objective[1,21]. Currently there are several standard bodies, consortiums and alliances trying to solve IoT standard issues including Open Interconnect Consortium (OIC) providing IoTivity and AllSeen Alliance providing AllJoyn. The IoTivity focuses on device interoperability irrespective of form factor, operating system or service provider through protocol plug-ins. The AllJoyn framework functions as a software bus between devices facilitating device interoperability for home automation and industrial lighting applications, providing also solutions for constrained devices.

## 4.5 Lack of penetration of IoT appliances

Connected devices come at a higher price compared to non-connected, often due to the post facto design approach, where manufacturers see the connectivity component as an add-on, which is attached to a standard non-connected product. Often, the priority is to provide high-end devices with connections. Consumers might not be informed about the potential energy savings through interconnected IoT and therefore cannot justify the increased price tags of

[22] United States Government Accountability Office Center for Science, Technology, and Engineering (2017), Internet of Things Status and implications of an increasingly connected world

[23] Department of Energy and Climate Change (2016), Barriers and Benefits of Home Energy Controller Integration

connected devices unless they come with other convenience benefits[24]. Also, the most promising energy savings are found in energy intensive products such as HVAC or water heaters. But when these crucial products break down, consumers have few requirements for the new unit other than buying a substitution that functions[24], thus connection and interoperability with existing smart home devices, are not in the front of consumers' minds.

EDNA report on the role of usability in Smart Homes (2021)[25] shows an evidence review to understand the extent to which poor usability can hamper the energy saving potentials on smart homes. Though interoperability did not arise as a main issue from the evidence found and the experts consulted, some significant questions about the lack of interoperability were raised:

- As uptake of smart home technologies increases, it is likely issues owing to lack of interoperability will also grow. An increase in the variety of options, and the manufacturers who develop them, will likely mean a broader (and potentially more complex) range of functionality will be offered to users. Then, interoperability is likely to become a much greater issue.
- Some specific features/functionality offered by smart homes are expected to be better received as part of a broader application. For example, controls to operate smart lighting may be better received as a sub-feature of a broader whole home application, rather than requiring its own application.

In summary, the role of the end-user to influence interoperability is also affected by the interoperability itself. The consumer-driver towards better interoperability (a greater uptake of smart home technology pushing the market to find interoperability solutions) will lose traction if consumers are discouraged by the lack of interoperability. Therefore, the demand for smart home technologies and its expansion towards IE, DF and smart grids should be promoted. This can be achieved by showing the benefits of smart technologies to reduce bills, save energy, health and security purposes, shifting a demand driven by trends to a demand driven by needs. This way, the presence of smart technologies in households could significantly increase, requiring optimal levels of interoperability.

[24] Xergy Consulting (2021), Harnessing IoT for Energy Benefits

[25] Energy Systems Catapult (2021) Are we getting the best out of Smart Home Technologies? The role of usability.

# 5 Impacts of lack of interoperability

## 5.1 What is the scope of the problem? To what extend does lack of interoperability limit IE and DF (currently and potentially into the future)?

**Energy consumed by IoT**

Smart technologies may induce energy savings of varying volume depending on the devices. An example is a smart fan, that can apply its sensors to operate when air temperature is high, and a person is present in the room. However, relatively to a household's total energy bill, fans consume little energy compared to other appliances such as heaters. The noticeable impact happens, if the fan uses its sensors to efficiently turn on and off the air conditioning or heating and work symbiotically with it. This is also an example of power management functions (turning on and off the device itself) vs. interoperability "smart" functions, where different devices exchanges information. Another example of the latter is a media player such as Apple TV and Chromecast turning off the TV when not streaming.

Furthermore, to truly enable the potential of IE, the algorithms need access to as many sensors as possible[26]. A key factor for a smart device's potential for intelligent efficiency, is the energy usage of the connection technologies. In most cases smart lighting for example does not displace or save energy, as the energy consumption for connectivity outweighs the savings from DF and IE[24]. However, smart lighting would be a subsystem of a smart home where this additional energy consumption would be compensated overall.

The energy consumption of small networking equipment such as modems, gateways, routers, switches and access points was estimated as part of the Ecodesign Working Plan study[27]. According to this study, the annual energy consumptions of the small networking equipment range from 13 of gateways to 72.6 kWh per year of home/office network equipment, amounting to 28.7 TWh for the EU27 stock. In smart home systems, different components and technologies show a variation in power or current consumption, which has been estimated by Zeadally et al[28] (2020), see Figure 5-1.

[26] EDNA (2018), Intelligent Efficiency - a case study of barriers & solutions - Smart Homes

[27] Viegand Maagøe A/S (lead), Oeko-Institut e.V. and Van Holsteijn en Kemna BV (2021) Preparatory study for the Ecodesign and Energy Labelling Working Plan 2020-2024

[28] Zeadally S, Shaikh F K, Talpur A, Sheng Q Z (2020). Design architectures for energy harvesting in the Internet of Things, Renewable and Sustainable Energy Reviews, Volume 128, 2020, 109901, ISSN 1364-0321, https://doi.org/10.1016/j.rser.2020.109901

| | Component | Power/Current consumption |
|---|---|---|
| Wireless technology | Wi-Fi | 835 mW |
| | Zigbee node | 36.9 mW |
| | MiMAX node | 36.78–36.94 W |
| | Bluetooth | 215 mW |
| | BLE | 10 mW |
| | Cellular | 0.1–0.5 W |
| | LoRa | 100 mW |
| Typical sensing devices | Temperature/humidity | 0.2–1 mA |
| | IR | 16.5 mA |
| | Ultrasonic | 4–20 mA |
| | PIR | 65 mA |
| | Light | 0.65 μA |
| | Camera | 270–585 mA |
| IoT node/gateway | WASP mote | 9 mA |
| | Pi | 100–500 mA |
| | Xbow | 17.5–19.7 mA |
| | Arduino | 3.87–13.92 mA |

*Figure 5-1: Power / current consumption of smart home components (Source: Zeadally et al, JRC)*

The Total Energy Model for Connected Devices, developed for EDNA,[29] estimates that the total energy consumption for connected devices (energy consumed by the network connection, the sensors and the standby consumption of devices connected to the network) globally was 100 TWh in 2010 and is expected to rise to 550 TWh in 2025.

**Impact of interoperability in energy consumption**

Quantification of the impact of lack of interoperability is connected with a great uncertainty, due to a lack of studies that actually attempt to measure the potential energy savings. It is widely acknowledged that an improvement on interoperability will lead to a better performance of IE and DF systems, however, the cause-effect relation is difficult to estimate.

Nevertheless, along this study, there is a clear example of how the lack of interoperability increases the energy consumption. Basic connectivity is affected by the co-existence of different protocols and technologies, such as Zigbee, Z-wave, etc., and the most common solution to this lack of interoperability is the use of adapters or gateways (also called bridges and hubs). These devices consume between 13 and 72 kWh per year, according to the Ecodesign Working Plan report, which estimates that the penetration rate in EU27 is approximately 2.3 (the average household owns more than one device). It is estimated that 23% of the EU27 stock are gateways, which covers those aimed to solve basic connectivity issues.

