*local **E**lectricity retail **M**arkets for **P**rosumer smart grid p**OWER** services*

Deliverable nº:	**D4.1**
Deliverable name:	**Communications Specifications Plan**
Version:	**1.0**
Release date:	**03/07/2015**
Dissemination level:	**PU**
Status:	Draft
Author:	**Schneider Electric**
Contributors	eSmart, UPC, FEN, MIEMA, NewEn

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under Grant Agreement No 646476.

Document history:

Version	Date of issue	Content and changes	Edited by
0.1	18/05/2015	First draft version	Cristóbal Cordobés
0.2	19/06/2015	Second draft version	Pau Olivella
0.3	24/06/2015	Third draft version	Bjorn Asvard
0.4	25/06/2015	Peer-reviewed version	Roberto Villafáfila
0.5	29/06/2015	Peer-reviewed version	Bjorn Asvard

Peer reviewed by:

Partner	Contributor
CITCEA-UPC	Roberto Villafáfila
eSmart	Bjorn Asvard

Deliverable beneficiaries:

WP / Task	Responsible
WP4	Per Gjerlow
WP3	Roberto Villafáfila
WP7	Per Gjerlow
WP5	Jo Morten

Table of contents

Abbreviations and Acronyms

Acronym	Description
WP	Work Package
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
DNP	Distributed Network Protocol
SESP	Smart Energy Service Provider
FTP	File Transfer Protocol
TCP	Transmission Control Protocol
UMTS	Universal Mobile Telecommunications Service
CP	Communication Platform
DER	Distributed Energy Resources
BPL	Business Process Layer
PL	Physical Layer
SGAM	Smart Grids Architecture Model
WAN	Wide area network
ASDU	Application Service Data Unit
DTE	Data Terminal Equipment
DCE	Data Circuit-terminating Equipment
RTU	Remote Terminal Unit
IED	Intelligent Electronic Devices
GSM	Global System for Mobile

Figures

1 Executive Summary

This deliverable is included inside **WP4 - LSG Communications platform,** in task *T4.1 Communications Specification Plan*.

The deliverable examines the communication requirements of the envisaged EMPOWER platform establishing the baseline for the adoption of the main required protocols and communications media, aimed at being deployed in the project for the pilots developments. Framed by the use of SGAM (Smart Grid Architecture Model), an high level architecture model, the document also presents the communication use cases that will be needed by the BPL (Business Process Layer) to control all relevant DERs (Distributed Energy Resources) and equipment in the PL (Physical Layer). On the other hand, the main characteristics of information exchanges (throughput, latency, security aspects, reliability and availability) are detailed.

The provided specifications of protocols and communications media would be the base for the final adoption of future platform physical implementation and pilots, so that all required technologies for communications for the project will be chosen among the specified options, as depicted in this deliverable D4.1.

This deliverable will be the basis for WP3 and WP5 developments and as well will be the starting point for the work package WP7.

2 Main Objtectives

Empower project is a very ambitious project from the technological point of view, in the meaning that one of the goals is to achieve a Smart Grid network for all the items within a network (field devices, communication platform, a platform for energy management and applications in the business layer to the end user).

One of the main objectives of the project is related with the installation of new network and storage elements. It aims to achieve a flow of information / control from the energy management system to these devices. All this will go through a new communication platform that will include everything related to communications both metering and control devices.

Charging posts for electric vehicles, photovoltaic generation and storage are some of the technologies that will be studied and implemented in the project.

All the before mentioned is the basis to develop a local market in the Smart Grid.

3 Introduction

In this document you can understand the main purpose of the task T4.1, which is no other than to establish basic functionalities for the future communication platform that will be developed and will be the link between field devices and applications located in the business layer.

The main works for this has been trying to find the most standard communication methods to facilitate integration tasks between the different systems.

In the following sections, we will see different points that are involved in communication platform definition:

- State of art (comm.. protocols, comm.. media, architecture, etc)
- Communications Plan
- Uses cases

4 State of art

In this section, technical requirements for deploying a local market are introduced and the communication protocols that are commonly used in power system and can meet the project needs are described.

4.1 Architecture

It is necessary to distinguish different levels of communication when discussing about communication specifications in the communication platform environment. Remembering SGAM architecture, as picture below:

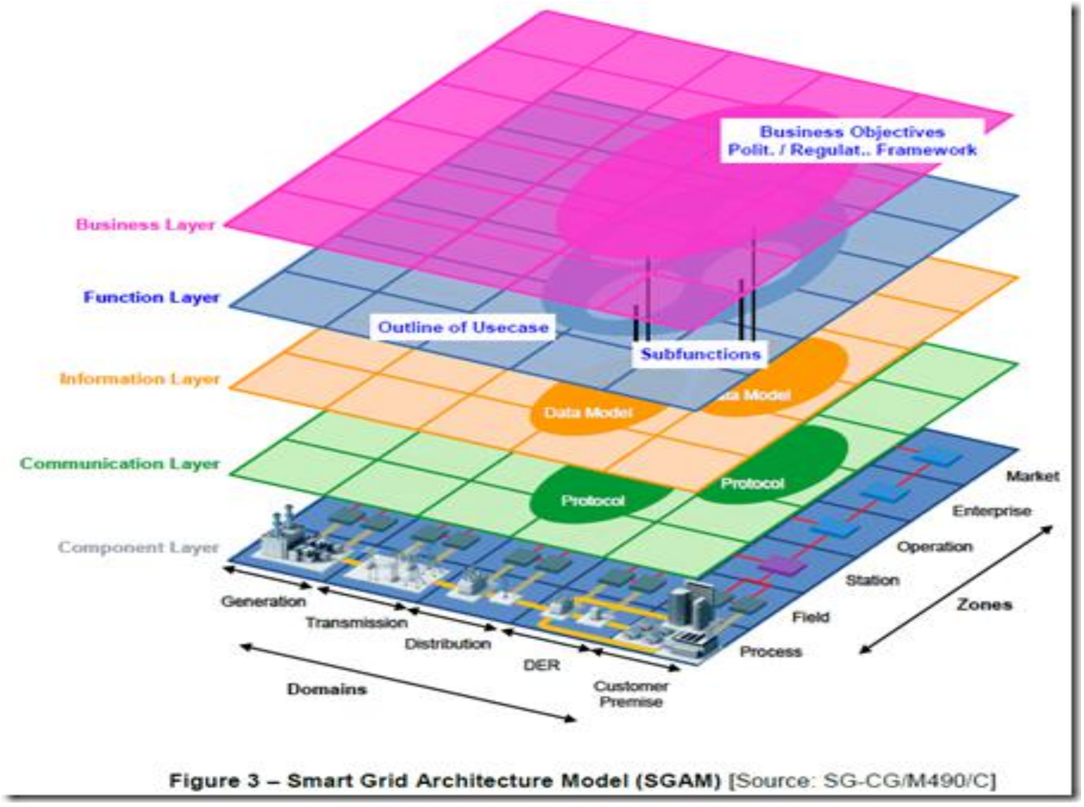

Figure 1: SGAM Architecture

The system architecture (Figure 2) is based on SGAM (Smart Grid Architecture Model), so the system architecture presents different levels.

