e-balance

FP7-SMARTCITIES-2013
Project number 609132
http://www.e-balance-project.eu

Co-funded by
the European Union

e-balance

Deliverable D4.5

Restatement of the communication platform specification

Editor:	Krzysztof Piotrowski (IHP)
Dissemination level: (Confidentiality)	PU
Suggested readers:	Consortium/Experts
Version:	1.0
Total number of pages:	15
Keywords:	Smart Grid; Energy balancing; Grid resilience; Communication Platform

Abstract

The deliverable describes the restatement of the communication platform specification due to results and observations collected during the implementation and tests of the platform.

Disclaimer

This document contains material, which is the copyright of certain e-balance consortium parties, and may not be reproduced or copied without permission.

All e-balance consortium parties have agreed to full publication of this document.

The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the e-balance consortium as a whole, nor a certain party of the e-balance consortium warrant that the information contained in this document is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using this information.

The information, documentation and figures available in this deliverable are written by the e-balance partners under EC co-financing (project number: 609132) and does not necessarily reflect the view of the European Commission.

Impressum

[Full project title] Balancing energy production and consumption in energy efficient smart neighbourhoods

[Short project title] e-balance

[Number and title of work-package] WP4 Communication Platform
[Document title] Restatement of the communication platform specification
[Editor: Name, company] Krzysztof Piotrowski, IHP

[Work-package leader: Name, company] Daniel Garrido, UMA

Executive Summary

This deliverable explains the changes to the initial specification of the Communication Platform as defined earlier in the project. These changes may be just suggestions for improvements or may be necessary for the system to work. All they are based on our experience with the system developed and tested during the project lifetime. The lessons learned and observations led us to these changes, from which some have already been implemented in the e-balance project, but others can be added later, after the project end to increase the value of the developed system.

The restatements presented here have a character of a supplement, extending the prior ideas with new concepts, technologies or common approaches. They are just informative on the interoperability, like it is the case for the communication technologies addressed in Section 2 and the Smart Appliance control approach in Section 5. Other present extensions to the e-balance system directly, like it is the case for the security and privacy protocol extension presented in Section 3 and the CMU server as a solution for the network partitioning, described in Section 4. From the latter two, the first one remains an extension to the initial concept, while the very last one was indeed implemented and is applied in the deployed version of the e-balance system.

List of authors

Company	Author
IHP	Krzysztof Piotrowski Peter Langendörfer Ievgen Kabin
INOV	Antonio Grilo Augusto Casaca Mario Nunes
UMA	Jaime Chen Daniel Garrido
UTWE	Marijn Jongerden Boudewijn Haverkort
EFA	Alberto Bernardo
CEMOSA	Juan Jacobo Peralta Escalante
EDP	Francisco Melo
ALLI	Marcel Geers

Table of Contents

List of Figures

Abbreviations

CMU	Customer Management Unit
DoW	Description of Work
DoS	Denial of Service
DSO	Distribution System Operator
FAN	Field Area Network
GMU	Grid Management Unit
GUI	Graphical User Interface
HAN	Home Area Network
HMI	Human Machine Interface
IEC	International Electrotechnical Commission
LAN	Local Area Network
LVGMU	Low Voltage Grid Management Unit
MVGMU	Medium Voltage Grid Management Unit
NAT	Network Address Translation
PLC	Power Line Communications
RF	Radio Frequency
SoC	System on Chip
SRD	Short Range Device
TLGMU	Top Level Grid Management Unit
WSN	Wireless Sensor Network

1 Introduction

According to the e-balance Description of Work (DoW), the deliverable D4.5 describes the restatement of the specification of the Communication Platform. The aim of this document is to show the changes in the running and evaluated system, compared to the prior specification. This additional loop in the design process allows keeping track of the final specification of the deployed system. Further, some of the suggestions have not been implemented, since they were not necessary for the system to work. These suggestions are reflecting the optional changes that can maybe improve the stability or efficiency of the system. These suggestions can be applied in further implementations or deployments of the e-balance system.

The following sections cover the restatements of definitions and specification defined by the individual deliverables in the WP4.

The restatements presented here have a character of a supplement, extending the prior ideas with new concepts, technologies or common approaches. They are just informative on the interoperability, like it is the case for the communication technologies addressed in Section 2 and the Smart Appliance control approach in Section 5. Other present extensions to the e-balance system directly, like it is the case for the security and privacy protocol extension presented in Section 3 and the CMU server as a solution for the network partitioning, described in Section 4. From the latter two, the first one remains an extension to the initial concept, while the very last one was indeed implemented and is applied in the deployed version of the e-balance system.