Standardisation of basic connection protocols would reduce the need of gateways, adapters, bridges or hubs, which would lead to a lower energy consumption of smart homes. However, the potential benefits of better interoperability would go beyond this issue, involving the rest of interoperability layers. There are several examples within the home systems and IE that illustrate this margin of improvement. A smart window that controls the amount of natural light for better heating or cooling could interoperate with the smart lighting system. The sensors of natural light and occupancy of these two systems would improve the smart HVAC systems by decreasing or increasing its load gradually. Each of these smart systems has an energy saving potential which has been estimated in several studies[13]. Most savings range 10% of the specific consumption (heating, cooling, lighting, etc.) and the maximum value is estimated for

[29] IEA 4E EDNA (2019) Total Energy Model for Connected Devices

occupancy-based lighting (30 – 40% of lighting consumption). The combination of smart home technologies that provide measurement, monitoring, information displays, management, control, automation, zoning, occupancy systems, etc. could reach 27% energy saving potential on the overall household consumption[13,30]. The difference between 10% and 27% could be a proxy to quantify the impact of interoperability, i.e. it would mean an additional energy saving potential of 17%.

McKinsey[31] estimated that 40% of the potential benefits are achieved through interoperability between the connected systems. It is unclear how this figure has been calculated, but it is likely that end-user uptake and behavioural aspects were taken into account, on top of the improvement in energy savings due to more interoperable smart homes.

**Impact of interoperability in end-users**

As mentioned previously, the smart-home ecosystem has reached households penetrations of 12% worldwide, 16% in EU27 and 40% in US, in 2021 (Statista). The estimated penetration in 2026 will be 25%, 39% and 63%, worldwide, EU27 and US respectively (Statista).

As pointed out in EDNA Usability report[25], integration of smart technologies into households will naturally happen in increments, so interoperability plays a role in this gradual progression, and its issues may discourage end-users to adopt smart home solutions. For example, users may need technical assistance to set up the smart home systems and the use of diverse technologies from various manufacturers make technical support a challenge[26].

Besides, interoperability issues may lead to misuse or underutilization. Due to lack of interoperability, users may often need to interact with fragmented systems and interfaces, such as smart meters, lighting control, heating and cooling displays, window displays and switching between various smartphone apps. This poor user experience might lead to users not making the effort to manage and reduce energy consumption. As an example, Hargreaves et al[32] report on new in-depth qualitative data that explore the domestication of a range of smart home technologies in 10 households participating in a nine-month field trial. Some of the households were frustrated at a lack of interoperability and other called for further development of the systems – particularly related to user-interface design and interoperability – to make the practical work of domestication easier.

Long-term issues emerge when the rapid evolution of IoT intersects with household appliances, whose average lifetime is 15 years. In this case, wireless technologies will remain along the lifetime of the appliance, despite the evolution towards low energy solutions (e.g. from Wi-Fi to Zigbee). Besides, bridges, hubs or signal amplifiers will also outlive any interoperability or technological improvement. For example, Philips Hue Bridge smart lighting hub will be automatically enriched with Matter, making all connected Philips Hue products compatible, however, the hub will still be needed to connect the light bulbs.

## 5.2 What are the commercial drivers for proprietary device ecosystems? What would be the commercial impacts if ecosystems were required to be "open"?

Closed ecosystems for smart devices communication represent the majority of IoT platforms, see Section 4.4. As a result, consumers are facing the "vendor lock-in" effect, where they cannot freely select new hardware, but are required to purchase from the same manufacturer to enable interoperability within the product ecosystem. Adding products from another vendor would include significant costs as the whole ecosystem would have to be changed[33].

The diversity of communication protocols and the use of closed proprietary ecosystems requires additional hardware to enable potential interoperability, and the increased hardware and energy use might make up for the potential energy

[30] BPIE (2017) Smart Buildings Decoded. https://www.bpie.eu/wp-content/uploads/2017/06/PAPER-Smart-buildings-decoded_05.pdf

[31] McKinsey Global Institute (2015) The internet of things: mapping the value beyond the hype

[32] Tom Hargreaves, Charlie Wilson & Richard Hauxwell-Baldwin (2018) Learning to live in a smart home, Building Research & Information, 46:1, 127-139, DOI: 10.1080/09613218.2017.1286882

[33] Kaltenbrunner, Neuschmid, Dr. Bieber, Baumann & Meir-Huber (2016), Future of Interoperability

savings in demand flexibility[18]. But such hardware would limit the complexity and confusion that is associated with the many individual ecosystems. An example is smart home hubs from Apple or Google, where multiple different protocols and ecosystems are connected to the hubs. The big corporations dictate which protocols are open and the smaller device manufacturers would be pressured to comply to sell products to customer segments that own that type of hub[34].

**Classification of platforms according to their "openness"**

In order to understand the nature and extension of closed ecosystems in the IoT landscape, it is necessary to define the different IoT platforms according to their level of openness. ETSI[21] provides a very useful classification to this purpose, from more open to less open platforms provided below in the excerpt of the ETSI report:

*Standards-based*

A standardized platform is referring to the development by a Standards Development Organisation or Standards Setting Organisation of (paper-based) specifications (with additional interoperability support such as plugtests). A standardized platform will typically encompass the description of a Reference Architecture (with potentially several models, the most frequently used being the Functional Model), a set of supported protocols, a set of interfaces (in particular Application Programming Interfaces), etc. The main advantages of a standardized platform are that it allows for multiple implementations, offers controlled interfaces, provable and proven interoperability, and maintenance over time with transparent control over the evolution of the features.

*Open source platform*

An open source platform is referring to the development by an Open Source community or ecosystem of a set of (source code-based) software components. An open source platform will typically encompass the provision of source code and documentation attached to a configuration and version management framework.

The main expected advantages of an Open Source platform are that it is likely to offer controlled interfaces, some support for proof of interoperability, maintenance over time with transparent control over the evolution of the features.

An important aspect when using open source is the licensing. Open Source licenses are organized in two main categories: copyleft and business-friendly licenses:

- Under a copyleft license, users have to copy, distribute, and update the software under the same license as the original software. Copyleft clause is assumed to have an automatic effect that can lead to "contamination" (that any software combined with copyleft licensed software could somehow be transformed to be licensed under a copyleft license). Copyleft supporters are concerned with ensuring that their work remains available to everyone.
- By contrast, business-friendly licenses do not restrict the licenses under which these acts can be done and do not cause any "contamination" effects. Business-friendly license supporters believe the licensing restrictions mean that the copyleft is not a free license and their alternative encourages the use of free software.

*Industry Group-based*

An Industry Group-based platform refers to the development by an Industry Group (IG) of (paper-based) specifications.

The specification can come-up with a reference implementation developed by some of the IG members (that may be proposed as Open Source sometimes during the platform development).

