Smart Grid

Marina Egea,
Atos S.A. (Spain),
marina.egea@atosresearch.eu

April 26, 2012

1 Motivation

The growing demand for energy, the need for a sustainable basis reducing the climatic impact of fossil energy sources, and the need for replacing old or outdated energy infrastructure, are some of the main drivers of a revolution in the energy market.

The increased use of renewable energy sources such as sunlight, wind, water reservoirs, etc. demands that energy is consumed in an optimal way, responding to strongly dynamical conditions. Moreover, energy should be also stored locally for later use, compensating peaks of high demand with periods of abundant supply. Indeed, renewable energy fluctuates strongly during day and night, depending on the weather and climatic conditions, while many current energy systems require the continuous availability of energy. An auto-balancing, self-monitoring and self-healing infrastructure is the goal, coupling generation, distribution, storage and consumption of energy. Not only the availability of electricity is a challenge, also electric service reliability problems, power quality disturbances, overload during peak periods, and blackouts must be avoided, especially if electricity is being produced in a distributed dynamic way.

Thus, industry and governments are engaged in the systematic optimization of the energy system.Behind this paradigm shift is a loosely coupled distributed, intelligent network – the Smart Grid.

What is the Smart Grid? Smart grid is an electricity network that can integrate in a cost-efficient manner the behaviour and actions of all users connected to it - generators, consumers and those that do both in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety. The smart grid is not a single system or network, and it is not a static concept. It will continue to evolve as the existing technologies evolve and new technologies are developed.

Smart grids use information and communication technology (ICT) to optimize the transmission and distribution of electricity from suppliers to consumers, allowing smart generation and bidirectional power flows – depending on where

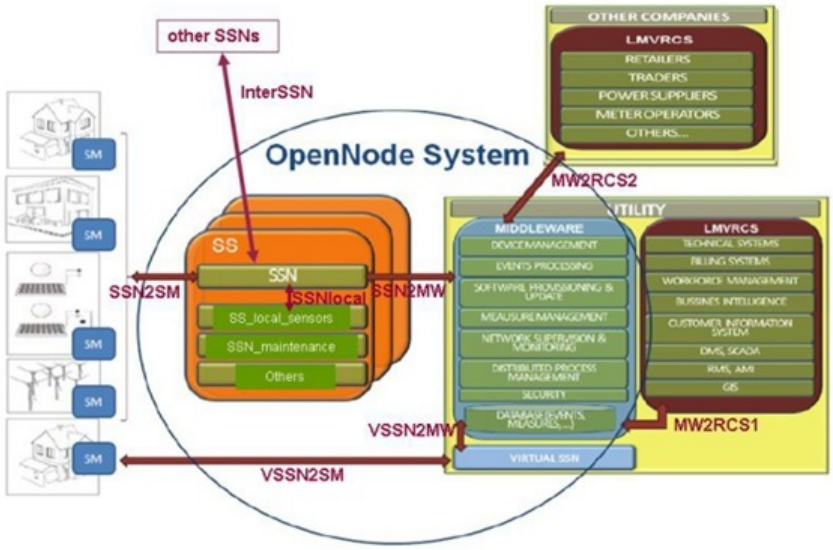

Figure 1: OpenNode architecture

generation takes place [8]. With ICT the Smart Grid enables financial, informational, and electrical transactions among consumers, grid assets, and other authorized users.

The end user sees already the initial impact of the smart grid on his daily life: the appearance of smart meters, smart appliances, and smart consumer devices. Advanced metering technology enables new price models through the ability to record energy usage at fine time intervals. The exchange of real-time prices and market data allows customers reduce their energy costs.

Smart Meters A smart meter is usually an electrical meter that records consumption of electric energy in intervals of an hour or less and communicates that information at least daily back to the utility for monitoring and billing purposes. Smart meters enable two-way communication between the meter and the central system. Unlike home energy monitors, smart meters can gather data for remote reporting. Such an advanced metering infrastructure (AMI) differs from traditional automatic meter reading (AMR) in that it enables two-way communications with the meter. For more information about the general scenario, please, read [7].