This Architecture is based on SGAM model for smart grids. SGAM is basically a three dimensional model that allows the representation of the essential elements, participants and interactions in a Smart Grid. It was prepared by the Smart Grid

Coordination Group (SG-CG) Reference Architecture Working Group (SG-CG/RA): CEN, CENELEC and ETSI. Using the own SGAM nomenclature, the three axis used in the Smart Grid model contain the different zones (the hierarchical levels of power system management), domains (which cover the complete electrical energy conversion chain) and interoperability layers. As interoperability layers: Business, Function, Information, Communication and Component layers. As zones: Process, Field, Station, Operation, Enterprise and Market. As domains: Bulk Generation, Transmission, Distribution, DER and Customers Premises. Each interoperability layer, zone and domain has an identifier (numbers for domains, lower case letter for zones and capital letters for interoperability layers) so as to easily locate it in the three-dimensional representation. SGAM is described extensively in WP3 deliverables.

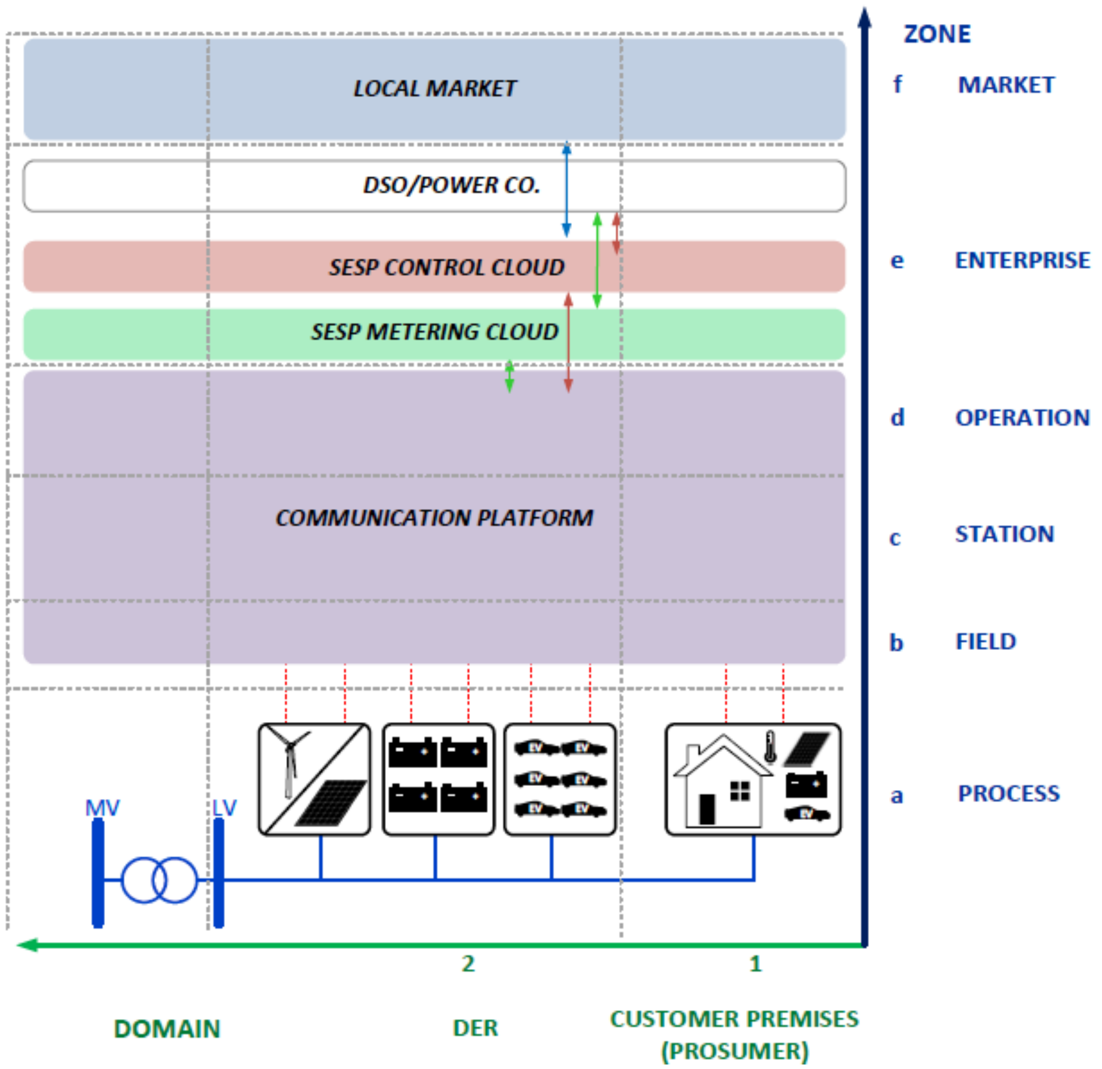

Figure 2: Empower Communication Architecture based on SGAM

The first level of the architecture (Zone a - Process) is the level where field devices are situated. There are different kind of field devices, such as those both from the Distributed Resources and equipment installed in homes, such as smart meters or home local controllers.

The communication platform system is situated on the second level, which corresponds to zones b, c and d (field, station and operations), and this platform is responsible for receiving the information from the different field devices and transmits this information to the SESP system. This information will be treated by different software applications which are developed and installed in the cloud or by new ones (Third Level) (SGAM - e Level: Enterprise).

After this, different protocols and existing communications media that can be applied for these cases will be defined.

4.2 Communication Platform

As mentioned above, there are three different types of technologies for the communication platform. Despite not being part of the project, these DER installation is being considered in one pilot site, so that Empower project leads to future developments.

One of these goals is to install new fast charging posts for electric cars, big and small solar panels and storage for, among other things, avoiding the peaks and valleys of consumption, and also balance substation load.

There will be a need for the communication platform to establish communication between each of the devices and the cloud. To achieve this, some standard communication protocols are listed and defined, in order to be studied in next Empower tasks. Then it will be chosen the most appropriate according to the characteristics of the chosen equipment.

4.2.1 Communications protocols

As we said in the introductory paragraph, we have addressed a set of protocols most commonly used in the market.

Among the existing protocols on the market, those which are standard and maybe more suitable for the project are defined and described. These are the most used and with greater range of devices using the following protocols:

4.2.1.1 IEC 60870-5-101

IEC 60870-5-101 [IEC101] is a standard for power system monitoring, control & associated communications for remote control, remote protection, and associated telecommunications for electric power systems. This is completely compatible with IEC 60870-5-1 to IEC 60870-5-5 standards and uses standard asynchronous serial tele-control channel interface between DTE and DCE. The standard is suitable for multiple configurations like point-to-point, star, etc.

