This project has received funding from the European Union's Horizon 2020
research and innovation programme under grant agreement N° 732679

ACTIVAGE
PROJECT

ACTivating InnoVative IoT smart living environments for AGEing well

Report on IoT devices

Deliverable No.	D3.6	**Due Date**	31-Dec-2017
Type	Report	**Dissemination Level**	Public
Version	1.0	**Status**	Release 1
Description	Analysis and compilation of the devices (Sensor/actuator nodes and Gateways) used in the nine ACTIVAGE Deployment sites.		
Work Package	WP3 – ACTIVAGE Secure Interoperability Layer		

Authors

Name	Partner	e-mail
Mario Diaz Nava	02 STMicroelectronics	mario.diaznava@st.com
Byron Ortiz Sanchez	03 Televes	byrort@televes.com
Pilar Sala	04 MYSPHERA	psala@mysphera.com
Juan Bautista Montalva	05 UPM	jmontalva@lst.tfo.upm.es
Alejandro Medrano	05 UPM	amedrano@lst.tfo.upm.es
Thomas Loubier	07 CEA	Thomas.Loubier@cea.fr
Mathieu Gallissot	07 CEA	Mathieu.Gallissot@cea.fr
Stephane Bergeon	07 CEA	Stephane.Bergeon@cea.fr
Nick Kaklanis	08 CERTH	nkak@iti.gr
Konstantinos Votis	08 CERTH	kvotis@iti.gr
Dimitrios Tzovaras	08 CERTH	Dimitrios.Tzovaras@iti.gr
Evangelos Mitsakis	08 CERTH	emit@certh.gr
Felipe Roca	12 HOPU	felipe@hopu.eu
Rubén Molina Moreno	12 HOPU	rmm120617@gmail.com
Rohit Ail	20 Samsung	rohit.ail@samsung.com
Ahmed Bangash	20 Samsung	a.bangash@samsung.com
Michele Girolami	23 CNR	michele.girolami@isti.cnr.it
Dario Russo	23 CNR	dario.russo@isti.cnr.it
Andrea Carboni	23 CNR	carboni@isti.cnr.it
Carsten Stocklöw	34 Sageliving	carsten.stockloew@sageliving.de
Vasileios Mizaras	42 INFOTRIP	vasili.mizaras@swarco.com
Rami Mäkelä	45 SE Innovation	rami.makela@seniorsome.com

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

History

Date	Version	Change
05-May-2017	0.0	Initial ToC proposal
24-Jul-2017	0.1	ToC Updated First Version of Appendix B
03-Nov-2017	0.2	Update Template Appendix B + Add Answers from DS 1, 3, 4 and 6
23-Nov-2017	0.3	Clarifications done in two Template tables in Appendix B
28-Nov-2017	0.4	Contributions from DS1, D2, D3, DS4, D5 and DS6 received
21-Dec- 2017	0.5	Contributions from DS1, D2, D3, DS4, D5 and DS6 updated Contributions from DS7, DS8, and DS9 added
21-Jan- 2018	0.6	Section 3 and 4 were completed
28-Jan- 2018	0.7	Appendix B fully reviewed and commented.
08-Feb- 2018	0.8	Section 1, 2 and 5 finished
23-Feb- 2018	0.9	Update considering Reviewers' remarks
14-Mar-2018	1.0	Official release

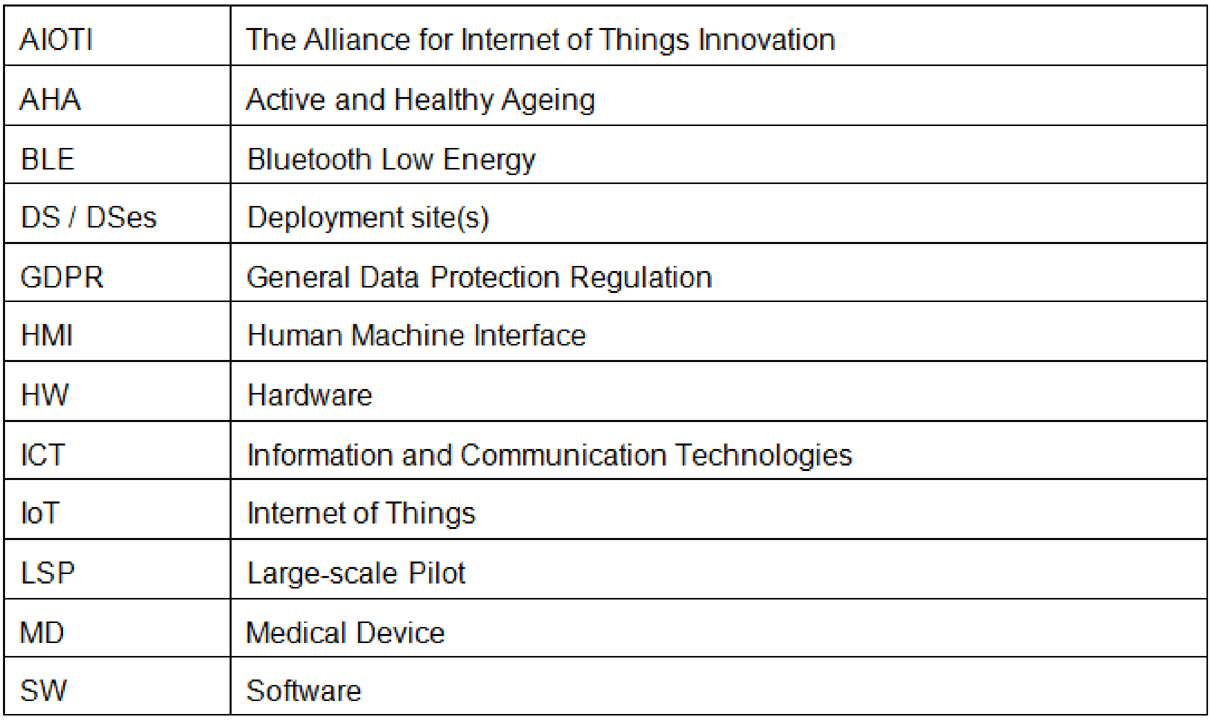
Key data

Keywords	Internet of Things, sensors, actuators, devices, smart nodes, gateways, connectivity, protocols, architecture, topology, layers, security, privacy, tools, Cloud, network, Internet, Deployment Site, applications
Lead Editor	Mario Diaz Nava, 02 STM
Internal Reviewer(s)	Isabelle Chartier, 07 CEA Stefano Nunziata, 10 CUP 2000 SPA

Abstract

In order to have a complete Architecture of the ACTIVAGE platform, the device domain constituted of smart sensor nodes, gateways, connectivity and its associated protocols must be also considered. Therefore, it is imperative to identify the different devices required to implement the uses cases considered in the different Deployment sites (DSes). A systematic analysis is performed on the device, gateway, cloud and applications domains constituting each of the nine DSes. This analysis is based on several registration forms in order to gather key elements of each domain. The original goal was to collect information concerning only the device domain. However during the first months of the project, this goal changed to also include the three other domains in order to get an overall, homogenised, and rich technical information view of each DS. The additional information includes, the DS topology, the applications foreseen, the security and privacy mechanism to be implemented in the overall system, the servers used and their locations, and other information required to facilitate, in Task 3.2, the Security and Privacy assessments. Furthermore, this document gives a summary and classification of the different devices used in each DS allowing the identification of communalities, potential synergies and knowledge sharing between DSs. For the cases where, no suitable solutions are available, new devices could be prototyped in order to support a given use case with the right device or the right security protection level. Finally and in order to have a more complete document, the following aspects are also included: a list of key concepts in the device and gateway domains are explicitly defined to be shared and used in the overall project, a short introduction on the evolution of the communication systems is given in order to understand key IoT concepts at IoT architecture level and in particular at the device and gateway domains, including some security ones, and a brief market analysis on the home automation and health care devices.

Glossary



AIOTI	The Alliance for Internet of Things Innovation
AHA	Active and Healthy Ageing
BLE	Bluetooth Low Energy
DS / DSes	Deployment site(s)
GDPR	General Data Protection Regulation
HMI	Human Machine Interface
HW	Hardware
ICT	Information and Communication Technologies
IoT	Internet of Things
LSP	Large-scale Pilot
MD	Medical Device
SW	Software

Table of contents

IMPORTANT NOTE: THIS DOCUMENT HAS A SECOND APPENDIX (APPENDIX B ACTIVAGE DEPLOYMENT SITES OVERVIEW AND COMPONENTS REQUIRED), WHICH IS PRESENTED IN A SEPARATE DOCUMENT DUE TO ITS CLASSIFICATION AS CONFIDENTIAL.

List of tables

List of figures

1 About This Document

The Internet and mobile revolution has transformed our world. The Internet of Things (IoT) has emerged over the last few years, aims to change our lives by forming a massive ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context to offer a variety of services. By 2020, market analysts expect between 20 and 50 billion connected devices in the world.

The Internet of Things revolution is ongoing but its deployment is on its inception. This revolution is based on the availability of a huge amount of information coming from the data sensed and transmitted by the Smart connected objects.

The “Big data deluge” will be efficiently analysed and exploited creating higher levels of automation (monitoring and control from anywhere at any time to any Vertical application) generating new opportunities and new ways of decision making. The ITC (including the Cloud) technologies in conjunction with the Smart connected objects will play an essential role in this revolution. It will completely change the society and the overall industry at all levels (design, production, exploitation, deployment, and services). This will also strongly impact internal organizations and the business models.

Many research projects have been funded by the European Union concerning the higher levels of the IoT system architecture and efforts are ongoing to consolidate and coordinate the research results by creating an IoT ecosystem through the AIOTI industrial alliance and the 5 IoT Large Scale Pilots concerning the following areas: Smart environment for ageing well, Smart Farming, Wearable, Smart Cities and Smart Mobility.

ACTIVAGE was selected as the Large Scale Pilot addressing Smart environment for ageing well. However, it should be noted that all these LSPs have many communalities from the technology and architecture point of view. Main differences come from the applications addressed and the specificity of the components needed in the lower architecture levels, the hardware devices such as sensors and actuators. It is very often forgotten or at least not too much highlighted the role of these components because without them the IoT revolution cannot take place. Of course, software is also a key differentiation aspect at application level as well the embedded software implemented in the hardware (HW) devices to become more intelligent and powerful.

If we say that the IoT revolution is on its inception, it is because many issues should be solved before getting a much higher market penetration. For instance, at the device level, the devices must: 1) Increase their autonomy by reducing significantly the power consumption; 2) Become more intelligent by embedding more software and new techniques as Artificial intelligence. This requires more processing power and higher memory capacity and for some applications moving from Cloud to Edge computing; 3) Become more reliable considering that the systems will depend on the devices availability and robustness; 4) Become more secure by implementing the right security and safety mechanisms to protect them against Cyber-attacks; 5) Reduce the price to facilitate adoption and large penetration. At the higher levels, some important issues must be also solved such as interoperability, end-to-end security and privacy, and identify and develop killer applications in order to ensure evident benefits to the end-user (gain in productivity, new useful services, reduce costs, increase automation, introduce not intrusive surveillance, etc.). Another issue is to define new business models for the commercialization IoT devices. The current consumer model, which consists to collect the user data on the vendor server, is not adapted to AHA and health services where data privacy is regulated through GDPR. For example, most smart connected objects such as weighing scale, indoor air monitoring, activity monitoring, etc. are not adapted to ACTIVAGE because it requires a full data control.

