Ref. Ares(2021)5959640 - 30/09/2021

H2020 – LC – SC3 – EE – 2019 – GA 894240

Operating System for Smart Services in Buildings

D9.4 Smart Buildings: Opportunities and Restrictions in the European Market

WP9 Dissemination, Exploitation and Communication

	Name	Date
Prepared by	Stéphane Genoud (HES-SO), Noemi Imboden (HES-SO)	16.08.2021
Peer reviewed by	Frédéric Revaz (HES-SO), Martin Vodnik (INEA), Adelia Gafurova (FENIX TNT)	17.09.2021
Reviewed and approved by	Dominique Gabioud (HES-SO)	27.09.2021

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 894240.

Distribution list

External		Internal	
European Commission	x	Consortium partners	x

Change log

Version	Date	Remark / changes
1.1	16.08.2021	First version by HES-SO
2.1	24.09.2021	Second version by HES-SO
3.1	30.09.2021	Final version by HES_SO

To be cited as

"D9.4 Smart Buildings: Opportunities and Restrictions in the European Market" of the HORIZON 2020 project domOS, EC Grant Agreement No 894240.

Disclaimer

This document's contents are not intended to replace the consultation of any applicable legal sources or the necessary advice of a legal expert, where appropriate. All information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user, therefore, uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability in respect of this document, which is merely representing the authors' view.

Table of contents

List of figures

List of tables

Terms, definitions, and abbreviated terms

AAL	Ambient Assisted Living
AI	Artificial Intelligence
API	Application Programming Interfaces
DSO	Distribution System Operator
EMS	Energy Management System
EV	Electric Vehicle
GA	Grant Agreement
GDPR	General Data Protection Regulation
HVAC	Heating, Ventilation and Air Conditioning
ICT	Information and Communication Technology
IoT	Internet of Things
SCADA	Supervisory Control and Data Acquisition
TSO	Transmission System Operator
USP	Unique Selling Proposal
V2G	Vehicle to Grid

Executive summary

The domOS project is expected to develop smart building technologies from Technical Readiness Level (TRL) TRL6 ("Technology demonstrated in relevant environment") to TRL8 ("System complete and qualified"). As the developed technologies will be close to the market, it is of prime importance to position them in the current and future European smart building landscape. To this end, the present document first describes the value proposition of domOS, next presents an overview of the smart home and smart building market and finally lists the opportunities and barriers for a large-scale adoption of the domOS technology.

domOS specifies a mediation layer between the in-building distributed infrastructure and the smart home and building automation applications. As the mediation layer provides a decoupling between the two layers, applications are no tighter to a single appliance type and can address appliances from different categories. For example, an energy management application can control an electrical vehicle charging station, a stationary battery, and a heat pump independently of their brands. The domOS mediation layer enables new roles: application developer, smart service developer and IoT platform operator for buildings. The main strength of domOS is to provide a comprehensive response to the need for an integrative approach to building management. The highest barrier is domOS new, yet unproven business model.

1. Introduction

1.1. Objectives of the document

The domOS project is a European research and innovation project that is expected to develop smart building technologies from Technical Readiness Level (TRL) TRL6 ("Technology demonstrated in relevant environment") to TRL 8 ("System complete and qualified"). As the developed technologies will be close to the market, it is of prime importance to position them in the current and future European smart building landscape.

This document provides an overview of the opportunities and restrictions of smart buildings in the European market. It will help identifying an adequate market position for the domOS technology and allow at the same time to get a better understanding of the associated risks and barriers.

1.2. Approach

In the first chapter, technical concepts used in the document are defined. Chapter 2 provides an overview of the domOS project, of its approach and of its value proposition. Chapter 3 contains an analysis of the following markets: smart home and smart building infrastructure, IoT platforms and smart services. Finally, Chapter 4 summarises market chances, opportunities, risks, and challenges.

1.3. Technical understanding

Internet of things, smart home, building automation / smart building, smart device, and smart service are terms used extensively in this report. This section defines them shortly, so that a common understanding of those terms among the readers can be created.

This document does not distinguish between smart system, smart device, and smart appliance. All three terms are used as synonyms in the deliverable.

1.3.1. Internet of Things (IoT)

Nowadays, the internet is no longer just a network of computers, as it used to be. Over the years it has evolved into an interconnected network of devices, people, buildings, places, businesses, etc., known as the "Internet of Things" (Figure 1). The term "thing" refers to connected devices or appliances[1] that have some interaction with their physical environment, either by monitoring it or by acting on it.

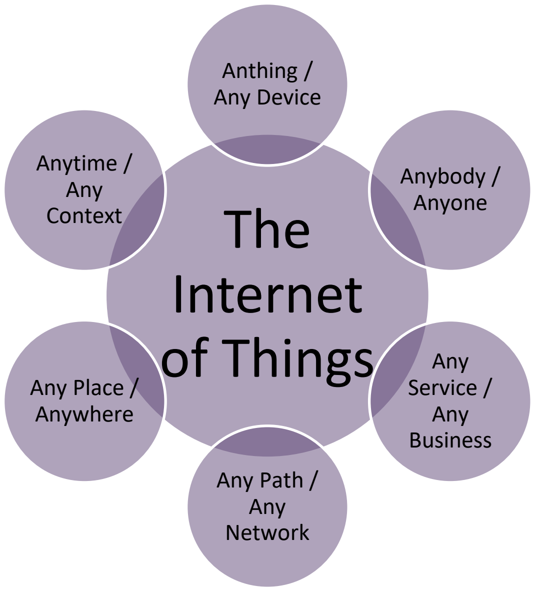

FIGURE 1: THE INTERNET OF THINGS (SOURCE: ADAPTED FORM (CLOUDGARAGE, 2017))

From a technical point of view, we consider that the IoT is not only made up of distributed online embedded devices or appliances[2], but also of hardware (gateways, cloud infrastructure, smart phones, laptops, etc.) and software components (databases, algorithms, user interfaces, etc.) needed for control, visualization, and storage.

The IoT presents specific security challenges which go beyond the cyber-security requirements of the legacy the internet:

1. As the IoT is acting on the physical environment of things, safety issues can occur.
2. The analysis of monitored parameters can possibly leak information on the private life of citizens. Special care must be taken to protect the citizens' privacy, in accordance with the European and national regulation.

The IoT platform is the middle layer between distributed things and business specific applications for control and visualization, mostly hosted in the cloud. The platform is responsible for things provisioning,

[1] In this document, the expression "smart systems" is generic expression covering both online devices and online appliances.
[2] All online devices and appliances are denominated under the generic term "smart systems".

system supervision, security and privacy rules enforcement, data collection and storage. It also provides Application Programming Interfaces (APIs) to applications.

The availability of well-designed platforms is a precondition for a large-scale deployment of the IoT.

Figure 2 shows the layered architecture of an IoT system: in-building embedded devices and appliances form the "Things" layer. The "Platform" layer is a layer providing middleware services. Finally, the "Application" layer hosts business specific monitoring and control components.

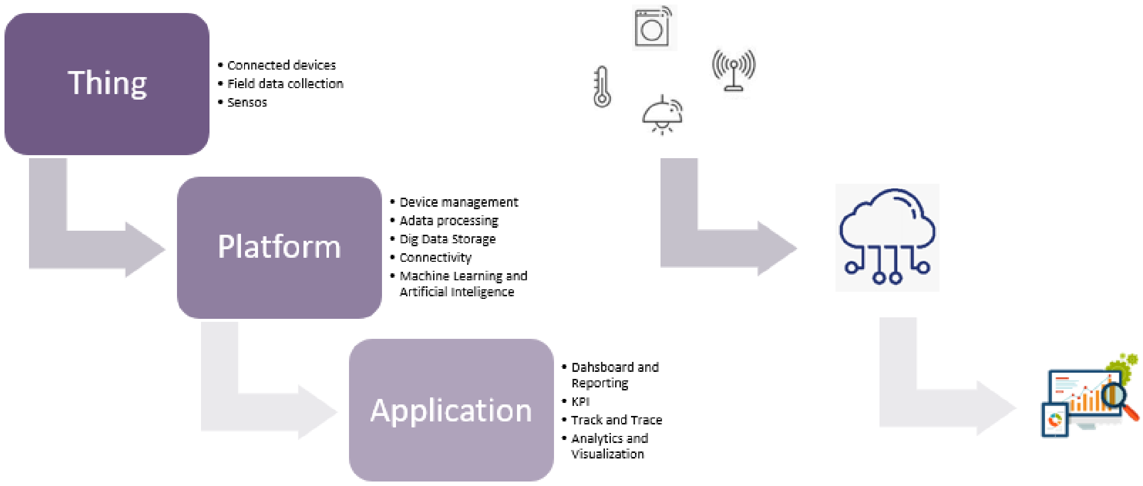

FIGURE 2: IOT ARCHITECTURE

Note that the Platform and the Application layers can be deployed either in the cloud or on a building-local gateway.