Features

- Supports unbalanced (only master initiated message) & balanced (can be master/slave initiated) modes of data transfer.
- Link address and ASDU (Application Service Data Unit) addresses are provided for classifying the end station and different segments under the same.
- Data is classified into different information objects and each information object is provided with a specific address.
- Possibility of classifying the data into different groups (1-16) to get the data according to the group by issuing specific group interrogation commands from the master & obtaining data under all the groups by issuing a general interrogation.
- Cyclic & Spontaneous data updating schemes are provided.
- Facility for time synchronization

4.2.1.2 IEC 104 protocol

IEC 60870-5-104 (IEC 104) protocol is an extension of IEC 101 protocol with the changes in transport, network, link & physical layer services to suit the complete network access. The standard uses an open TCP/IP interface to network to have connectivity to the LAN (Local Area Network) and routers with different facility (ISDN, X.25, Frame relay etc.) can be used to connect to the WAN (Wide Area Network).

Generally in energy systems, IEC 104 protocol is used for remote control center and the IEC 101 protocol is used for communications with field RTU and field devices.

Features

- The IEC 60870-5-104 protocol defines the use of a TCP / IP network as a means of communication.
    - It is not necessary specific software network in the end systems
    - Routing capabilities are not necessary in the end systems
    - Network management is not necessary in the end systems
    - Facilitates that the end system will be provided remote specialist
    - Facilitates the routers provide telecommunications specialists
    - A change in the type of network requires only a change in the type of router, without affecting end systems

4.2.1.3 Modbus

Modbus is a serial communications protocol, and it is now a common available means of connecting industrial electronic devices.

Modbus is often used to connect a supervisory computer with a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems. Many of the data types are named from its use in driving relays: a single-bit physical output is called a *coil*, and a single-bit physical input is called a *discrete input* or a *contact*.

Features

- The main reasons for the use of Modbus in the industrial environment are:
    - developed with industrial applications in mind
    - openly published and royalty-free
    - easy to deploy and maintain
    - moves raw bits or words without placing many restrictions on vendors
- There are many modems and gateways that support Modbus, as it is a very simple protocol. Some of them were specifically designed for this protocol. Different implementations use wireline, wireless communication (i.e. GPRS). One of the more common designs of wireless networks makes use of Mesh networking.
- Communication and devices

- Allows the receiver to detect transmission errors.
- Modbus commands can instruct an RTU to change the value in one of its registers, control or read an I/O port, etc.
- Typical problems that designers have to overcome include high latency and timing issues.
- Since Modbus is a master/slave protocol, there is no way for a field device to "report by exception" (except over Ethernet TCP/IP, called open-mbus)- the master node must routinely poll each field device, and look for changes in the data. This consumes bandwidth and network time in applications where bandwidth may be expensive, such as over a low-bit-rate radio link.

4.2.1.4 DNP3

DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies. Usage in other industries is not common. It was developed for communications between various types of data acquisition and control equipment. It plays a crucial role in SCADA systems, where it is used by SCADA Master Stations (Control Centers), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs). It is primarily used for communications between a master station and RTUs or IEDs.

There are different possibilities in using this protocol in communications platforms depending on the architecture selected. For example, it can be used to communicate RTU´s from offshore plants to connect another RTU situeated in control center room, acting as a concentrator in order to receive information from all the offshore RTU´s. Communications between RTU´s should be DNP3.

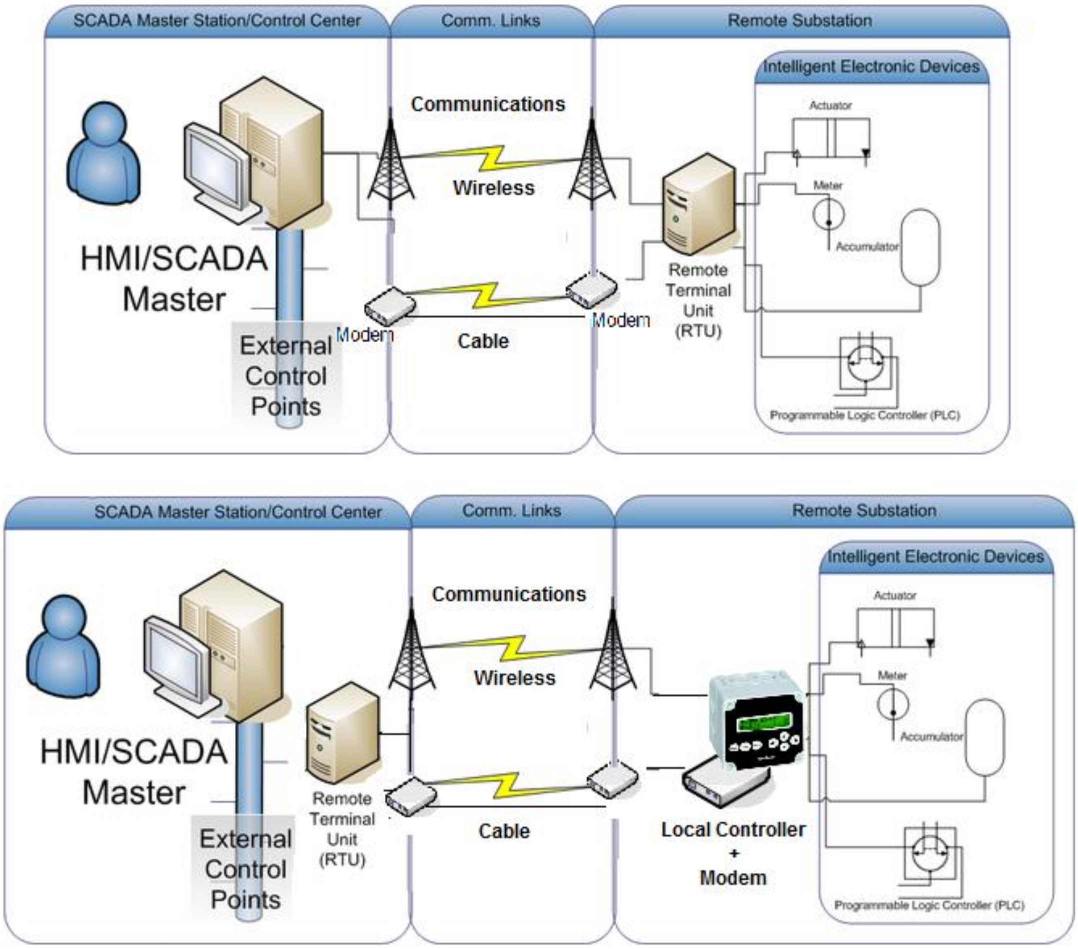

Figure 3: DNP Communications

Features

The DNP3 protocol has significant features that make it more robust, efficient, and interoperable than older protocols such as Modbus, at the cost of higher complexity.

In terms of the OSI model for networks, DNP3 specifies a layer 2 protocol. It provides multiplexing, data fragmentation, error checking, link control, prioritization, and layer 2 addressing services for user data. It also defines a Transport function (somewhat similar to the function of layer 4) and an Application Layer (layer 7) that defines functions and generic data types suitable for common SCADA applications. The DNP3 frame strongly resembles, but is not identical to the IEC 60870-5 FT3 frame. It makes heavy use of cyclic redundancy check codes to detect errors.