Two examples of this revolution is the arrival of: 1) the Personal assistant with new HMI (Human Machine Interface) the voice instead to browse through the Web; 2) Concerning the security, the introduction of more robust biometrics technics such 3D Face recognition to facilitate user identification rather to use a password. These technologies, more robust today, are currently being introduced on the market. These are good examples of the impact created by the fast technologies evolution and maturity level got in few years. These new solutions should be a source of inspiration for the ACTIVAGE project and they must be considered on top of the existing ones in order to develop more advanced use cases and services and in the different Deployment sites.

1.1 Purpose

This report aims at identifying and describing the ACTIVAGE devices used by the different use cases implemented in each of the nine ACTIVAGE Deployment sites. The concerned devices are the sensors/actuators nodes and gateways deployed in the Device/Edge domain.

The purpose is also to identify commonalities (hardware and software components, needs, knowledge, etc.) between the DSes that they can share and provide benefits to the overall ACTIVAGE ecosystem, such as exchanging use cases, enhancing use cases with new functionalities, reducing development costs and risks, etc.

Over the time, the purpose of this document has evolved to get more benefit from this work. Thereby, two more goals were defined:

- Use this document as a complement of the Task 3.2 to facilitate the Security and Privacy assessments of each DS. To reach this goal, the Topology of each DS has been requested to identify the different assets, the connectivity and communication links between the different components of the overall architecture. The Topology will also allow the identification of the different data flows and see where the data is processed and stored. Furthermore, the different security and privacy mechanisms foreseen to put in place in each DS were also requested.
- Harmonize the nomenclature of several concepts used in the project in order to facilitate the common understanding between the different groups, coming from different fields, participating in ACTIVAGE.

In order to gather the information from each DS, several register forms were specified for each of the four system domains: Application, Cloud, Gateway and Device/edge (see Annex A).

This deliverable is a living document that will be updated across the project execution according to the work progress performed in Task T3.6 and the interaction with the other tasks for instance Task 3.2 ACTIVAGE Security and Privacy, and Task 9.1 concerning the Deployment sites implementation.

In order to reach the objectives defined above, the following activities were defined and carried on:

- Analysis and Compilation of main DSes Components
  - Define the suitable information to collect at each Domain.
  - Elaborate the register forms and the associated guidelines to get the information.
  - Send the register forms to the responsible of each DS to be fulfilled.
  - Fulfil the register forms by the DS responsible and send them back to Task 3.5 leader.

  - Review and comment the register forms of each DS.
  - Send back comments and recommendations to update the forms considering homogenization of the information to facilitate exploitation.
  - Update the register forms by the DS responsible and send them back to Task 3.5.
  - Update D3.6 report and use as the first release. A second release is foreseen in M24 according to modifications done in the second year by the DS.
  - Analyse, compile and classify the information provided by each DS.
  - Create a synthesize view of the different types sensors/actuator and gateways devices used by each DS in order to easily identify communalities and potential reuse and collaboration.
  - Disseminate this report inside the DSes for exploitation and creation of higher synergy between them.
- **Define some concepts related to communication, devices, and security to have same understanding inside ACTIVAGE project:**
  - Identify the main terms to be defined.
  - Limit these terms to the Device Domain, connectivity, communication technology and security.
  - Define these terms to be adopted in ACTIVAGE to facilitate the communication having a common understanding.
  - Disseminate this list of concepts inside ACTIVAGE project.

This document reports the work performed during the first twelve months of the project. It includes the results obtained from the lists of activities defined just above. The main achievement was the elaboration and completion of the register forms for each deployment site. A compilation and summary of the devices to be used in the different DSes was done. It should be noted that not all the devices have been identified in the first year by the DSes. This work will be completed by DSes during the second year. The same can be said about the security and privacy mechanisms. They will be completed in collaboration with task 3.2.

1.2 Target Audience

This deliverable targets the following audience:

- The DSes technical managers in charge to define the architecture and implement of the different ACTIVAGE pilots. They are directly concerned to contribute and follow the devices required, and their potential reuse, in the implementation of the DSes.
- The DSes security managers in charge to define and implement the different security and privacy mechanism of the ACTIVAGE pilots. They are directly concerned to contribute and follow the security and privacy guidelines issued in collaboration with the Task 3.2.
- The different ACTIVAGE stakeholders interested to learn more about the technical aspects of the nine DSes. This report provides to them a synthesized way that can help to identify differences, communalities and complementarities between DSes.
- The stakeholders interested to know which devices should be improved, identify the devices missing and such that should be secured in priority.

1.3 Deliverable context

Project item	Relationship
Objectives	O2 (To set up a European Multi Centric Large Scale Pilot distributed across nine interconnected Deployment Sites of seven European countries): by analysing the use case requirements at the device domain, D3.6 identifies the list of the sensor nodes and gateways required for the implementation of the use cases considered in the different Deployment sites.
Exploitable results	The analysis and compilation done in D3.6 on the devices (Sensor/actuator nodes and Gateways) used in the nine ACTIVAGE Deployment sites allows the identification of common components between DSes and facilitates their potential reuse, knowledge sharing and synergy increase inside the project. Furthermore, this study allows the identification of key elements required to perform the Security and Privacy assessment
Work plan	This document is the results of work in T3.5 "Identification of the Smart Nodes and Gateways to be used in ACTIVAGE". Moreover, this deliverable is linked with the following WPs and tasks: WP3 T3.2: ACTIVAGE solution for security and privacy, as well as WP9/ T9.2 Experiment
Milestones	D3.6 is a key deliverable for assessing the achievement of MS1 - BUILD in Month 12.
Deliverables	This deliverable is using the outcomes of D9.1 Detailed experiment plan. Deliverable D3.6 has to be delivered on M12 (first version) and on M24 (final version).
Risks	Rk15: "Risk of time consuming due to multiple technology" D3.6 contributes to gaining control of new technologies & IoT related equipment by identifying and sharing knowledge on the most relevant platforms and components with big potential of reuse, adaptability and flexibility.

1.4 The rationale behind the structure

The rest of the deliverable is organized as follows. Section 2 briefly introduces the main concepts related to an IoT System architecture focusing on Device domain, communication and security components. Section 3 gives a short market overview of the IoT devices related to the ACTIVAGE project mainly home automation, healthcare and the Personal Assistants. Section 4 provides a synthesis of the gateways and sensors-actuators nodes used in the different DSes. Finally, Section 5 concludes this report and lists future work to be done. Appendix A provides standard definitions as background information underlying this document, and Appendix B, **which is presented in a separate document due to its specific classification as confidential**, gives a synthetized and technical overview of the main components constituting each IoT domain of the nine DSes, focusing specially to the Gateway and Device Domains.

2 ACTIVAGE IoT High-Level System Architecture and Definitions

This Section aims to defining some terms and concepts that will be used through the whole report. This Section provides a brief overview to the stakeholders no familiar with technical aspects of IoT and communication technologies. The terms and concepts introduced here will help to have a common nomenclature inside the ACTIVAGE project, considering that the stakeholders come from different disciplines.

The second subsection of this Section gives a brief introduction of ACTIVAGE IoT high-level system Architecture and a short description of its four domains associated components.

The third subsection introduces the concepts of Edge, Fog and Cloud Computing. It also makes a brief comparison between these three architectures.

Finally, the fourth subsection provides some definitions concerning several key components related to communication and security infrastructure used in the ACTIVAGE Deployment sites.

2.1 Brief description of the ACTIVAGE IoT high level system Architecture

Figure 1 shows the ACTIVAGE IoT high level System Architecture. Four main layers or domains (Application, Cloud, Gateway and Device/Edge) constitute this architecture.

2.1.1 Application Domain

This domain executes the applications in charge of monitoring and/or control the IoT system. In this domain, the processed information will be available to the user via a HIM (Human Interface Machine) for decision taking. Current HIM are based on smart mobile devices and lap tops to browse the processed information and fetch the results. A new generation of devices like the Personal Assistants arrives on the market supporting voice recognition a more natural way to interact with the system. This feature could be interesting for the elderly people to facilitate the adoption of the IoT technology proposed by ACTIVAGE.

It should be noted that the Application Domain is not always connected to the Cloud domain. In the case of some systems, the application can directly run in a Gateway server. This system type is known as Edge computing because the processing and decision taking are close to the place (for instance < 100 mts) where the raw data is generated.

Appendix B (subsections B.1.2, B.2.2, … B.9.2) of this report lists the different applications running in the DSes and gives a brief description.

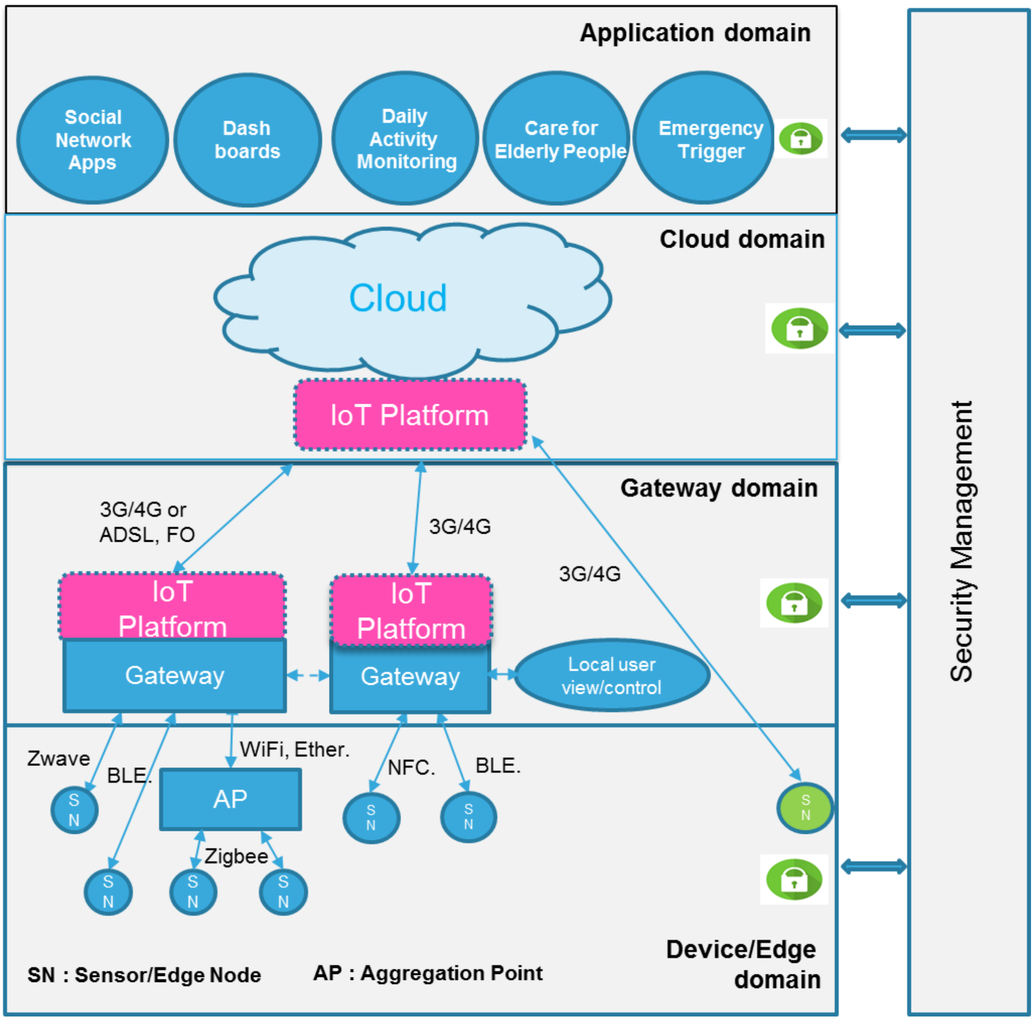


Figure 1: ACTIVAGE IoT high level System Architecture

2.1.2 Cloud Domain

This domain is in charge to provide the infrastructure (Hardware and Software) required to store the raw data received from the gateway domain. It performs data analysis on the big data received and store the obtained results. They will be available to the Application for further exploitation.