Such solutions are typically organized around the solutions of a leading company or a set of leading companies, in an attempt to enlarge the ecosystem and reach market recognition. These specifications are often (but not always) developed openly with clear and usually fair IPR rules, even though they tend to be associated with specific technology players. In most of the cases these groups develop around specific protocols, API and data models, and they limit the specification to IoT components and in some cases frameworks for platform development specifying platform solutions

[34] Hannu Järvinen (2015), Web Technology based Smart Home Interoperability

*Proprietary*

A proprietary platform is referring to the provision by a company (ranging from SME to Multinational Corporations) of a set of (executable) software components and documentation provided under the form of standalone software or as Software as a Service (SaaS) over a public, private or hybrid cloud. There are some differences whether the addition of some support to openness:

- Closed specifications. They are fully integrated and developed in house, and rely on a closed ecosystem of providers, developers and integrators. It is very common to find specialized solutions for specialized components of the IoT systems, and sometimes in some vertical IoT business sectors. This is also the case of large providers of more traditional solutions, that are now being positioned in the market in a way to take advantage of the current interest in IIoT technology. An example is the case of a proprietary middleware product for which, due to lack of proper documentation, some OEMs willing to extend and customize some functionality had to resort to the use of communication protocols sniffing in order to understand inner system working.
- Open Specifications. Such solutions are based on a proprietary solution (that may include components based on existing standards or adapted from existing standards) initially developed by a single organization (often a very large corporation) and further opened to an ecosystem of other companies and players. The intention is to create a market or to accelerate its consolidation, and to steer the market towards their solution. This approach tends to confer a major role to the developer of the proprietary solution, thus making the market dependent upon it. The success of such an approach is depending on the ability to quickly become a de facto standard for the market.

**Drivers**

Manufacturers design IoT devices to use proprietary protocols or specifications that limit interoperability with other brands to establish a market advantage. Proprietary vendor standards may increase functionality and consistency with that vendor's products, but can complicate integration by other companies. Closed proprietary ecosystems also allow for increased functionality and consistency between their existing devices, to establish a market advantage over their competitors[35]. Other reasons why manufacturers choose to keep a protocol closed includes security and encryption concerns, and the intellectual property related to the benefits of their closed protocol[36]. At the same time, proprietary protocols or specifications may create opportunities for companies looking to manufacture and sell "bridge" capabilities that allow that vendor's proprietary products to have some interoperability with open standards.

Despite that there are many interests from legacy companies to protect their proprietary systems advantage, there is a wide consensus that open standards and sources are required to fully implement interoperability in all the sectors from industry to smart homes. It is particularly critical to ensure the interoperability among several platforms and business contexts, as it would the case of IE, DF and smart grids. Besides that, it has become evident that interoperability issues hinder the full deployment of effective IoT solutions, and hence the uptake of smart home systems. One of the biggest obstacles of using the IoT is the perception that certain products or services do not have any obvious IoT application or benefit. The full potential of the IoT will be unlocked when small networks of connected things become one big network of connected things extending across industries and organizations[39]. ETSI also points out another driver for adopting open standards, which is to steer the market towards their solution, making the market dependent upon it. The success of such an approach depends on the ability to quickly become a de facto standard for the market.[21]

Therefore, there are drivers currently working towards more "openness" where closed ecosystems are dominant. For example, Z-Wave was a closed standard owned by Silicon Labs until 2020 when it became completely open, a strategic decision to not be left behind in the IoT market. Matter also illustrates how big companies need to reconcile their

[35] United States Government Accountability Office Center for Science, Technology, and Engineering (2017), Internet of Things Status and implications of an increasingly connected world

[36] Department of Energy and Climate Change (2016), Barriers and Benefits of Home Energy Controller Integration

closed systems with common and more open solutions in order to expand their markets. In words of Z-Wave Executive Director Mitch Klein, “if this [Matter] is successful, everyone sells more”[20].

Matter is developed and managed by the Connectivity Standards Alliance (former ZigBee Alliance), whose members are most of the big tech companies[37]. The Connectivity Standards Alliance has three levels of membership: promote, participant, adopter and associate, from more to less power and access, and consequently, larger to smaller fees[38].

**Closed ecosystems to be open?**

However, the market drivers may not be sufficient to reach the optimal level of open sources that would untap IE and DF potential. In that case, a public intervention to require closed ecosystems to be open could be considered as a possible solution, and there could be many advantages. The most relevant one would be that IoT innovation is not hampered by the silo vision of proprietary platforms and then can create added-value solutions that move from devices to real services with a perceivable benefit for consumers[39]. It would also prevent that a player dominates the market, enabling more competition[21].

The IoT market is growing fast, but it is still in a learning curve, meaning that it relies on research and innovation. As IoT proliferates, the value creation is changing and the implications for business model innovation are very important. The current situation is already pushing the borders between the legacy business models and the emergent players and start-ups, so all players are defining their strategies[39]. Some solutions found in literature identify critical elements that require special focus, such as semantic interoperability and open standards for platform interoperability[1,21]. Mandatory requirements towards more open ecosystems can help to drive the market towards better solutions and innovation.

The organisational interoperability is crucial particularly for DF, where different systems and actors must work coordinately to deliver optimal results. In this regard, the term “IoT platform federation” is commonly found in literature to define multiple partnering institutions that collaborate by sharing IoT resources[40]. Another definition of IoT platform federation is an association of a number of platforms enabling their secure interoperation, collaboration and sharing of resources. Platforms can be enabled to perform collaborative tasks and to interact directly so as to trade/share resources[42]. UNIFY-IoT report also concludes that IoT platforms need to be and act as a complete ecosystem converging the consumer/business/industrial applications by collecting and sharing data broadly within an organization, sectors, and IoT applications. It points to the development of IoT Platforms as a Service as a strategy that is pushed by several large IoT players, and the federation of different IoT platforms together with other types of platforms[14]. Some authors call for a concept of federation of IoT that allows the connectivity of a large number of various IoT heterogeneous devices, and is able to collect and aggregate the huge quantities of data generated - while guaranteeing the privacy of the information exchanged - to support a variety of IoT applications[39].

The current IoT landscape shows that the main players are aware of the need to work together for harvesting the full market potential. Collaboration across the complex IoT ecosystem is required to create a value chain, including the deployment and implementation of new IoT technology and applications. Much of the potential value will come from moving beyond the proprietary technology silos, and new added value may come from product and service innovations beyond current products and market segments[39].

---

[37] https://csa-iot.org/members/

[38] https://csa-iot.org/become-member/#membership

[39] Ovidiu Vermesan, Mario Diaz Nava and Hanne Grindvoll (2015) Driving Innovation through the Internet of Things – Disruptive Technology Trends

[40] European Platforms Initiative (2018) Advancing IoT platforms interoperability

# 6 Standardisation efforts and gaps

The aim of the subtask is to provide an overview of ongoing standardisation efforts and gaps related to interoperability. In order not to re-do the comprehensive work that has already been done in this area, we build on previous studies, mainly the 2016, ETSI TC Smart M2M IoT standards mapping and gap analysis[41], ETSI STF547 Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms[21] and AIOTI report High Priority IoT Standardisation Gaps and Relevant SDOs[42].

In 2016, ETSI TC Smart M2M mapped IoT standards and analysed gaps in the IoT standards landscape[43]. The report divided the IoT standardisation landscape into eight domains:

- Smart cities
- Smart living
- Smart farming and food security
- Smart wearables
- Smart Mobility (smart transport/smart vehicles/connected cars)
- Smart Environment (smart water management)
- Smart Manufacturing

Even though smart grid is not specifically mentioned as a category, smart grid related standards are included in the overview, such as IEEE PLC[44], and through other standards encompassing the functions necessary for a smart grid, such as Zigbee[45].