The improved bandwidth efficiency is accomplished through event oriented data reporting. The Remote Terminal Unit monitors data points and generates events when it determines that the data should be reported (for example, when it changes value). These events are each placed in one of three buffers, associated with "Classes" 1, 2 and 3. In addition to these, Class 0 is defined as the "static" or current status of the monitored data.

The DNP3 protocol supports time synchronization with an RTU. The DNP Protocol has time stamped variants of all point data objects so that even with infrequent RTU polling, it is still possible to receive enough data to reconstruct a sequence of events of what happened in between the polls.

A Remote Terminal Unit for the DNP3 protocol can be a very small, simple embedded device, or it can be a very large, complex rack filled with equipment. The DNP User Group has established four levels of subsets of the protocol for RTU compliance. The DNP Users Group has published test procedures for Levels 1 and 2, the simplest implementations.

While this protocol is robust, efficient, and compatible; it is getting more and more complex and subtle as it ages. While this is partly due to more demanding industrial applications, it is also a reflection that SCADA concepts are not as simple as they might first seem. The goal of compatibility seems more and more elusive as issues emerge from field experience.

4.2.2 Wireless communications media

4.2.2.1 Wi-Fi (WAN communications)

The great success of WLANs is using frequencies of free use, in example, don´t need to ask permission to use them. However, it is necessary to keep in mind that regulation on managing the spectrum varies from country to country.

Advantages

- Adds flexibility to network structures by reducing connections between cables.
- Uses electromagnetic waves to transmit and receive data over radio waves medium.
- They combine data connectivity with user mobility contribute.

- Various types of interoperability as technology and implementation of the designer.
- Objective standards (802.11a / b): full interoperability between products that fulfill the specification

Disadvantages

- Higher loss-rates due to interference
  - emissions of, e.g., engines, lightning
- Restrictive regulations of frequencies
  - frequencies have to be coordinated, useful frequencies are almost all occupied
- Low data transmission rates
  - local some Mbit/s, regional currently, e.g., 53 kbit/s with GSM/ GPRS
- Higher delays, higher jitter
  - connection setup time with GSM in the second range, several hundred milliseconds for other wireless systems
- Lower security, simpler active attacking
  - radio interface accessible for everyone, base station can be simulated, thus attracting calls from mobile phones
- Always shared
  - medium secure access mechanisms important

4.2.2.2 GPRS/UMTS/GSM communications

Wireless WANs consist of towers and antennas that transmit radio waves or microwave technology used to connect LANs using point-point and point-multipoint links.

GSM, GPRS and UMTS are wireless transmission technologies and are characterized by speed information supported, type of payment and connection establishment time.

1. ***GSM***

GSM is a cellular network, which means that cell phones connect to it by searching for cells in the immediate vicinity. There are five different cell sizes in a GSM network—macro, micro, pico, femto, and umbrella cells. The coverage area of each cell varies according to the implementation environment. Macro cells can be regarded as cells where the base station antenna is installed on a mast or a building above average rooftop level. Micro cells are cells whose antenna height is under average rooftop level; they are typically used in urban areas. Picocells are small cells whose coverage diameter is a few dozen metres; they are mainly used indoors. Femtocells are cells designed for use in residential or small business environments and connect to the service provider's network via a broadband internet connection. Umbrella cells are used to cover shadowed regions of smaller cells and fill in gaps in coverage between those cells.

GSM is a public, non-proprietary standard. This makes it very powerful GSM internationally communicating over 170 countries and covering not very accessible land areas.

2. GPRS

The actual transmitting data trend at higher speeds led to the emergence of a development within GSM, General Packet Radio Service (GPRS).

GPRS extends the GSM Packet circuit switched data capabilities and makes the following services possible:

- SMS messaging and broadcasting
- "Always on" internet access
- Multimedia messaging service (MMS)
- Push to talk over cellular (PoC)
- Instant messaging and presence—wireless village
- Internet applications for smart devices through wireless application protocol (WAP)
- Point-to-point (P2P) service: inter-networking with the Internet (IP)
- Point-to-Multipoint (P2M) service: point-to-multipoint multicast and point-to-multipoint group calls

If SMS over GPRS is used, an SMS transmission speed of about 30 SMS messages per minute may be achieved. This is much faster than using the ordinary SMS over GSM, whose SMS transmission speed is about 6 to 10 SMS messages per minute.

Protocols supported

GPRS supports the following protocols:

- Internet protocol (IP). In practice, built-in mobile browsers use IPv4 since IPv6 was not yet popular.
- Point-to-point protocol (PPP). In this mode PPP is often not supported by the mobile phone operator but if the mobile is used as a modem to the connected computer, PPP is used to tunnel IP to the phone. This allows an IP address to be assigned dynamically (IPCP not DHCP) to the mobile equipment.
- X.25 connections. This is typically used for applications like wireless payment terminals, although it has been removed from the standard. X.25 can still be supported over PPP, or even over IP, but doing this requires either a network-based router to perform encapsulation or intelligence built into the end-device/terminal; e.g., user equipment (UE).

When TCP/IP is used, each phone can have one or more IP addresses allocated. GPRS will store and forward the IP packets to the phone even during handover. The TCP handles any packet loss (e.g. due to a radio noise induced pause).

3. UMTS

UMTS (Universal Mobile Telecommunications Service) seeks to build on and extend existing mobile, wireless and satellite technologies providing higher capacity data transmission possibilities, and a much wider range of services using an innovative radio program and a core network access improved.

UMTS services support low and high speed, has any connection with public networks for voice and data transmission and allows access by multiple different terminals. Wireless technology provides the ability to bring telecommunications services to people living outside major urban areas and have no fixed telephony. This would even run a business from a small town and still keep in touch with customers and suppliers. Powered via satellite to the most remote points of a country can have access to advanced services.

4.2.2.3 Zigbee

Zigbee is a wireless communications standard, regulated by IEEE 802.15.4 working group in 2004, which allows wireless networking capabilities enable control and monitoring that are safe, low power consumption and low cost processor, bidirectionally.

Network topologies

ZigBee supports three network topologies:

- Star topology: The coordinator is in the center.
- Topology in tree: the coordinator will be the root of the tree.
- Mesh topology: at least one of the nodes will have more than two connections.

The most interesting topology (and one of the reasons why it seems that ZigBee can prevail) is the mesh topology. This allows that if, at a given moment, a node fails and falls way, can continue communication between all other nodes because all the paths are redone. The management of paths depends on the coordinator.

4.2.2.4 Radio communications

Radio networks offer a far-reaching and cost-effective way of connecting physically disparate equipment, with the added ability to reach mobile devices.

Using radio to achieve the robust connectivity demanded by the energy industry has, on occasion, proved an insurmountable challenge.

A self-forming mesh can balance loading between connections, and reroute traffic in the event of node failure, creating a network as robust as any cable and capable of reaching the farthest point of the most-remote operating site.

4.2.3 Wired communications media

4.2.3.1 Twisted pair cable copper (RS485)

A twisted copper pair using the RS485 standard is the communication standard media. The necessary equipment and the cable itself are robust and their price is not high. Furthermore, the installation would be simpler, being able to provide even wide wires within submarine power cables. RS485 specification indicates a maximum distance of 1,200 meters to 4 Mb/s. The disadvantages of using copper connections are that there is no inherent isolation between devices and drivers used for communications and they would be susceptible to be affected by transient voltage levels.