A large number of servers and large storage capabilities constituted the hardware infrastructure deployed in any place in the world. Its access is done via Internet.

Data analysis, databases, cloud management, and many other programs constitute the software infrastructure.

It should be noted that in ACTIVAGE, Private Clouds will be developed to support Cloud computing capabilities and they will be located near to the DSes (~<50 Kms). Appendix B (subsections B.1.3, B.2.3, … B.9.3) gives the list of the servers to be deployed and their location.

2.1.3 Gateway Domain[1]

In the upper link direction, a gateway gathers the raw data coming from the sensor nodes, aggregates them and transmits the resulting frame (set of data) to:

- The Cloud to remotely process the data (in case of Cloud computing).
- The local server, associated to the gateway, to locally process the data (in the case of Edge computing).

In the downlink direction, it transports the commands that will control the different actuator nodes in the device domain.

Supporting the Middleware in charge of handling the communication with the sensor actuators nodes to perform data gathering and/or transmit commands to the actuators. In ACTIVAGE, there are seven Middleware developed in previous European projects and called here IoT Platforms. They are the following: IoTivity, FireWare, OpenIoT, SeniorSome, sensiNACT, Sofia2, and universAAL.

2.1.3.1 IoT Gateways Functional Operation

In general, a Gateway acts as a "protocol convertor and data router" between the IOT sensor- actuator nodes and Internet. IOT gateways not only make transmission medium abstraction but also provide encryption to protect the data transmission. Gateways usually run real-time operation systems (RTOS) or a form of Linux to drive their systems. Figure 2 gives an example of a Gateway structure.

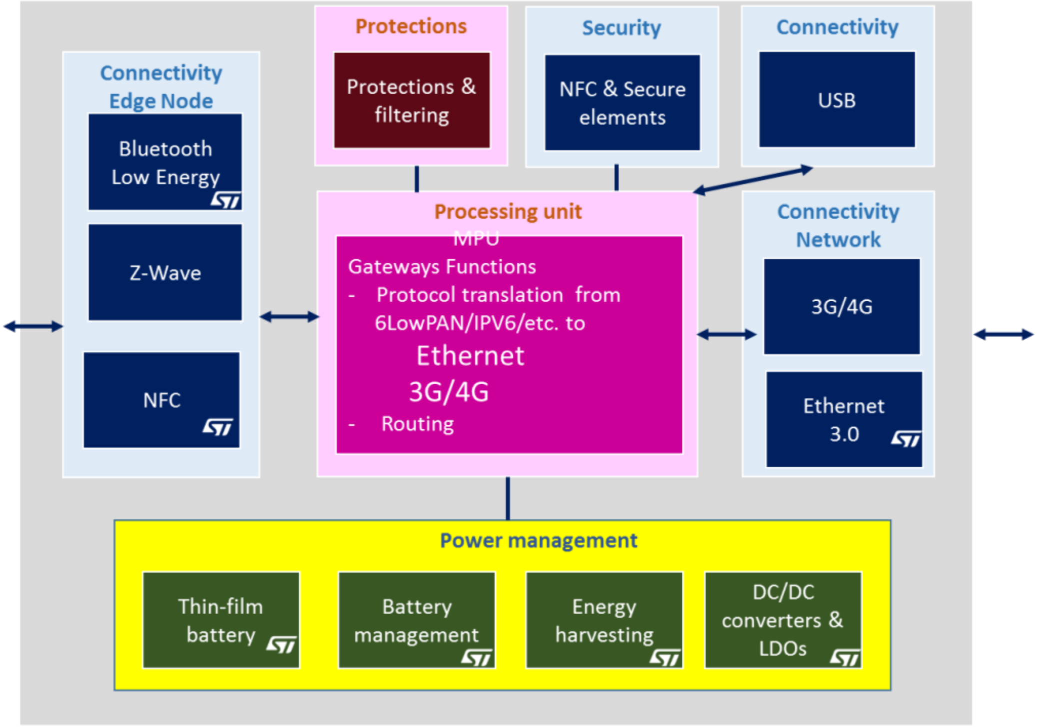


Figure 2: Example of a Gateway block diagram

[1] In the ACTIVAGE IoT System Architecture, the Gateway domain is considered as a separated domain from the Device domain.

In reality, different types of Gateways exist in an IoT system performing different functions according to the type of IoT implemented architecture. In this report, we will distinguish three types of Gateways as illustrated in Figure 1:

- **IoT Aggregation Point**: It is a gateway in charge of, from one side, gathering data coming from the different sensor nodes, and from another side, aggregate this data in a single frame and send it to a second Gateway with the capabilities to send the aggregated data to the Cloud through Internet. This gateway also includes and run the Middleware to handle the sensor- actuators nodes.
- **Gateway**: This kind of gateway is in charge of receiving the data from the IoT Aggregation Point and sending it to the Internet. This gateway has routing, modulation and demodulation capabilities allowing the data transmission/reception to/from Internet using different Physical medium (Twisted pair, Optical Fiber, Air, Coaxial Cable, etc.) and its associated Physical protocols (ADSL/VDSL, DOCSIS, 2G/3G/LTE, etc.). Gateways often include NAT (Network Address Translation) routing and DHCP (Dynamic Host Control Protocol) services. These create and provide the individual IP addresses all the wireless (and wired) clients need to function in a network and also enable, for instance, a single Wi-Fi gateway to simultaneously provide Internet access to numerous users from a single shared Internet connection . Gateways may also include other applications and features such as encryption and security, VPN, firewall, and Voice over Internet Protocol (VoIP). This gateway does not support the Middleware to handle the sensor- actuators nodes.
- **Mobile Gateway**: This Gateway, in ACTIVAGE, is in general a Smartphone or Tablet supporting the functions performed by the two previous Gateways, i.e., Aggregation point + Routing and Modulation and demodulation. This gateway also includes and run the Middleware to handle the sensor- actuators nodes.

Appendix B (subsections B.1.4, B.2.4, … B.9.4) of this report gives a brief description of the different Gateways used in the various DSes. Subsection 4.2 makes a classification of the different gateways and their association with the various DSes.

2.1.4 Device Domain

The Device domain is in charge of:

- In the upper link direction, detecting/reading/capturing information coming from the sensors in contact with the Physical world.
- In the downlink direction, transmitting the commands to the actuators in charge of controlling the physical assets (machines, pumps, motors, etc.).

2.1.4.1 Sensor

A Sensor is a transducer whose purpose is to sense (that is, to detect) some characteristic of its environments, it converts one form of energy into another. It detects events or changes in quantities and provides a corresponding output, generally as an electrical or optical signal; for example, a thermos-couple converts temperature to an output voltage. A sensor includes signal processing with standardized interface for further processing. Some sensors might incorporate more than one sensor element and smart processing characteristics.

2.1.4.2 Actuator

An actuator is a component of a machine that is responsible for moving and controlling a mechanism or system, for example by opening a valve or switch on/off a lamp. An actuator requires a control signal and a source of energy. When it receives a control signal, it responds by converting the signal's energy into mechanical motion.

2.1.4.3 Sensor Node

A sensor node, also known as end-node or smart connected object, collects data from the sensor(s) and send them to the outside world, through mainly wireless connectivity devices such as Bluetooth, BLE, ZigBee, Z-wave, Wi-Fi or through wired communication. These sensor nodes forward the collected data to an Aggregation Point or mobile Gateway, according to the definition given here above.

A sensor node is constituted of four main elements: one or several sensors, a microcontroller, one or several connectivity devices, and a power management unit. Figure 3 illustrates these four elements. It should be noted that the wireless or wired devices will be selected according to several parameters (power consumption, reach, throughput and the connectivity protocol and in line with the application needs.

2.1.4.4 Actuator Node

An actuator node has a similar structure and elements to the sensor node. However, it has an actuator element instead of a sensor. The data flow is in the opposite direction to a sensor node. The actuator receives commands to control the machine or device interacting with the environment. The three other elements are practically the same. This is why we can talk about a sensor-actuator node because these common elements can be shared with a sensor node.

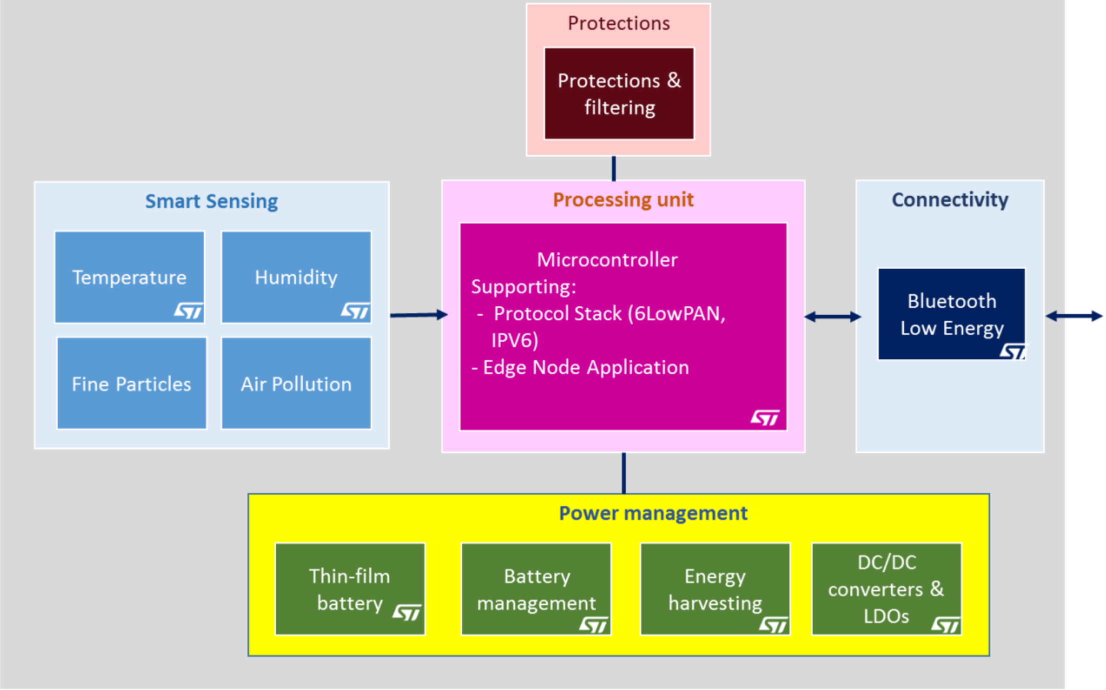


Figure 3: Example of a Sensor block diagram

Appendix B (subsections B.1.5, B.2.5, … B.9.5) of this report makes an exhaustive analysis of the devices used in the different use cases of the nine ACTIVAGE DSes. Section 4.3 makes a classification of the different of devices according to the type of application and their association with the various DSes.