2 Communication technologies for LV-FAN

The communication architecture and protocols used in the Batalha pilot fully match the ones specified in D4.1 [2]: LV-FAN with DLMS/COSEM service supported by an IPv6 protocol stack on top of RF-Mesh. The selected RF-Mesh technology for the LV-FAN was IEEE 802.15.4 at 868 MHz, with a 6LoWPAN adaptation layer and RPL routing underlying IPv6 protocol within the RF-Mesh network. A gateway performs the interface between the LVGMU and the RF-Mesh network. All these aspects comply with the D4.1 specification.

2.1 Lessons learned / observations

During the course of the e-balance project new communication technologies gained focus and have proven their usefulness for the foreseen application, namely Low Power Wide Area Network (LWPAN) technologies.

2.2 Solution for the issue

While RF-Mesh, namely IEEE 802.15.4g [3], is still considered a good candidate to support smart metering, as well as monitoring and control in Smart Grids, LWPAN technologies have recently changed the Internet of Things (IoT) landscape, since they are able to provide long range and low energy consumption at the same time. Some technologies like LoRaWAN [6] and NB-IoT [7], whose first products are appearing now, are capable of supporting the data rates required by the applications implemented as part of the Batalha demonstrator and are alternative technologies to be considered for future deployments. Integration of these new communication technologies with appropriate wireless security mechanisms may also boost overall security and privacy. Longer range allows single-hop communication, increasing the capacity of the wireless interface in comparison with multi-hop RF-Mesh. However, it all depends on the propagation conditions offered by the deployment environment, which will always require an experimental assessment.

3 Security and privacy protocol improvements

The security and privacy protocol defined for the e-balance system is a powerful tool that allows controlling the access to the data in the e-balance middleware. It was defined in deliverable D4.2 [3] and also in deliverable D5.4 [4]. Using the policies defined by the data owner it allows the data owner to specify the stakeholder and its service that shall have access the owner’s data, together with the kind of allowed access, i.e., only reading, only writing or both.

3.1 Lessons learned / observations

During the implementation and testing of the e-balance system we identified the issue that the individual policies can cause the security and privacy protocol definitions (the set of policies) to become quite large, for more complex settings. The approach defined only one kind of wildcard to increase the scope of the policy, i.e., the “ALL” wildcard, meaning that either all stakeholders or all services are mentioned by the security and privacy policy definition. If the specific data should be accessible only to some of the stakeholders/services then the definition can become complex.

3.2 Solution for the issue

The proposal for an improvement for the definition of security and privacy policies is twofold. On one hand, if the stakeholders’ or services’ names can be defined by a mask using the SQL-like wildcards defined by using the asterisk (“*”) and question mark (“?”) these can be used directly in the definitions. For instance if the data owner wants only the CMU owners to have access to its data, then she can define the stakeholder and service name (which are identical in the case of a CMU) in the policy definition as “CMU*”. In this case only the CMUs can access the specific data item, but other stakeholders not. The definition is very much compact and understandable.

On the other hand, if the first simple solution will not help, because the stakeholders’ and services’ names are completely different, then the stakeholders and services can be grouped and the name of the group is used directly in the definition. Here we can support three approaches: the grouping can cover individually the stakeholder names, the service names, or the groups can collect individual services of specific stakeholders.

This approach will be implemented in the future implementation of the security and privacy module.

4 CMU Server – network partitioning issue

This section presents the issue of the network partitioning due to different reasons, like devices located in different security zones or other network topology related connectivity limitations.