4.2.3.2 Fiber optics

Fiber optic cables provide a high bandwidth communications for longer distances. Also they have the advantage of electrical isolation and immunity to electrical noise. There are two types of fiber optic cables available: single-mode optical fiber and multi-mode.

The optical fiber is single-mode slightly presents economic and lower losses, but instead requires the use of laser-based devices communications. By contrast, the optical fiber multi-mode is somewhat less economical but may be used with communications devices based on LEDs, which are more affordable than based lasers. As with the case of copper twisted pair, fiber optic cables could be provided within the submarine power cables.

Bandwidth and distance that can be achieved with laser devices based communications and fiber optic cables using single-mode are greater than those achieved with communications devices based LED cables and multi-mode fiber. The bandwidth that can be obtained depend on the type of communication device used, being those with a higher price those which can obtain a higher bandwidth. For single-mode cables fiber, the bandwidth would be up to 2 Gb/s over distances up to 100 km. With fiber optic cable multi-mode, you can achieve bandwidths of up to 100 Mb / s for distances up to 6 km.

The disadvantages of fiber optic cables are having less robustness compared to copper and specialized tools required to perform the connection, which was not necessary with twisted pair cables.

4.2.3.3 Smart metering communications

SESP Control Cloud will support communication towards the smart meters for collecting meter values, events/alarms – both in a periodic and on-demand manner.

Dependent on the support for integration methods within the meter-collecting system, the meter values can be transferred to SESP by either push, or where the SESP initiate the collection within SESP Control Cloud workflows that runs periodically.

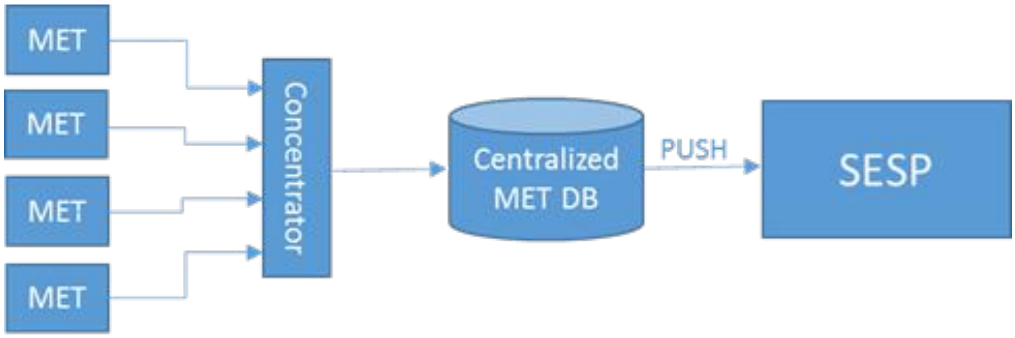

Figure 4: An example of push of meter values to SESP

4.3 Exchange between the Communication Platform and the SESP System

Communications between Communication Platform and SESP system will be based on pure software communications.

It has to be discussed and chosen the best and optimal possibility in order to transmit and receive data from different systems.

There are two communications methods which are more used in systems connections and the way data are exchanged between them (apart from the method, it needs to be defined types of messages, etc.)

These types of communications are:

- Web Services
- FTP transmission

4.3.1 Web Service

A **Web service** is a method of communication between two electronic devices over a network. It is a software function provided at a network address over the Web with the service *always on*..

Different software applications developed in different programming languages, and executed on any platform, can use web services to exchange data on computer networks like the Internet. Interoperability is achieved by adopting open standards. OASIS and the W3C organizations are the committees responsible for the architecture and regulation of Web services. To improve interoperability between different implementations of Web services has created the WS-I organization responsible for developing profiles to define more fully these standards. It is a machine that responds to requests from Web clients and sends the requested resources.

These are some different web services that use markup languages:

- JSON-RPC
- JSON-WSP
- Web template
- Web Services Description Language (WSDL) from the W3C
- Web Services Conversation Language (WSCL)
- WS-Metadata Exchange
- XML-RPC - XML - Remote Procedure Call

4.3.2 FTP file transfer

FTP (File Transfer Protocol) in computing, is a network protocol for transferring files between systems connected to a TCP (Transmission Control Protocol) network, based on the client-architecture server. From a client computer you can connect to a server to download files from it or to send files, regardless of operating system used on each computer.

The FTP service is offered by the application layer model layer TCP / IP network to the user, usually using the network port 20 and 21. A basic problem is that FTP is designed to offer maximum connection speed but not maximum security, since all the information exchange, from the login and password of the user on the server to transfer any file, is done in plain text without any encryption, so that a potential attacker can capture this traffic, access the server and / or ownership of the transferred files.

To solve this problem, there are useful applications like SCP and SFTP, SSH included in the package, but can transport files by encrypting all traffic

4.4 The SESP Platform

The SESP Control Cloud will be based entirely on Microsoft Azure cloud services, where Azure Machine Learning (ML) will act as the brain of the modern smart grid.

SESP Control Cloud collects data from virtually any type of meter or sensor. It then runs predictive models in Azure ML to forecast potential capacity problems and automatically control load to buildings or other infrastructure to prevent outages. The solution provides a short-term 24-hour forecast, a long-term monthly forecast, and a temperature forecast, and it offers a centralized way to monitor and manage the entire grid.

Key features for SESP Control Cloud:

- Real time dashboards
- Automated & customizable processes & workflows
- ESRI-based GIS-platform with real time data visualization
- 2-way communication with meter infrastructure
- Event & alarm handling
- Customer alerts
- Real-time customer compensation visualization
- Outage handling per individual customer
- Remote opening and closing of meters
- Tap into data sources which have been off limits
- Information model built on CIM standards
- Built on eSmart's big data analytics system platform

SESP Control Cloud must supports integration towards multiple systems and data sources, such as Smart meters (values, events, etc.), Customer Information System (CIS), Network Information System (NIS), Weather data and Social Media. Standard message formats, such as XML, CIM and GS2 are supported, and the most used integration methods are:

- Microsoft Azure Event Hub (HTTPS)
- Microsoft Azure Service Bus Queue (HTTPS)
- Web Services (SOAP, RESTful)

The SESP Control Cloud client should be a click-once application which always ensure that the users are using the latest application version. The client runs on

Windows Client operating systems, and it requires an internet connection to operate.

By only utilizing cloud-based services, there will be no need for any physical or virtual servers for operating the system. Another major advantage is the scalability in the solution, as Windows Azure gives the ability to use and pay for only what you actually need, while being able to increase and decrease the resources you use on demand without being forced to invest in spare or standby capacity.

Microsoft has decades-long experience building enterprise software and running some of the largest online services in the world. It has leveraged this to implement and continuously improve security-aware software development, operational management, and threat mitigation practices that are essential to the strong protection of data in the cloud.

Security is built into Azure from the ground up, starting with the Secure Development Lifecycle, a mandatory development process that embeds security requirements into every phase of the development process.