2.2 Definition and differences between Edge, Cloud and Fog Computing

This section provides other important concepts used to define where the computing (for instance data analysis, the application) processing and storage is performed in an IoT System. In this section, the concepts of Edge, Fog and Cloud computing according to the literature.

2.2.1 Edge computing

Edge computing is a method of optimizing Cloud computing systems by performing data processing at the edge of the network, near the source of the data. This reduces the communications bandwidth needed between sensors and the central data centre (Cloud or Private Cloud) by performing analytics and knowledge generation at or near the source of the data [1] [2].

An Edge Device is any computing or networking resource residing between data sources (physical assets) and cloud-based data centres. For example, an edge device could be a sensor or an actuator node connecting the physical asset and the Cloud. Sensor/Actuator nodes provide Edge computing capabilities to determine what data should be stored locally or sent to the cloud for further analysis. In Edge computing, intelligence is literally pushed to the network edge, where the physical assets are first connected together and where IoT data originates [3].

Edge computing will play a more important role over the time considering the increase of power computing in the sensors/actuators nodes thanks to the new features and capabilities provided by the progress of different technologies areas such as Semiconductors, Machine and deep learning, Artificial Intelligence, etc.

2.2.2 Fog computing

Cisco Systems introduce the term "Fog Computing" as new model to ease wireless data transfer to distributed devices in the Internet of Things (IoT) network paradigm. Cisco defines Fog Computing as a paradigm that extends Cloud computing and services to the edge of the network. Similar to Cloud, Fog provides data, compute, storage, and application services to end-users.

The distinguishing Fog characteristics are its proximity to end-users, its dense geographical distribution, and its support for mobility. Services are hosted at the network edge or even end devices such as set-top-boxes or IoT Gateways. By doing so, Fog reduces service latency, and improves QoS, resulting in superior user-experience. Fog Computing supports emerging Internet of Everything (IoE) applications that demand real-time/predictable latency (industrial automation, transportation, networks of sensors and actuators). Thanks to its wide geographical distribution the Fog paradigm is well positioned for real time big data and real-time analytics. Fog supports densely distributed data collection points, hence adding a fourth axis to the often-mentioned Big Data dimensions (volume, variety, and velocity) [4] [5].

2.2.3 Cloud computing

Cloud computing is usually a model for enabling convenient, on-demand network use of a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that may be rapidly provisioned and released with minimal management effort or vendor interaction. It is a new computing technique, which achieves options for renting of storage infrastructure and computing services, renting of business processes and overall applications. This new technique simplifies the clients computing jobs by renting resources and services.

Cloud systems are located within the Internet, which is a large heterogeneous network with numerous speeds, technologies, topologies and types with no central control. Because of the non-homogeneous and loosely controlled nature of the Internet, there are many issues especially quality of service related ones that remain unresolved. One such issue that affects the quality of service severely is network latency. Real time applications with which users directly interact with are badly affected by delay and delay jitter caused by latency in networks.

In terms of architecture and IT infrastructure, the Cloud has become the right solution to meet the needs for reliability, security, scalability needs, and maximize the servers by using them whenever necessary. Most of the architectures of the ACTIVAGE Deployment sites have adopted this kind of solution, but they are based on Private Clouds managed by the stakeholders of the ACTIVAGE project.

2.2.4 Architectural Differences between Edge, Fog and Cloud computing

2.2.4.1 Edge vs. Fog Computing

The key difference between Edge and Fog computing architectures is exactly where that intelligence and computing power is placed [2]:

- Fog computing pushes intelligence down to the local area network level of network architecture, processing data in a fog node or IoT gateway.
- Edge computing pushes the intelligence, processing power and communication capabilities of a sensor/actuator node device.

2.2.4.2 Fog vs. Cloud Computing

Fog computing performs better than cloud computing in meeting the demands of the emerging paradigms. But of course, it cannot totally replace cloud computing as it will still be preferred for high end batch processing jobs that are very common in the business world. Hence, we can conclude that fog computing and cloud computing will complement each other while having their own advantages and disadvantages. Edge computing plays a crucial role in Internet of Things (IoT).

Studies related to security, confidentiality and system reliability in the fog-computing platform is absolutely a topic for research and has to be discovered. Fog computing will grow in helping the emerging network paradigms that require faster processing with less delay and delay jitter, cloud computing would serve the business community meeting their high-end computing demands lowering the cost based on a utility pricing model.

The advantages of Fog Computing are [3]:

1. The significant reduction in data movement across the network resulting in reduced congestion, cost and latency, elimination of bottlenecks resulting from centralized computing systems, improved security of encrypted data as it stays closer to the end user reducing exposure to hostile elements and improved scalability arising from virtualized systems.
2. Eliminates the core-computing environment, thereby reducing a major block and a point of failure.

3. Improves the security, as data are encoded as it is moved towards the network edge.
4. Edge Computing, in addition to providing sub-second response to end users, it also provides high levels of scalability, reliability and fault tolerance.
5. Consumes less amount of bandwidth.

The disadvantage of Fog Computing is that it introduces certain demerits on the selections of technology platforms, web applications or other services.

2.3 Concepts and Definitions on Communication and Security

Considering that the stakeholders of the ACTIVAGE project come from different competence areas, this section provides (rather Annex B) a minimum of background to facilitate the understanding of this document for those people no familiar with the communication and security concepts presented in Appendix B. In general, these concepts will allow having a common understanding inside the project.

In fact, it is in Annex B where the basic concepts related to the main elements constituting the architecture of the Deployment Sites are defined. Annex B is organized in the following three subsections:

- General Concepts
- Protocols for communication and security
- Infrastructure components for communication and security.

3 Brief State-of-the-art on Smart Home and Healthcare devices

This section gives a brief overview on the different kind of devices existing in the market related to home automation and health-care.

Over the time, these devices have evolved from single ones working in standalone mode to more sophisticated and connected ones. Technology evolution in different domains (semiconductor, telecom, software, Big data, Intelligence artificial, etc.) has allowed the design and development of smaller (higher integration, higher performances), more autonomous (low power), higher connectivity, smarter (software, IA) and cheaper devices.

In the next subsections, a market overview is given for each of the following IoT devices segments: Smart Home/Home automation, Healthcare, Wearables and Personal Assistants.

This analysis is not exhaustive, its main purpose is to give an overview of the market related to the devices used in ACTIVAGE and new ones that could be considered to extend the ACTIVAGE applications and use cases.

3.1 Smart Home

Nowadays, the society develops its activities in a global context where the technology influence is increasing every day. The IoT (Internet of Things) technology is increasingly becoming popular thanks to its highly expected benefits. Smart environments, smart cars, smart home, smart cities are some of the vertical pillars that are providing information in real-time through personal devices like smartphones.

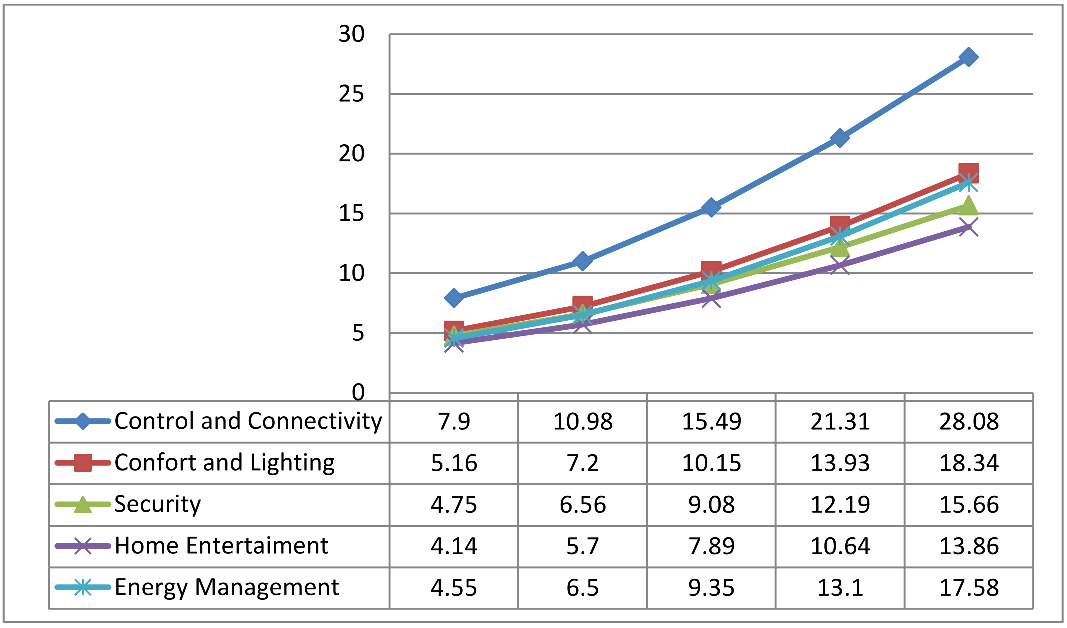
For instance, focusing on Smart home, this pillar could be defined as a place with capabilities to control and monitoring several tasks at home such as illumination control, security survey, temperature regulation, presence detection, health monitoring, etc. According to Kelley Branch[2], since their introduction in 1975, its usages have become widespread and have presence in many places around the world thanks to the introduction of IoT based systems. The main reasons are comfort increase, home monitoring and control at any time at anywhere.

The market forecast indicates that by 2020, the number of Smart Homes will be 75 million installed worldwide, generating 27.5 $ billion in revenues from products and services. This will require robust solutions to manage the data, according to the Broadband Technology Report.[3]

Europe will be the market place where the implementation of Smart Home will experience a great growth, for instance, in control and lighting, security, home entertainment, energy management or smart appliances. Figure 4 shows the evolution of some Smart Home areas in Europe between 2016 and 2020.

[2] http://www.ehowenespanol.com/informacion-casas-inteligentes-sobre_79661/.

[3] http://www.broadbandtechreport.com/articles/2016/02/smart-home-market-to-hit-27-billion-in-2020.html.



◆ Control and Connectivity	7.9	10.98	15.49	21.31	28.08
■ Confort and Lighting	5.16	7.2	10.15	13.93	18.34
▲ Security	4.75	6.56	9.08	12.19	15.66
✕ Home Entertaiment	4.14	5.7	7.89	10.64	13.86
✳ Energy Management	4.55	6.5	9.35	13.1	17.58

Source: Own elaboration with data of Statista

Figure 4: Evolution of home market penetration in Europe (millions of houses, 2016-2020)

According to Figure 4.1, the highest home market area is control and connectivity with 7.9 million of household for 2016, this amount will increase until 28.08 million in just 5 years (2020). The home market area is comfort and lighting with 5.16 million of household. On the other hand, the less home market penetration is entertainment with just 4.14 million of household with this extension[4].