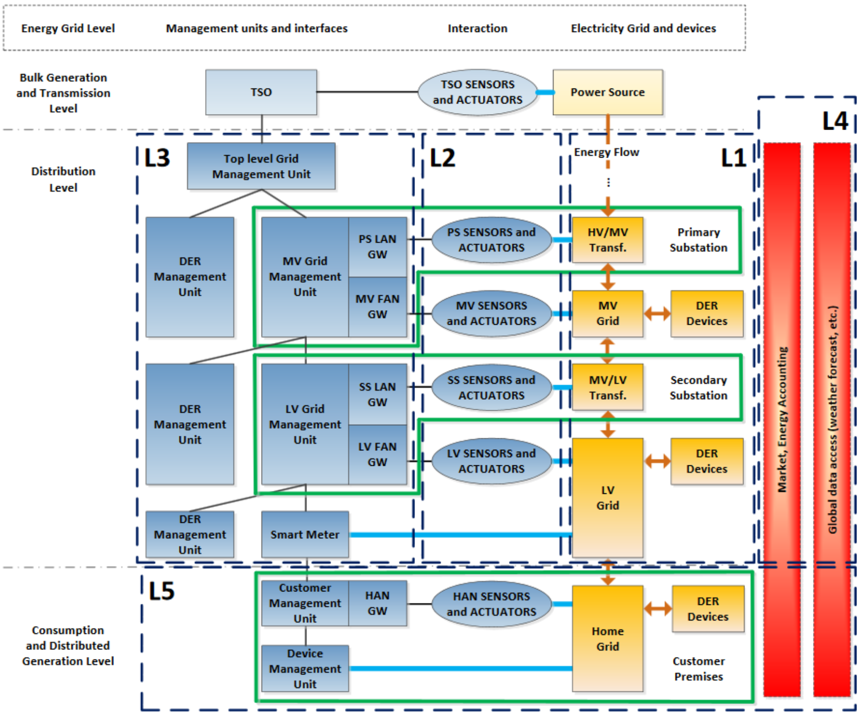

Figure 1: e-balance architecture and the different security zones

The e-balance system is composed of a heterogeneous set of devices (as defined in deliverable D3.2 [1]), which do not necessary have the same security policies. Figure 1 shows the different management units, coloured in blue, involved in the e-balance system and where in the architecture hierarchy they are located. The figure also shows the different security zones (L1 to L5) as proposed by the IEC62351 standard. Different security zones correspond to different security requirements and guidelines that the devices must meet. The e-balance system must follow the e-balance architecture but must also cope with external security requirements imposed by general guidelines or specific deployment requirements.

4.1 Lessons learned / observations

It is mandatory to disallow access to devices deployed in the grid from the Internet as this poses important security problems. The general architecture of e-balance allows direct communication (from a logical point of view) between the CMU and LVGMU. However, if we directly implement this logical architecture, by allowing devices to directly talk to each other we might not be meeting the security guidelines required for a particular deployment.

Furthermore, communication from the LVGMU to the CMU must also be allowed. Unfortunately, nowadays it is a common practice for devices in the households to be connected to the Internet through a router and therefore access from outside to the devices in the local network is not allowed (typically using NAT). This particular scheme was introduced because of security reasons but also to overcome the IPv4 address depletion. In terms of the e-balance project, it means that CMU behind a conventional router cannot be contacted from a LVGMU which is located in a remote location. Finally, direct access to devices gives opportunities to attackers to render devices useless (even without the proper credentials, e.g. DoS attack).

All these problems arose during the design and implementation of the demonstrators and made it clear that a solution is needed in order to follow the logical architecture of e-balance, meet the security requirements and allow the management units in the e-balance system to exchange information.

Working with many different types of devices makes it hard to ensure interoperability. That is why WP4 proposes the use of a generic middleware that is used by all these devices. However, other interoperability issues due to external reasons such as the architecture of the underlying physical communication infrastructure or the company (e.g. DSO) security requirements of each deployment were not taken into account during the earlier specification and design phases.

4.2 Solution for the issue

In order to cope with all these issues a special device called CMU-server has been logically placed between the LVGMU and CMU. The CMU-server is a piece of software that runs on a dedicated machine and acts as a proxy server relaying message from/to the CMU and LVGMU. The CMU-server acts as a passive device which means that it processes requests received, but does not initiate communication with any other device. Direct communication between the CMU and LVGMU is not allowed. Moreover, CMU and LVGMU are not accessible from outside their security zone. This architecture copes with the requirements imposed by IEC 62351 and follows the e-balance architecture as the CMU-server acts in a transparent manner.

The LVGMU and CMU need to periodically poll the CMU-server to know if there are answers or requests for them coming from remote management units. In addition, management units can buffer requests in the CMU-server that will be processed by a remote management unit. The use of the CMU-server means that all communication between the LVGMU and the CMU must necessarily go through this proxy server.

On the one hand, since management units initiate the communication the NAT problem is avoided in the households. Communication is possible from the CMU to the CMU-server, which is located in a remote location outside the local network. On the other hand, LVGMU are able to communicate with the CMU-server without being accessible from outside their security zone.

The CMU-server also validates that the requests it receives are correct and have the corresponding credentials. Therefore, it introduces an additional security measure. Moreover, if attacks to the system are detected, communication between the Internet and the grid can be effectively disallowed by turning off the CMU-server.

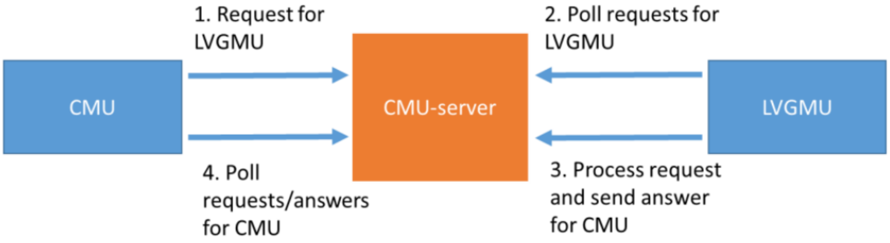
1. Request for LVGMU
2. Poll requests for LVGMU
CMU
CMU-server
LVGMU
4. Poll requests/answers for CMU
3. Process request and send answer for CMU

Figure 2: Communication between a CMU and a LVGMU through the CMU-server

If direct communication is allowed between management units, synchronous communication is trivial to implement and handle since for example web services act this way. However, with the addition of the CMU-server the new architecture copes better with an asynchronous communication scheme. For example if a CMU sends a request to the CMU-server it has no way to know if the request has been received in the remote management unit. It has to poll the CMU-server until it gets the answer from the remote management unit (via the CMU-server as indicated in Figure 2). In this new approach it is better to implement asynchronous communication. When a request is issued a callback is specified. The callback will be automatically called by the communication middleware when the answer of the request is available.

