Services Enabler Architecture for Smart Grid and Smart Living Services Providers under Industry 4.0

N.C. Batista[a,b], R. Melício[a,b]*, V.M.F. Mendes[b,c]

[a]*IDMEC, Instituto Superior Técnico, Universidade de Lisboa, Lisbon, Portugal*
[b]*Departamento de Física, Escola de Ciências e Tecnologia, Universidade de Évora, Évora, Portugal*
[c]*Department of Electrical Engineering and Automation, Instituto Superior de Engenharia de Lisboa, Lisbon, Portugal*

Received 21 November 2016

Abstract

For an industry 4.0 environment, the management and offering of services, falls over the construction of a stable and reliable sensor and actuator infrastructure. Industry 4.0 is undergoing increase advancement, infrastructure availability and public acceptance, mainly boosted by the Interconnected Things. The public acceptance drives an increase on investments, carrying an insurgence of companies competing with each other to gain market. Although lessening costs, this insurgence has brought heterogeneous infrastructures and solutions availability, challenging services providers. Among the challenges the security and different technology solutions support are of the most importance. The scattering of solutions and software code have to be conveniently gathered to avoid weak-points, eventually, a menace to be explored by hackers. This paper is a contribution in order to embraces those challenges in a new architecture framework able of supporting the creation of solutions for Smart Grid and Smart Living services providers under the industry 4.0 paradigm. The architecture framework design offers security, simplicity of implementation and maintenance, and is resilient to failures or attacks and technologically independent. Field tests are reported in order to evaluate key aspects of the proposed architecture.

Keywords: Industry 4.0; Smart Grid; Smart Living; services architecture; field tests.

1. Introduction

The term industry 4.0 refers to a further developmental stage in the organization and management of the entire value chain process involved in manufacturing industry, sensor and actuator infrastructures. Another term for this process is the fourth industrial revolution [1]. Smart grid is an important component of industry 4.0, such as the cyber-physical systems, the internet of things, the internet services for smart product, the machine-to-machine, the big data and cloud computing, cyber security [1] and mechatronics.

The Industry 4.0 increasing interest is being pushed by the Interconnected Things (IT) increasing public acceptance, leading to augmented interest on investment and development [2-5]. The available cloud services infrastructures supported the insurgence of dedicated IT cloud infrastructures, allowing device representations that facilitate the integration of sensors and actuators connected with each other by software solutions and Artificial Intelligence (AI) bots [6,7].

*Corresponding authors. Tel.: +351 266 745372; fax: +351 266 745394.
E-mail address: ruimelicio@gmail.com (R. Melício).

The general public acceptance, especially from Do It Yourself (DIY) public, had lead the creation of democratized IT cloud services and infrastructures, sometimes as Open Source nature. Many cases of democratized IT offer free reduced features services, leading to an insurgence of entrepreneurs that bring new ideas to the market, offering heterogeneous solutions to the same challenges.

The heterogeneous offers bring a larger variety of solutions to choose from for certain IT challenge, leading to a reduction of implementation costs. Also the user experience for IT services compromise added challenges [8] and the spread of IT implementations specially with IT open development platforms introduce security vulnerabilities, weak-points, that can be hackable [9].

The increase investment and adoption of IT support lead to an increase of IT solutions spread and offers in the market, bring several opportunities to Smart Grid (SG) and Smart Living (SL) services providers. But the heterogeneity contribution of different players of IT due to the entrance of different technology and solutions to solve the same problems and suppress the same needs, bring added challenges [10] and drawbacks [3,4]. This heterogeneity brings an extra effort to support what is seen as the main players to the future IT and to create extra security measures that are able to overcome existing threats and overseen future risks [11].

Taking in consideration of the Industry 4.0 paradigm, a new view of IT is offered in this work and called Industry 4.0 Interconnected Things (I4IT). With the goal of contributing for implementing a flexible, secure, easy to maintain and capable to evolve infrastructure, this paper contribution proposes an IT architecture developed over the Industry 4.0 paradigm called Industry 4.0 Service Enabler Architecture (I4SEA). The architecture targets the development of an infrastructure capable of enabling the creation of Smart Grid and Smart Living added value services under the Industry 4.0 design principles. The architecture aims to be aware of all the main technologies, products, protocols and services available in the market in order to be an enabler of integrated services empowering the interrelationship of the heterogeneous ecosystem of the present and future IT. By being an enabler of heterogeneous technologies integration, the proposed I4SEA help SG and SL services providers to create innovative services supported by an all aware, robust and secured infrastructure. The paper is organized as follows. Section 2 presents the challenges that IT bring to the SG and SL services providers. Section 3 presents the IT services proposed architecture for buildings. Section 4 presents the field tests conducted to evaluate the key aspects of the proposed services architecture. Finally, Section 5 outlines the conclusions.

2. Interconnected Things Challenge

The British technology pioneer Kevin Ashton cofounder of the Auto-ID Center at the Massachusetts Institute of Technology (MIT) is known by introducing the term IoT in 1999 coined to be a global standard system for radio-frequency identification and other sensors. The interconnected things are not a new definition [12], but the development explosion phenomenon has been driven by the recent developments and price reduction of cloud computing services commercial offers, sensors, actuators and smart devices that are able to interconnect to each other over the internet. The reduction of price for those components, allied to the open source nature of many of them and market big players investment, has exerted an expansion of this concept adoption.

Several definitions and designations of interconnected things have been presented by different technological companies, research institutes, independent organizations and governments. Some of those designations are: IoT; Internet of Sensors and Actuators; Internet of Everything; Smarter Planet; Social Web of Things; Smarter Planet; Industrial Internet; Industry 4.0.

The Industry 4.0 defines the fourth industrial revolution, defining the automation and data exchange in manufacturing technologies and services including cyber translated physical systems, machine-to-machine communication and interaction, big data and cloud computing [1]. Currently lead by the constant evolution needs, the Industry 4.0 embraces IoT as a way to offer the cyber physical systems the ability to communicate and cooperate with cloud enabled services and humans in real time.

On this work the Industry 4.0 Interconnected Things (I4IT) will be referring the interrelationship of physical and digital world supported by embedded technology and software services connected over the internet, aiming to simplify, facilitate and enhance business processes and human life (indoor environment quality, including health and thermal comfort), offering at the same time a platform to interconnect all the intervenient.

Although the investment and adoption of I4IT support an increase development, the heterogeneous contribution of different players in the market to the I4IT evolution, creates a drawback. The drawback of the appearance of different technology and solutions to solve the same problem and suppress the same needs. This heterogeneity brings an extra effort to support what is seen in the moment as the main players to the future I4IT and to create extra security measures that are able to overcome existing threats and overseen future risks.

In the core of I4IT is the hardware for the embedded technology that brings the physical to the digital world. The hardware is becoming less expensive and with increased functionality. Also the hardware is becoming more accessible to the masses leading to the insurgence of small entrepreneur companies, which bring new insights of the I4IT solutions to the market. The embedded technologies may have restricted intelligence that help objects to sense, control and interact with the physical world, offered by simple and cheap microcontroller kits. Among the most known microcontroller kits are: Arduino [13]; Raspberry Pi [14]; Intel Edison [15]; Electric Imp [16]; Beaglebone [17]; Netduino [18]; Particle [19]. The embedded devices need to be connected with services that bring the I4IT alive by wire or wireless communication devices. Several I4IT connection protocols exist: ZigBee [20-22]; Wi-Fi [23,24]; Bluetooth [21]; Z-Wave [25]; Wavenis [26]; GPRS [27-29]; WiMax [30]; DASH7 [31]; Insteon [32]; Power-line Communication (PLC) [33,34]; MQTT [35], RFID [36]. The embedded devices although having some internal processing capabilities are not able to offer a full I4IT experience. To simplify, facilitate and enhance business processes and human life with the I4IT experience, the embedded devices must be supported by services, which live in their majority in the Cloud. These services bring the needed of introducing intelligence to the I4IT that bound all the interrelationship of physical and digital world, the embedded technology and software services connected over the internet.