2 General Use Case

The overall scenario that we address here is provided by the OpenNode project [1, 2, 3, 4] intended to achieve the optimization of the whole power distribution system. Therefore, it is not focused on metering functionalities but in how all

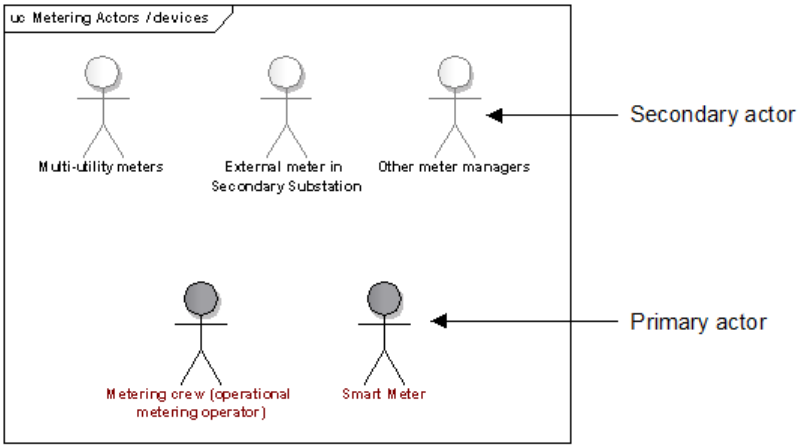

Figure 2: Primary and Secondary Actors

the information from / to the SMs (Smart Meters) is communicated and how is responsible for giving or receiving the information. It aims to achieve new functionalities that allow a more efficient and automatic way of operating. Many of these functions are related with information gathered in the SS (Secondary Substations). Fig. 1 depicts the main h components that are supposed to be present in an Open Node architecture. Secondary substations are key components to monitor and control the distribution grid status. Based on Information and Communication Technology (ICT) major energy industry challenges are addressed by a network of embedded devices the SSNs capable of communicate to each other and contribute to the efficient exploitation of the energy resources. SSN denotes an intelligent unit to be installed in every SS (secondary substation). Middleware (MW) will denote a central software in charge of receiving the information from the SSNs, storing it, and providing it to the LMVRCS. Actually, for some local functions, both the SSN and the MW shall be able evaluate the information, to take decisions, to store relevant information and to provide it to the LMVRCS. LMVRCS denotes Low / Medium Voltage Related Company System, in Fig. 3 the actors that LMVRCS represents are graphically depicted.

3 Actors involved

Figure 2 shows how principal and secondary actors are differently coloured to enable their distinction. Figures 3 and 4 show hierarchies of actors involved in the Smart Grid.. The amount and the hierarchies that are present provide a rough idea of the complexity of the network of stakeholders that are involved in the SmartGrid.