The second of the ETSI reports (TS 103 376), contains the gap analysis, which addresses three categories of gaps:

- Technology gaps. Some examples in this category are communications paradigms, data models or ontologies, software availability.
- Societal gaps. Some examples in this category are privacy, energy consumption, ease of use.
- Business gaps. Some examples in this category are siloed applications, value chain[46], and investments.
- The report continues with a description of the gaps in terms of:
    - The characterization of gaps, in particular by understanding the type of gaps (see above), the scope of the gap, the difficulties it generates, and other appropriate descriptions.
    - The mapping of the gaps on an architectural framework that allows for the mapping of the gaps on a reference that can be understood by the IoT community and, in particular, that can be related to other frameworks e.g. those developed in other organizations, for instance in Standards Setting Organizations.

---

[41] ETSI TS 103 375 https://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf and ETSI TS 103 376 https://www.etsi.org/deliver/etsi_tr/103300_103399/103376/01.01.01_60/tr_103376v010101p.pdf

[42] AIOTI WG03 – IoT Standardisation (2020) High Priority IoT Standardisation Gaps and Relevant SDOs

[43] ETSI TS 103 375 https://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf and ETSI TS 103 376 https://www.etsi.org/deliver/etsi_tr/103300_103399/103376/01.01.01_60/tr_103376v010101p.pdf

[44] IEEE 1901.2 and amendment IEEE 1901.2a (2015) (Low-Frequency Narrowband Power Line Communications for Smart Grid Applications), which has been assigned to the categories “Smart Cities”, “Smart living” and “Smart environment” in the report.

[45] Note from Report: ZigBee Smart Energy version 1.1. The latest version for product development, adds several important features, including dynamic pricing enhancements, tunnelling of other protocols, prepayment features, over-the-air updates.

[46] Unbalanced costs/benefits (benefits end up with different supply/value chain partner), unavailable business models or value chains in certain domains and incapability of developing service-oriented solutions as result.

In a report from 2016[47], the authors state that: “standardisation in IoT has largely focused on the technical communication level, leading to a large number of different solutions based on various standards and protocols, with limited attention to the common semantics contained in the message data structures exchanged at the technical level. The Smart Appliance REFerence ontology (SAREF) is a shared model of consensus developed in close interaction with the industry and with the support of the European Commission.”

Hence, SAREF is a new development not trying to replace any existing technology, but trying to bridge a gap in interoperability through collaboration and development of new solution, as described in the ETSI reports: encourage the large SDOs/SSOs to strengthen collaboration and cooperation, and to accelerate the provisioning of necessary IoT standards and specifications that will strengthen the adoption of IoT as a major ICT platform, thus supporting the EC's objective to make the IoT available and secure. Collaboration should aim to develop new solutions rather than recreate silos or duplicate solutions.

Another such collaboration initiative is the EEBUS, which is an industrial initiative, which originated in Germany, but now has members globally. EEBUS seeks to develop an open, standardised networking specification for energy in IoT to allow manufacturer-independent communication between actors in the smart grid. EEBUS has global partnerships with various associations in Europe, Asia and the USA. EEBUS is active in several standardisation bodies, such as the VDE standardisation organisation DKE in Germany, and relevant organisations at European (CENELEC and ETSI) and international level (IEC).

The third of the ETSI reports (TR 103 536) addresses the issues related to the interoperability and interworking of IoT platforms, in particular standardised IoT platforms, and how the way they are handled can foster their adoption by the IoT community. It outlines the nature, the role of IoT platforms and proposes elements for the identification of the most relevant ones. The issues related to the interoperability and interworking of IoT platforms are explained, and strategies and recommendations for the IoT community for their platform-related decisions.

AIOTI report presents the study of resolution of High Priority IoT Standardisation Gaps by relevant standardisation organisations and add new gaps approved by the AIOTI WG03 group. This work had the support of ETSI STF 547 and addressed the topic of standards gaps in the Technical Report TR 103 376. This report identifies the main gaps in the field of connectivity and interoperability and will serve as backbone and main reference for the description of the current standardisation gaps, together with ETSI TR 103 536 on platforms. Most parts of this section are excerpts from those reports in order to keep the rigour and integrity of the technical information.

## 6.1 Connectivity

**Description of the issue**

As explained in previous sections, there are different wireless and wireline technologies in the IoT ecosystem which currently co-exist and hinder interoperability. AIOTI does not envisage a convergence to a single technology, therefore it is difficult to standardise a single connectivity mechanism in IoT.

**Current standardisation work**

Standardisation activities for are already going on in Open Networking Foundation (ONF), ETSI Industry Specification Group, and IEEE is standardizing Time Sensitive Networks (TSN).

**Potential solutions**

The use of multiple communication infrastructures is here to stay due to the characteristics of each communication technology (LoRa, GPRS/3G/4G, Satellite, etc.). ETSI report signals IP as the best candidate for convergence layers. Other authors also suggest IP-based solutions for the connectivity gap.

[47] Laura Daniele, Monika Solanki, Frank den Hartog, Jasper Roes, ”Interoperability for Smart Appliances in the IoT World”, 2016

## 6.2 Semantic interoperability

**Description of the issue**

Semantic interoperability in IoT platforms is considered as a step towards further global interoperability as required for different domains including industrial IoT and smart cities. There needs to be standards to interpret and process the sensor data in an identical manner across heterogeneous platforms, i.e. a global and neutral data model. Several standardised information models, which could be used for this purpose, already exist, but they are not provided in a machine-interpretable form.

**Current standardisation work**

Some standards addressing these issues are oneM2M base ontology, ETSI SAREF, ETSI NGSI-LD, OPC UA, W3C SSN, schema.org.

The oneM2M standards support different approaches for semantic interoperability:

- Pure ontology-based solution (RDF/OWL serialisation format)
- Common vocabulary (basic serialisation format XML or JSON): Smart Device Template (SDT) for the home domain
- Resources specialisations using oneM2M FlexContainer resources;
- Blackbox resources: Basic oneM2M resources (Container, ContentInstance and Group) extended with an external domain-specific data model

The Smart Applications Reference Ontology (SAREF) is a standardised ontology for IoT devices and solutions published by ETSI in a series of Technical Specifications. SAREF is conceived in a modular way in order to allow the definition of any device from pre-defined building blocks, based on the function(s) that the device performs. These building blocks allow separation and recombination of different parts of the ontology depending on specific needs. The SAREF ontology supports a direct mapping with the oneM2M Base Ontology oneM2M TS-0012 and thus runs with oneM2M-compliant communication platforms.

ETSI ISG CIM (Industry Specification Group for cross-cutting Context Information Management) working group defines an API called NGSI-LD. The NGSI-LD Information Model prescribes the structure of context information supported by an NGSI-LD system. It is defined at two levels: The Core Meta-model and the Cross-Domain Ontology.

OPC UA (Unified Architecture) is a standard for horizontal communication from machine to machine (M2M) and for vertical communication. OPC UA provides a framework that can be used to represent complex information as Objects in an Address Space.

The Semantic Sensor Network (SSN) ontology focuses on the description of sensing devices and the observations they make of the physical world, the involved procedures, the studied features of interest, the samples used to do so, and the observed properties, as well as actuators. It follows a horizontal and vertical modularization architecture by including a lightweight but self-contained core ontology called SOSA (Sensor, Observation, Sample, and Actuator) for its elementary classes and properties.