There are already several services that offer an I4IT experience. These services offer limited I4IT experiences, presenting products that automate specific business and life activities. Among the existing services there are: Apple Homekit [37]; Samsung SmartThings [38]; Amazon Echo [39]; WeMo [40]; Wink [41]; ABB Living Space [42]; Vector AMS [43]; EcoFactor [44]. In the heterogeneous explosion of different services, protocols and embedded devices, some overlap or complement each other and some are exclusive to their products ecosystem. This variety of products and solutions raise the issue of the nonexistence of plug-and-play (PnP) integration of the different services with each other. The I4IT brings new market possibilities for Smart Grid (SG) and Smart Living (SL) services providers, but at the same time brings several technology and security issues that need to be considered in order to offer products that are appellant to the clients and market competitive for the present and for the future I4IT.

3. Industry 4.0 Services Proposed Architecture

With the goal of contributing for implementing a flexible, secure, easy to maintain and capable to evolve infrastructure, this paper contribution proposes an IT architecture developed over the Industry 4.0 paradigm called Industry 4.0 Service Enabler Architecture (I4SEA). The architecture targets the development of an infrastructure capable of enabling the creation of Smart Grid and Smart Living added value services under the Industry 4.0 design principles. The I4SEA is aware of all the main technologies, products, protocols and services in order to be an enabler of integrated services empowering the interrelationship of the heterogeneous ecosystem. The I4SEA is illustrated in Fig. 1.

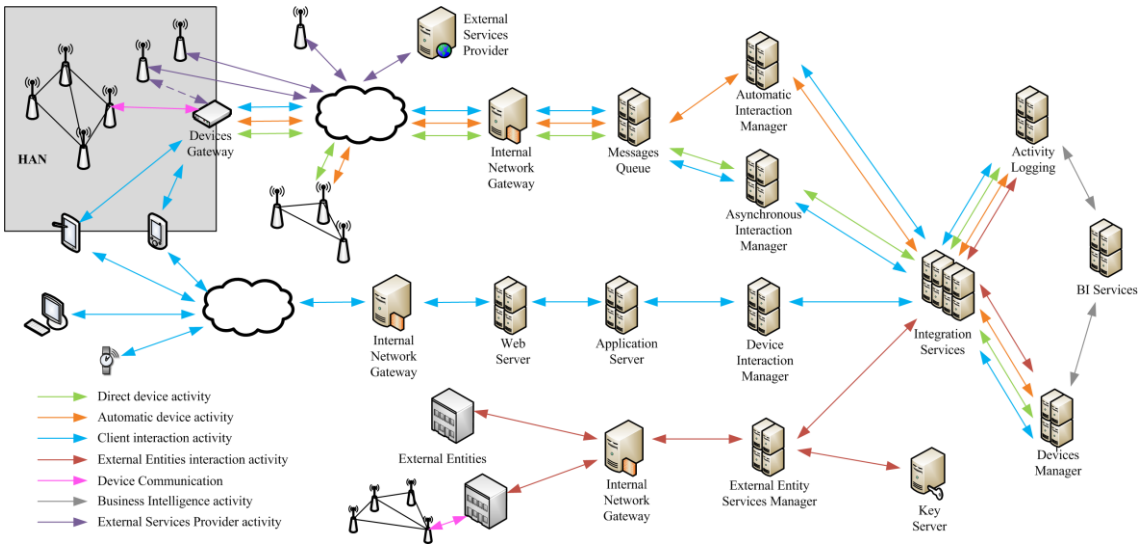

Fig. 1. I4SEA illustration.

The proposed I4SEA through the interaction with the I4IT market main players and trend products aims at helping SG and SL services providers to create innovative services supported by an all aware, robust and secured infrastructure. Several data exchange routes between the different I4SEA modules are presented in Fig. 1, which will be further explained in the following:

- Direct device activity: are routes used form direct interaction between the integration services and the embedded devices;
- Automatic device activity: are routes used for the automatic services used for the creation of autonomous smart activities with the embedded devices;
- Client interaction activity: are routes used for the interaction of the client with the provided services and device gateway;

- External Entities (EE) interaction activity: are routes used for the integration of offered services and other external entities provided services;
- Device communication: is the route for communication between the embedded devices and the I4SEA or external entities architecture;
- Business Intelligence (BI) activity: are routes used by the BI services for data mining;
- External Services Provider (ESP) activity: are routes used for the interaction with ESP services and embedded devices.

The I4SEA architecture built blocks are modules having restrictive services, actions and task over the I4SEA architecture. This modularity and restriction of responsibility to which the I4SEA modules are responsible for offers the advantages of:

- Independence of software solution implementation: the modules can be implemented with different technology and software solutions;
- Increase security of the architecture: the reduction of responsibilities of each module confines the impact of the action of hackers in case of a compromised module, i.e., different technology solutions avoid hacking several modules at the same time;
- Responsibility division: the assignment of well-defined responsibilities to the modules allow a simplified substitution of the module by other ones with different technology and implementation.
- Redundancy existence: the modules can be implemented aside other modules with the same responsibilities to add in redundancy and performance.

These advantages increase the resilience of the architecture failures.

The medium for the data exchange between the different modules are call commands. The commands encapsulate the type of interaction. The main activities can be characterized as: status request, action order, and data transport. A module data exchange command frame is illustrated in Fig. 2.

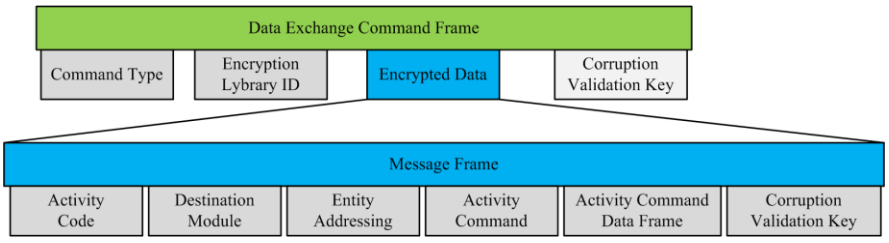

Fig. 2. Module data exchange command frame.

The data exchange command frame comprises a command type, encryption library identification, encrypted data, and a data corruption validation key. The command type defines the activity and nature of the command. The encryption library identification defines the library to be used for the encryption and decryption of the message data. The I4SEA can implement at the same time different encryption systems for each module or within the same module as illustrated in Fig. 3.

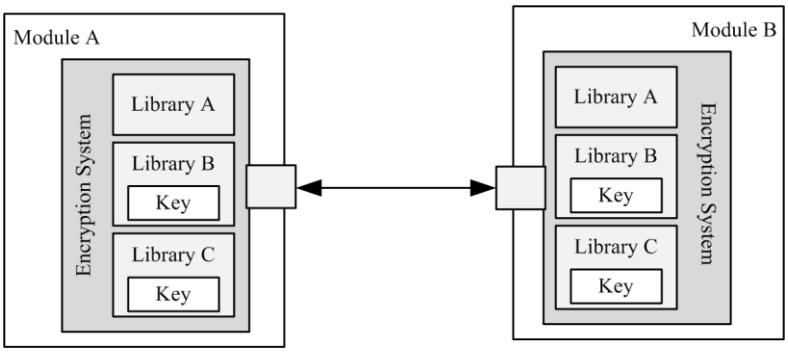

Fig. 3. I4SEA module encryption system example illustration.

The encrypted data contains the message frame to be decrypted. The corruption validation key is used to verify if the message has been modified during transmission. The corruption validation key is computed using the other fields in the frame data. The encrypted message data contains a message frame that is used for the activity itself. The message frame contains an activity code, destination module reference, entity addressing, activity command, activity data frame, and a corruption validation key. The activity code defines the usage for the message that can be a command, depending on the modules interaction activity. The destination module indicates the module to which the message is sent. The entity addressing indicates the involved entities to which and from the message is sent. The activity command along with the activity command data frame present the requested activity and associated data. In the encrypted message data, the corruption validation key functions in the same way as in the data exchange command frame. The double data encryption of the data that is exchange between I4SEA modules along with the data communication technology encryption, offers a safer exchange of client data and activity.