Technological safeguards, such as encrypted communications and operation processes, help to keep customer data secure.

For data in transit, Azure uses industry-standard transport protocols between user devices and Microsoft data centres, and within data centres themselves.

In addition, Microsoft conducts regular penetration testing to improve Azure security controls and processes.

5 Communications Specification plan

To determine the characteristics of the communications platform we must go into details of the equipment and systems that will be part of the entire system in order to perform an analysis as complete as possible.

5.1 Defining the system architecture

It is determined that the complete architecture of the entire system is going to follow SGAM model format as it is shown in the picture below.

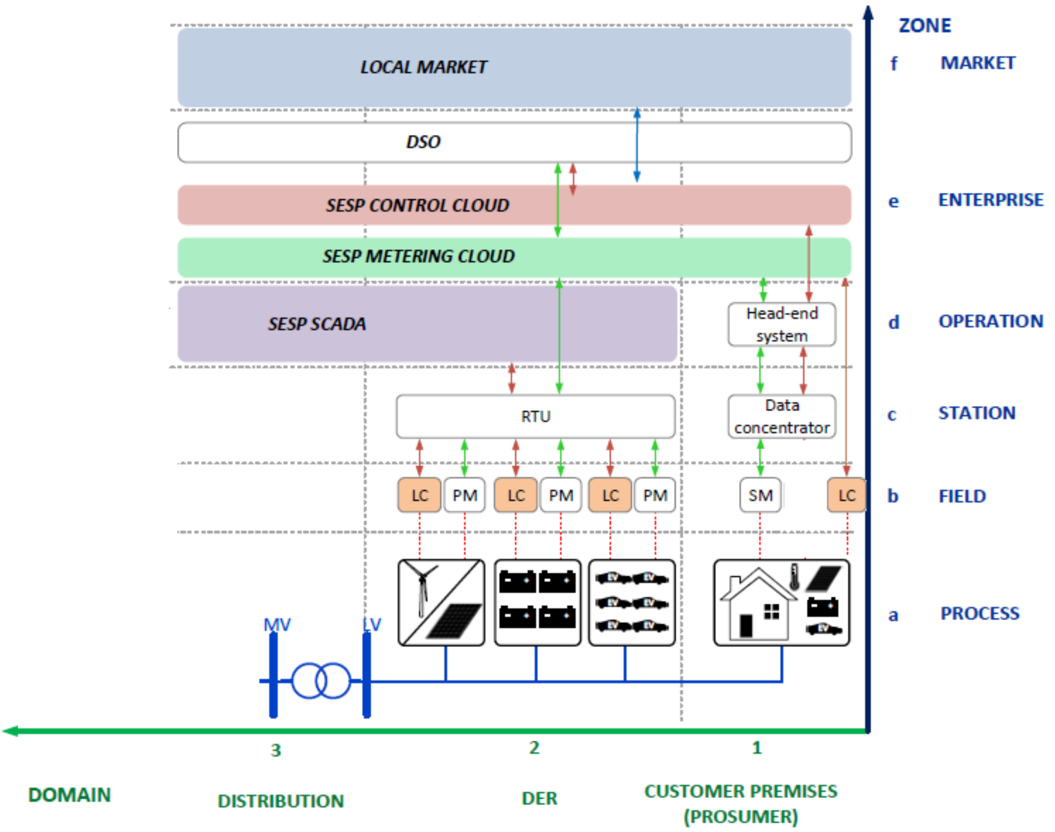

Figure 5: Empower SGAM Architecture

In this scheme, it can be seen the different elements are part of the complete system.

Within the communications platform, the links between the field devices and the SESP system is defined, that´s to say, everything needed and related with the communications infrastructure.

These elements are:

a. **DER systems** - including storage, solar power generation and electric vehicle charging points.
b. **RTU**: A electric data acquisition and control device that connects on real time with the SCADA and the DER Controllers.
c. **SCADA**: Software acquisition and control
d. **Mete**r: home smart meter
e. **Data concentrator**: smart meters concentrator to collect information from a number of meters
f. **Head-end system**: Smart metering proprietary system software.
g. **SES**P: Smart Energy Service Provider to collect information from head system and send information to market tools (billing programs, customer programs, etc.)
h. **Local controller**: Communicates with the DER and prosumers teams and communicates with the RTU or the SESP system

5.2 Defining each communications link capabilities between each system

As can it can be seen, there are different links within the architecture where it has to be selected an appropriate protocol and appropriate communication media for each link.

a. Local Controller / PM ←→RTU

The communication protocol of the link is given by the capacities of IED equipment. They must be able to establish communications with any of the protocols set out in previous sections.

b. RTU←→SCADA

As in the previous point, the RTU will use a standard protocol including into defined ones.

c. SCADA ←→ SESP

To establish communication between the SCADA system and SESP system, Web services or otherwise be used, if this is not possible by software incompatibilities, file sharing via FTP or a similar system.

d. Meter ←→Data Concentrator

Communication between the smart meter and data concentrator use to be wireless radio frequency in Norway pilot, but there are also new PLC smart meters communications technologies that will be treated in order to define the rest of the pilots.

The communications protocol to connect these smart metering devices are own manufacture proprietary, so that both the meter and data concentrator will be the same manufacturer.

e. Data concentrator ←→ Head End System

As in the previous case, the data concentrator belongs to the same head end system manufacture, so the protocol remains closed to be used with new equipment frok others manufacturers.

Communication between the concentrator and the head end system will be TCP-IP communication as provided in section related to smart metering.

f. Head end system←→SESP

Communication between the head end system is done through web services using some Apis provided by the head end system in order to connect any system with the metering system software so that it can be performed reading tasks among others functionalities.

g. Home prosumers←→SESP

In the case of home prosumers, these will be connected either directly from the local controller to the SESP system via TCP-IP, or else by the smart meter.

5.3 Research and Election of the monitored measurements

Once the communication protocols between each system link are defined it will be chosen what kind of measures is required by the SESP system from IED field devices.

These values shall be sent following the direction:

Local Controller / PM ←→RTU←→SCADA ←→ SESP

Is a two-way communication because data are sent to the SESP system, but this system will also send control commands to the field devices.

5.4 Research and election of communication media

Once variables to monitor are defined and communication protocols selected, media between communication links annotated in step 2 ,will be selected.

There are different types of wired and wireless communications defined in that section.

5.5 Research and Election of the physical communication devices

Once defined measurements, protocols and communication media, it is needed to select what kind of physical field devices must be installed, the same as control center elements.

The appropriate equipment will be acquired following the specifications obtained in steps before.

5.6 Laboratory Installation

Before installing field devices, tests should be made in the laboratory to verify that the computers and equipment communicate correctly. For this, a test plan will be developed to proceed to execute the communications test established.

5.7 Field installation - Pilot testing.

Once all the tests have been passed, systems and equipment shall be field installed but this is part of the work package 7.

6 Communication use cases

The use cases (UC) are the explanation of the minimum information exchanged between the SESP and the actors connected through the communication platform (CP). Use cases are limited to communication platform environment and they do not take into account the external agents that don't use the CP. The UC variables described correspond to the network dynamic variables.