Table 1 summarizes the total variation rate of the different home markets areas in Europe between 2016 and 2020. All of them have a growth rate beyond 225%, although the two more representative extensions are applications of control and connectivity along with comfort and lighting with a growth rate of 255.44% and 255.43% respectively, in a period of five years.

Table 1: Total Variation Rate (%) of different home market areas in Europe between 2016-2020 Period

	Control and Connectivity	Comfort and Lighting	Security	Home Entertainment	Energy Management	Smart Appliances
Period Variation Rate (2016-20)	255.44	255.43	229.68	234.78	286.37	254.68

Source: Own elaboration with data of Statista

Table 2 shows the penetration rate per year of different household market areas in Europe between 2016-2020 period. One of the most interesting data of Table 4.2 is a general growth in all the areas, being the control and connectivity the most representative increased with a growth rate of 10.47% for 2020. To the other extend, the growth rate is defined as a range of 5% to 6% for 2020.

[4] https://www.statista.com/outlook/279/102/smart-home/europe#marketStudy.

Table 2: Variation Rate per year of different household market areas in Europe (%) between 2016-2020

	2016	2017	2018	2019	2020
Control and Connectivity	2.96	4.11	7.95	5.79	10.47
Comfort and Lighting	1.93	2.70	5.20	3.79	6.83
Security	1.78	2.46	4.55	3.39	5.84
Home Entertainment	1.55	2.13	3.97	2.95	5.17
Energy Management	1.71	2.43	4.89	3.50	6.55
Smart Appliances	1.76	2.44	4.70	3.43	6.21

3.2 Smart Health Devices

The IoT applications are very large, being one of the most interesting applications their applicability in the Health sector. Glucose meter, blood pressure monitor, heart rate monitoring, audio level meters, emergency button or coagulometers are some of the devices connected into the IoT world.

A blood glucose meter is a portable instrument used to measure the level of glucose in the blood. People with diabetes normally uses a blood glucose meter to help them manage their current health state. Traditionally, people without the possibility to transmit in real time the gathered data have used this device. Nowadays, the situation has changed and people can send these data in real time to the doctor. Many solutions exist in the market such as Medidor Free Style Libore[5] from Abbott Laboratories. This device can measure the level of glucose in an easy and intelligent way using a smartphone; Contour diabetes solution[6] is another smart health instrument, in this case the enterprise provide an app ("Contour Diabetes") for smart phone that´s connect with blood glucose meter ("Contour Next One") allowing detect the levels in a continuous and intelligent way. These smart solutions allow receive alert about the levels, share reports with your health professional, insert comments in the meter reading, etc.

A Blood pressure is a medical device used to measure the pressure that the blood exerts against the walls of the arteries as it passes through them. Nowadays, there are a large number of devices to measure this pressure, but the more useful are the IoT blood pressure devices. Some companies such as NOKIA (Nokia BPM+), Omron Evolv, Blipcare or QardioArm provide smart device where the users can measure the blood pressure and collect a historical data in their smartphone.

A Heart rate monitor is a device used to measure the individuals' heart rate. It detects each heartbeat, it counts them and displays the number of beats per minute. Personal heart rate monitors are used for instance to measure exercise intensity. It can continuously track and record heart rate during exercise. It provides more information compared to an on-demand pulse monitor which only shows a value at a single point. Many heart rate monitors save and display the workout heart rate on a graph compared to time, speed, elevation and other

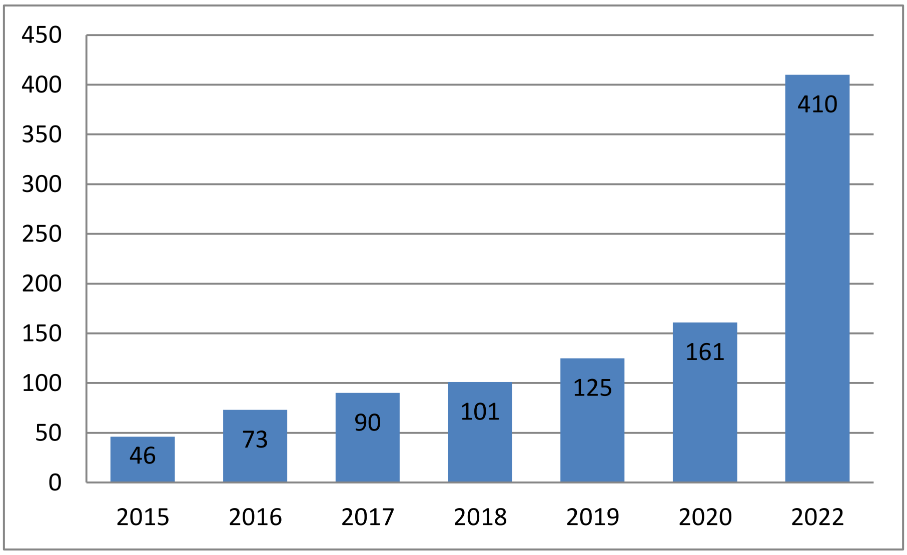
[5] http://www.abbott.com/our-products/for-professionals/diabetes-care.html.

[6] http://www.contourone.es/inicio_paciente/#section3.

aspects measured during the workout. The time in different heart rate zones may be shown at the end of the workout. Walkers, runners, bikers, elderly people use heart rate monitors to survey the intensity of workout performed and to manage the effort to stay in the selected heart rate zone avoiding additional efforts causing heart troubles. Furthermore and according to the analysis report from Business Wire, the forecasts of the global heart rate monitoring device market will grow at a CAGR of 13.12% during the period 2016-2020" [7]. Thereby, it is a device with a good future acceptance in the market.

Today, there are many IoT health devices. However, the expectations are much more on the future of this market. According to Business insider with data of the firm Grand View Research[8], "IoT devices for healthcare are dominated by wearables, which make up 60% of the connected medical device market, according to the report. However, the report predicted fast growth in the near future for implantable medical devices like connected pace makers and implanted sensors that allow for real time patient monitoring. BI Intelligence estimates that 73 million IoT devices will be installed for the healthcare sector this year worldwide, rising to 161 million installations in 2020".

Therefore, the trend is rising and every year the investment amount grows until the quantity of 410 billion of dollars to 2022. Figure 5 shows evolution of investment in the global HealthCare sector in billions of dollars to the period 2015 to 2022.



Source: Own elaboration

Figure 5: Evolution of investment in the global HealthCare sector (Billions of dollars, 2015-22)

The data reflected in Figure 5 shows that the investment has an important increase. An interesting data is that the global investment every year is better being 2022 the best year where the global healthcare sector will invest more than $400 billion in IoT devices, software and services.

The health devices applicability is very useful for healthcare monitoring of elderly people. The market in this area is optimistic expecting a growth annual rate of 26% until 2021

[7] https://www.businesswire.com/news/home/20161014005241/en/Global-Heart-Rate-Monitoring-Devices-Market.

[8] http://www.businessinsider.com/the-global-market-for-iot-healthcare-tech-will-top-400-billion-in-2022-2016-5.

according to Kiversal[9]. The main reasons of this success are related to the advantages provided such as:

- Remote patient monitoring
- Patient-doctor connection
- Information exchange
- Connection to cloud platforms where data can be stored and exported easily
- Analysis of data gathered
- Follow-up of patients' medication orders and their location
- Healthcare cost savings in the medium and long term

With these advantages, the IoT technology provides a support well adapted to cope with the health requirements that achieve a global benefit to the society. This is one of the major goals of the ACTIVAGE project. For these Health applications, more than for the other markets, the security, safety and privacy of the connected Medical Device is a critical point. Cybersecurity risks have to be addressed along the whole lifecycle of the medical device (MD) including hardware and embedded software. This is even more critical when the MDs are linked to Health Information Systems including hospitals, remote care and homecare.

3.3 Wearables

In previous sections has been analysing the smart Home applications and different devices in the global healthcare sector. This section will describe the market impact of wearable devices such as smart wristband or smart watch.

Smart wearables are smart gadgets that can be worn on the wrist and it is supposed to make your life easier. The actual market has three main smart wearables: smartwatches, smart bracelets and smart wristbands.

Smart wristband is the first launched wearable computing device used for fitness monitoring worn on the wrist. This kind of devices support functions, such as pedometers, heart rate monitoring and gravity sensor.

A smartwatch is a wearable computing device that closely resembles a wristwatch or other time-keeping device. Many smartwatches are Bluetooth-capable and become, in effect, a wireless Bluetooth adaptor capable of extending the capabilities of the wearer's smartphone to the watch or vice-versa. In such a case, the wearer can use the watch's interface to initiate and answer phone calls from their mobile phone, read email and text messages, get a weather report, listen to music, dictate email or text messages or ask a digital assistant a question. From another side, the smartwatch supports similar functions that the smart wristband devices and uses the smartphone communication capabilities to transit outside (to a PC, to the cloud, etc.) the gathered data.

A smart bracelet is a wearable computing device with similar features than a smartwatch.

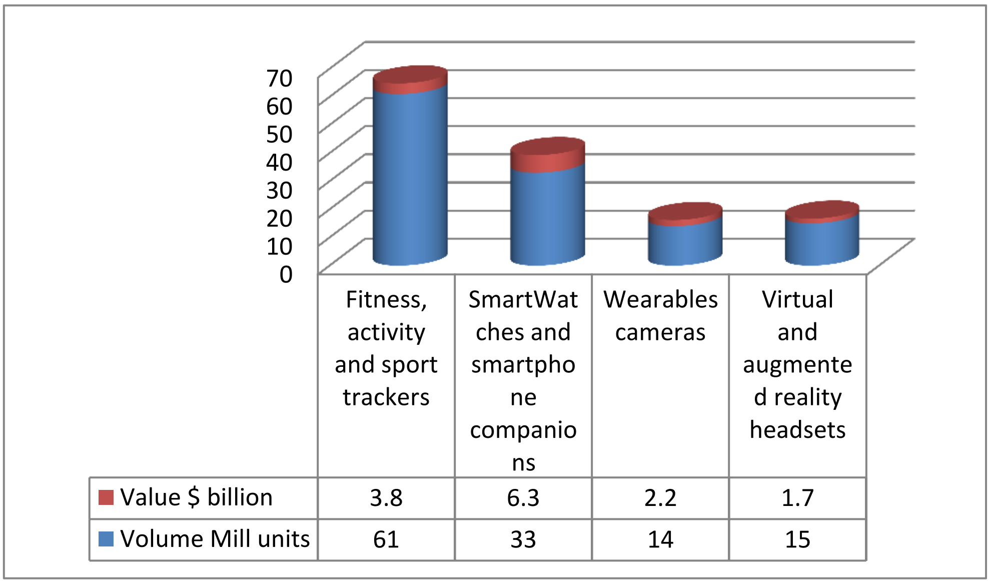
Companies such as Apple, Samsung, Xiaomi, Huawei, Brigmton or Mykronoz provide these devices on the market. Products such as Apple’s iWatch, Smart Watch Amazfit pace of Xiaomi, Samsung gear Fit2Pro of Samsung, Huawei Band Smartwatch, etc. are between the more popular on the market. Thereby, Smartwatch is a product established in a growth market.