3.1 Integration Services Module

The Integration Services module is responsible for the business logic of the integration of the interrelationship of physical and digital world. This module comprises the services needed to understand

the necessities of a certain I4SEA entity activity and the creation of the corresponding actions. The module receives and sends commands from the Device Interaction Manager module, the Device Manager module, the Automatic Interaction Manager, the Asynchronous Interaction Manager and the External Entity Services Manager. The Integration Services manager can dispatch commands to the Activity Logging module which is responsible for the I4SEA entity activity logging. The Activity Logging module defines the level of activity logging and the level of collected data intercepted in the Integration Services module. The Devices Manager module defines the embedded devices status reporting cycles, which are reported to the embedded devices by the Integration Services module. The embedded devices status data is received by the Integration Services module and delivered to the Device Manager module. The Integration Services module can request information about the devices to the Devices Manager module instead of requesting to the embedded devices, in order to reduce data communication traffic. The client activity is received by the Integration Services module from the Device Interaction Manager. This activity can be saved to the Activity Logging module. A command can be generated in the Integration Services module and sent to an embedded device or a I4SEA module.

3.2 Direct Device Activity Data Exchange Route

The Direct Device activity data exchange route represents the data route associated to the direct interaction with the existing embedded devices managed by the I4SEA. The direct interaction with the embedded devices is managed by the Integration Services module. The direct interaction can be requested by the Device Manager module or by the client and embedded devices through their interaction activity. The Devices Manager module may request the embedded device status update, configuration or software update to the Integration Services module. The client can interact directly with a certain device over a Integration Services module that requests the activity. External Services Providers like Apple Homekit [37], Samsung SmartThings [38] or Amazon Echo [39] can also request direct interaction activity to a certain embedded device over the Integration Services module that requests the activity. An Amazon Echo [39] with a voice command can turn the car air condition or turn lights over the I4SEA by connecting with the Integration Services module. The devices activity can be logged by the Activity Logging module through the Integration Services module. The logged data is previously requested by the Activity Logging module for the Integration Services module that intercepts the requested activity in its

services and delivers the requested activity to the Activity Logging module. The Integrations Services module sends a command message to a certain device by interacting with the Asynchronous Interaction Manager module. The Asynchronous Interaction Manager creates the appropriate command to be sent to the device. In this command the information of the respective device address, device type and appropriate route is elaborated. The device can be accessed directly over a cloud communication service, an External Services Provider or a Devices Gateway module. The command is sent to a Messages Queue module waiting for a transmission opportunity. The command is then sent over an Internal Network Gateway to the appropriate cloud communication service.

3.3 Automatic Device Activity Data Exchange Route

The Automatic Device activity data exchange route represents the data route associated to the automatic interaction with the existing embedded devices managed by the I4SEA. For the SG and SL services providers, the automatic services support the creation future innovative smart services offer. All the embedded devices and client behavior data is collected in the Activity Logging module, allowing the creation of smart interactions between them. Creation, management and control of the automatic smart services happen in the Automatic Interaction Manager. Certain automatic services can be created and maintained by the client over the Device Interaction Manager module. The client manages the information maintained by the Automatic Interaction Manager module and controls the level of the desired services automation. Certain automation services, namely indoor environment quality, including health and thermal comfort can be activated or deactivated by the client at any time, example: activate the automatic garage door open or close depending on a car operation and proximity during winter and deactivate otherwise. The automatic creation of services facilitates the client life and services usability, but the management and control has to be transparent for the client.

3.4 Client Interaction Activity Data Exchange Route

The client can interact directly with an embedded device over a computer, mobile devices, wearables or other embedded devices, but in an asynchronous way. The interacting is over cloud communications services, delivering the interaction to a Web Server module. This module stays behind an Internal

Network Gateways, offering, for instances, data and communication filtering and firewall. The module delivers several communication protocols for web communication to the services that live in the Application Server module, offering several types of communications with the clients, using web services and web sites over the Web Server module. The Application Server module communicates with the Device Interaction Manager module which in turn translates the information or data request in a command that communicates to the Integration Manager module. The Device Interaction Manager module creates the necessary request for the Integration Manager module that in turn distributes the corresponding actions to other modules and in the end receives and delivers their response. Also, the client has limited control over the configuration of automatic smart services, creating automatic activities. The Client Interaction activity data exchange route sends commands to the Automatic Interaction Manager module trough the Integration Services module. If authorized by the client, the activity is logged using devices like wearables, smart watches, doors and others over the Client Interaction activity data exchange route and saved in the Activity Logging module. The logged activity data can be used by the Automatic Interaction Manager module for enhanced creation of SG and SL diverse services.

3.5 External Entities Interaction Activity Data Exchange Route

The External Entities Interaction activity data exchange route represents the data route associated to the interaction between the I4SEA architecture and its intervenient and external SG and SL services providers and their intervenient. The ability of interacting with other SG and SL services enhances the interaction of the client services with external activity monitoring outside the I4SEA. The I4SEA can interact with existing government services that monitor traffic, air quality or weather, advising the client for alternative routes or configuring the home appliances to the new air quality and weather conditions, i.e., indoor environment quality. The external entities can be built with an I4SEA architecture. The External Entities Interaction activity is controlled by the External Entity Services Manager module. This module oversees all the activity between the I4SEA the external entities. All the communication is secured with a validation key controlled by a Key Server module. This key has a structured data frame that validates the external entity and the type of exchanged command from and to the I4SEA. If validation occurs, the External Entity Services Manager translates the command and sends the command to the external entity over the Internal Network Gateway module or to the Integrations Services module.

3.6 Device Communication Activity Data Exchange Route

The Device Communication activity data exchange route represents the data route associated to the interaction with the I4SEA embedded devices. The embedded devices communicate directly with a Devices Gateway module, translating the data messages from and to the embedded devices and the commands for the I4SEA. This module is responsible for the implementation of directly communication technology of the embedded devices or a local mesh of embedded devices managed by the I4SEA. The module communicates with External Services Provider embedded devices by sending commands to the External Services Provider cloud communication services. The module is illustrated in Fig. 4.

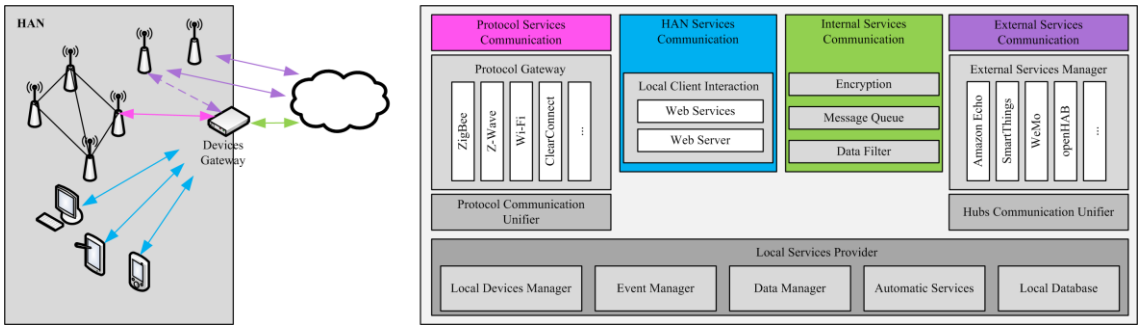

Fig. 4. Devices Gateway module.