1.3.2. Smart home

> *"A smart home, or smart house, is a home that incorporates advanced automation systems to provide the inhabitants with sophisticated monitoring and control over the building's functions. For example, a smart home may control lighting, temperature, multi-media, security, window, and door operations, as well as many other functions… Smart homes use 'home automation' technologies to provide homeowners with 'intelligent' feedback and information by monitoring many aspects of a home."* (Smart Home Energy, 2021).

Sovacool & Furszyfer Del Rio (Sovacool, et al., 2020) proposes six different levels of smartness for a home. Those range from level zero, where no smart home technologies are installed to level five where several smart devices are integrated, interconnected, and automated in order to best meet the homeowner's needs. Figure 3 shows the different levels of smartness defined by the authors and gives a short explanation of each level.

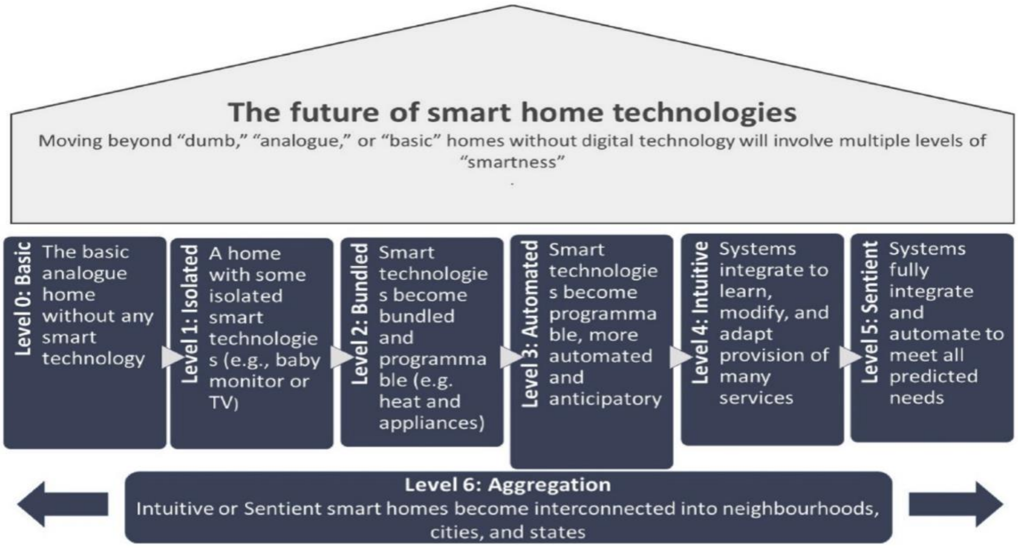

FIGURE 3: LEVELS OF SMARTNESS WITH SMART HOME TECHNOLOGIES (SOURCE: (SOVACOOL, ET AL., 2020))

1.3.3. Building automation / smart building

Building automation is a branch of industrial automation: the building is considered as an industrial plant with specific processes (Heating, Ventilation and Air Conditioning (HVAC), access control, etc.). It is no surprise that the architecture of building automation systems and of industrial automation systems (SCADA) are similar.

The costs for designing and deploying a building automation system are significant. Hence, they are deployed mostly in large or high-end buildings, either service or residential. Smart home technologies are often bought, installed, operated, and developed at a smaller scale by inhabitants, while building automation is handled by professionals and installed directly at construction type or as part as a deep renovation.

Building automation systems are designed with an engineering approach. They control the most important energy appliances or devices in a building. By contrast, the installation of smart home technologies is often driven by opportunities: inhabitants see a possibility to improve their comfort, lifestyle, security, energy, etc. by installing and operating smart home devices.

While having basically different approach, smart home and smart building tend to merge as they use similar technologies and have overlapping application fields.

> "*Recent developments suggest that the boundary between the two definitions* (smart home and building automation) *is being increasingly blurred - the formerly separate operating sectors are increasingly detecting and developing mutual interfaces*" (ZVEI, 2018).

Table 1 gives an overview of the most important differences between smart home and smart building.

TABLE 1: SMART HOME VS SMART BUILDING

	Smart home	Smart building
Main objective	Comfort, lifestyle, security	Energy efficiency, heating / cooling management, security, and access control
Driven by	Inhabitants	Owners
Cost structure	Low cost Standard devices	High end Customised products
Deployment	By inhabitants	By professional system integrators
Dynamics	Evolving over time	Installed at construction or at deep renovation time
Communication technology	Wireless	Wired
Life cycle	A few years	Tens of years

1.3.4. Smart service

Smart services provide added value for users, either building occupants or facility operators. From a technical point of view, a smart service arises from the interaction of an application and of a smart device inside a building.

Balta-Ozkan et al. (Balta-Ozkan, et al., 2014) group the smart services into three main groups: energy consumption and management, safety, and lifestyle and support. Figure 4 presents some of the main smart services identified by them.

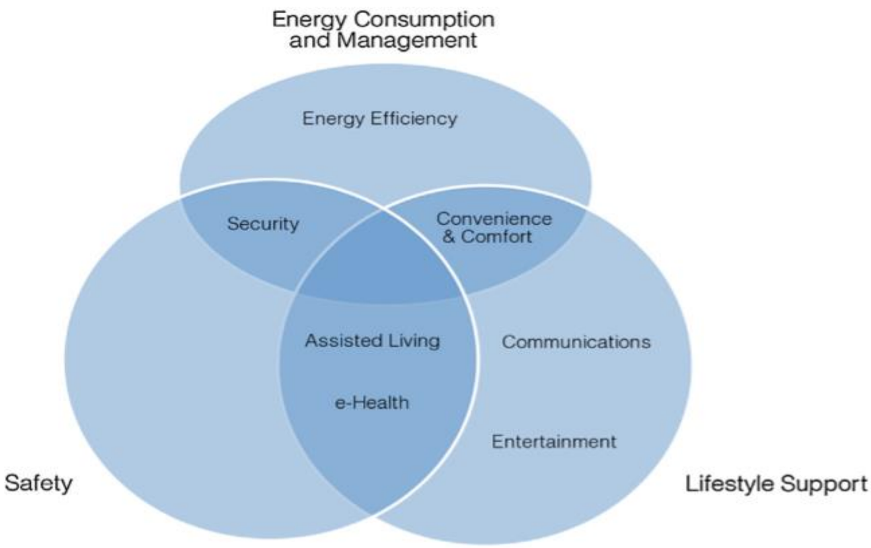

FIGURE 4: SMART SERVICE GROUPS (SOURCE: (BALTA-OZKAN, ET AL., 2014))

Smart services support the development of a service-oriented economy, where consumers do not buy goods but subscribe to services. For example, instead of buying a new heating system, building owners subscribe for example to a “heat as a service”, where they pay for an agreed ambient temperature. A smart service provider is then responsible for delivering the contracted temperature while the building owner pays for this service.

From a technical perspective, a smart service results from the interplay of an application and of "things" inside a building.

2. The domOS project and its value proposition

2.1. Environment

2.1.1. Energy context

As a result of the climate conference in Paris in 2015, the Paris Agreement was adopted for the period after 2020, which for the first time committed all signatory countries to reduce their greenhouse gas emissions, so that the global warming can be kept below 2°C. To achieve this, the countries agreed to reduce CO_2 emissions drastically, through decarbonisation of the energy generation and through energy efficiency measures.

In 2017, in the European Union (EU), more than 27% of the final energy consumption was caused by households. 64% of the energy consumption in households was used for space heating and 14% for water heating. Another 14% was used to power electrical appliances (eurostat, 2019). To reduce the energy consumption, it is possible – and desirable – to renovate existing buildings and replace the current installations by cleaner technologies. However, the current installed technology can also be used in a more efficient way among other things thanks to smart building technologies. Compared to deep renovations, gains induced by smart building technologies require less investment and can be achieved in a shorter time. As an example, the closed-loop energy efficiency service developed by CSEM for the Neuchâtel (CH) demonstration site predicts a reduction 8the primary energy between 8% and 18% (domOS, 2021).

With the rise of renewable energies, electricity flexibility will become increasingly important in the future, because it allows balancing new distributed renewables at the level of buildings, distribution grids and / or energy markets. Buildings feature processes that are inherently capable of providing electrical flexibility: thermal processes (heating, cooling, domestic hot water preparation) can store heat thanks to the thermal inertia of the building envelope or of ad hoc thermal storage systems, EVs are usually connected to the grid for lengths of time much larger than required for charging, and battery energy storage systems can be controlled to provide services at the site level (self-consumption increase), at the grid level (peak shaving), and / or at the market level.