The Web of Things (WoT) is a standardisation activity by the World Wide Web Consortium (W3C). WoT seeks to counter the fragmentation of the IoT through standard complementing building blocks (e.g., metadata and APIs) that enable easy integration across IoT platforms and application domains. A Thing is an abstraction of a physical or virtual entity that needs to be represented in IoT applications. Thing is represented by a Thing Description (TD), which is a machine-readable description. A TD provides general metadata of a Thing as well as metadata about the Interactions, data model, communication, and security mechanisms of a Thing. Thing's Interactions are specified in a so-called Interaction Model. The model defines three types of Interactions: Property, Action, and Event.

iotschema.org is a W3C Community Group for extending Schema.org to connected Things. The organization provides an open, publicly available, repository of semantic definitions for connected Things. It is an extension of well-known schema.org to enable descriptions of Things in the physical world and their data. iotschema.org can be effectively used to semantically enrich W3C Thing Description. It provides a way for domain experts to easily create semantic definitions that are relevant to their application domain. iotschema.org reuses existing standardised semantic definitions whenever possible.

**Potential solutions**

The previous paragraphs show that there are currently standards and directions being followed for the semantic description of systems. As the different IoT platforms often choose one of these solutions, there is a need for (standardised) entities or reference / abstract ontologies able to perform the mapping between the different existing ontologies. The mapping can be realized directly between the ontologies used by the different systems or by translating each used ontology to a generic ontology that serves as a common reference. Several initiatives are addressing reference models such as oneM2M Base ontology and ETSI SAREF ontology.

## 6.3 Platform interoperability

**Description of the issue**

As explained in previous sections, the heterogeneity of IoT platforms raises interoperability issues from technical to organizational level. These issues may lead to a broad range of interoperability difficulties, ranging from total impossibility of exchanging data to being able to exchange messages that cannot be understood, up to not being able to assign the correct meaning to data that has been exchanged.

**Current standardisation work**

ETSI report analyses the technical approaches in support of interoperability and outlines some criteria for best support of interoperability within and between platforms.

First, ETSI defines a standardised platform as the specifications developed by a Standard (Development or Setting) Organisation. A standardised platform will typically encompass the description of a Reference Architecture (with potentially several models, the most frequently used being the Functional Model), a set of supported protocols, a set of interfaces (in particular Application Programming Interfaces), etc. The main advantages of a standardised platform are that it allows for multiple implementations, offers controlled interfaces, provable and proven interoperability, and maintenance over time with transparent control over the evolution of the features.

Figure 6-1 shows the different interoperability criteria that may be covered by standardised platforms, according to two dimensions considering the horizontal interoperability (with three levels H1, H2, H3 each of them being an extension of its predecessor) and the vertical interoperability (with two sub-categories, each composed of two levels: V1, V2 and V3, V4).

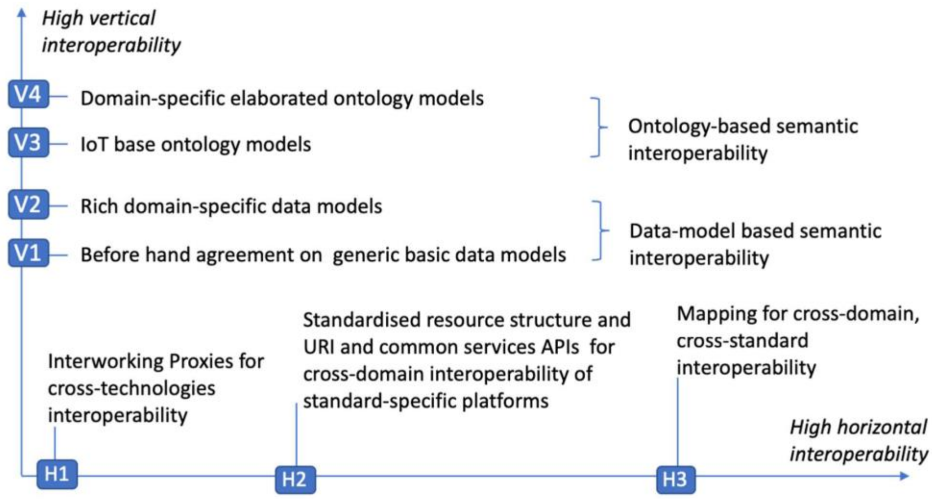


*Figure 6-1: Synthetic view of interoperability dimensions (Source: ETSI)*

In order to better understand how the criteria would be applied, ETSI report evaluates H2020 AUTOPILOT project[48] (devoted to automated cars) against these levels of horizontal and vertical interoperability, resulting in the following conclusions:

- H1: The system architecture of AUTOPILOT is composed of several interworking proxies for interworking with heterogeneous technologies from the ITS domain such as CAN, 6LowPan, etc.
- H2: AUTOPILOT platform is based on oneM2M standard which offers a unified resource structure and common service APIs paving the way to interoperability with specific platform such as Fiware context broker, Watson IoT and Ocean.
- V1: In AUTOPILOT devices and applications could exchange data in a seamless way however a beforehand agreement still required to understand the exchanged data.
- V2: AUTOPILOT offers a rich data model inspired from DATEX and SENSORIS that serves as a common vocabulary between the interacting entities.

AUTOPILOT does not support the H3 level since the current architecture and data model remain specific to ITS domain and are not extended and validated with other domains. In addition, AUTOPILOT does not support V3 and V4 interoperability levels since the data model does not rely on ontologies.

Another approach mentioned in ETSI report is the model of market places, where actors involved in the provision of the IoT service are seen as consumers and providers within an application market. An IoT marketplace is a new platform to extend the "traditional" IoT platforms with brokerage concepts supporting automated discovery, trading and even pricing. Within an IoT marketplace platform, the IoT device owners will have the possibility to selectively grant access and trade their data with many potential vendors. An example of IoT market place is within the BIG IoT project[49]. BIG IoT architecture for IoT is based on an open marketplace for IoT platforms and services as providers to trade available resources (information and functions). The architecture is centred around a common set of interfaces, referred to as the BIG IoT API[42], a generic unified Web API for smart object platforms to address the interoperability gap[49]. According to AIOTI report, the interface specifications in the BIG IoT project have influenced the standardisation at W3C's Web of Things initiative, in particular BIG IoT API "access", a crucial interface as it is the basis for communication within IoT applications[42]

[48] https://cordis.europa.eu/project/id/731993/reporting

[49] https://iot-epi.eu/project/big-iot/

**Potential solutions**

ETSI indicates that the "Standardized approach" (originated by Standard Development Organisations) to IoT platforms could be a promising solution. The approach is relying on the choice of a reference (technical) architecture with a layered model, an information and interoperability strategy, a selection of Reference Points and APIs. This standardized approach will help platforms to fulfil the criteria described by ETSI advancing in both axis of interoperability, vertical or functional and horizontal[21].

# 7 Implications of interoperability and lack thereof for policy makers

Interoperability spans a wide scope, which ranges from connectivity to organisational issues. The IoT landscape is characterised by a rapid growth and high heterogeneity, which lead to issues on market uptake, lack of standardisation and proprietary platforms. The main actors of the IoT market are already aware of these issues and how they hamper the expansion of the market and the evolution to added-value services, and they collaborate to resolve them in their own interests. Other issues are essential, such as ensuring business interoperability for the proper development of DF solutions. In any case, some specific areas deserve a closer focus and could be considered priorities for public intervention:

- Support of open platforms and standards
- Stimulation of market uptake
- Information to end-users to support their purchase choice, given the proliferation of IoT devices and systems
- Support of standardisation for interoperability
- Organisational interoperability

There are different policy options that could be adopted to address these areas: mandatory minimum requirements, mandatory information to consumers, voluntary labelling, incentive programs, standardisation support, self-regulation frameworks. These policy options are applied on the priority areas identified, analysing the implications for policy makers and their potential impact.