In order to reduce communication data exchanged with the I4SEA and to prevent service limitation from communication loss with the I4SEA, the Devices Gateway module has a local implementation of direct and automatic services. The automatic interaction with the embedded devices are controlled and managed by the Integration Services module and the Automatic Interaction Manager module, but the configuration is automatically updated to Local Services Provider internal submodule of the Devices Gateway module. The Devices Gateway offers local web services for the client to interact with the I4SEA services over smart devices or computers. The Devices Gateway module is built over several internal submodules. The Local Services Provider submodule saves and manages a local devices database and its communication data logging along with the available interaction events. The local services provider submodule is also responsible for the automatic interaction between the embedded devices. The Devices Gateway module interacts directly with the embedded devices by interacting with the Protocol Communication Unifier submodule that translates the I4SEA command to a data exchange event that the embedded device understands. The data exchange event is delivered to the Protocol Gateway submodule,

which has several embedded devices communication technology protocols enabling the Devices Gateway module to communicate directly to the embedded device over the Protocol Services Communication submodule. The client can interact directly with the I4SEA provided services by communicating with the HAN Services Communication submodule over smart devices or computers. If a communication problem occurs between the Devices Gateway module and the I4SEA, the client still has access to the same services, by interacting with the Local Services Provider submodule. All of these interactions are transparent to the client, with or without communication with the I4SEA. The Internal Services Communication submodule is responsible for encrypting and decrypting the commands exchanged with the I4SEA. This submodule has an internal Message Queue where the commands await for the opportunity to be sent to the I4SEA. The data filter is controlled and configured by the Activity Logging module and defines the level of the local Devices Gateway module activity logging to be sent to the Activity Logging module. The interaction between the I4SEA and embedded devices from External Services Providers like Apple Homekit, Google Nest, Samsung SmartThings or Amazon Echo are made over cloud communication services provided by the External Services Providers. An internet communication problem with the Devices Gateway module limits the ability to interact with these kinds of embedded devices. If available by the External Services Providers embedded devices a direct communication can be made from the Devices Gateway module to the embedded devices. The Devices Gateway module interact with External Services Providers embedded devices and hubs by interacting with the Hubs Communication Unifier submodule that translates the I4SEA command to a data exchange event that the External Services Providers cloud communication services understand. The data exchange event is delivered to the External Services Communication submodule that is responsible for the appropriate protocol communication selection.

3.7 Business Intelligence Activity Data Exchange Route

The Business Intelligence activity data exchange route represents the data route associated to the data mining of the I4SEA activity. The data miming for the SG and SL services providers is an important area business, providing insights about the business, among other information offers a view on how clients interact, how embedded devices are working, the needs and the most used features of the provided services. The Bi Services module gathers information from the Activity Logging module and the Devices

Manager module. With the examination of the information from the Activity Logging module about the activity of the intervenient in the I4SEA and the information from the Devices Manager module about the status of the devices, new information is generated with an insight of the I4SEA activity and business offer and needs.

3.8 External Services Provider Activity Data Exchange Route

The External Services Provider activity data exchange route represents the data route associated to the interaction of the I4SEA and the embedded devices controlled by External Services Providers like Apple Homekit [37], Samsung SmartThings [38] or Amazon Echo [39]. These market trend smart services solutions offer enhanced smart services kits of embedded devices that are controlled by proprietary hubs. The External Services Provider hubs and embedded devices can be controlled by proprietary software. For external software interaction the External Services Providers offer software Application Program Interface (API) and cloud web services to which the I4SEA can interact with.

The heterogeneous contribution of different External Services Providers offers creates a drawback to the I4IT evolution, with the appearance of different technologies and solutions to solve the same problems and suppress the same needs. This variety of products and solutions raise an issue, the inexistence of plug-n-play integration of the different services with each other. This heterogeneity brings an extra effort to support what is seen in the moment as the main players to the future I4IT and to create extra security measures that can overcome existing threats and overseen future risks. By integrating the External Services Providers solutions the I4SEA offers a framework to seemly integrate the different offers, being controlled and managed by the same platform and software services. The clients no longer need to access different software platforms to manage and interact with different embedded devices from different External Services Providers.

4. I4SEA Implementation Tests

Two projects are developed for testing the feasibility and simplicity of the implementation of activity data exchange routes, modules, Devices Gateway and the interaction with External Services Providers

cloud communication services. The first project tests the difficulty of the I4SEA and the components implementation. The second project tests the I4SEA agility to implement added value services.

4.1 I4SEA Components Implementation Test

The I4SEA components implementation test comprises the implementation of the Direct Device, Automatic Device and Client Interaction activity data exchange routes and the Devices Gateway module. Two types of embedded devices are tested: I4SEA direct controlled embedded devices and External Services Provider embedded devices. The I4SEA direct controlled embedded devices are developed with ZigBee wireless protocol. The ZigBee standard is a low-power wireless networking standard designed for controlling and monitoring applications [45,46].The ZigBee standard is designed to interconnect autonomous sensors and actuators to control units with emphasis on low power consumption. It's a specification based on the IEEE 802.15.4 standard [47,48], extending that definition by developing new extra higher layers. The wireless communications devices, i.e., ZigBee uses small, cheap, ultra-low power digital radios for the creation of low data rate wireless networks with more than 65000 nodes that are secure and with long battery life nodes [22,49,50]. There are three different types of ZigBee devices. The ZigBee coordinator is a full function device (FFD) that coordinates the network and forms its root, making a bridge with other external networks, managing the network security and its security keys, and being also able to store information about the network. The ZigBee router is a FFD that, although having sensors and actuators, has capacity enabling relay messages from other nodes acting as a router. The ZigBee end device is a reduced function device (RFD) that can be connected to sensors and actuators and can be asleep most of the time to extend the battery life, but cannot relay messages. So, the processing capacity is reduced and the production is cheaper. The ZigBee has tree topologies: star, tree and mesh as illustrated in Fig. 5.

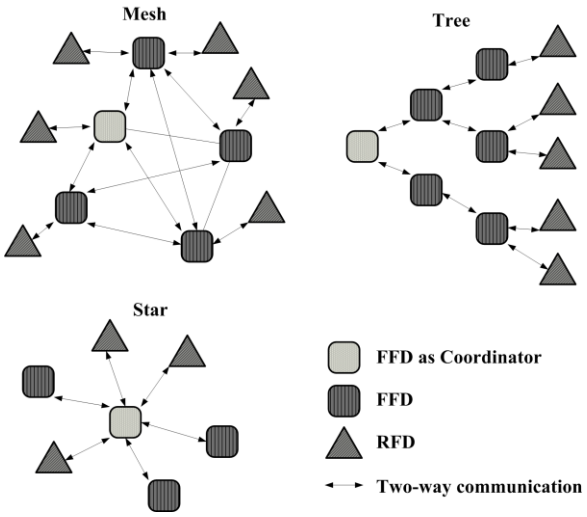

Fig. 5. ZigBee network topologies.

Interference between ZigBee and other wireless communications devices technologies as well as solutions is reported in [51-53] and is stated that interference is smaller than with other technologies [52,54].

Common wireless technologies are compared with the ZigBee [55] standard in Table I.

Table I

Wireless standard comparison [55]

Name	**ZigBee (802.15.4)**	**GSM/GPRS**	**Z-Wave**	**WI-FI (802.11b)**	**Bluetooth (802.15.1)**
Application	Monitoring and Control	Wide Area Voice and Data	Home control	Email, Video, Web	Peripherals connection
System Resources	4KB–32KB	16MB+	2KB-16KB	1MB+	250KB+
Battery Life (Days)	100 to 1000+	1 to 7	300-600	0.5 to 5	1 to 7
Network size (nodes)	+65000	1	232	32	7
Bandwidth (Kb/s)	20-250	64-128+	40-100	11000+	720
Latency (seconds)	< 0.030	-	-	< 0.003	< 10
Transmission Range (meters)	1-100+	1000+	30	1-100	1-10+
Success Metrics	Reliability, low power, low cost	Transmission range, quality	Number of available devices	Speed, flexibility	Convenience, Cost

ZigBee technology is most useful for sensors, control, and other short-message applications and in comparison with the other technology quickly attaches exchange information, detaches and goes to sleep to save battery power. So, this technology is ideal for industrial applications, advantaging from low latency, and a low duty cycle. GSM/GPRS is most useful for voice and data. Z-Wave is most useful for

residential or buildings control (indoor environment quality), providing wirelessly control of: lighting, HVAC, security systems, home cinema, automated window, swimming pool and spa controls, garage and home access controls. WI-FI uses radio waves and is most useful for email video and web, connecting Internet routers to computers, tablets and phones. Also, WI-FI is possible to be used for connection of any two hardware components. Bluetooth is most useful in the transfer of data over short distances: wireless headsets, hands-free calling through cars, and wireless file transfers.