5 Smart device control

This section address the discrepancy between the ideal smart device steering approach that we envisioned at the beginning of the project and the approach the smart appliance manufacturers implement in most of the cases. We assumed that it would be optimal to control the devices directly in the local network; however the common approach on the market is to use a cloud supported control approach. Moreover, this approach has been established by such manufacturers and perceived by the researchers during the course of the project.

5.1 Lessons learned / observations

In the e-balance architecture that the researchers defined in deliverable D3.2, they stated that the communication with and steering of the smart devices in the customer's homes would be directly performed via the home network. The communication would be through the available home WIFI network or via PLC, depending on the capabilities of the devices. Some devices, such as the home appliances by Miele, indeed can be controlled in this manner. However, for many others, including the used Whirlpool appliances and the MasterVolt inverters, all the communication and control goes via an intermediate cloud server provided by the device manufacturer.

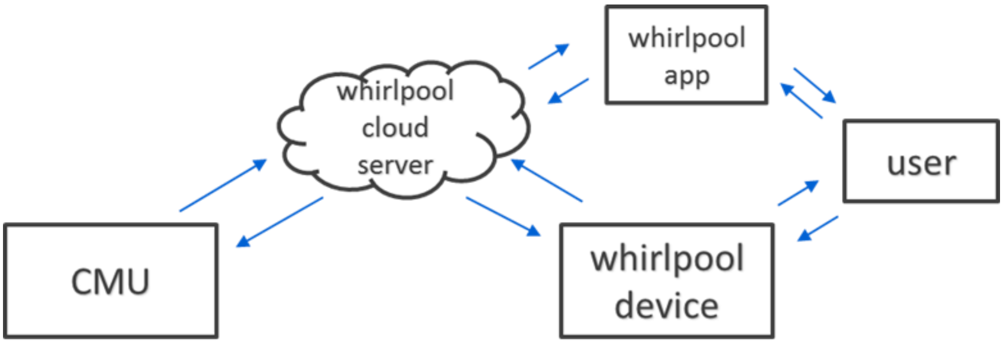

Figure 3: Interaction structure for the Whirlpool devices – the cloud server acts as intermediate between the device and the e-balance CMU.

Figure 3 shows that the e-balance CMU only interacts with the Whirlpool cloud server. All information from the smart appliance itself and from the mobile Application that controls the appliance to the CMU, and the control signals from the CMU to the smart appliance, are sent through the cloud. Although both devices are in the same home network, the communication flows through the cloud server.

5.2 Solution for the issue

The observation is not really an issue, but a fact that the users and owner of the deployed system have to be aware of. It adds a new communication element in the chain, where the status and control data is transported. The indirect communication with the appliance does not have any impact on the balancing algorithms or any other functionality of the e-balance system. But, the cloud server must adhere to the security and privacy regulations of the e-balance system when used in a commercial setting. The privacy of the customers should be guaranteed, and the gathered data should not be used without permission of the customer. Also, the system should be secure against attacks. Since the cloud server can potentially control a large fleet of devices, a change of the steering signals may disrupt the grid and the electricity supply.

6 Summary

This deliverable contains a set of updates to the definitions taken prior in the project. It is intended to be a wrap-up of the work package 4 presenting in short our observations and lessons learned on how the initial definitions and concepts fit with the reality we were confronted with during the implementation and testing of the proposed solutions.

References

[1] e-balance, Deliverable D3.2, “Detailed System Architecture Specification”, 2015.

[2] e-balance, Deliverable D4.1, “Detailed Network Stack Specification and Implementation”, 2015.

[3] e-balance, Deliverable D4.2, “Detailed Security and Privacy Specification and Implementation”, 2015.

[4] e-balance, Deliverable D5.4, “Detailed Specification, Implementation and Evaluation of Security and Privacy Means”, 2015.

[5] IEEE 802.15.4g, “IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks”, IEEE, 2012.

[6] LoRa Alliance, “LoRaWAN Specification”, July 2016.

[7] 3GPP TR 36.802, Narrowband Internet of Things (NB-IoT), Technical Report TR 36.802 V1.0.0, Technical Specification Group Radio Access Networks, June, 2016.