All use cases have the possibility to be periodic or on demand. On demand means that the SESP can request information from any agent in any moment.

Electrical state variables are needed from all agents connected to the grid and they are defined as:

- Active power
- Reactive power
- Voltage in the connection point
- Current in the connection point

There are five use cases, one for each type of agent:

- EV charging station
- Storage
- Generation
- Smart metering
- Prosumer

The following sections describe each UC.

6.1 EV charging station

Use Case ID:	UC-1-EV_CS
Use Case Name:	EV charging station communicating with SESP
Actors:	- EV charging station/point - SESP - Communication platform
Description:	This UC describes the information exchanged between the SESP and the EV charging station (EV_CS). The EV_CS has to send the information periodically to the SESP. Furthermore, the SESP can request information in any moment. According to the charging station capabilities, SESP can: - Modify active power consumed or generated - Modify reactive power, inductive or capacitive
Pre-conditions:	- EV owner parks in the EV_CS - The owner identifies its needs - EV_CS authorize the connection - SESP authorize the connection - EV owner connect the EV to the station - EV owner has established the needed contract with its conditions - The EV_CS is connected to the CP
Post-conditions:	During the charge or discharge: - The EV_CS modifies its energy consumed/generated - The EV_CS modifies its power factor
Information exchanged:	SESP -> Charging station - Electrical state variables set-points Charging station -> SESP - Electrical state variables measurements - Charging power - Charging range capacity
Exceptions:	- No valid identification - No communications with the SESP
Assumptions:	- The EV owners from the SESP will have an ID card to access the charging point. - The charging point dash board will permit to access other non SESP EV owners with their credit card. - The EV owner will send its requirements through a dash board in the charging point or through its mobile phone.

Table 1: EV charging station use case

6.2 Storage

Use Case ID:	UC-2-STO
Use Case Name:	Storage communicating with SESP

Actors:	- Storage unit - SESP - Communication platform
Description:	This UC describes the information exchanged between the SESP and the Storage unit (STO). The STO has to send the information periodically to the SESP. Furthermore, the SESP can request information in any moment. According to the storage unit capabilities, SESP can: - Modify the active power consumption or generation - Modify reactive power, inductive or capacitive - Maintain the voltage and frequency in the connection point
Pre-conditions:	- The STO is connected to the grid - The STO unit is connected to the CP - The STO unit has established the needed contract previously with its conditions - The STO is available
Post-conditions:	During the charge or discharge: - The STO modifies its energy consumed/generated - The STO modifies its power factor - The STO gives grid support contributing to voltage control - The STO gives grid support contributing to frequency control
Information exchanged:	SESP -> Storage - Electrical state variables set-points Storage -> SESP - Electrical state variables measurements - State of charge - Lifespan - Temperature - Real capacity - Charge rate
Exceptions:	- No valid identification - No communications with the SESP
Assumptions:	- The storage can provide the information - The storage can control its active and reactive power - The storage can give support contributing to voltage and frequency control.

Table 2: Storage use case

6.3 Generator

Use Case ID:	UC-3-GEN
Use Case Name:	Generator communicating with SESP
Actors:	- Generator unit - SESP - Communication platform
Description:	This UC describes the information exchanged between the SESP and the Generator unit (GEN). The GEN has to send the information periodically to the SESP. Furthermore, the SESP can request information in any moment.

	According to the GEN unit capabilities, SESP can: - Modify the active power generation - Modify reactive power, inductive or capacitive - Maintain the voltage and frequency in the connection point
Pre-conditions:	- The GEN unit is connected to the grid - The GEN unit is connected to the CP - The EN unit has established the needed contract previously with its conditions - The GEN unit is available
Post-conditions:	- The GEN modifies its energy generated - The GEN modifies its power factor - The GEN gives grid support contributing to voltage control - The GEN gives grid support contributing to frequency control - The SESP notifies that it has received the information
Information exchanged:	SESP -> Generation unit - Electrical state variables set-points Generation unit -> SESP - Electrical state variables measurements - Weather information - Generation capacity over the maximum
Exceptions:	- No valid identification - No communications with the SESP
Assumptions:	- The generation unit can provide the information - The generation unit can control its active and reactive power - The generation unit can give support contributing to voltage and frequency control.

Table 3: Generator use case

6.4 Smart metering

Use Case ID:	UC-4-MET
Use Case Name:	Meter communicating with SESP
Actors:	- Meter - SESP - Communication platform
Description:	This UC describes the information exchanged between the SESP and a meter (MET). The MET has to send the information periodically to the SESP. Furthermore, the SESP can request information in any moment.
Pre-conditions:	- The meter unit is connected to the CP
Post-conditions:	- The meter will send measurements to SESP. - SESP receive information and it is stored in databases
Information	SESP -> Meter - Commands Meter -> SESP - Electrical state variables measurements

exchanged:	- Alarms and events
Exceptions:	- No valid identification - No communications with the SESP
Assumptions:	- SESP can read all residential meters - Meters can send information to SESP. (Smart Meters)

Table 4: Smart metering use case

6.5 Prosumer

Use Case ID:	UC-5-PRO
Use Case Name:	Prosumer communicating with the SESP
Actors:	- Prosumer - SESP - Communication platform
Description:	This UC describes the information exchanged between the SESP and the Prosumer (PRO). The PRO has to send the information periodically to the SESP. Furthermore, the SESP can request information in any moment. The prosumer receives set-points from SESP to adapt its generation to its requirements. The prosumer could have different types of resources: storage, generation, demand side management, electric vehicle According to the PRO unit capabilities, SESP can: - Modify the active power produced/consumed - Modify reactive power, inductive or capacitive
Preconditions:	- The prosumer is connected to the grid - The prosumer is connected to the CP - The prosumer has stablished the needed contract previously with its conditions
Post-conditions:	- The PRO modifies its energy consumed/generated - The PRO modifies its power factor - The SESP notifies that it has received the information
Information exchanged:	SESP -> Prosumer - Electrical state variables set-points of all resources Prosumer -> SESP - Electrical state variables measurements of all resources - State of charge of EV - State of charge of Storage - Lifespan of Storage - Room temperature - Outside temperature - Capacity of deferrable loads - Generation capacity over the maximum
Assumptions:	- The PRO can provide the information - The PRO can control its active and reactive power

Table 5: Prosumer use case

6.6 Communication use cases specification

In this section, the criteria for determining the information exchange for the previous communication use cases will be depicted for each of them.

6.6.1 Specifications criteria

Communication requirements can be evaluated using some special characteristics. Some of the more significant features that can be used to evaluate the specifications of the information to be exchanged are the following: throughput, latency, security aspects, reliability and availability.

Before specifying the information exchange requirements, a definition of these variables are described. As it is difficult to define an exact value for all these parameters, reference ranges are defined to evaluate the communication requirements.

Throughput:

- It defines the number of bits that can be transmitted in each specified period of time using a communication system.
- It is highly related to the transmission speed and the quantity of information that need to be exchanged.