The test for the I4SEA implementation is carried out with ZigBee mesh network topology. In this topology the ZigBee coordinator is responsible for starting a new network, when appropriate, and assigning addresses to newly associated devices. The network may be extended through the use of ZigBee FFD nodes to relay messages from other nodes acting as routers. The I4SEA External Services Provider embedded devices are developed with Electric Imp device [56]. The Electric Imp provides connectivity for the devices through a cloud service and embedded hardware and software. The Electric Imp modules connect hover Wi-Fi to the Imp Cloud services take care of the security, reliability and connectivity. In this test the I4SEA connects over the internet to the same Imp Cloud. The Wi-Fi configuration of the Electric Imp modules is made with a proprietary BlinkUp system with a mobile phone. The Electric Imp module has a physical and a digital existence named device and agent accordingly. The agent lives in the Imp Cloud and functions as an assistant to the physical module, in a one to one relation. The agent is programmable to do some activities in response to commands coming from outside or configurable events. The agent reacts and sends commands to the devices only reachable through the agent. The device is also programmable, so operation even when no internet connection is available to the agent. The programming language for both Electric Imp agent and device is Squirrel. The communication between the I4SEA and the Electric Imp device is illustrated in Fig. 6.

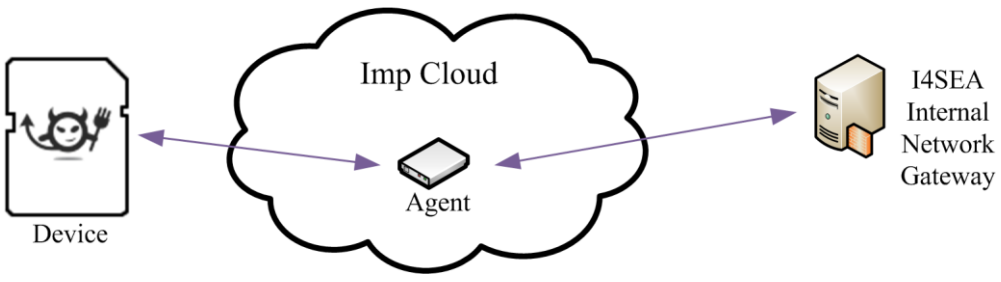

Fig. 6. Communication between the I4SEA and the Electric Imp device.

The Devices Gateway module for the I4SEA implementation test is developed with an Electric Imp device for simplification. The Electric Imp device takes care of the security and of the cloud services for communication with the I4SEA. Since the I4SEA direct controlled embedded devices are developed with ZigBee wireless protocol, a ZigBee-Electric Imp gateway not available in the market is developed specifically for the I4SEA components implementation test in order to communicate with the Device Gateway. The ZigBee-Electric Imp gateway and two ZigBee testing modules developed for the I4SEA implementation test are shown in Fig. 7.

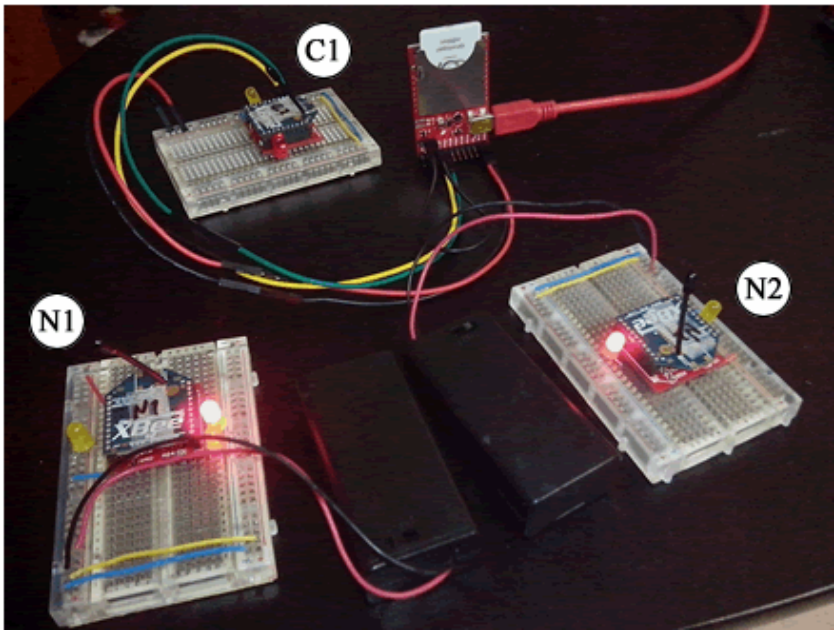

Fig. 7. I4SEA test ZigBee-Electric Imp gateway and two ZigBee modules.

In Fig. 7 the ZigBee module connected to the Electric imp functions as the coordinator of the HAN controlling all the nodes under the controlled wireless network. Also in Fig. 7 the ZigBee modules labeled as N1 and N2 are under the control of the ZigBee gateway labeled C1. The I4SEA connects to the Electric Imp agent over HTTP sending a command. The command is then processed and a message is sent by the agent to the device over the Imp Cloud. In the Electric Imp device, the message is received and the command translated. The command is send to the ZigBee coordinator module by UART. The ZigBee coordinator sends the command to the right ZigBee module in the HAN. The response is received by the ZigBee coordinator and delivered to the I4SEA over the Electric Imp device, its agent and over the

Imp Cloud. The Electric Imp integrated development environment (IDE) showing ZigBee-Electric Imp gateway agent and device code is shown in Fig. 8.

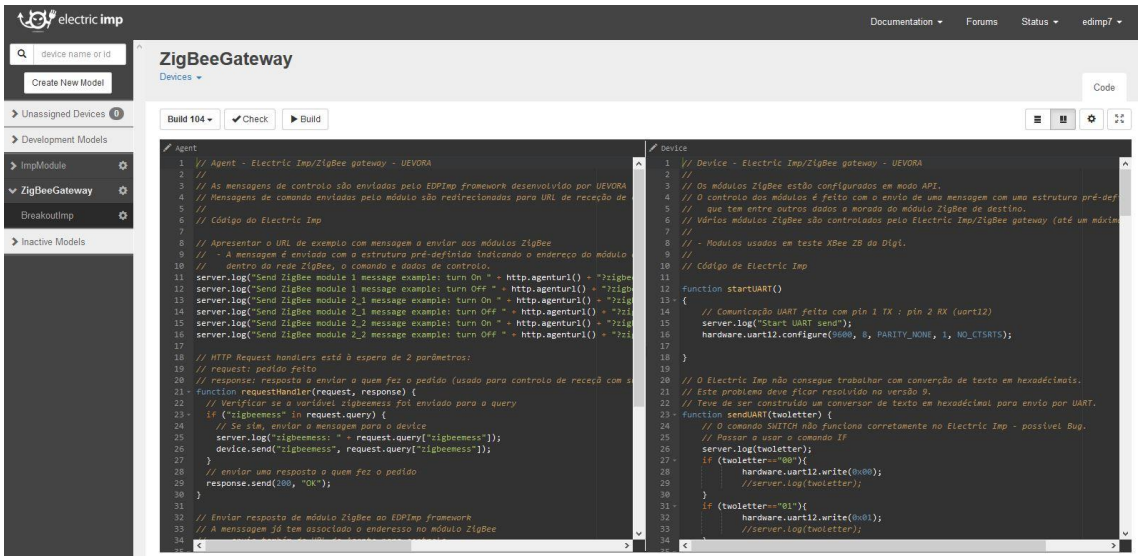

Fig. 8. Electric Imp IDE showing ZigBee-Electric Imp gateway.

The Client Interaction activity data exchange routes comprises the interaction of the client with the embedded devices over asynchronous or automatic interaction. The client interaction with the embedded devices is supported by a web site. The technology used for the web site services is Railo [57] an open source software that implements a server side scripting language ColdFusion Markup Language (CFML). The data management is supported by a MySQL database [58] used by several business critical systems and high volume web sites. Screens of the developed web site are shown in Fig. 9.