[9] https://blog.kiversal.com/que-es-la-iot/.

According to Paul Lankin in Forbes, 411 million smart wearables devices will be sold in 2020, being Wristbands, smartwatches and Eyewear the devices more sold with sales of 164, 110 and 97 million respectively. These sales will generate $34 billion in 2020.

The following figures show the global wearables sales in 2016 and 2020 respectively.

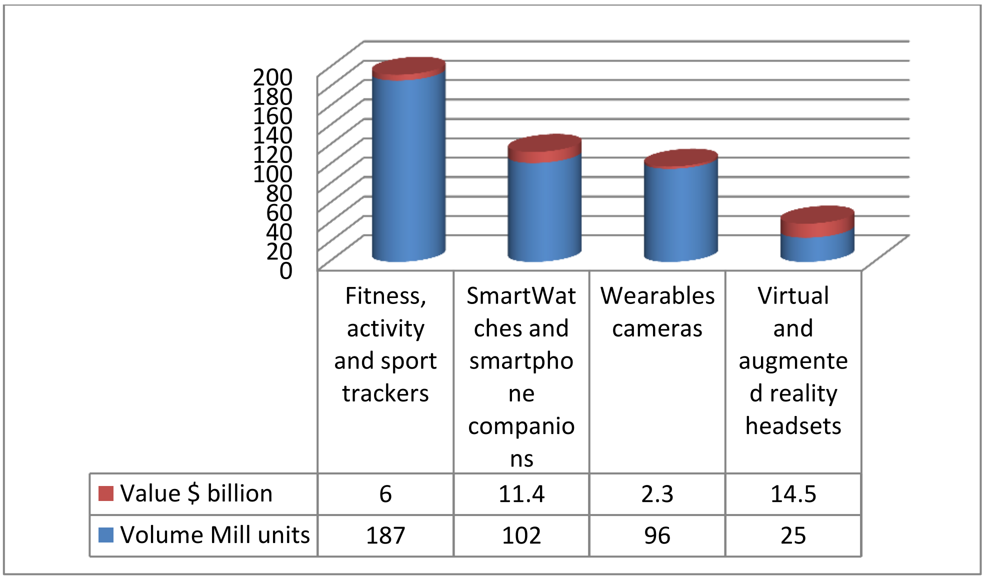
Figure 6 shows that the first sales concerns the Fitness market as activity and sport trackers. The Number of devices sold in 2016 was 61 million and the value was 3.8 $ billions. On the other hand, the Wearables cameras are the devices with fewer sales although the value is bigger than Virtual and augmented reality headsets (devices nowadays with less contribution in this area).



	Fitness, activity and sport trackers	SmartWatches and smartphone companions	Wearables cameras	Virtual and augmented reality headsets
🟥 Value $ billion	3.8	6.3	2.2	1.7
🟦 Volume Mill units	61	33	14	15

Source: Own elaboration

Figure 6: Global wearables sales in 2016, (Millions of units; billions of dollars, 2016)



	Fitness, activity and sport trackers	SmartWatches and smartphone companions	Wearables cameras	Virtual and augmented reality headsets
🟥 Value $ billion	6	11.4	2.3	14.5
🟦 Volume Mill units	187	102	96	25

Source: Own elaboration

Figure 7: Global wearables sales 2020 forecast, (Millions of units; billions of dollars)

Figure 7 shows a large increase of sale volume compared to 2016. Although the Fitness, activity and sport trackers will continue to be the sales leader, the contribution of

Smartwatches and smartphone companions will be bigger than the leader. Table 3 gives the variation rate of the different device families during 2016-2020.

Table 3: Total Period Variation Rate of different extension (%) between 2016-20

	Fitness, activity and sport trackers	Smartwatches and smartphone companions	Wearables cameras	Virtual and augmented reality headsets
Value	57,89	80,95	2,06	752,94
Volume	206,56	209,09	585,71	66,67

Source: Own elaboration

The most representative data is that the Wearables cameras will have the best growth rate (585,71%) although with a strong price erosion. On the other hand, the best growth value rate will be the sales of Virtual and augmented reality headsets devices.

Indeed, the trade future of these products will be great; all the companies developing activities in this sector need to exploit the market niche to achieve a good position in the future.

3.4 Personal assistant

A new generation of Smart home connected objects is being introduced in the market since June 2015, **the Personal Assistant**. For instance, Amazon was the first company to do it with its **Echo** loudspeaker. **Echo** is a real intelligent (voice) assistant who can talk to you, give you information and even anticipate your needs. It allows you to be connected everywhere and all the time in your home. Some of the main features provided by this new Smart Connected object are the following:

- Echo speaker offers good bass for optimal sound broadcast 360°, i.e. throughout the room.
- Seven microphones allow to be heard from any corner and interact with the device
- If you are alone you can converse with “Alexa”.
- It understands everything you say, as long as you use simple and fluent language.
- It can give the weather, broadcasts news feeds on demand, recorder your shopping list, and can event do your research on Wikipedia for you.
- It can recorder for you your appointments ad will remind you in due time.
- It can remotely control all your other connected objects: turn on off your lights (including Philips HE bulbs, by voice), control your alarms, your heating, etc.
- Smart assistant owners will be able to pay their bills and administer their bank accounts by chatting with Alexa.
- …

Furthermore, Amazon has also launched Echo Connect, a little gadget terminal that connects its speakers Echo range to a fixed line. Amazon’s Echo speakers can already make calls through the VoIP system, but if the internet connection does not work then this system is not operational …unless the device owner has an Echo Connects

Alexa is the name given to this speech synthesis tool powered by artificial intelligence. Alexa Voice service, the technology integrated into Echo box, will be made available to third-party developers. They can integrate it into their objects (equipped with a microphone, a speaker and an internet connection) by adding a few lines of code to their software. Amazon also launches several APIs, the Alexa Skill kits, to allow developers to give new features to the tool. 10000 applications is the number of applications develop by a Third party in Q1, 2017.

Amazon Echo has a considerable advantage over its direct competitors Apple HubPod, Google Home, Microsoft Cortana and certainly in the next future the Facebook AP.

Google Home, arrived well after the Amazon model, the google Home is nonetheless a very serious competitor. The main reason for this is its direct link to the company’s famous search engine, which makes voice interaction much more interesting.

Despite this aggressive competition, Amazon will dominate the smart loudspeaker sector by the end of 2017. The group will hold 70.6% market share in the United States according to the study by eMarketer. Google, the number two in this ranking, has a ceiling of 23.8%

Intelligent assistants are becoming increasingly presents on the market but they could quickly become updated. The Japanese are already developing the first hologram assistant. The Azuma Hikari hologram features 3D virtual assistance, designed to provide personalized assistance to the individuals in their daily lives.

The very advanced technology available in the Personal Assistants gives them high potentiality to be rapidly deployed in the emerging market. However, data privacy and confidentiality are very important issues that should be carefully handled by the companies in charge to commercialize these devices in order to facilitate their deployment in Europe coping with new GDPR EU directive.

It should be valuable for ACTIVAGE and its associated Deployment Sites to evaluate the potentiality of these new devices. The Personal Assistants bring advanced technology that can help to develop and propose smarter and more sophisticated applications and use cases with high potential benefits for all ACTIVAGE stakeholders (patients, caregivers, etc.).

4 Summary and use of existing devices per Deployment Site

This section compiles the information provided by the nine Deployment sites concerning the devices (Gateways and Sensor nodes) used in the implemented of their architectures. These devices concern the Device and Gateways domains as illustrated in Figure 6.1.

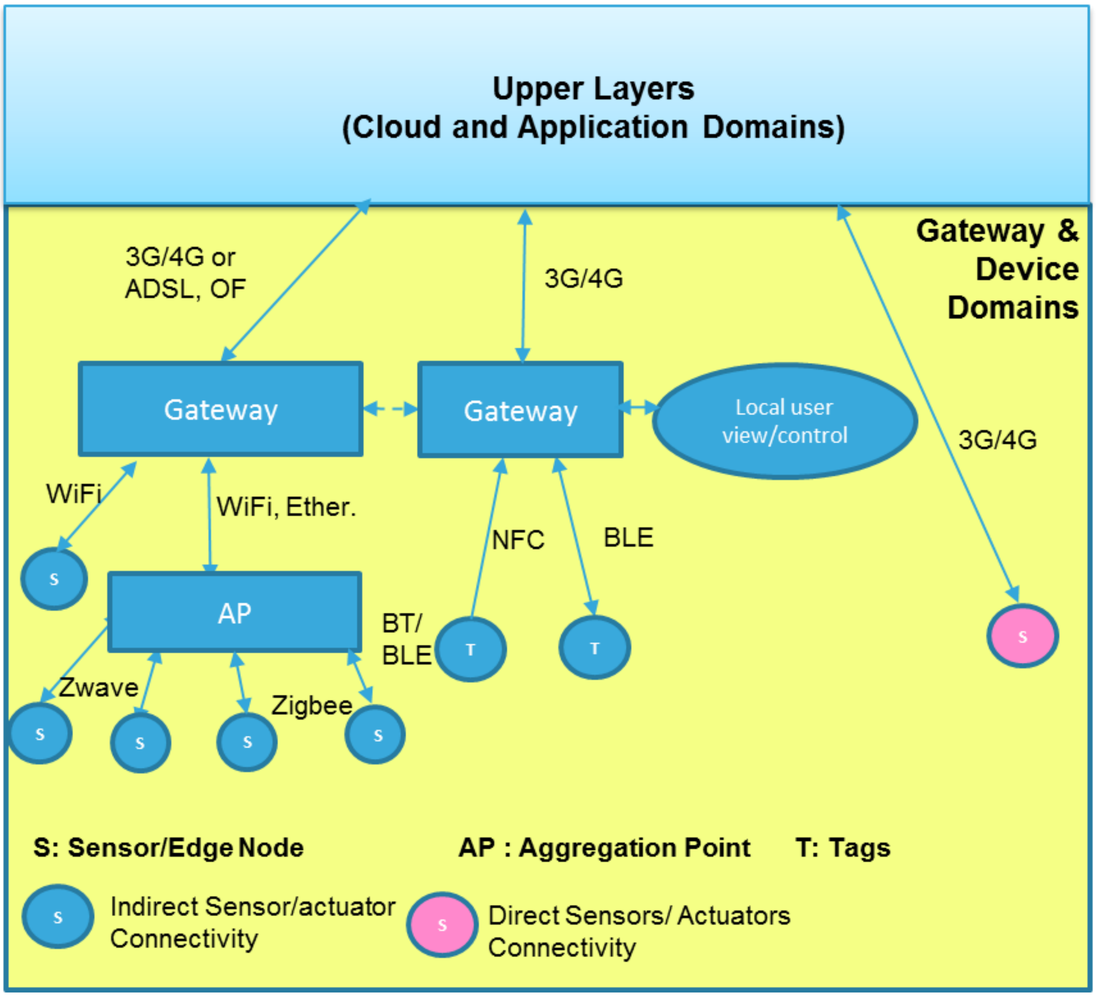


Figure 8: Gateway and Device Domains Reference Architecture

The following subsections provide several Tables indicating the types of Gateways and Smart nodes used in each Deployment site. Moreover, these Tables give a complete view of the devices that will be deployed in the ACTIVAGE project till T0+12. However, the suppliers of some devices should be identified.