In general, and not only for electricity, flexibility control allows limiting the size of an infrastructure for a given usage.

2.1.2. Technology context

Overall, the digitalization of the building sector – more specifically of the energy – is low compared to other domains. One of the main reasons is that energy appliances have a life duration of several tens of years and that many of them date from the pre-digital area.

Hence, energy appliances can be broadly classified in two categories: non-digital appliances without data interface, and digital appliances. Smart services will of course make use of available data interfaces. Non-digital appliances can also be integrated in smart services thanks to external digital monitoring and control hardware.

Considering that the cost of adding a data interface to any device or appliance goes to zero, and that internet connectivity is ubiquitous, it's not surprising that most recent devices and appliances installed in buildings feature a data interface. These devices and appliances use their own gateways, IoT platforms and applications.

Currently, the smart services market is vertically organized: smart system manufacturers operate – possibly by delegation – an IoT platform and smart services. This silo approach is not scalable with tenths or even hundredths of devices per building, as users will have to deal with a lot of services, with their own access control mechanisms and user experience. Moreover, services involving several smart systems are today almost impossible to deploy.

2.2. The domOS approach to smart building

The domOS project aims to promote the development of smart buildings by bringing buildings to smartness level 5 "Sentiment - Systems fully integrate and automate to meet all predicted needs", according to the classification defined in Figure 3.

2.2.1. domOS key features

The domOS project addresses the smart building sector through two axes:

In the first axis, **technology**, guidelines for an open, secure, multi-service Internet of Things (IoT) ecosystem for smart buildings are defined: in-building gateways, which connect to local smart devices and the smart appliance so that the IoT platforms and applications operated by different parties can be integrated seamlessly into a IoT ecosystem. Building owners can enforce privacy rules, they can allow / forbid access to any measurement or control point.

The objective of the second axis is the development of **smart services**. Demonstrators will develop, operate, and assess a cluster of smart services. Their specifications will serve as input for the design of the domOS technology. In the final stage, the relevance of the technology for the smart service operation will be assessed.

The overall goal of the project will be achieved mainly through four steps, which are explained in the following paragraphs.

- **Design an open, secure, multi-service Internet of Things (IoT) ecosystem for smart buildings**

  In a first step, domOS aims to design an IoT ecosystem for smart buildings (Figure 5). The idea is that any application for visualization, home automatization or energy estimation, once the homeowner has given the authorization for the data transmission, can access the specific field data.

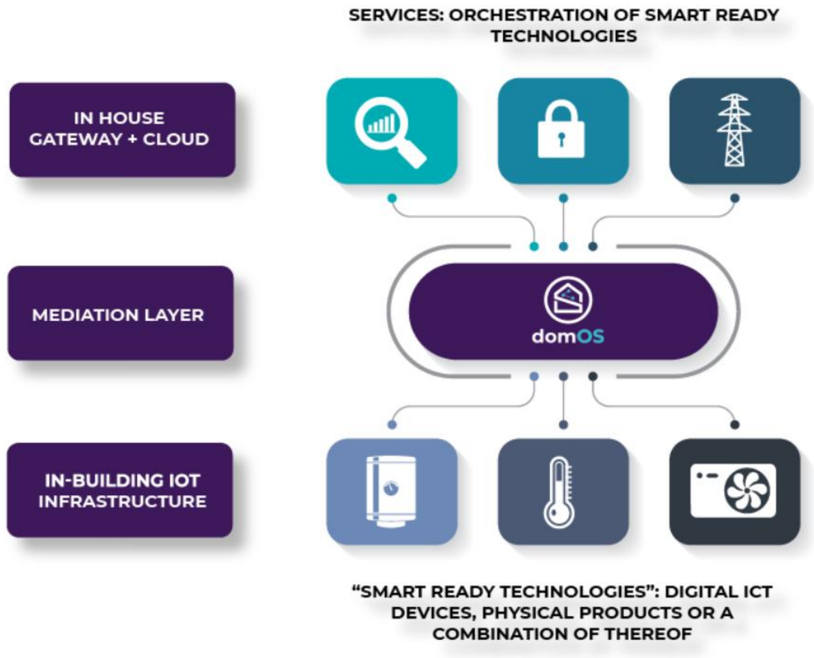

FIGURE 5: GLOBAL VIEW OF THE DOMOS IOT ECOSYSTEM SPECIFICATION

The ecosystem designed in the case of domOS must be:

- **Open:** different applications for multiple vendors must be able to control the building set points through access to the building sensor data.
- **Secure:** the system developed shall respect the data protection laws and regulation and has to be able to secure the data and to limit access to it.
- **Multi-service approach:** the ecosystem must be able for different applications to access the building infrastructure at the same time. Moreover, the access rights will assign control capability for a set point to a unique application.

- **Enable interoperability of data and services for smart buildings through ontologies**

  Sharing a common nomenclature (ontology) for the field data (i.e., time series of measurement data) as well as for the building metadata (description of building structure, technical infrastructure, households' sizes…) is a prerequisite for interoperability. domOS will use demonstrators' use cases to identify concepts to include in the ontology and will define standard names for them, if possible, by reference to existing ontologies.

- **Increase energy performance through smart services**

  Demonstration site will create new services compliant with the domOS IoT ecosystem (or adapt existing services to fit the IoT ecosystem), demonstrate them in a real-life environment and assess their performance.

- **Demonstrate and evaluate smart services deployed on IoT ecosystem compatible IoT frameworks**

  The smart services for existing buildings are deployed in five demonstration sites: Sion (CH), Neuchâtel (CH), Paris (FR), Aalborg (DK) and Skive (DK).

  This approach based on experimentation helps designing an IoT ecosystem in phase with the needs of smart building.

2.3. The domOS ecosystem and the IoT platforms

domOS does not intend to develop a new IoT platform – many mature and comprehensive ones do already exist. The domOS ecosystem should be understood as a specification that can be implemented on multiple IoT platforms. Incidentally, three IoT platforms will be enhanced to comply with the domOS IoT ecosystem as part of the domOS project, and each compliant platform will be used in at least one demonstrator.

Note that the domOS ecosystem leverages current and emerging IoT standards to ease its adoption by existing platforms.

2.4. Value proposition of the domOS ecosystem

2.4.1. Bridge smart home, smart building, and smart metering,

domOS aims to provide a unique (virtual) connector for all smart systems in a given building, on which a cluster of applications can be plugged in. domOS intends to enable buildings' owners, inhabitants and facility operators to integrate smart systems and deploy smart services in a dynamic environment inspired by today's smart home technologies. These services can be indifferently classified as smart home, smart building, or smart metering[3] services.

2.4.2. Enable integration of any existing smart system

The domOS ecosystem takes the diversity of the communication protocols for smart building devices / appliances as a fact and does not request conformance to a unique, "better", standard. It only requires that the device / appliance interface is described in a machine-readable document (whose format is part of the ecosystem specification).

2.4.3. Decouple applications and smart systems

As of today, a smart service relates to a model (or to a compliant cluster) of smart systems. For example, the heat pump manufactured by a specific company operates a smart service limited to the heat pumps of the same brand (or even a subset of them). This leads to two technical limitations:

- smart services are tightly coupled with specific device / appliance models, and
- smart services spanning over multiple devices / appliances cannot be deployed.

[3] The term "smart metering" refers to the set of regulated services for measurement and possibly control of energy resources in buildings.

The domOS mediation layer is meant to lift this limitation by providing applications with a generic (i.e., model type independent) view the building infrastructure.

2.4.4. Provide tools to manage privacy

The smartphone ecosystems have deployed functions enabling users to control their privacy: applications may only access peripherals (position, contacts, etc.) if an explicit permission has been granted.

domOS intends to develop a similar approach for buildings: inhabitants and facility operators (or persons responsible for the facility management) can decide to install applications for a given smart service. These applications should indicate which access rights they need, and those rights must be granted.

2.4.5. Trigger the dissemination of applications developers and smart service operators

As explained above, the smart service market is mostly vertically organized today, with smart system manufacturers also operating corresponding smart services.

Offering a uniform access to buildings is expected to trigger the advent of new players:

1. Application developers could develop applications interacting with the building infrastructure through the generic interface defined in the IoT ecosystem.
2. Smart service operators run applications and supervise the operation of smart services.

Application developer and IoT building platform operators are roles that can – but must not – be played by the same entity.