## 7.1 Mandatory minimum requirements

Mandatory requirements could be a way to ensure a level of openness that ensures interoperability. As an example, the voluntary ENERGY STAR Connected Functionality criteria require devices to use open standards for energy consumption reporting, operational status reporting, and demand response activities. The products covered by this specification are:

- Connected thermostat
- Electric Vehicle Supply Equipment
- Pool pumps
- Water heaters
- Central AC and heat pumps
- Ice makers

If this voluntary requirement were adopted as mandatory, proprietary solutions for specific functions would be excluded. The most popular standard protocols currently used in smart home applications are already open, however, a market analysis would be needed to get a closer insight into the potential impact of this mandatory requirement in proprietary solutions. In this regard, New Zealand government acknowledges how proprietary systems restrict the potential of DF and is studying to either ban proprietary systems or make proprietary system providers use open communication protocols.

Another example of mandatory requirement can be found in UK, where EV chargers must be able to switch aggregators seamlessly according to a recent policy announcement. In this case, the requisite does not prescribe any specific way to reach this level of interoperability, so it could be considered technology-neutral.

At more complex levels beyond smart devices, i.e. IE and DF systems and smart grids, interoperability could benefit from a common testing methodology as the one developed by JRC for smart grids[50]. A harmonised and recognised

[50] Papaioannou I., Tarantola S., Lucas A., Kotsakis E., Marinopoulos A., Ginocchi M., Olariaga Guardiola M., Masera M., Smart grid interoperability testing methodology, EUR 29416 EN, Publications Office of the European Union, Luxembourg, 2018, ISBN 978-92-79-96855-6, doi:10.2760/08049, JRC110455

testing method could evaluate smart home systems as a whole and would allow a fair comparison and setting minimum. However, this option requires time, resources and in some cases establishing additional testing facilities that may be too costly.

Specific mandatory requirements could be set at semantic interoperability. The EU preparatory study on smart appliances[19] discusses the different policy options and technical requirements, and regarding interoperability, the focus is on semantic interoperability. If smart energy capable appliances share a common understanding of the demand side flexibility concepts by means of “supporting a common data model”, then this enforces the capability for appliances and energy management applications to understand each other. A common data model means that it complies with an imposed reference ontology, i.e., the model can be mapped to the reference ontology. The preparatory study of smart appliances recommends the use of ETSI SAREF to implement the semantic interoperability requirements[19], however, extending this recommendation at global scale should require further analysis. International collaboration on interoperability standard development would be the way to support international trade since many manufacturers sell their products in different areas.

## 7.2 Mandatory information to consumers

This type of policy options provides information that show the differences in a specific feature or parameter performed in products on the market. The information must be digestible for all consumers, provided in the form of a rating system, for example, as it would be the case of energy labelling. The interoperability criteria would cover different aspects, such as connectivity, open sources, standard protocols, etc., and the rating system would be developed according to the compliance with the interoperability criteria. This would need a further development based on a deep understanding of interoperability issues applied to the various devices and systems, and also designed for different consumers (small private consumers, big consumers as companies, public authorities). For small private consumers, the information could be too complex, but it could be appropriate for companies and public authorities.

As inspiration for a rating system, there is the Decision-Maker’s Interoperability Checklist developed by the GridWise Architecture Council[51]. This checklist is a tool to help regulatory and utility decision-makers evaluate options such as capital asset investments or new information technology opportunities to determine whether they have the characteristics and attributes that contribute to interoperability. It is considered just a first filter and users are encouraged to scrutinise more deeply, but it is an interesting approach that could be used for public procurement, for example. The checklist could also be a basis for establishing mandatory consumer information requirements i.e. the information the suppliers should provide covering the topics of the checklist. Some of the questions within the checklist are quoted below:

*1. Does the proposal specify the points of interface, where this part of the system interacts with other elements (whether that interaction is with grid equipment, software, the market, other business organizations, or human users or operators)? Does the proposal lay out what information or functionality will flow across these interfaces? Does the proposal specify technology and information requirements only at the points of interface (and not inside the subsystem at issue)?*

*2. Does the device/system use an open architecture? Does the proposed approach consider the technical, informational, and organizational aspects of interoperability?*

*3. Does the proposal maintain technology neutrality; in that it specifies performance results and outcome requirements rather than prescribing a specific technology or method to achieve those results?*

*4. Can the device or system be supplied by multiple vendors?*

*5. Does the system or device rely on openly available standards, specifications, or generally agreed-upon conventions? Do profiles and/or testing and certification programs exist to support implementations based on such standards,*

[51] GridWise Architecture Council (2020) Introduction to interoperability and decision-maker’s interoperability checklist version 1.6

*specifications, or generally agreed-upon conventions? Does the device or system connect to the electric system and communications network elements in ways that comply with applicable standards for its type?*

*6. Does the device have the physical and electronic capability to interconnect with communications media (e.g., network, fiber optic or broadcast capabilities to access Ethernet or other communications capabilities)? Can the communications networks used by the system or device coexist or exchange data with the networks used by other devices or systems, built by other vendors or electricity providers?*

*7. Does the device/system use standard communications protocols? Are such communication protocols and information models supported by commonly identified profiles? Is there widely used and generally agreed upon standards or specifications for the data formats (and the information models) used by the system or device so it can be understood by a variety of communications technologies and devices?*

Another source of inspiration for interoperability criteria is provided by ETSI and the two-dimensions vertical and horizontal of interoperability (see Section 6.3) could be used to evaluate IoT platforms and rate them according to interoperability levels, ensuring interoperable devices through the platforms.

Information to consumers can be a powerful market driver that avoids the exclusion of products, which could be too restrictive for immature markets such as IoT. Both rating systems and labels require a strong support from governments to become visible and understandable by consumers. Communication is crucial for the implementation of this type of policies for raising public awareness and creating a demand for these products. In this regard, information to consumers can work at two levels: orienting their purchase choices and stimulating the uptake of IE and DF systems.

## 7.3 Voluntary initiatives

Instead of a rating system, a voluntary label would be the simplest signal for consumers to best identify interoperable products in the market, which would comply with certain criteria. There would not be a rating system, the label would be awarded to compliant products. It would be much easier to develop than a rating system, but it would not enable comparison between products, though it could provide useful information on which protocols for interoperability are supported. This approach is being considered by New Zealand government as an option to improve interoperability.

Another example of voluntary initiative is the European Commission work to develop the Code of Conduct to the energy smart appliances manufacturers for adherence[52]. The design of the Code of Conduct addresses two main challenges:

- The definition of the principles for data sharing among appliances, home & building automation systems, EV chargers, aggregators, DSOs (Distribution System Operators)
- The development of Interoperability requirements for energy smart appliances

Voluntary initiatives are effective if there is a strong support from the involved sectors, or there is a significant demand because consumers are aware of the issue covered by the voluntary label. On the other hand, an advantage of voluntary labels is that the criteria can be much more ambitious than mandatory requirements and could be used to recognise innovative initiatives aimed to improve interoperability in the fields of open sources and standardisation, among others.