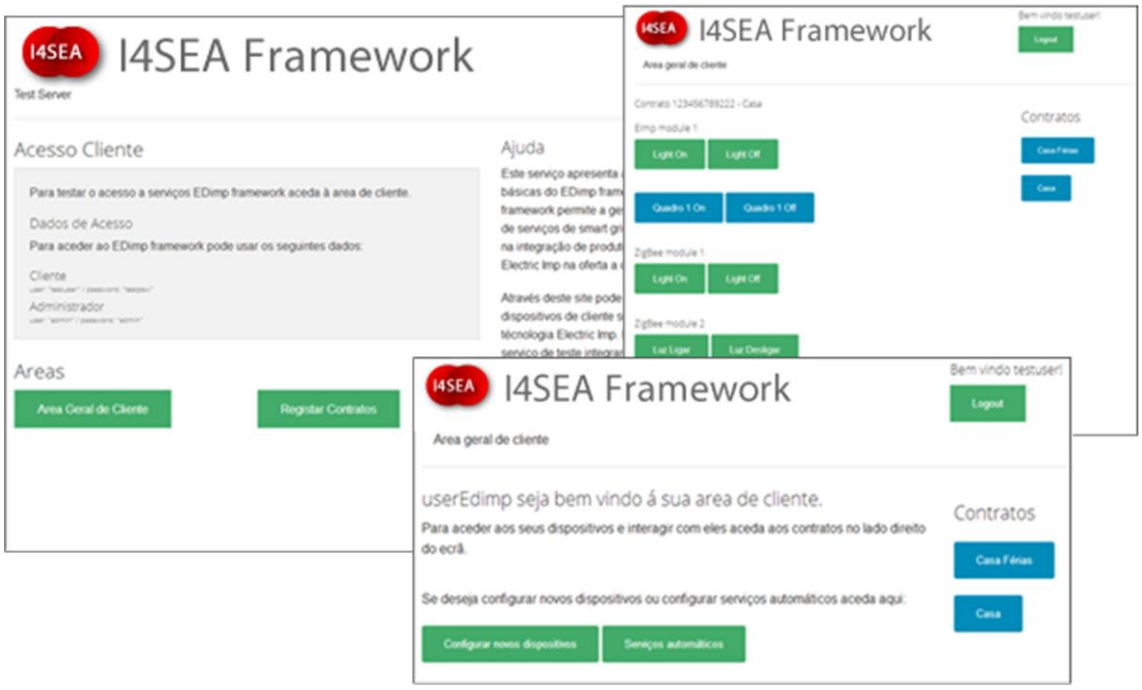

Fig. 9. I4SEA implementation test developed web site.

In order to facilitate and accelerate the implementation of embedded devices offered by external suppliers, the web site implements a library, where the embedded devices specific behaviors are implemented. Part of the web site structure where the embedded devices suppliers implement the products specific behaviors in shown in Fig. 10.

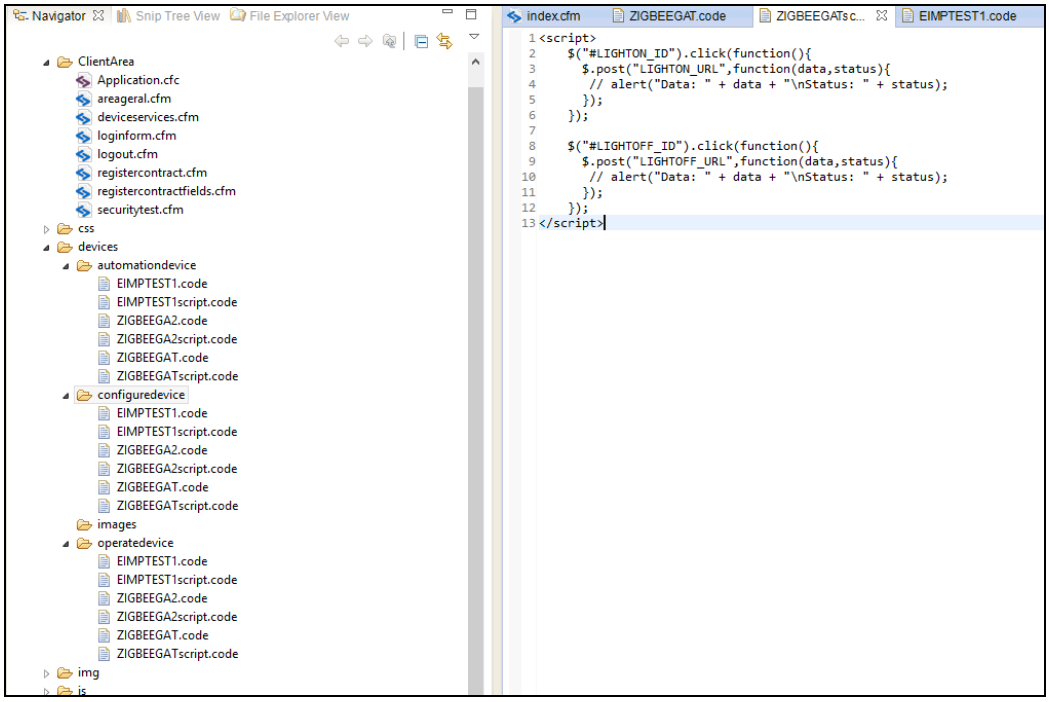

Fig. 10. Part of the I4SEA implementation test developed web site structure.

An implementation of the I4SEA components test 1 comprising the implementation of the Direct Device, Automatic Device and Client Interaction activity data exchange routes and the Devices Gateway module has the estimates costs for:

I4SEA infrastructure modules:

- supported by a Amazon Elastic Computing (EC2) [59], for two Linux virtual servers with 8 processors, 15 GB of RAM and 2 SSD disk with 80 GB each, 2 extra volumes of 100 GB each for storage and 10 GB of in and out of the Amazon Web Services infrastructure data transfer, is 1344.63 €

I4SEA Development service:

- a ready to use I4SEA infrastructure with the components proposed in the test 1 is 60000 €.

I4SEA Device Gateway:

- per box is 150 €.

4.2 I4SEA Added Value Services Implementation Test

The I4SEA agility to implement added value services is assessed by the second test, comprising the ability to offer the client a way to easily create simple or complex automatic services. The modularity, structure, activity routes and exchange data commands of the I4SEA facilitates the creation of new services, with special emphasis on the ability to fast create services that communicate with each other and run on the Integration Services module, Device Interaction Manager module and Automatic Interaction Manager module. The most challenging aspect of the I4SEA added value services implementation test is user interaction design, the usability of the service in the client side. A complex set of different sensors can be aggregated to create an event that will activate an action. The event creation can be created with the sensors in the range of the Device Gateway or reachable to the I4SEA over the cloud or External Entities. The goal is to facilitate the automation services configuration and to make the configuration interaction appealing to the client. An example of a graphical user interface when creating an automatic event is shown in Fig. 11.

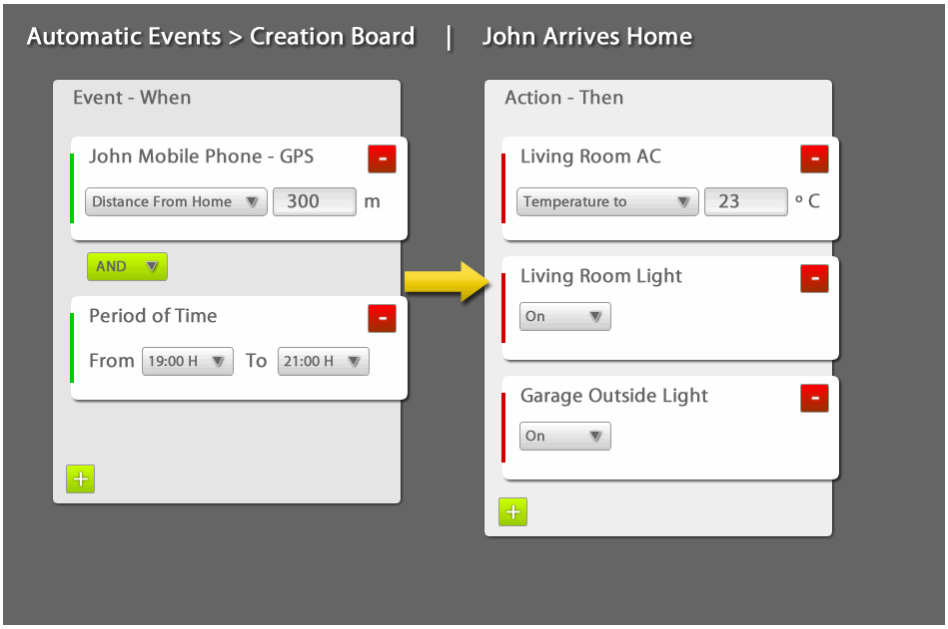

Fig. 11. Example of a graphical user interface when creating an automatic event.