2.4.6. Trigger the dissemination of IoT platforms dedicated to buildings

As of today, IoT platforms are generic and not dedicated to a single applications domain. The domOS ecosystem envisions that IoT platforms will have building specific features.

Foreseen building specific functions relates to directory services for buildings topology including their smart systems, translation between generic and device /appliance specific messages, cybersecurity, and privacy management.

2.4.7. Promote inter-platform interoperability

The domOS ecosystem provides a “high” API for applications and a “low” API for smart devices and appliances. Let’s assume this ecosystem is applied in a coherent way by multiple IoT platforms for buildings.

The inter-platform interoperability in domOS is illustrated on Figure 6. It has two main features:

1. The smart infrastructure in a building can be connected to any compliant platform using similar connection procedures.
2. Application operators can deploy smart services on top of any compliant platform in a transparent way.

To reach this long-term vision, domOS will rely on projects dedicated to platform interoperability such as the European Platforms Initiative – Advancing IoT Platforms Interoperability (European Platforms Initiative, 2018).

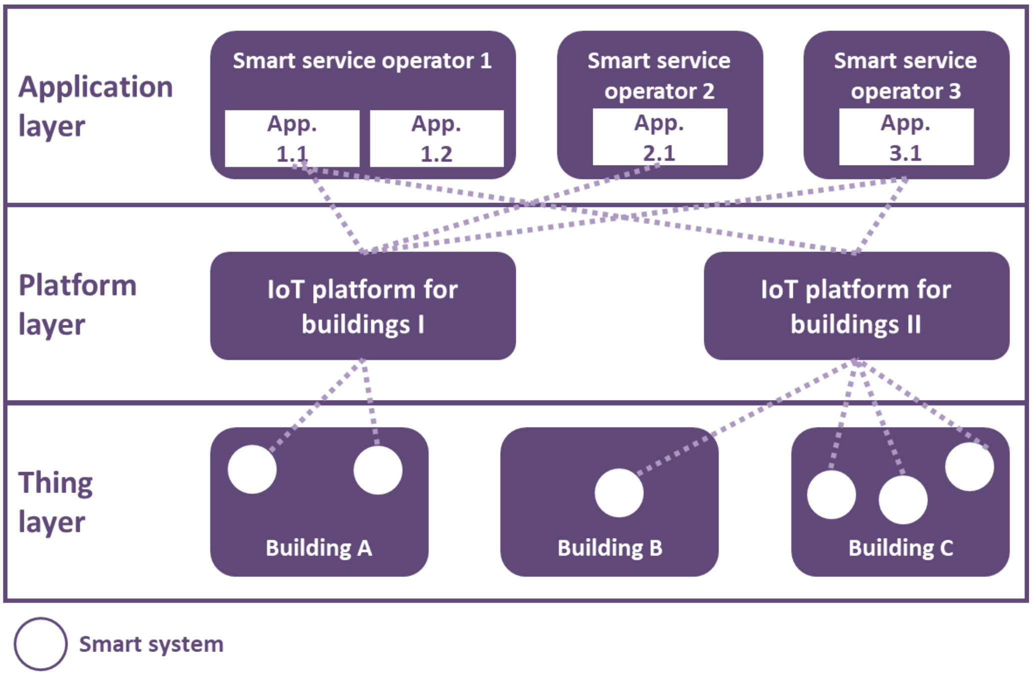

FIGURE 6: PLATFORM INTEROPERABILITY IN DOMOS

In the proposed structure, the IoT platforms would compete on costs, catalogue of applications (applications could enter in contract with a limited set of platforms), business models and/or usability.

3. Market analysis

In this chapter, the current and forecasted market for in-building infrastructure (smart home and smart building), IoT platforms and smart services are analysed. This allows to obtain a better understanding of the market evolution as well as of the opportunities and the risks linked to it.

For this analysis, the two concepts smart home and smart building were treated separately. However, as mentioned in Section 1.3.3, it is not always possible to distinguish between these two concepts. Moreover, in the future it is likely that there will be bridges between the two concepts or that they even merge, as they feature similar purposes, architectures, and technologies.

3.1. Generic IoT platforms

Generic IoT platforms can be used for any application domain, including buildings. As domOS compliant IoT platform will be developed as specialised platforms built on top of generic platforms, the main features of the generic IoT platform market are presented below in this section.

3.1.1. Functions

Generic IoT platforms handle the following functions: connection to the field devices, global, device management, storage of historical data, support for data analysis, and API for applications.

Over years, IoT platforms increase their performance – and complexity (IoT Analytics, 2021).

3.1.2. Market evolution

The growth of IoT platform market in the past years has exceeded almost every expectation. In 2016, it was predicted that IoT platforms would be worth 1.3 billion dollars by 2020. This prediction was not accurate, as the actual market in 2020 was estimated to be worth 5.0 billion (i-SCOOP). The strong growth in the IoT industry was mainly caused by some big players who were little active in the IoT market in 2015 and 2016 but invested heavily in this market in the following years.

Some market experts are wary of the market and especially of its future development because the market is extremely fragmented and complex. Not only has the number of IoT platforms increased significantly, but the structure of the IoT platform has also changed and has become more complex in recent years.

3.1.3. Players

It is not surprising that the big cloud operators provide IoT modules for their hosting services: Azure IoT (Microsoft), Google Cloud IoT (Google), AWS IoT (Amazon), IoT Cloud Connect (Cisco), Watson IoT (IBM). These IoT platforms are made available in B2B mode for IoT solution operators, using a “Platform as a Service” model.

Many open-source platforms challenge the commercial products. The offered functions, their quality, and their maturity are uneven. Note that they can be installed on a private cloud or on a public cloud like Amazon AWS, using an “Infrastructure as a Service” model.

3.1.4. Relevance for domOS

domOS compliant IoT platforms will be able to rely on existing mature platforms, both commercial and open source. The fact that they develop well increases the number of connected smart systems and makes more visible the need for an integrated approach.

To sum up, the technology of the generic IoT platforms represents a solid basis for domOS and their widespread use creates an appeal for integration mechanisms such as those designed in domOS.

3.2. Smart home

3.2.1. Smart home services

Smart home devices can be divided into different groups: home entertainment system, lighting control system, security and access control, and healthcare / Ambient Assisted Living (AAL).

3.2.2. Smart home market evolution

According to a study done by Prescient & Strategic Intelligence, an industry analyst and consulting firm, in 2017 there was 111.9 million smart home devices in use in Europe, compared to the year before where they were only 89.9 million. These systems are distributed in about 40.3 million homes, which represents 17.4 percent of all households in Europe (Prescient & Strategic Intelligence Private Limited, 2017).

While the US smart home market is currently more important than the European one, this is expected to change in the future. This due to the faster growing rate of the European market (Berg Insight AB, 2018). The forecasted number of homes hosting smart home devices in Europe and in North America is shown in Figure 7.

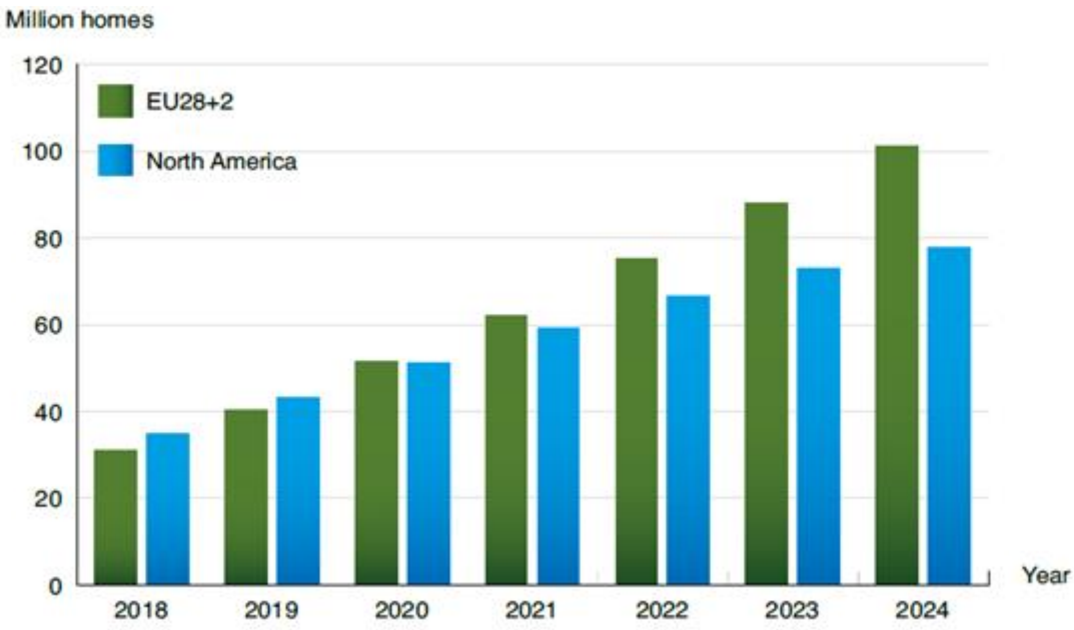

FIGURE 7: TOTAL NUMBER OF SMART HOMES (SOURCE: (BERG INSIGHT AB, 2018))

Most common smart home devices are smart bulbs / smart lights and smart thermostats, followed by security and alarm systems (Deloitte, 2016). Moreover, smaller, less expensive devices are most likely to be replaced by smart equivalents.