## 7.4 Incentive programmes

Incentive programmes are important instruments to support those projects and initiatives that innovate in the field of interoperability or promote open sources and standardisation. An example of these initiatives would be the IoT European Platforms Initiative (IoT-EPI)[49] which has been cofounded by European Union's Horizon 2020 research and innovation programme. The projects address the topic of Internet of Things and Platforms for Connected Smart Objects and the specific areas of focus of the research activities are architectures and semantic interoperability. The IoT-EPI ecosystem has been created with the objective of increasing the impact of the IoT-related European research and

[52] https://ses.jrc.ec.europa.eu/development-of-policy-proposals-for-energy-smart-appliances

innovation, and covers seven European projects on IoT platforms: AGILE, BIG IoT, INTER-IoT, VICINITY, SymbIoTe, bIoTope, and TagItSmart. More than 50% of the platforms that the IoT-EPI projects are utilising are open source, while the proportion of open source platform is below 5% and the majority dominated by commercial offerings[14]. This shows the relevance of open source in interoperability, and it could be strengthened by establishing it as a requisite to access to the public financial support. Besides, specific incentive programmes could be aimed at financing those projects that are more relevant, require more collaboration or face financial difficulties.

## 7.5 Standardisation and openness support

Several standards address the need for semantic interoperability to unlock the real potential of IoT, such as ETSI SAREF, ETSI NGSI-LD, OPC UA, W3C SSN, schema.org or oneM2M base ontology. As the different IoT platforms often choose one of these solutions, there is a need for (standardised) entities or reference / abstract ontologies able to perform the mapping between the different existing ontologies. The mapping can be realized directly between the ontologies used by the different systems. Semantic interoperability is being addressed in different standardisation organisations, which deliver ontology and semantics standards, but gaps remain and coordination between various groups would be needed to avoid a fragmented offer for IoT semantics[42]. Platform interoperability can be also improved by an "standardised approach" as outlined by ETSI. Supporting the use of SDO platforms such as oneM2M standard will help improve the interoperability of platforms, which is seriously hindered by the fragmentation and heterogeneity. This solution usually consists of the federation of different platforms through a standardized middleware, solving the issues of platform interoperability.

South Korea's 'Master Plan for Building the Internet of Things (IoT)' puts forward an open platform environment provided by the government, on which the private sector can develop IoT technologies, as part of the strategy to support open innovation. Service providers would access IoT data through an open platform accessible to everyone[53]. This measure would also increase the interoperability among devices and services. This approach is in line with ETSI recommendations to support standardised and open platforms which develop solutions that focus on interoperability and the integration of multiple technologies[21]. Standardised platforms also avoid a dominant stakeholder since they operate in a transparent manner to offer solutions that have a global, worldwide applicability. With this approach, the development of the platform is simplified and open to multiple, interoperable implementations that allow their adopters to focus on the development of IoT services.

## 7.6 Self-regulation

As explained in other sections, organisational interoperability can be realised by IoT platform federations formed by multiple partnering institutions that collaborate by sharing IoT resources. Some examples of federations are found in IoT-EPI projects, such as SymbIoTe or AUTOPILOT[14]. UNIFY-IoT report highlights the relevance of developing and deploying IoT technologies and applications using a federation of IoT platforms and a strong IoT ecosystem of industrial, consumer and business stakeholders. In that way, the IoT federation will span all the value chain and will create managed services offerings and co-create added-value products, services, experiences. This is of particular interests for IE, DF and smart grids where many different devices need to interact and different players need to collaborate to deliver results.

In this context, policy-makers can contribute by promoting a self-regulation framework to develop the different protocols and agreements that will rule the IoT platforms federations, such as the Service Level Agreements indicated by AIOTI[41]. This self-regulation framework could help enhance aspects such as openness, standardisation and the participation of stakeholders.

[53] South Korea ICT Ministry (2014) Master Plan for Building the Internet of Things (IoT)

# 8 Conclusion and policy recommendations

The IoT market has developed rapidly creating a fragmented and heterogeneous landscape that hinder interoperability among the different devices and systems, and this situation has not helped the standardisation efforts aimed at solving these gaps. There are already solutions for interoperability that require certain levels of openness, but most platforms are proprietary, leading proprietary protocols or specifications that limit interoperability with other brands to establish a market advantage.

Despite that there are many interests from legacy companies to protect their proprietary systems advantage, there is a wide consensus that open standards and sources are required to fully implement interoperability. Besides that, interoperability issues hinder the full deployment of effective IoT solutions, and hence the uptake of smart home systems. One of the biggest obstacles of using the IoT is the perception that certain products or services do not have any obvious IoT application or benefit.

Therefore, there is certain traction already in the IoT market to surmount these interoperability issues, though some areas need the focus of policy makers to evaluate whether a public intervention is necessary:

- Support of open platforms and standards
- Stimulation of market uptake
- Information to end-users to support their purchase choice, given the proliferation of IoT devices and systems
- Support of standardisation for interoperability
- Organisational interoperability

There are different policy options to address these areas with different levels of impact. A simplified starting point for setting priorities in policy recommendation may be established attending to:

a) What areas the policy option can influence. For this purpose, Table 8-1 shows the scope of each policy option proposed.

*Table 8-1: Policy options proposed and the areas within their scope*

| | Support of open platforms and standards | Stimulation of market uptake | Information to end-users to support their purchase choice | Support of standardisation for interoperability | Organisational interoperability |
|---|---|---|---|---|---|
| Mandatory minimum requirements | x | x | | x | |
| Mandatory information to consumers | x | x | x | x | |
| Voluntary initiatives | x | x | x | x | |
| Incentive programmes | x | | | x | x |
| Standardisation support | x | | | x | x |
| Self-regulation | x | | | x | x |

b) The nature of the IoT market in terms of maturity, fragmentation and innovation. In this regard, those measures that enable the entrance of new players can be the most appropriate at this stage of the IoT market development.

Attending to the scope of influence (point a), mandatory information to consumers and voluntary labelling may be powerful market drivers, with the potential to orient the market development towards the standardisation, openness and stakeholder involvement for the necessary interoperability. Besides, these policy options do not restrict the entrance of new IoT players, which is needed to develop innovative solutions as the nature of the IoT market requires (point b).

Mandatory requirements, on the contrary, may initially exclude some players, but at the same time, they have a clear advantage of “impact certitude”. A well-designed minimum requirement can effectively address issues for which there are already solutions available in the market, to which all players will converge sooner or later, as it may be the case of minimum requirement on open standards from ENERGY STAR. However, this measure must be further studied and its impact on market carefully evaluated.

Finally, measures such as incentive programs, standardisation support and self-regulation can help improve organisational interoperability, which is crucial for IE, DF and smart grids. Policy makers can support the interoperability solutions currently being deployed as enablers of an environment for innovation, standardisation, and collaboration among different stakeholders. The support provided in the shape of financial aid to the many initiatives coming from the academia and industry must be continued and amplified, considering the main gaps and most promising solutions. The same applies to the work of standardisation organisations which is essential for semantic interoperability in particular, and which requires the coordination of the different efforts developed. For IE, DF and smart grids, the collaboration among many different players must be enhanced, for example, setting self-regulation frameworks that enable the necessary channels to promote it.