These Tables also allow the identification of common functions (at Gateway and Device domains) between Deployment sites and thus create stronger synergies by exchanging experience and increasing the cooperation in order to provide higher impact at European level.

4.1 Gateways

The following three tables summarize the different Gateways devices that will be used by the different deployment sites. These Gateways are classified in three types:

- **Aggregation Points** in charge to gather the data, from the sensor nodes, and transmitted them to the Cloud through the Gateway with modem and routing capabilities. (See Table 4.1).
- **Gateways** in charge to receive the data from the Aggregation Points and send them to the Cloud. (See Table 4.2).
- **Mobile Gateways** in charge to gather the data and send them directly to the Cloud. They are generally based on mobile devices as smartphones. (See Table 4.3).

Table 4: List of Aggregation Points to be used by the Deployment Sites

Name	Supplier (brand) + Model	Deployment Sites								
		DS1	DS2	DS3	DS4	DS5	DS6	DS7	DS8	DS9
CareLife	Televes “CareLife”	U				U	U			
Rasberry	Rasberry Pi model 3			U		U	U	U		
ACTIVAGE Center	Kiosk artemedia serie			U						
Mi-Home Gateway	OpenThings								U	
Senescreen	SeniorSome, SE1001									U

Table 5: List of Gateways to be used by the Deployment Sites

Name	Supplier (brand) + Model	Deployment Sites								
		DS1	DS2	DS3	DS4	DS5	DS6	DS7	DS8	DS9
User/Home Gateway Modem/router	Telecom Provider	U		U		U	U		U	
Home-spot wireless router	ZYXEL LTE4506				U					
WLAN Router	WLAN (WIFI), several onsite models									U

Table 6: List of Mobile Gateways to be used by the Deployment Sites

Name	Supplier (brand) + Model	Deployment Sites								
		DS1	DS2	DS3	DS4	DS5	DS6	DS7	DS8	DS9
Tablet Home	Tablet Android 4.0 with		U							U

Gateway	support 3G and WIFI									
Smartphone Gateway	Android 4.0 smartphone, various brands and models are being validated			U						U
Embedded Gateway	Embedded gateway on the bus			U						

4.2 Smart Nodes, Smart Objects, Wearables

Table 7: List of Home Monitoring Sensors to be used by the Deployment Sites

Name	Supplier (brand) + Model	Deployment Sites								
		DS1	DS2	DS3	DS4	DS5	DS6	DS7	DS8	DS9
Presence/Motion sensor	Televes.	U								
	Panasonic – Texas Instruments		U							
	UNIPR custom device				U					
	Fibaro FGMS-001 (zwave)					U				
	Fibaro, Aeon Labs						U			
	Energenie - Mi|Home Smart Motion Sensor								U	
	To be defined									U
Contact Sensor	Televes	U								
	Standex-Meder Electronics Texas Instruments -		U							
	Fibaro			U						
	UNIPR custom device				U					
	Fibaro FGK-10x or Centralite 3-Series Micro Door Sensor – 3323 (ZigBee)					U				
	Aeon Labs						U	U		
	Fibaro							U		
	Energenie - Mi|Home Smart Door/Window Open Sensor MIHO033									
	SEI									U

Smoke detector	Televes	U								
	To be defined							U		
Air quality Sensor CO, CO2,… Detector	Televes	U								
	Fibaro CO sensor FGCD-001					U				
	Sensoair, Netatmo,						U			
	MCO-Home							U		
Temperature / Humidity sensor	To be defined		U							
	Centralite 3-Series Temp & Humidity Sensor 3310					U				
	Weather Station						U			
NFC tag	Smartcard focus			U						
eBeacon	Estimote			U						
Smart bulb	Hank			U			U			
Energy Plug	Energenie – Mi|Home Monitor adapter								U	
Energy House monitor	Aeotec Voltaware						U			
	Energenie – Mi|Home Whole House Monitor								U	
Smart shower head	Hydrao						U			
Flood sensor	To be defined							U		
Multisensor (motion, temperature, humidity, light intensity)	Aeon, Fibaro							U		

Table 8: List of Health Monitoring Sensors to be used by the Deployment Sites

Name	Supplier (brand) + Model	Deployment Sites								
		DS1	DS2	DS3	DS4	DS5	DS6	DS7	DS8	DS9
Weighing scale	A&D UC-352BLE	U								
	To be identified						U			
	To be identified				U			U		
Tensiometer	A&D Medical UA-651BLE	U								
Coagulometer	Roche CoaguCheck	U								
FitBit	FitBit Alta HR2			U						
Equimetrix Floormat	Tecnalia			U						
Webcam	Logitech C525			U						
Camera	SEI									U
Blood pressure	UNIPR custom device					U				

	To be defined							U		
	Samsung S3								U	
Glucose device	UNIPR custom device					U				
	To be defined							U		
	Samsung A3								U	
Heart Rate Monitor	To be defined							U		
	Samsung – Gear S3 / Gear Fit 2								U	
	SEI									U
Water Intake	Samsung A3								U	

Table 9: List of Daily Activity Monitoring Sensors to be used by the Deployment Sites

Name	Supplier (brand) + Model	Deployment Sites								
		DS1	DS2	DS3	DS4	DS5	DS6	DS7	DS8	DS9
Daily Activity monitoring	Smartphone MEMS To be defined		U							
	Smartwatch (To be defined)		U							
	UNIPR custom device				U					
	Wearable motion (To be defined)					U				
	Samsung A3								U	
	Samsung Smart watch – Gear S3 / Gear Fit 2								U	
	SEI									U
Bed occupancy sensor	UNIPR custom device				U					
	To be selected between: Emfit (Abilia), IGD (cross-pilot with WoQuaZ), Murata SCA11H and Anaxi Etolya)						U			
	AHS							U		
Chair occupancy sensor	UNIPR custom device				U					
Sleep monitoring	Samsung A3								U	
Podometer	To be defined						U			

Table 10: List of Mobility Monitoring Sensors to be used by the Deployment Sites

Name	Supplier (brand) + Model	Deployment Sites								
		DS1	DS2	DS3	DS4	DS5	DS6	DS7	DS8	DS9
Bluetooth detectors	MIZAR i-travel					U				
Connected traffic signals	SWARCO					U				
Connected taxi vehicles	To be defined					U				
Pedestrian presence detectors	To be defined					U				

Table 11: List of Home actuators to be used by the Deployment Sites

Name	Supplier (brand) + Model	Deployment Sites								
		DS1	DS2	DS3	DS4	DS5	DS6	DS7	DS8	DS9
Emergency push button	Televes	U				U				
	To be defined							U		
	Samsung – Gear S3 / Gear Fit 2								U	
Lamp/Smart Bulb	To be defined			U						
	Hank						U			
	To be defined							U		
RF Module	Fibaro						U			
Wired switch light	SWIID						U			
Wall switch	Nodon						U			
Smart outlet	Fibaro						U			
	TKB							U		
	Energenie - Mi|Home Monitor adapter								U	
Electrical device switch	Qubino Flush 1 Relay with Energy Meter							U		
Shut off Water Valve								U		
Oven switch	To be defined							U		
Blind control	To be defined							U		
Door Lock	2N EntryCom IP Vario							U		
Speakerphone	To be defined							U		
Telephone (SIP)	Asterisk/ Unify OpenSpace							U		

4.3 Re-used devices between Deployment Sites

This Subsection will be completed in the second year during the consolidation of the different deployment sites. The results will be reported in the second version of this deliverable.

5 Conclusions and Future Work

5.1 Conclusions

During the first reporting period (T0 to T0+12), Task 3.5 team; in collaboration with Task 9.1, have achieved the following outcomes:

On DSes System Architecture

A first overview of the System architecture of the nine ACTIVAGE DSes has been obtained including the following elements:

- The Identification and description of the main components constituting each DS at the different Domains, including Applications, infrastructure components, etc.
- The Topologies of the nine DSes has been provided. The DSes' topologies provide a twofold information: it depicts the main components constituting the DSes and the identification of the possible data flows.
- The DSes architectures have being analysed. They are most of them Cloud computing based but one. However, it should be noted that those are Private Clouds managed by the ACTIVAGE stakeholders.

On security

A first version of the different security and privacy mechanism to be implemented by each DS has been provided.

On DSes Devices

- A first list of the devices (Aggregation Points, Gateways and Smart nodes and Actuators) to be implemented in each DS has been identify and described.
- A first overall view of the different devices to be implemented in ACTIVAGE has been obtained according to the following categorization[10]:
    - Gateways (Total 11):
        - Aggregation Points (5).
        - Gateways (3).
        - Mobile Gateways (3).
    - Smart Sensor and Actuator Nodes, Smart Objects, Wearables (Total 33):
        - Home monitoring sensors (13).
        - Health monitoring sensors (11).
        - Daily activity monitoring sensors (5).
        - Mobility monitoring sensors (4).
        - Home Actuators used to control home appliances(11)
        - In the Gateways case, the number corresponds to different suppliers in the same category.

[10] The number between brackets corresponds to the total number of devices in its category.

- In the case of Smart nodes, the number corresponds to different types of devices in its categories. However, there are some devices that performs the same function but they come from different suppliers, this depends of the DS. This information is not given inside the brackets but indicated in the corresponding Tables in Section.

On Concepts and Definitions

Finally, a list of concepts has been provided to create a common nomenclature inside the project.

On Marketing

A short marketing overview was done on the following market areas Smart home, automation, Smart health devices, Wearables and Personal assistants. The analysis shows good perspectives of market growth.

5.2 Future Work

In the second period (T0 + 13 to T0 + 24), the list of activities to be performed are the following:

On DSes System Architecture

A follow-up of the DSes System Architecture evolution will be done and changes reported.

On Security

The list of security and privacy mechanisms to be implement in each deployment site will be completed in coordination with Task 3.2

On DSes Devices

– Follow up of the devices to be implemented in the nine DSes will be done. This will include to push, the different DSes, to deploy common devices to facilitate the implementation, reduce risk, increase knowledge sharing and cooperation.

– Follow up of news devices able to provide an added value or enhance the functions provided by the different uses cases or devices able to facilitate the implementation of the current functions or new ones. For instance, the use of Personal assistant could be a good candidate for this analysis.

– Update the D3.6 according to the evolution of the DS implementation.

On Concepts and Definitions

Update, if necessary, the list of concepts and definitions, and eventually add other ones.

On Marketing Analysis

The marketing analysis will be reviewed in the second year. It will be completed with the existing solutions for elderly tele-alarm/ tele-assistance solutions with more or less smart connected objects.

References

[1] Gaber, Mohamed Medhat; Stahl, Frederic; Gomes, Joao Bártolo (2014), “Pocket Data Mining - Big Data on Small Devices” (1 ed.). Springer International Publishing.