In parallel to the growth of connected homes, the number of connected devices an average household owns is also expected to grow exponentially as shown in Figure 8

Buyers indicate that they bought smart home technology to have a better control over their homes (12%), to make their home safer (10%), to improve their quality of life (9%), to acquire trendy devices (8%), to increase productivity (7%) or to save on home bills (6%) (PwC, 2017).

Experts estimate that the main benefits for smart home and smart building users are energy savings, convenience, and controllability, as well as financial benefits (Furszyfer Del Rio, et al., 2020).

Reasons to not invest in smart home are high prices, privacy concerns, lack of perceived relevancy, obsolescence risks, lack of reliability, difficulty to monetise the benefits, lack of interoperability between brands (Furszyfer Del Rio, et al., 2020).

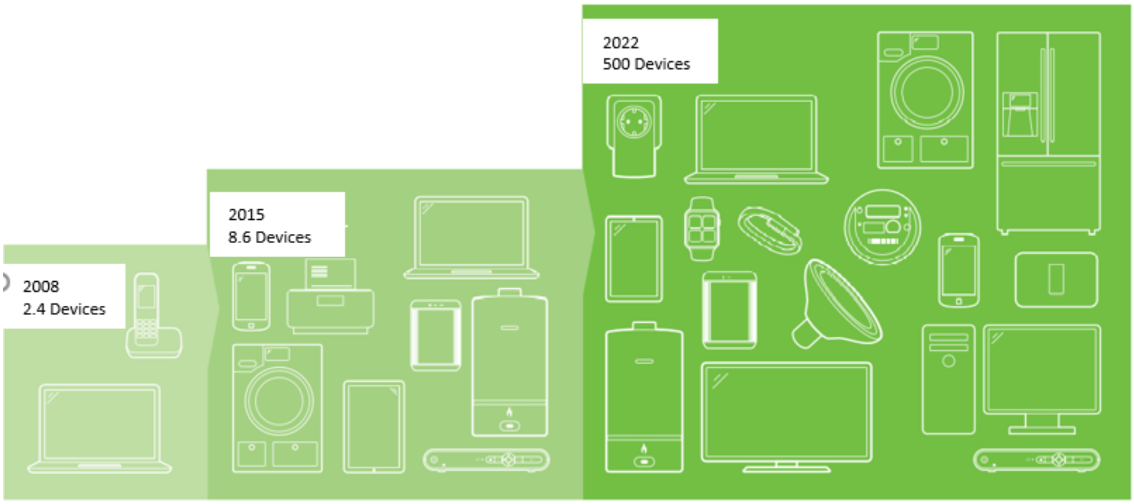

FIGURE 8: NUMBER OF CONNECTED DEVICES[4]

3.2.3. Trends for smart home devices

Device interoperability (capability to connect to multiple platforms) and device interchangeability (capability to use multiple device models performing a given function in a transparent way) is essential for a mature smart home market. Two initiatives are worth mentioning which promote the aspects of interoperability and interchangeability are Thread and Matter: Thread[5] is a low power radio technology for smart home and Matter[6] defines IP based protocols and semantical data models for smart home devices.

3.2.4. Smart home IoT platforms and ecosystems

A smart home ecosystem is made up of a specialised IoT platform, of a large cluster of compliant devices models and of smart home services. Smart home ecosystems are most of the time operated by big players. The preeminent IoT platforms dedicated to smart home are Alexa by Amazon, Google Home by Google, and HomeKit by Apple.

Figure 9 illustrates the architecture of a smart home IoT platform, using Alexa as example. Alexa smart devices for user interaction, third party devices, all kind of computers / smart phones and third-party applications team up to deliver a full range of smart home services.

IoT devices from third party manufacturers can obtain a certification for one or more ecosystem.

Smart home platforms can have some energy specific functions like energy dashboard (Amazon) or smart thermostat (Google Nest). Currently, these platforms offer generic functions like basic control (on/off) and data visualisation. Regulation functions are embedded in the devices and rely on built-in sensors. Triggers are very limited and rely on voice or application commands, time of day and in some cases

[4] Note that considered devices go beyond smart home (smart watches, PCs, laptops, and smart phones are also considered)
[5] Home (threadgroup.org)
[6] Matter (buildwithmatter.com)

presence, but usually not on sensor signals. These platforms lack the richness of functions and the level of customisation needed to operate proper energy services.

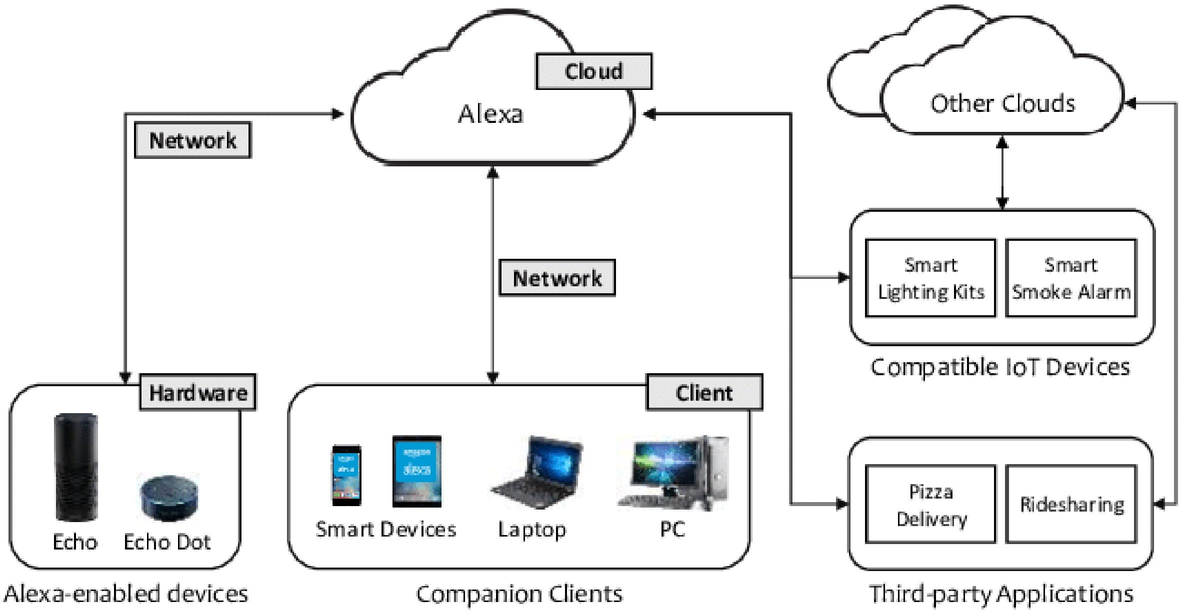

FIGURE 9: ALEXA PLATFORM (SOURCE: (CHUNG, ET AL., 2017))

3.2.5. Relevance for domOS

Because of its size, the smart home market will most probably continue to be dominated by closed ecosystems (in particular by the three big ones having a leading position today). Smart devices will be compliant to one or more ecosystems, and an integrating specification à la domOS will certainly be unnecessary, especially if emerging standards like Thread and Matter establish themselves.

Nevertheless, domOS can take profit of the booming development of smart home in several ways:

1. People get accustomed to the handling of connected devices (including cybersecurity and privacy aspects).
2. Command to or status of domOS installations can be integrated into a smart home ecosystem.

3.3. Smart building

As it strongly relates to energy, smart building is at the heart of the domOS project.

In this section, an overview of smart services and related appliances and devices is presented first. Then the market for IoT platforms dedicated to buildings is shortly described. Finally, the relevance of this market for domOS is deduced.

3.3.1. Smart building services

3.3.1.1. Energy as a Service (EaaS)

In the classical model, house owners buy energy in an intermediate form (e.g., electricity) and operate appliances (e.g., heat pumps) that transform the intermediate energy into the final desired good (e.g., heat). The operation of appliances is often sub-optimal as system integrators or maintenance companies target trouble-free operation rather than efficient operation.