# 9 Reference list


1. Mahda Noura, Mohammed Atiquzzaman, Martin Gaedke: Interoperability in Internet of Things: Taxonomies and Open Challeng-es, Published online: 21 July 2018 in Mobile Networks and Applications (2019) 24:796 – 809. Available: https://doi.org/10.1007/s11036-018-1089-9
2. ISO/IEC 2382-1:1993 Information Technology – Vocabulary Part 1: Fundamental terms. International Organization for Stand-ardization (ISO). Available: http://www.iso.org/iso/catalogue_detail.htm?csnumber=7229
3. Radatz J, Geraci A, Katki F (1990) IEEE standard glossary of software engineering terminology. IEEE Std 610121990(121990):3, Available: https://ieeexplore.ieee.org/document/159342
4. Kiljander J, D ' Elia A, Morandi F, Hyttinen P, Takalo-Mattila J, Ylisaukko-Oja A, Soininen JP, Cinotti TS (2014) Semantic in-teroperability architecture for pervasive computing and internet of things. IEEE Access 2:856 – 873
5. InterFuture – Future of Interoperability, for "ICT of the Future" programme by the Austrian Ministry for Transport, Innovation and Technology and the Austrian Research Promotion Agency (FFG). Authored by Mag. Kaltenbrunner Rainer – IDC, Mag. Neuschmid Julia – IDC, Dr. Bieber Ronald – OCG, DI Baumann Wilfried – OCG, Mag. Meir-Huber Mario.
6. IEC61850-2010 https://joinup.ec.europa.eu/collection/ict-standards-procurement/solution/iec-61850-7-42010-communication-networks-and-systems-power-utility-automation-part-7-4-basic
7. http://project-respond.eu/what-is-interoperability/
8. Hannu Järvinen, Web Technology based Smart Home Interoperability, doctoral dissertation, Aalto University, School of Science, Department of Computer Science, Web Services Group. ISBN 978-952-60-6510-6 (pdf).
9. Tolk A (2004) Composable mission spaces and M&S repositories – applicability of open standards. In Spring simulation interop-erability workshop, Arlington (VA)
10. Pantsar-Syväniemi S, Purhonen A, Ovaska E, Kuusijärvi J, Evesti A (2012) Situation-based and self-adaptive applications for the smart environment. J. Ambient Intell. Smart Environ. 4(6):491 – 516. https://www.researchgate.net/figure/Interoperability-levels-of-smart-environments_fig1_236131773
11. CEN-CENELEC-ETSI Smart Grid Coordination Group , Smart Grid Reference Architecture , 2012 and Covrig, C.F., Munoz Diaz, M.A.,
12. Papaioannou I., Tarantola S., Lucas A., Kotsakis E., Marinopoulos A., Ginocchi M., Olariaga Guardiola M., Masera M., Smart grid interoperability testing methodology, EUR 29416 EN, Publications Office of the European Union, Luxembourg, 2018, ISBN 978-92-79-96855-6, doi:10.2760/08049, JRC110455
13. GridWise® (2008) Interoperability Context-Setting Framework v 1.1
14. intelligent efficiency - A case study of barriers & solutions - Smart homes
15. UNIFY-IoT (2016) Report on IoT platforms
16. https://iot-analytics.com/iot-platform-companies-landscape/
17. EDNA (2021), Retrofitting Connectivity for Energy Benefits
18. Daniele, Solanki, den Hartog, Roes (2016), Interoperability for Smart Appliances in the IoT World
19. Guidehouse Inc. (2020), Policy Guidance for Smart, Energy-Saving Consumer Devices
20. VITO, Viegand Maagøe, Universität Bonn, Armines, Wuppertal Institut (2018) Preparatory study on Smart Appliances
21. https://www.theverge.com/22787729/matter-smart-home-standard-apple-amazon-google
22. ETSI (2019) SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms
23. United States Government Accountability Office Center for Science, Technology, and Engineering (2017), Internet of Things Sta-tus and implications of an increasingly connected world
24. Department of Energy and Climate Change (2016), Barriers and Benefits of Home Energy Controller Integration

25. Xergy Consulting (2021), Harnessing IoT for Energy Benefits
26. Energy Systems Catapult (2021) Are we getting the best out of Smart Home Technologies? The role of usability.
27. EDNA (2018), Intelligent Efficiency - a case study of barriers & solutions - Smart Homes
28. Viegand Maagøe A/S (lead), Oeko-Institut e.V. and Van Holsteijn en Kemna BV (2021) Preparatory study for the Ecodesign and Energy Labelling Working Plan 2020-2024
29. Zeadally S, Shaikh F K, Talpur A, Sheng Q Z (2020). Design architectures for energy harvesting in the Internet of Things, Re-newable and Sustainable Energy Reviews, Volume 128, 2020, 109901, ISSN 1364-0321, https://doi.org/10.1016/j.rser.2020.109901
30. IEA 4E EDNA (2019) Total Energy Model for Connected Devices
31. McKinsey Global Institute (2015) The internet of things: mapping the value beyond the hype
32. Tom Hargreaves, Charlie Wilson & Richard Hauxwell-Baldwin (2018) Learning to live in a smart home, Building Research & Information, 46:1, 127-139, DOI: 10.1080/09613218.2017.1286882
33. Kaltenbrunner, Neuschmid, Dr. Bieber, Baumann & Meir-Huber (2016), Future of Interoperability
34. Hannu Järvinen (2015), Web Technology based Smart Home Interoperability
35. United States Government Accountability Office Center for Science, Technology, and Engineering (2017), Internet of Things Sta-tus and implications of an increasingly connected world
36. Department of Energy and Climate Change (2016), Barriers and Benefits of Home Energy Controller Integration
37. Ovidiu Vermesan, Mario Diaz Nava and Hanne Grindvoll (2015) Driving Innovation through the Internet of Things – Disruptive Technology Trends
38. European Platforms Initiative (2018) Advancing IoT platforms interoperability
39. ETSI TS 103 375 https://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf and ETSI TS 103 376 https://www.etsi.org/deliver/etsi_tr/103300_103399/103376/01.01.01_60/tr_103376v010101p.pdf
40. AIOTI WG03 – IoT Standardisation (2020) High Priority IoT Standardisation Gaps and Relevant SDOs
41. ETSI TS 103 375 https://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf and ETSI TS 103 376 https://www.etsi.org/deliver/etsi_tr/103300_103399/103376/01.01.01_60/tr_103376v010101p.pdf
42. IEEE 1901.2 and amendment IEEE 1901.2a (2015) (Low-Frequency Narrowband Power Line Communications for Smart Grid Applications), which has been assigned to the categories “Smart Cities”, “Smart living” and “Smart environment” in the report.
43. Note from Report: ZigBee Smart Energy version 1.1. The latest version for product development, adds several important features, including dynamic pricing enhancements, tunnelling of other protocols, prepayment features, over-the-air updates.
44. Laura Daniele, Monika Solanki, Frank den Hartog, Jasper Roes, ”Interoperability for Smart Appliances in the IoT World”, 2016
45. https://cordis.europa.eu/project/id/731993/reporting
46. https://iot-epi.eu/project/big-iot/
47. GridWise Architecture Council (2020) Introduction to interoperability and decision-maker’s interoperability checklist version 1.6