In Fig. 11 the client mobile phone GPS can be monitored by an automatic event to activate an action. The actions can be diversified and complex with theoretical infinite number of actions. In Fig. 11 the action has three steps. During the development of the I4SEA added value services implementation test, a need to physically interact with or directly activate an automatic activity event arose. Under certain circumstances the client may have the need to physically or directly activate a complex action. There are several ways to accomplish the physical or direct interaction: a physical switch in a wall, balcony or remote; a digital switch in a smart device; a voice command to a device like Amazon Echo [39]. The need to physically interact with automatic actions is especially important with elderly technology adverse clients. For these clients the physical interaction, especially with a physical switch, resembles an activity that is already known to their lives, bringing comfort in their interaction with the developed services. Certain client activities and desires are difficult to attain in order to activate the right action, for instances, some client activities and desires are difficult to analyze, as for example, to know if a client wants to see a movie or watch a television show and configure the living room accordingly when arrives to the living room. Artificial Intelligence (AI) service bot is needed for asserting these activities. An AI bot is a software service designed for a specific need and supported by an AI infrastructure. There are several AI solutions in the market in an open source software library fashion like: TensorFlow from google [60]; Computational Network Toolkit CNTK from Microsoft [61]; Torch from Facebook [62]. Also there are AI cloud services solutions available like: Google Cloud Platform Machine Learning [63]; Amazon

Machine Learning [64]. The availability of open source AI software libraries and the availability of those AI services as cloud services enriches the I4SEA modules allowing for specific AI, learning what the client may need at a certain time. This learning consists in gathering information from the module, about the client activity from Activity Logging module and a data mining view from the BI Services module. The AI bots in turn can propose to the client certain action activation by issuing a message or a voice suggest over a service like the Amazon Echo [39]. The AI services are not implemented in the I4SEA added value services implementation test.

5. Conclusions

This paper focused on the study and development of an Interconnected Things (IT) services enabling architecture for Smart Grid and Smart Living services providers based on the Industry 4.0 design patterns for Interconnected Things (I4IT). A proposed architecture solution for enabling Smart Home and Smart Living under a I4IT paradigm is presented and denominated Industry 4.0 Services Enabler Architecture (I4SEA). The architecture is aware of all the market main technologies, products, protocols and services in order to be an enabler of integrated services empowering the interrelationship of the heterogeneous ecosystem of the present and future I4IT by intervenient interconnection.

The I4SEA facilitates these heterogeneous technologies and services integration addressing the concerns of integration and at the same time offering extra security measures that can be an important added to overcome existing threats and overseen future risks. The I4SEA modularity offers the ability to integrate in the same architecture different technology solutions, security measures, high availability measures and fast failure recovery procedures.

To evaluate the proposed architecture, two test are reported to evaluate aspects of the I4SEA. The main goal of the tests is the feasibility and simplicity of the implementation of activity data exchange routes, modules, Devices Gateway and the interaction with External Services Providers cloud communication services.

The first test comprises the implementation of the Direct Device, Automatic Device and Client Interaction activity data exchange routes and the Devices Gateway module. Two types of embedded devices are tested: I4SEA direct controlled embedded devices and External Services Provider embedded devices. The I4SEA direct controlled devices are developed with the ZigBee standard and the I4SEA

External Services Provider embedded devices are developed with Electric Imp device. A ZigBee-Electric Imp gateway not available in the market is specifically developed for the first test.

The second test is intended to test the I4SEA agility to implement added value services comprising the ability to offer the client a way to easily create simple or complex automatic services. The creation of services is supported by the automation of complex services implementation. During the second test development, several needs arose like the physical activation of certain automatic services or the implementation of AI bots to automate the client environment configuration.

With the I4SEA first and second tests, it can be concluded that the proposed I4SEA architecture offers simplicity and easy implementation of added value services under an Industry 4.0 paradigm for Smart Grid and Smart Living Providers.

Acknowledgment

This work is funded by Portuguese Funds through the Foundation for Science and Technology-FCT under the project LAETA 2015-2020, reference UID/EMS/50022/2013.

References

[1] Deloitte AG. Industry 4.0 challenges and solutions for the digital transformation and use of exponential technologies. Switzerland, 2015.

[2] P. Friess. Driving european internet of things research. In: O. Vermesan , P. Friess (Eds.). Internet of things-converging technologies for smart environments and integrated ecosystems. River Publisherss, Aalborg, 1–6, 2013.

[3] O. Vermesan, P. Friess, P. Guillemin, H. Sundmaeker, M. Eisenhauer, K. Moessner, F. Le Gall, P. Cousin. Internet of things strategic research and innovation agenda. In: O. Vermesan , P. Friess (Eds.). Internet of things-converging technologies for smart environments and integrated ecosystems. River Publisherss, Aalborg, 7–152, 2013.

[4] A. Zanella, N. Bui, A. Castellani, L. Vangelista. Internet of things for smart cities. IEEE Internet of Things Journal, vol. 1(1):22–32, February 2014.

[5] H.H.W.J. Bosman, G. Iacca, A. Tejada, H.J. Wörtche, A. Liotta. Spatial anomaly detection in sensor networks using neighborhood information. Information Fusion, vol. 33:41–56, January 2017.

[6] F. Zhao, Z. Sun, H. Jin. Topic-centric and semantic-aware retrieval system for internet of things. Information Fusion, vol. 23:33–42, May 2015.

[7] J. Liu, Z. Yan, L.T. Yang. Fusion – an aide to data mining in internet of things. Information Fusion, vol. 23:1–2, May 2015.

[8] C. Rowland, E. Goodman, M. Charlier, A. Light, A. Lui. Designing connected products: UX for the consumer internet of things. O'Reilly Media, Amsterdam, 2015.

[9] E. Fernandes, J. Jung, A. Prakash. Security analysis of emerging smart home applications. In Proceedings of 37th IEEE Symposium on Security and Privacy, p. 1–19, San Jose, USA, May 2016.

[10] F. da Costa. Rethinking the Internet of Things: A Scalable Approach to Connecting Everything. Apress Media, New York, 2013.

[11] N. Dhanjani. Abusing the internet of things: blackouts, freakouts, and stakeouts. O'Reilly Media, USA, 2015.

[12] C. Perera, C.H. Liu, S. Jayawardena, M. Chen. A survey on internet of things from industrial market perspective. IEEE Access, vol. 2:1660–1679, January 2015.

[13] Arduino. Arduino-home. https://www.arduino.cc/. [Accessed 2016-06-06].

[14] Raspeberry pi. What is a Raspeberry pi. https://www.raspberrypi.org/help/what-is-a-raspberry-pi/. [Accessed 2016-06-06].

[15] Intel edison. Intel edison-one tiny module, endless possibility. http://www.intel.com/content/www/us/en/do-it-yourself/edison.html. [Accessed 2016-06-06].

[16] Electric Imp. Electric imp-about us. https://electricimp.com/aboutus/. [Accessed 2016-06-06].

[17] Beagle Board. BeagleBoard.org-community supported open hardware computers for making. http://beagleboard.org/. [Accessed 2016-06-06].

[18] Netduino. Netduino-hardware. http://www.netduino.com/hardware/. [Accessed 2016-06-06].

[19] Particle. Particle-prototyping tools for the internet of things. https://www.particle.io/prototype/. [Accessed 2016-06-06].

[20] T. Liu, Y. Lui, Y. Mao, Y. Sun, X. Guan, W. Gong, S. Xiao. A dynamic secret-based encryption scheme for smart grid wireless communication. IEEE Transactions on Smart Grid, vol. 5(3):1175–1182, April 2014.

[21] N. Langhammer, R. Kays. Performance evaluation of wireless home automation networks in indoor scenarios. IEEE Transactions on Smart Grid, vol. 3(4):2252–2261, December 2012.