Throughput reference ranges		
LOW	✓	Lower than 10 kbps
AVERAGE	✓✓	Between 10 kbps and 1 Mbps
HIGH	✓✓✓	Greater than 1 Mbps

Table 6: Ranges used to define throughput requirements

Latency:

- It defines the period of time it takes for a message or packet of data to get from the sender to the receiver.
- It is also known as response time or delivery time
- It is highly related to the transmission speed and the media access method.

Latency reference ranges		
LOW	✓	Greater than 5 seconds
AVERAGE	✓✓	Between 0,5 and 5 seconds
HIGH	✓✓✓	Less than 500 milliseconds

Table 7: Ranges used to define latency requirements

Security aspects:

- Security aspects include characteristics such as difficulty of external access, confidentiality and integrity of data, or system vulnerability.
- Encryption, passwords or codification can be used in order to improve security aspects.

Security aspects reference ranges		
LOW	✓	Exchanged data is not confidential nor critical for the system performance
AVERAGE	✓✓	Exchanged data is not confidential, but manipulation has to be avoided as changes in the data are critical for the system performance
HIGH	✓✓✓	Exchanged data is highly confidential and any kind of manipulation or external access has to be prevented by all means

Table 8: Ranges used to define security aspects requirements

Availability:

- It is the ability of the system to perform a determined action at any instant of time.
- In communications, it can be translated as the necessity to send a determined data in a specified instant.

Availability reference ranges		
LOW	✓	All data can wait until link becomes available (availability needed lower than 90%)
AVERAGE	✓✓	Some data can wait for a limited time (between 90% and 99,9%)
HIGH	✓✓✓	No data can wait (greater than 99,9%)

Table 9: Ranges used to define availability requirements

Reliability:

- It is the ability of the system to perform a determined action under specified conditions for a specified period of time, and it describes how errors can affect the performance of the system.
- It can be quantified as the Bit Error Ratio (BER), which determines the percentage of bit errors per unit time.
- It can be highly affected by external interferences or noise.

Reliability reference ranges		
LOW	✓	Some errors allowed (information loss greater than 0,1%)
AVERAGE	✓✓	Limited number of errors allowed (between 0,01% and 0,1%)
HIGH	✓✓✓	No errors allowed (smaller than 0,01%)

Table 10: Ranges used to define reliability requirements

6.6.2 Information exchanged specification

	Throughput	**Latency**	**Security**	**Availability**	**Reliability**	**Pulling**
SESP to CS/P						
Electrical state variables set-points	✓	✓✓	✓✓	✓✓	✓✓✓	5-15 min
Commands / requests of information	✓	✓✓	✓✓	✓✓	✓✓	Read on demand
CS/P to SESP						
Electrical state variables measurements	✓✓	✓	✓✓	✓	✓✓	5-15 min
Charging power	✓	✓	✓	✓	✓	5-15 min
Charging range capacity	✓	✓	✓	✓	✓	5-15 min

Table 11: EV charging station requirements

	Throughput	**Latency**	**Security**	**Availability**	**Reliability**	**Pulling**
SESP to Storage						
Electrical state variables set-points	✓	✓✓✓	✓✓	✓✓	✓✓✓	5-15 min
Commands / requests of information	✓	✓✓	✓✓	✓✓	✓✓	Read on demand
Storage to SESP						
Electrical state variables measurements	✓✓	✓✓✓	✓✓	✓✓	✓✓	5-15 min

State of charge	✓	✓	✓✓	✓✓	✓✓	5-15 min
Lifespan	✓	✓	✓	✓	✓	5-15 min
Temperature	✓	✓	✓	✓	✓	5-15 min
Real capacity	✓	✓	✓✓	✓	✓	5-15 min
Charge rate	✓	✓	✓✓	✓	✓✓	5-15 min

Table 12: Storage requirements

	Throughput	Latency	Security	Availability	Reliability	Pulling
SESP to Generator						
Electrical state variables set-points	✓	✓✓✓	✓✓	✓✓	✓✓✓	5-15 min
Commands / requests of information	✓	✓✓	✓✓	✓✓	✓✓	Read on demand
Generator to SESP						
Electrical state variables measurements	✓✓	✓✓✓	✓✓	✓✓	✓✓	5-15 min
Weather information	✓	✓	✓	✓	✓	5-15 min
Generation capacity over the maximum	✓	✓	✓	✓	✓	5-15 min

Table 13: Generator requirements

	Throughput	Latency	Security	Availability	Reliability	Pulling
SESP to Meter						
Commands / requests of information	✓	✓	✓✓	✓✓	✓✓	Read on demand
Meter to SESP						
Electrical state variables measurements	✓	✓	✓✓✓	✓	✓✓✓	1 per day
Alarms and events	✓	✓	✓✓✓	✓✓	✓✓✓	1 per day

Table 14: Smart metering requirements

	Throughput	Latency	Security	Availability	Reliability	Pulling
SESP to Prosumer						
Electrical state variables set-points of all resources	✓✓	✓✓✓	✓✓✓	✓✓	✓✓✓	5-15 min
Commands / requests of information	✓	✓✓	✓✓✓	✓✓	✓✓	Read on demand
Prosumer to SESP						
Electrical state variables measurements of all resources	✓✓	✓✓✓	✓✓✓	✓✓	✓✓	5-15 min

State of charge of EV	✓	✓	✓	✓	✓	5-15 min
State of charge of Storage	✓	✓	✓✓	✓✓	✓✓	5-15 min
Lifespan of Storage	✓	✓	✓	✓	✓	5-15 min
Room temperature	✓	✓	✓	✓	✓	5-15 min
Outside temperature	✓	✓	✓	✓	✓	5-15 min
Capacity of deferrable loads	✓	✓	✓✓✓	✓	✓✓✓	5-15 min
Generation capacity over the maximum	✓	✓	✓	✓	✓	5-15 min

Table 15: Prosumer requirements

7 Conclusions

The report has been aimed at exploring the most adequate communication choices, considering the existence of a wide variety of products, protocols and elements well suited to be deployed in local markets. The work carried out will allow for fine-tuning -in later stages of the project- the more specific requirements, which would then be further analysed without the project being exposed to communication's technical incoherence.

Among all the possibilities analysed, the characteristics of the systems that should be installed in different pilots will be chosen in accordance with the best options in terms of technical, economic and project dimensions.

They final adoption of the specific multi-layer communication protocols in each implementation will always be coherent with an established architecture, and based upon the proposed standard protocols. The final adoption at pilot level will be subject to the discussions to be held between WP4 partners and the responsible for each of the pilots in Norway, Germany and Malta.

8 References

1. GUIA TECNOPYME. Fase II. "Bassic Guide for TIC´s applications in PYMES "

2. Vigilancia Tecnológica Estudio Sectorial: Tecnología Inalámbricas. Agencia de Innovación y Desarrollo de Andalucía (IDEA).
3. IEC 60870-5-101: Transmission Protocols, companion standards especially for basic telecontrol tasks
4. IEC 60870-5-104: Transmission Protocols, Network access for IEC 60870-5-101 using standard transport profiles
5. DNP Users Group: www.dnp.org
6. Communication Protocols : www.ipcomm.de