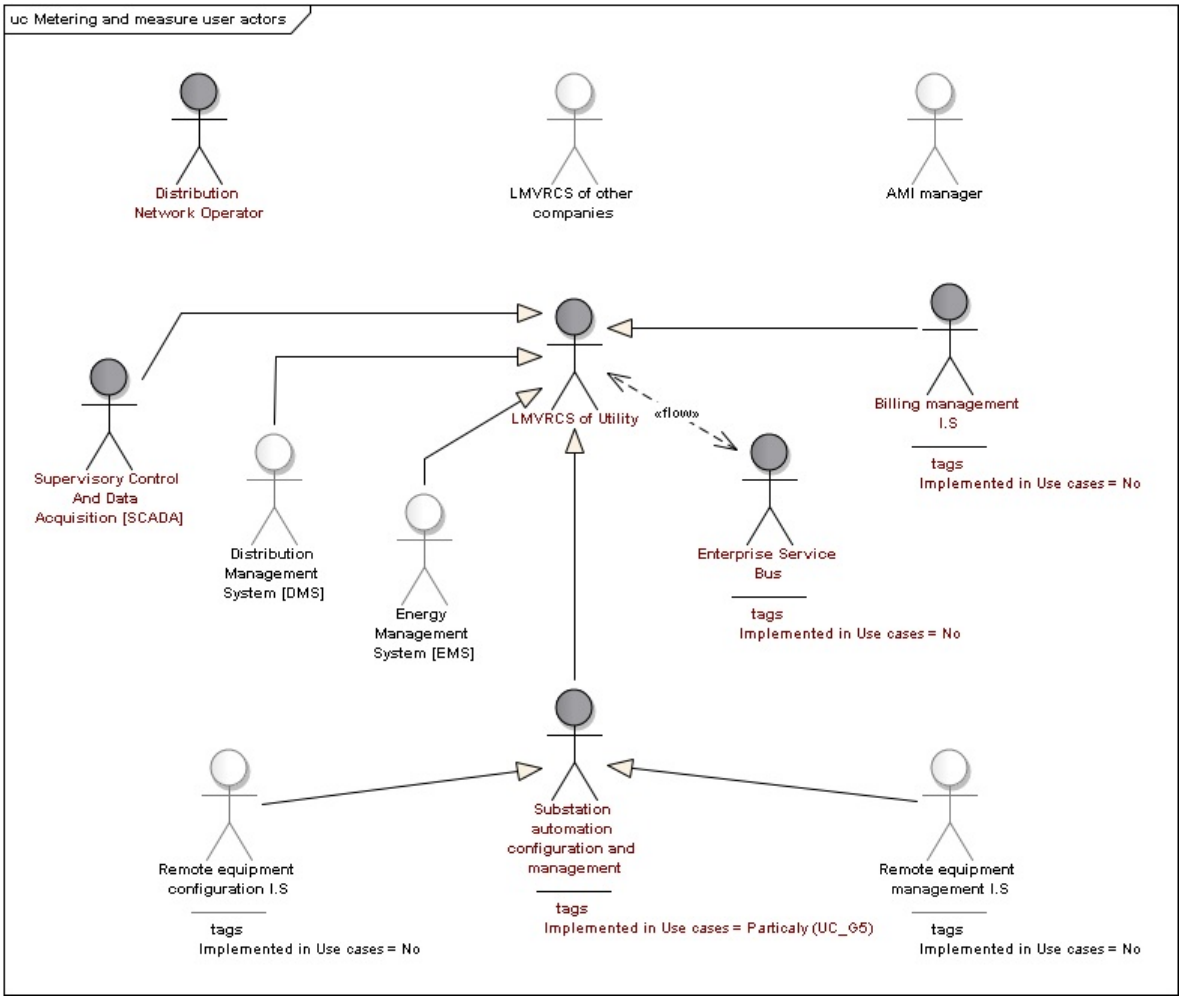

Figure 3: Hierarchy within LMVRCS

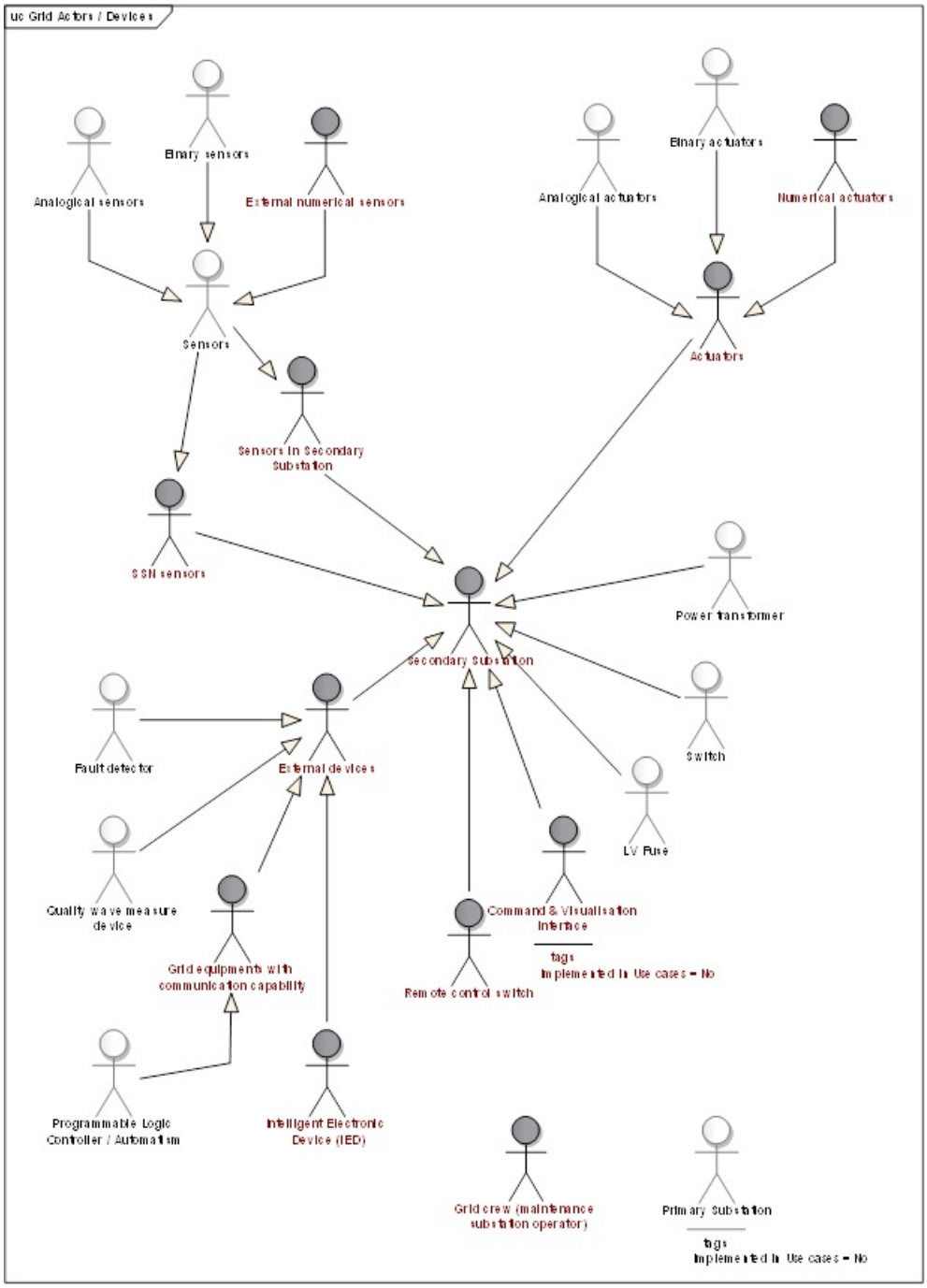

Figure 4: Substation Actors

4 Use Case: Electricity SMs reading (For billing)

This use case describes the SM data acquisition process for billing purposes. The SSN will periodically gather metering information for billing from the SMs connected to it according to a configurable time period. It will store this information in its internal data base and it will periodically report this information up to the Middleware on a configurable time period basis too. The information will be stored in the Middleware database and every certain periods of time, attending to legal and contracting reasons, this information will be sent by the Middleware to the corresponding LMVRCSs that need the information. Also, and due to some legal and confidentiality aspects in some countries, a direct SM information access and not to the information stored in any SSN or Middleware database might be considered necessary for some LMVRCSs. Some verification and validation data checks may be considered necessary during the reading process in order to minimize possible billing errors both in the SSN and in the Middleware.

The data acquisition process is described next: A LMVRCS might ask the MW for the current metering readings in one or several SMs. The MW will request this information to the SSN. The SSN will request the information to the corresponding SM. The SM will provide the metering information with time stamp and an identification name to the SSN, the SSN to the MW, and the MW to the LMVRCS

Actors

SM : Smart Meter

SSN : Secondary Substation Node

MW : Middleware

LMVRCS : Information System of Utilities (LMVRCS)

Applicable preconditions