In the Energy as a Service (EaaS), building owners buy the final good (heat), which is provided by Energy Service Companies (ESCOs) that buy the intermediate energy (electricity) and operates the transforming appliance (heat pump). This model is meant to increase the economic and energy performance, because the ESCO's financial reward increases with performance.

The pattern presented in the above example (electrical heat pump) is found in further contexts.

EaaS require smart services for billing, monitoring and control. Hence, IoT can be considered as an enabling technology for EaaS.

3.3.1.2. Energy dashboards

Energy, in particular heat, gas, and electricity, is an obscure field for most citizens. They often mix power and energy and known neither a rough estimate of their own consumption nor the biggest consuming appliances in their home / buildings. In this context, it is hard for them to make enlightened investments or to adopt thrifty behaviours.

Energy dashboards are meant to provide synthetic, context-based, ready-for-action feedback on the building energy to its inhabitants.

Energy dashboards require IoT devices for gathering monitoring data to be used to elaborate dashboards. Data of interest are global consumption data, per appliance / process consumption data[7], temperatures and further environmental data.

3.3.1.3. Energy Management Systems (EMSs)

In the legacy model, buildings draw power and energy from grids without limitation: grids are assumed to be able to cope with any demand.

The large-scale deployment of stochastic and distributed generation by new renewables (mainly PV) and the electrification of processes (heating, mobility) lead to congestion problems in grid and to global unbalance between production and consumption. Hence, a paradigm change is required.

To offset these problems, the intrinsic flexibility of processes must be managed. Flexible processes are mainly heating (the building envelope or technical heat stores acts as heat buffer) and EV charging.

[7] Note that per processing consumption data can be obtained either by dedicated sensor installed on the processes themselves or by disaggregation of a global load curve.

Energy Management Systems (EMSs) take care of controlling the flexibility of processes, either to increase self-consumption at the local level, for peak shaving on distribution grids or as part of energy market transactions.

EMSs require data links to the local appliances, for monitoring and control. Those appliances are of different types (PV inverter, battery storage system, heat pump, EV charger…) and of different manufacturers, and feature different data models, which can be accessed with different protocols.

Providing tools to cope with this heterogeneity is at the heart of the domOS approach.

This section has been illustrated with examples related to electricity. Similar patterns can be observed for other energy grids (district heating and gas).

3.3.1.4. Smart regulation

Heat (and cold) generation and distribution form a complex interconnected system whose efficiency and flexibility can be improved by advanced closed-loop control. This control can involve distributed data acquisition (flow, temperature, valve state…) and distributed actuation (valve control, heating system set points).

3.3.1.5. Comfort and building control

Current cooling and heating systems lack fine tuning capability. Smart building systems could let inhabitants / users control temperature per room, possibly based on calendar entries (day, night, workdays / weekend, etc.).

3.3.1.6. Smart metering

Traditionally, meters were devices that measured integrated values (so-called indexes) of streams (potable water, gas, electricity, etc.) entering or leaving the building. Indexes were read locally by an employee of a metering operator at long time intervals (typically one year).

So-called smart meters are online version of meters.

The metering process – including the communication with back-end systems – is regulated by national laws. In most countries, the grid operator is in charge of metering.

Typical metering regulations require the upload of a limited set of parameters (index) with a limited resolution (quarterly values) and allow long delays (parameters available day after).

Two levels of integration for smart metering and smart building are possible:

1. Smart meters are connected to their metering operator' back-end system through a dedicated communication network. Real-time data are made available to the building occupants or operators through a (usually local) dedicated interface[8]. These data can be fed in a domOS compliant building information system.

[8] Note that the interface can provide a rich set of high-resolution data (down to one sample per second).

2. Smart metering is considered as a smart service, implemented on top of a generic service independent smart building infrastructure. This approach is admittedly innovative but limits the required infrastructure and hence the costs (single data connection for a building). Local regulation (often) forbids it because the official metering process would use the supposed unreliable building internet connection.

In any case, smart metering data provide valuable input for many smart services. As smart meters are official meters, they can be used to derive billing information.

3.3.1.7. Data services for energy suppliers and grid operators

As indicated above, smart metering is a low-resolution, high latency service, handling a limited set of parameters.

An IoT infrastructure would allow more parameters to be transmitted in near real-time more frequently, with the current smart meter device acting as sensor.

These parameters (e.g., currents, voltages, powers, and cos phi) can provide valuable measurements to grid operators, who are often "blind" for the last mile.

Energy suppliers can also profit from high resolution measurement to adapt in real-time their supply strategy.

3.3.2. Smart building market evolution

3.3.2.1. Global market perspectives

With the rise of the number of installed smart systems, the increased focus on energy efficiency and environmental concerns, it is no surprise that the smart building market is also flourishing.

In 2020, the European smart building market was estimated to be worth USD 3.08 billion. For the years 2021 until 2028 the market is expected to have a compound annual growth rate of 17.6% (Fortune Business Insights, 2021).

These figures relate to legacy building automation systems including such operations as ventilation, air conditioning, heating, lighting, and access control.

Equipment of small residential or service buildings – in particular of the existing buildings not undergoing a deep renovation – is not concerned by the above forecast.

3.3.2.2. Market evolution for smart building appliances / devices

The market perspective for the most relevant smart building appliances / devices is presented in Table 2.

TABLE 2: MARKET PERSPECTIVE FOR SMART APPLIANCES

Appliance	Market Perspective
EV Charging Stations	In many European countries, EV sales multiplied in recent years. In 2017-2018 the market grew by 34% and in 2018-2019 by 44% (McKinsey, 2020). The figures for the first quarter of 2020 also confirm this trend. Especially markets like Germany, the Netherlands, Denmark, or Norway experimented a particularly large growth. This rapid development in EV also has a positive impact on the development of new technologies, such as smart charging and V2G.
Stationary Batteries	Different market studies have shown a strong growth for home batteries in Europe. In 2019, a total of 745 MWh battery capacity from 96,000 systems was installed, representing a 57% year-on-year growth. However, over 90% of this capacity was installed by only 5 countries (Germany, Italy, UK, Austria, Switzerland), of which Germany alone was responsible for two thirds of the entire installation volume last year (Solar Power Europe, 2020). According to the European Market Outlook Report, the installed capacity of residential batteries grew from an installed capacity of 200 MWh in 2016 to 745 MWh in 2019.
Heat Pumps	The European heat pump market is expected to grow over 8% in the years from 2020 until 2026. The total European market size is expected to be over 11 billion USD (Global Market Insights, 2020).
Smart Meters	The European Union passed a law which requires all member states to implement intelligent metering system. The target set by the EU is that by 2020, 80% of the houses are equipped with smart meters. How ambitions this goal can be seen when analysing the starting point. According to a study done by for the European Commission in 2020, a total of 123 million smart meters were installed up until that year, which would represent a penetration rate of 43% (European Commission, 2020). This percentage is expected to rise to 77% until 2024 (Eichberger, 2020). Despite the fact, that the number of the installed smart meters did not reach the set target, the number of installed smart meters is still impressing. Moreover, even if the set target was not reached, this does not mean that the rollout stopped. In the coming years, the number of installed smart meters will be rising.
PV Inverters	The estimated compound annual growth rate for PV inverters for the years 2021 until 2026 is around 6% (Business Wire, 2021).

3.3.3. Smart buildings platforms

3.3.3.1. Current situation

Most energy appliances are sold today with a data interface for monitoring and control. Three patterns are encountered:

1. The data interface is not used. Monitoring and control – if any – is performed through a local unit (buttons and display).
2. The appliance manufacturer operates a vertical silo solution including the appliance itself, an IoT platform and an application. Manufacturers use instances of generic IoT platforms for this purpose.

3. The appliance is connected to a legacy building automation system developed as part of a construction or deep renovation process. As stated in Section 1.3.3, this approach is limited to large buildings.

As of today, there are no building specific IoT platforms enabling the plug-and-play integration of appliances and presenting a uniform interface for applications. Platforms like IFFT[9] or Qivicon[10] take an integrative approach, but their openness to smart systems and their programmability is limited.

Modern energy solutions for buildings involve a "choreography" of energy appliances, users, and operators. An integrated approach is today possible through costly building automation systems realised as engineering project. Connectivity is present on recent appliances, but services are limited to individual appliances.

Providing building automation services for smaller buildings in a dynamic way (smart systems and applications can be added / removed) using low-cost state-of-the art IoT and web technologies is not possible as of today. With its vision to seamlessly integrate energy appliances and smart home devices into a building information system, the domOS ecosystem specification enables compliant platforms to offer solutions for deploying building automation services in smaller buildings in a cost-effective way.