[2] David Greenfield, Blog on “Fog Computing vs Edge Computing: What’s the difference? https://www.automationworld.com/fog-computing-vs-edge-computing-whats-difference

[3] Welsong Shi, Schahram Dustdar, “The promise of Edge Computing”, Computer Magazine May 2016

[4] Amir Vahid Dastjerdi, Rajkumar Buyya, “Fog Computing Helping the Internet of Things Realize Its Potential”, Computer Magazine August, 2016

[5] Maher Abdelshkour “IoT, from Cloud to Fog Computing”, March 25, 2015 http://blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing

[6] Shanon Harris “CISSP All-in-One Exam guide, Sixth Edition, McGraw-Hill

Appendix A Concepts and Definitions on Communication and Security

This annex describes important concepts related to the main elements constituting the architecture of the Deployment Sites. Annex B is organized in the following three subsections: General Concepts, Protocols for communication and security, and Infrastructure components for communication and security. The information provided here comes from [6].

Note: the concepts and definitions given here below are grouped by type and context in order to provide a better understanding of certain concepts, which can involve several terms.

A.1 General Concepts

Concept	Description
Network Topology	It is the physical arrangement of computers and devices.
Topology	It refers to the manner in which a network is physically connected and shows the layout of resources and systems.
Networking devices	Several types of devices are used in LANs, MANs, and WANs to provide intercommunication among computers and networks. The different networking devices vary according to their functionality, capabilities, intelligence, and network placement. These devices are the following: Repeaters/Hubs, Bridges, Routers and Switches.
LAN	Local Area Network.
MAN	Metropolitan Area Network.
WAN	Wide Area Network.
NIC	Network interface card.
Internet	It is the collection of physical devices and communication protocols used to traverse the web sites and interact with them.
Web	The Web is not Internet. The Web runs on top of Internet, in a sense. The Web is the collection of HTTP servers that hold and process web sites we see.
HTTP	The HTTP is the protocol of the Web. HTTP sits on top of TCP/IP.make sure that the data is routed properly throughout the Internet to get from, for instance, the web server to the user. So the IP protocol find the way to get from A to Z, TCP makes sure the origin and the destination are correct and that no packets are lost along the way, and, upon arrival at the destination, HTTP presents the payload, which is a web page.
Web browser	It enables users to read web pages by enabling them to request and accept web pages via HTTP, and the user's browser coverts the language (HTML, DHTML, and XML) into a format that can be viewed on the monitor. The browser is the user's window to the World Wide Web.
Wireless Communication	It involves transmitting signals via radio waves through air and space, which also alters airwaves. There are different types of wireless networks depending of the communication reach (distance): Satellite, Wireless wide area networks, (2G, 3G, LTE, etc.), Wireless metropolitan area networks (WiMax, 5G, etc.), Wireless local area networks (WiFi: IEEE 802.11 a, b, g, n, ac) Wireless personal are networks (Bluetooth, Z-Wave, UWB, Zigbee, etc.).

Access Point	It is a transceiver used by a WLAN, which connects to an Ethernet cable that is the link wireless devices use to access resources on the wired network. When the access point is connected to the LAN Ethernet by a wired cable, it is the component that connects the wired and the wireless words.

A.2 Protocols

A.2.1 Communication

Concept	Description
OSI Model	It is a reference model constituted of seven protocol layers from (top to down): 7 Application, 6 Presentation, 5 Session, 4 Transport, 3 Network, 2 Data link, 1Physical.
Protocol	A network protocol is a standard set of rules that determines how systems will communicate across networks. Two different systems that use the same protocol can communicate and understand each other by using the same language.
TCP/IP Model	Application (Layers 7, 6 and 5 of OSI model, Host-to Host (Layer 4 of OSI model), Internet (Layer 3 of OSI model) and Network access (Layer 2 and 1 of OSI Layer
TCP/IP	It is the protocol suite of the Internet. TCP protocol controls the handshaking and maintains the connection between, for instance, the user and the server or between two users. IP protocol
Data Link Layer	Is is divided in two functional sublayers: the logical Link Control (LLC) and The Media Access Control (MAC).
Media Access Technologies	The physical topology of a network is the lower layer (Physical), or foundation, of a network. It determines what type of media (cabling, or air) will be used and how the media will be connected between different systems. The media access technologies deal with how these systems communicate overs this media and are usually represented in protocols, NiC drivers and interfaces.
Media Access Control	Data communication protocol sublayer of the data link specified in the OSI model. It provides hardware addressing and channel access control mechanism that make it possible for several nodes to communicate within a multiple-access network that incorporates a shared medium.
Cabling	Network cabling and wiring are important when setting up a network or extending an existing one. Particular types of cables must be used with specific data link layer technologies. Cable types vary in speeds, maximum lengths and connectivity issues with NICs. The type of cables used are coaxial cable, twisted-pair cable, Fiber-Optical Cable.

A.2.2 Security

Concept	Description
HTTP Secure (HTTPS)	It is HTTP running over SSL. HTTP works at the application layer and SSL works at the transport layer.)
Secure Sockets Layer (SSL)	It uses public key encryption and provides data encryption, server authentication, message integrity, and optional client authentication. In the protocol stack, SSL lies beneath the application layer and above the network layer. Since, SSL was developed by Netscape, it is not an open-community protocol.
Transport Layer Security (TLS)	it is the open-community and standardized version of SSL. The difference between SSL 3.0 and TLS are slight, but TLS is more extensible, it is backward compatible with SSL and interoperable with other technologies.

Link encryption	It encrypts the entire packet, including headers and trailers, and has to be decrypted at each hop.
End-to-end encryption	It does not encrypt the headers and trailers, and therefore does not need to be decrypted at each hop.
IPsec:	It is a protocol suite used to protect IP traffic through encryption and authentication. De facto standard VPN protocol. IPsec protocols can work in transparent mode (the data payload is protected) or tunnel mode (the payload and headers are protected). In IPsec, AH (Authentication header) provides integrity and authentication, and ESP (Encapsulating Security payload) provides those plus confidentiality. IPsec uses IKE (Internet key exchange) as its key exchange protocol. IKE is the facto standard and it is a combination of ISAKMP (Internet Security Association and Key Management Protocol) and OAKLEY. ISAKMP is key exchange architecture that is independent of the type of keying mechanism used. Basically, ISAKMP provides the framework of what should be negotiated to set up an IPsec connection (algorithm, protocols, modes, keys). The OAKLEY protocol is the one that carries out the negotiation process.
VPN	A virtual private network is a secure, private connection through an untrusted network. It is a private connection because the encryption and tunneling protocols are used to ensure confidentiality and integrity of the data in transit. It is important to note that VPN technology requires a tunnel to work and it assumes encryption.
VLANs	They enable administrators to separate and group computers logically based on the resources requirements, security, or business needs instead of the standard physical location of the systems. VLANs are an important part of switching networks because they enable administrators to have more control over their environment and they can isolate users and groups into logical and manageable entities. When repeaters, bridges and routers, are used, systems and resources are grouped in a matter dictated by their physical location. A VLAN exist on top of the physical network.
Trusted Platform Module	It is a secure crypto-processor that can be used for platform integrity, disk encryption, password protection, and remote attestation.

A.3 Infrastructure Components

A.3.1 Communication

Concept	Description
Repeater	A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable or wireless segments. Which enables it to extend a network. Repeaters work at the Physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.
Hub	A hub is a multiport repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.
Bridge	A bridge is a LAN device used to connect LAN segments. It work at the Data link layer and therefore works with MAC addresses. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment, the bridge forwards the frame to the necessary network segments. Three types of bridges are sued: local, remote and translation. A local bridge connects to or more LAN segments within a local area, which is usually a building. A remote bridge can

	connect two or more LAN segments over a MAN. By using telecommunications links. A translation bridge is needed if the two LANs being connected are different types and use different standards and protocols.
Router	The router can peel back the first header information and look farther into the frame and find out the IP address and other routing information. The farther a device can look into a frame, the more decisions it can make based on the information within the frame. Routers are layer 3, or network layer, devices that can connect different networks. A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destination. A bridge uses the same network address for all its ports, but a router assigns a different address per port, which enables it to connect different networks together.
Switch	Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multiport connection device that provides connections for individual computers or other hubs and switches. Any device connected to one port can communicate with a device connected to another port with its own virtual private link. When a frame comes to a bridge, the bridge sends the frame to the port to which the destination network is connected. When a frame comes to a switch, the switch sends the frame directly to the destination computer or network, which results in a reduction of traffic. When switches are used, contention and collisions are not issues, which results in more efficient use of the network's bandwidth and decrease latency. Switches reduce or remove the sharing of the medium network and the problem that come with it.
Multilayered switches	These combine data link layer, network layer, and other layer functionalities. Basic switches work at the data link layer and forward traffic based on MAC address. However, today's layer 3, layer 4 and other layer switches have more enhanced functionality than layer 2. These high level switches offer routing functionality, packet inspection, traffic prioritization, and QoS functionality. Switches provide a security service that other devices cannot provide. The technology within switches has introduced the capabilities to use Virtual LANs (VLANs).
Gateway:	It is a general term used for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions. Usually a gateway is needed when an environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. Gateways perform much more complex tasks that connection devices such as routers and bridges. Several types of gateways can be used in a network. For instance, a network access network (NAS) can function as a gateway between the telecommunications and network connections.

A.3.2 Security

Concept	**Description**
Firewalls	They are used to restrict access to one network from another network. Most companies use firewalls to restrict access to their networks from the Internet. They may also use firewalls to restrict one internal network segment from accessing another internal segment. A firewall devices supports and enforces the company's network security policy. The firewall is described as a "choke point" in the network because all communication should flow through it, and it is where traffic is inspected and restricted. A firewall may be a server running a firewall software product or a specialized hardware appliance. It monitors packets coming into and out of the network it is protection. There are many types of firewalls available, because the environment may have unique requirements and security goals. The existing types of firewalls are for instance: Packet filtering, Stateful, Proxy, Dynamic packet filtering and kernel proxy.
Proxy Firewalls	A proxy is a middleman. It intercepts and inspects messages before delivering them to the intended recipients. A proxy firewall stands between a trusted an untrusted network

	and makes the connection, each way, on behalf of the source. What is important is that a proxy firewall breaks the communication channel; there is not direct connection between the two communicating devices. Where a packet-filtering device just monitors traffic as it is traversing a network connection, a proxy ends the communication session and restarts it on behalf of the sending system. Now a proxy technology can actually work a different layers of a network stack. A proxy-based firewall that works at the lower layers of the OSI model is referred to as a circuit-level proxy. A proxy-based firewall that works at the application layer is strangely enough, called an application-level proxy.

Firewall Type	OSI Layer	Characteristics
Packet filtering	Network Layer	Looks at destination and sources addresses, ports and services requested. Routers using ACLs to monitor network traffic
Application-level proxy	Application Layer	Looks deep into packets and makes granular access control decisions. It requires one proxy per protocol.
Circuit-Level Proxy	Session Layer	Looks only at the header packet information. It protects a wider range of protocols and services than an application-level proxy, but does not provide the detailed level of control available to an application-level proxy.
Stateful	Network Layer	Looks at the state and context of packets. Keeps track of each conversation using a state table.
Kernel Proxy	Application Layer	Faster because processing is done in the kernel. One network stack is created for each packet.