[22] N.C. Batista, R. Melício, J.C.O. Matias, J.P.S. Catalão. Photovoltaic and wind energy systems monitoring and building/home energy management using ZigBee devices within a smart grid. Energy, vol. 49:306–315, January 2013.

[23] A. Usman, S.H. Shami. Evolution of communication technologies for smart grid applications. Renewable and Sustainable Energy Reviews, vol. 19:191–199, March 2013.

[24] F. Gómez-Cuba, R. Asorey-Cacheda, F.J. González-Castaño. Smart grid last-mile communications model and its application to the study of leased broadband. IEEE Transactions on Smart Grid, vol. 4(1):5–12, March 2013.

[25] S. Ahmad. Smart metering and home automation solutions for the next decade. Proceedings of International Conference on Emerging Trends in Network Computer Communications, 200–204, Udaipur, India, April 2011.

[26] C. Gomez, J. Paradells. Wireless home automation networks: a survey of architectures and technologies. IEEE Communications Magazine, vol. 48(6):92–101, June 2010.

[27] F. Wu, N. Han, P. Chen, D. Chen. Monitoring system for fatigue driving based on the internet of things. Proceedings of International Conference on Information Technology and Applications, 43–46, Chengdu, China, November 2013.

[28] P.P. Gaikwad, J.P. Gabhane, S.S. Golait. 3-level secure Kerberos authentication for smart home systems using IoT. Proceedings of 1st International Conference on Next Generation Computing Technologies, 262–268, Dehradun, India, September 2015.

[29] X. Pang, W. Hong, X. Yao, M. Miao. Design and implementation of a smart mini-base station for the internet of things. Proceedings of Asia-Pacific Microwave Conference, 3:1–3, Nanjing, China, December 2015.

[30] Z. Yichi, W. Lingfeng, S. Weiqing, C. Robert, A. Mansoor. Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Transactions on Smart Grid, vol. 2(4):796–808, November 2011.

[31] A. Usman, S.H. Shami. Evolution of communication technologies for smart grid applications. Renewable and Sustainable Energy Reviews, vol. 19:191–199, March 2013.

[32] C. Deng, X. Xiao, Z. Fu, G. Liu, H. Yang, J. Liu. Terrestrial-satellite hybrid backbone communication network for smart power grid. Energy Procedia; vol. 12:27–36, December 2012.

[33] L.T. Berger, A. Schwager, J. Escudero-Garzás. Power line communications for smart grid applications. Journal of Electrical and Computer Engineering, vol. 2013:1–16, 2013.

[34] S. Tsuzuki, Y. Yamada. Feasibility study of ubiquitous sensor networks by inductively coupled PLC over PV power systems. Proceedings of International Symposium on Power Line Communications and its Applications, 274–279, Austin, USA, March, April 2015.

[35] V. Lampkin, W.T. Leong, L. Olivera, S. Rawat, N. Subrahmanyam, R. Xiang. Building smarter planet solutions with MQTT and IBM websphere MQ telemetry. IBM Redbooks, New York, 2012.

[36] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash. Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, vol. 17(4):2347–2376, November 2015.

[37] Apple Homekit. Homekit-apple developer. https://developer.apple.com/homekit/. [Accessed 2016-06-06].

[38] Samsung SmartThings. How it works-smart things. https://www.smartthings.com/how-it-works. [Accessed 2016-06-06].

[39] Amazon Echo. Amazon echo: always ready, connected, and fast. Just ask. http://www.amazon.com/Amazon-SK705DI-Echo/dp/B00X4WHP5E. [Accessed 2016-06-06].

[40] WeMo. Wemo that-home automation made easy. http://www.wemo.com/. [Accessed 2016-06-06].

[41] Wink. Wink-about us. http://www.wink.com/about/. [Accessed 2016-06-06].

[42] ABB Living Space. ABB LivingSpace: Home. http://abb-livingspace.com/. [Accessed 2016-06-06].

[43] Vector AMS. About us - AMS. http://vectorams.co.nz/about-us. [Accessed 2016-06-06].

[44] EcoFactor. EcoFactor-Energy Efficiency, Demand Response, HVAC Performance Monitoring. http://www.ecofactor.com/services/. [Accessed 2016-06-06].

[45] R. Walawalkar, S. Fernands, N. Thakur, K.R. Chevva. Evolution and current status of demand response (DR) in electricity markets: insights from PJM and NYISO. Energy, vol. 35(4):1553–1560, April 2010.

[46] L.-C. Huang, H.-C. Chang, C.-C. Chen, C.-C. Kuo. A ZigBee-based monitoring and protection system for building electrical safety. Energy Build, vol. 43(6):1418–1426, June 2011.

[47] D.-M. Han, J.-H. Lim. Smart home energy management system using IEEE 802.15.4 and ZigBee. IEEE Transactions on Consumer Electronics, vol. 56(3):1403–1410, August 2010.

[48] Bonifácio TG, Pantoni RP, Brandão D. SMAC multi-hop mesh routing protocol using IEEE 802.15.4. Computers & Electrical Engineering, vol. 38(3):492509, May 2012.

[49] N.C. Batista, R. Melício, V.M.F. Mendes. Layered smart grid architecture approach and field tests by ZigBee technology. Energy Conversion and Management, vol. 88:49–59, December 2014.

[50] N.C. Batista, R. Melício, J.C.O Matias, J.P.S. Catalão. ZigBee standard in the creation of wireless networks for advanced metering infrastructures. In: Proceedings of 16th IEEE Mediterranean Electrotechnical Conference, p. 220–223, Medina Yasmine Hammamet, Tunisia, March 2012.

[51] K. Shuaib, M. Alnuaimi, M. Boulmalf, I. Jawhar, F. Sallabi, A. Lakas. Performance evaluation of IEEE 802.15.4: experimental and simulation results. Journal of Communications, vol. 2(4):29–37, June 2007.

[52] Peizhong Yi, Iwayemi A, Chi Zhou. Developing ZigBee deployment guideline under WiFi interference for smart grid applications. IEEE Trans. on Smart Grid, vol. 2(1):110-120, February 2011.

[53] P. Yi, A. Iwayemi, C. Zhou. Frequency agility in a ZigBee network for smart grid application. Proceedings of Innovative Smart Grid Technologies, p. 1–6, Gaithersburg, USA, January 2010.

[54] G. Betta, D. Capriglione, L. Ferrigno, G. Miele. Influence of Wi-Fi computer interfaces on measurement apparatuses. IEEE Transactions on Instrumentation and Measurement, vol. 59(12):3244–3252, November 2010.

[55] N.C. Batista, R. Melício, J.C.O Matias, J.P.S. Catalão. ZigBee wireless area network for home automation and energy management: field trials and installation approaches. In: Proceedings of 3rd IEEE PES Europe Conference on Innovative Smart Grid Technologies, p. 1–5, Berlin, Germany, October 2012.

[56] Electric Imp. Electric Imp-About Us. https://electricimp.com/aboutus/. [Accessed 2016-06-06].

[57] Railo. Railo server-fast and free open source web development with CFML: railo-history. http://www.getrailo.org/index.cfm/about-railo/. [Accessed 2016-06-06].

[58] MySQL. MySQL: Why MySQL?. https://www.mysql.com/why-mysql/. [Accessed 2016-06-06].

[59] Amazon EC2. Elastic computing-amazon. https://aws.amazon.com/ec2/. [Accessed 2016-06-06].

[60] TensorFlow. TensorFlow-an open source software library for machine intelligence. https://www.tensorflow.org/. [Accessed 2016-06-06].

[61] CNTK. CNTK-computational network toolkit. http://www.cntk.ai/. [Accessed 2016-06-06].

[62] Torch. Torch-scientific computing for LuaJIT. http://torch.ch/. [Accessed 2016-06-06].

[63] Cloud Machine Learning Products. Google cloud machine learning at scale-google cloud platform. https://cloud.google.com/products/machine-learning/. [Accessed 2016-06-06].

[64] Amazon Machine Learning. Amazon machine learning-predictive analytics with AWS. https://aws.amazon.com/machine-learning/. [Accessed 2016-06-06].