3.4. Conclusion

The smart home as well as the smart building market have developed very well in recent years. This trend does not seem to diminish in the coming years. The market will grow rapidly in the next few years, which means that not only new providers (IoT, smart devices or event smart services) will enter the market, but also that business models will have to be rethought and adapted to better respond to customer needs. To find one's way around the already crowded market, it will become increasingly important in the future to be able to attract the attention of customers through innovation, new products, or an outstanding business model.

No integrated approach for smart buildings or for global smart services exist as of today. Silo operation of smart services will not be manageable anymore when the number of connected smart systems will grow in order of magnitude of tens. In this rather chaotic context, smart home platforms bring some level of interoperability but are not – at least not yet – up to the expectations. They don't cover the building automation / smart building area, a must for energy smart services, they request smart systems to comply with their requirements, and they often do not offer open APIs for smart services.

[9] IFTT (https://ifttt.com/) allows to program scenarios including smart systems and legacy internet services and smart home platforms.
[10] Qivicon is a smart home / smart building initiative led by Deutsche Telekom (https://www.qivicon.com/).

4. Opportunities and restrictions

4.1. Opportunities

4.1.1. Expectations for an integrative approach for smart buildings

The multiplication of smart systems, each one with its own platform and application degrade user experience and is not a sustainable solution.

With its integrative concept, domOS brings a solution, admittedly centred on smart building, but also capable to cope with smart home.

4.1.2. Compliance with requirements for energy management

Energy management involves by nature monitoring and control of energy appliances, whose heterogeneity is a fact that energy management systems must cope with. domOS simplifies the development of such applications as it provides an abstract, model-independent interface to energy appliances.

4.1.3. Support for Energy as a Service (EaaS)

One of the difficulties that slows down the deployment of Energy as a service (EaaS) solutions is that on-site appliances need to be remotely monitored and controlled for optimum operation. Moreover, billing – as it is no more based on legacy meters - needs additional sensors.

domOS provides a ready-to-use solution for EaaS providers, who can concentrate on their business - and not on IoT.

4.1.4. Reduction of energy costs

Two factors can lead to cost reduction: firstly, increased energy efficiency will reduce the consumed energy and therefore reduce the energy bill. Secondly, flexibility control can generate revenues for the owner the controlled flexible infrastructure.

4.1.5. Streamlined infrastructure

Silo solutions in buildings require parallel, basically similar infrastructure for each solution (sensors, gateways, platforms…). Integration has the potential to reduce the number of hard- and software components and hence to reduce costs.

4.1.6. Coherence with legacy IoT

With the tremendous development of IoT, de facto or de jure standards have established themselves. The domOS ecosystem specification is not in competition with those standards, but defines a business (i.e., smart building) specific layer on top of legacy IoT standards. Ideally, the domOS layer is independent of the underlying IoT architecture.

All domOS stakeholders (compliant platforms operators / developers, manufacturers of smart systems, application developers, smart service operators) are assumed to be familiar with IoT legacy technology. For them, the step to enter domOS ecosystem is low.

4.1.7. Alignment with citizens' expectations

Generally, a global environmental awareness and a movement towards eco-friendly technologies and energy conservation can be observed.

Citizens, either in the role of inhabitants, owners, or facility operators, have a basic motivation to contribute to a more sustainable world. This includes the will to understand their buildings as an energy system and to improve its operation.

4.1.8. Contribution to public policies

Government have set ambitious goals for reduction of CO2 emissions. As big energy consumers, buildings must (and can) contribute to the reduction, which can obtain through a greater energy efficiency.

As domOS compliant platforms have the potential to optimise energy in buildings, they could get subsidies by governmental programs promoting green buildings.

4.1.9. Digitalisation trends

Digitalisation is penetrating all sectors of society. Digitalisation in buildings is admittedly late, but buildings won't elude digitalisation. The vision of domOS is to be an enabler for digitalisation in small buildings. The domOS ecosystem should profit from the expected "digitalisation wave" for smart buildings.

4.1.10. Privacy management

In smart buildings, different services should have access to different set of in-building parameters. domOS compliant platforms enable central access management: permissions for applications to access individual parameters can be granted / suppressed. Building operators / users can be associated to access right management

4.2. Restrictions

4.2.1. New, unproven business models

Smart buildings appliances, IoT platforms and services are nowadays mostly operated by the appliance manufacturer, which controls the whole vertical chain.

The concept of a mediation layer is thus interesting from a technical point of view, but business models for the operation of the underlying platform are not yet established. Basically, the platform could be financed by building owners, smart services operators and/or appliance manufactures.

Note that the concept of smart service operator is also new, and its viability remains to be proven. A smart service operator is a pure software player who deploy its service on top of an in-building infrastructure made available by the building owner.

4.2.2. Unclear limit of liability

If decoupling of infrastructure and applications is a priori an attractive idea, the question of liability remains open. For example, a smart service controlling a heat pump can accelerate ageing and cause failures, in case of (too) frequent on/off switching.

The lack of clearly limited liability areas can restrict the development of domOS solutions.

Historically, the first data interfaces of appliances were designed for technicians, for configuration and diagnostics. These interfaces were relatively open, as it was assumed that technicians behave in an appropriate way. Often, the interfaces for building operators stems from the interface for technicians, and inappropriate command sequences could jeopardise the proper functioning of the appliance.

This is one of the reason pushing manufacturers for silos solutions, where they can control and filter operators' commands.

Independently of domOS, it is expected that manufacturers provide "risk free" data interfaces, but the domOS model depends on their availability.

4.2.3. Market rejection of underlying emerging standards

The domOS specification relies on legacy IoT technical standards, but also on the merging standard Web of Thing (WoT) elaborated by the World Wide Web Consortium (W3C). The fate of domOS is somehow linked to the WoT: should the latter established itself as a widely used standard, then domOS will profit from its slipstream.

It is out of the scope of domOS to provide a solution for interoperability. It is assumed that "some" IoT interoperability concept will "win the race and become an industry standard. If that standard is not WoT, the domOS ecosystem specification will have to undergo a redesign, even if the basic concepts of domOS can apply on any interoperability framework.

4.2.4. Lack of smart system descriptions

To integrate various appliance models, the WoT concept requires that each smart system instance features a description document. This document is made up of two parts: a first part is model-specific, and a second (limited) is instance specific.

The capability to readily integrate various appliances is a key element of domOS. It implies that description documents covering a large set of smart systems are available. Missing documents can still be written solely based on the user manual.

It is unclear yet who will elaborate, store, and make available the model specific description documents. Several models are possible: collaborative model where any stakeholder can upload such descriptions on a public repository, one or more IoT platform operators for buildings maintain a repository for their customers…

How to guarantee the quality and accuracy of those description is still an open question.

The Swiss association SmartGrid Ready[11], which has goals like domOS', sets up a certification process. As members of the association, manufacturers can submit descriptions for certification and hosting. Partnership with established or ad hoc professional association is certainly a way to manage elaboration, validation, hosting and dissemination of smart systems descriptions.

4.2.5. Start-up constraints

Buildings will adopt domOS if there is a large set of compliant smart systems. On the other hand, manufacturers or other parties will be motivated to make smart systems domOS compliant (concretely, to elaborate their descriptions) if domOS buildings are many.

A close partnership with big players: utilities, telecom operators or professional associations is probably the way to advance domOS technology and to let it reach the critical mass.

4.2.6. Citizens' reservations on privacy

Data protection and privacy is indeed a concern for all IoT application domains, and wary citizens will decline all IoT applications for all domains – including buildings.

There are however specific aspects that could prevent citizens to specifically refuse IoT in buildings: buildings do not relate to an individual but to a set of individuals (one or more family). It is possible that the behaviour of a family of an individual leaks to the building operator or to other habitants.

Citizens can have reservations regarding the privacy of domOS compliant platforms. Admittedly, domOS provides the technical tools for privacy management, and service design should prevent leaks, but trust of many citizens is not available by default and must be proven.

4.2.7. Unsatisfying smart home and smart building integration

Today, smart building is part of the building infrastructure and, as such under the responsibility of facility operators. Smart home, on the other hand, is installed, configured, and maintained by inhabitants. For single family houses, owner and facility operator are roles played by inhabitants and the integration is not an issue. In larger buildings, where operation is under the responsibility of a dedicated person or company, the concept of a global building information system mixing smart home and smart building functions can deter stakeholders.

4.2.8. Complexity

Inquiries have learned that of demonstrators' participants give a high value to "peace of mind", i.e., to the feeling that "everything is OK". This means on one hand that prosumers don't want to invest time for energy matters, but on the other hand, want high level indicators proving the appropriate operation of the building.

[11] http://www.smartgridrady.ch

The quality of the user experience depends on the design of the concerned smart services. However, domOS technology should allow a straightforward integration of smart systems and applications / services. Simple processes should not only be designed, but also known to potential users.

4.2.9. Ontology not in line with expectations

The domOS core ontology is an important part of the ecosystem specification. The ontology attributes standard names to resources in buildings (e.g., “heat pump” or “instantaneous active power”) and allows to express relations between the resources.

The domOS ontology is the corner stone for interoperability. Thanks to it, applications and smart systems give the same name to the same resource.

If the ontology does not cover the right resources, non-standard names will be used, and interoperability will be lost.

4.2.10. Difficult integration of non-digital appliances

Non-digital appliances, which still represents a significant part of the installed stock, can basically be monitored, or even controlled using external hardware and thus integrated in smart services. This apparently simple process features three problems:

1. First experiences gathered in demonstrators have shown that space for monitoring / control appliances is often missing in cabinets.
2. Control of non-digital appliances is limited to enable or disable power supply. Smart services could require a less coarse approach.
3. In practice, monitoring / control infrastructure require wireless communication, as installing wires in existing buildings is not doable. Operating stable wireless links in the environment of technical rooms is challenging (thick concrete walls, sensors located in metallic cabinets).

4.2.11. Lack of support from appliance manufacturers

As sated above, manufacturers also operate smart services related to their appliances. Manufacturers had to take this approach, as no shared platforms were available, but they could be reluctant to open their appliances to their parties. They can be interested to operate services in addition to sell hardware (or even as a replacement of hardware sell).

Concretely, manufacturers could be reluctant to publish the specification of the data interface and could change it without notice.

4.2.12. Incompatible appliance models

In the domOS ecosystem, applications “see” appliances through a model defined in the domOS ontology. Real appliances of a given type (i.e., heat pump) feature different approaches for their data interface. This can make it difficult to map the common model defined in an ontology to models of individual appliances.

4.3. SWOT analysis

The opportunities and restrictions described above are synthetised in the SWOT analysis presented in Table 3.

TABLE 3: SWOT ANALYSIS

Strength	Weaknesses
1. Compliance with requirements for energy management 2. Reduction of energy costs 3. Streamlined infrastructure 4. Coherence with legacy IoT 5. Privacy management	1. New, unproven business models 2. Start-up constraints 3. Difficult integration of 4. non-digital appliances 5. Incompatible appliance models
Opportunities	**Threats**
1. Expectations for an integrative approach for smart buildings 2. Support for Energy as a Service (EaS) 3. Alignment with citizens' expectations 4. Contribution to public policies 5. Digitalisation trends	1. Unclear limit of liability 2. Market rejection of underlying emerging standards 3. Lack of smart system descriptions 4. Citizens' reservations on privacy 5. Unsatisfying smart home and smart building integration 6. Complexity 7. Ontology not in line with expectations 8. Lack of support from appliance manufacturers

5. Conclusion

The IoT environment as well as the smart home and smart building sectors did evolve and will continue evolving at a rapid pace. Current smart services are still deployed as silo solutions, but integration will be more and more asked for, because the management of many parallel services will become cumbersome, but also because services – especially in the energy sector - need it.

Even if the context provides a breeding ground for an integrative approach, the domOS ecosystem specification will have to climb over walls to become an established standard in the European smart building environment. The main difficulty will be to make the installed basis of compliant systems reach a critical mass, required to attract many stakeholders. To take up this challenge, domOS will have not only to provide excellent technical solutions, but also to dialog with the smart building community to understand the needs and to explain its possible contribution.

6. Bibliography

Balta-Ozkan N., Boteler B. and Amerighi O. European smart home market development: Public views on technical and economic aspects across the United Kingdom, Germany and Italy [Journal] // Energy Research & Social Science. - 2014. - Vol. 3.

Berg Insight AB Smart Homes and Home Automation [Online] // Berg Insight AB. - 2018. - https://media.berginsight.com/2021/02/11125039/bi-sh8-ps.pdf.

Business Wire Global Solar PV Inverter Market Report 2021: Industry Trends, Share, Size, Growth, Opportunity and Forecasts, 2015-2020 & 2021-2026 [Online] // Business Wire. - 11 6 2021. - https://www.businesswire.com/news/home/20210611005310/en/Global-Solar-PV-Inverter-Market-Report-2021-Industry-Trends-Share-Size-Growth-Opportunity-and-Forecasts-2015-2020-2021-2026---ResearchAndMarkets.com.

Chung H., Park J. and Lee S. Digital forensic approaches for Amazon Alexa ecosystem [Journal] // Digital Investigation. - 2017. - Vol. 22.

CloudGarage IoT Envisioning [Online] // CloudGarage. - 22 8 2017. - https://www.cloudgarage.in/strategic-consulting/iot-envisioning/.

Deloitte Switch on to the connected home [Online] // Deloitte. - 7 2016. - https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-16.pdf.

domOS D4.1 Report on Requirement Analysis for Common Services [Report]. - 2021.

Eichberger S. Smart Meter - Clean Energy for all Europeans - The Role of Regulators and Active Consumers [Online] // e-control. - 6 11 2020. - https://www.energy-community.org/dam/jcr:a00932e4-140d-4940-9aca-96c600f40900/E-Control_Smart%20Meter_Eichberger.pdf.

European Commission Benchmarking smart metering deployment in the EU-28 [Online] // Publications Office of the European Union. - 18 3 2020. - https://op.europa.eu/en/publication-detail/-/publication/b397ef73-698f-11ea-b735-01aa75ed71a1/language-en.

European Platforms Initiative Advancing IoT Platforms Interoperability [Online] // IoT-European Platforms Initiative. - 2018. - https://iot-epi.eu/wp-content/uploads/2018/07/Advancing-IoT-Platform-Interoperability-2018-IoT-EPI.pdf.

eurostat Energy consumption and use by households [Online] // eurostat. - 20 06 2019. - https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20190620-1.

Fortune Business Insights Europe Smart Building Market [Online] // Fortune Business Insights. - 2021. - https://www.fortunebusinessinsights.com/europe-smart-building-market-105128.

Furszyfer Del Rio D.D. [et al.] Critically reviewing smart home technology applications and business models in Europe [Journal] // Energy Policy. - 2020. - Vol. 144.

Global Market Insights Europe Heat Pump Market Size By Product (Air Source, Ground Source, Water Source), By Application (Residential, Commercial, Industrial), Industry Analysis Report, Country Outlook, Competitive Market Share & Forecast, 2020 – 2026 [Online] // Global Market Insights. - 10 2020. - https://www.gminsights.com/industry-analysis/europe-heat-pump-market.

IoT Analytics 5 Things to Know About the IoT Platforms Market [Online] // IoT Analytics. - 8 6 2021. - https://iot-analytics.com/5-things-to-know-about-iot-platforms-market/.

i-SCOOP IoT platforms – IoT platform definitions, capabilities, selection advice and market [Online] // i-SCOOP. - https://www.i-scoop.eu/internet-of-things-iot/iot-platform-market-2017-2025/.

McKinsey McKinsey Electric Vehicle Index: Europe cushions a global plunge in EV sales [Online] // McKinsey. - 17 7 2020. - https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/mckinsey-electric-vehicle-index-europe-cushions-a-global-plunge-in-ev-sales.

Prescient & Strategic Intelligence Private Limited Global Smart Homes Market Size, Share, Development, Growth and Demand Forecast to 2023 [Online] // Prescient & Strategic Intelligence Private Limited. - 9 2017. - https://www.psmarketresearch.com/market-analysis/smart-homes-market.

PwC Smart home, seamless life - Unlocking a culture of convenience [Online] // PwC. - 2017. - https://www.pwc.com/us/en/industry/entertainment-media/publications/consumer-intelligence-series/assets/pwc-consumer-intelligence-series-iot-connected-home.pdf.

Smart Home Energy What is a Smart Home [Online] // Smart Home Energy. - 2021. - https://smarthomeenergy.co.uk/what-smart-home/.

Solar Power Europe Solar Power Europe [Online] // European Market Outlook For Residential Battery Storage. - 2 10 2020. - https://www.solarpowereurope.org/european-market-outlook-for-residential-battery-storage/.

Sovacool B.K. and Furszyfer Del Rio D.D. Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies [Journal] // Renewable and Sustainable Energy Reviews. - 2020. - Vol. 120.

ZVEI Smart Home and Smart Building [Online] // ZVEI. - 20 09 2018. - https://www.zvei.org/en/subjects/buildings/smart-home-and-smart-building.