PRE1 : The [SSN] must be detected and referenced by the [MW]

PRE2 : [SM]s must be detected

PRE3 : [SM]s and [SSN]s must have the updated firmware and compatible

PRE4 : [SM]s and [SSN]s must be synchronised

PRE5 : For 'periodic reading' process: During the [SSN] configuration, the [MW] send request of the periodic time 'reading order of the group Smart meter managed by the SSN and report.' So with this information [SSN] manages itself the [SM] reading

PRE6 : Communications must be secure

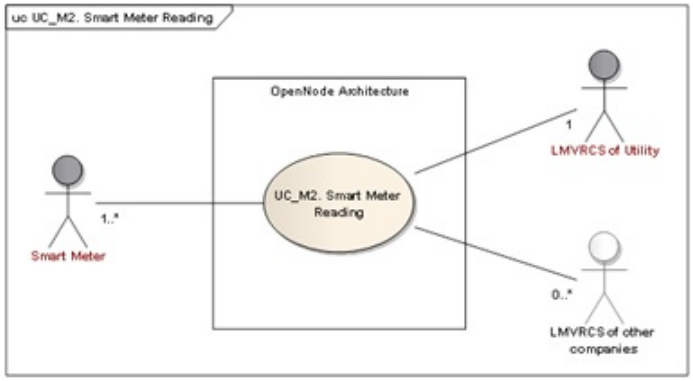

Figure 5: Actors in the reading Use Case

Postconditions

POST1 : [MW] had received periodic information (identifier, accumulator, status, power quality) or dedicated (on demand) information (identifier, accumulator, status, power quality) of Smart Meter.

5 Use case: Alarm and Event Management

This use case describes the process of checking constantly for errors in each SM and in those SS meters and devices associated to each SSN, and also the process of managing the event reports created in those different devices. The SSN must check periodically the correct functioning of each connected device (SMs and also local SS meters, relays and sensors) and its own status. If any problem is detected, the SSN must report it to the Middleware immediately. The SSN will give the correct priority to both the alarm and event reports in order to avoid possible negative delays. The Middleware shall check then this information, store it in its database, and act accordingly: it may take a corrective decision by itself or it may decide to warn the corresponding LMVRCSs. The Middleware shall be able to request the last alarm and event reports stored in any SM or SSN, and also it shall have all those reports available for sending in case they are requested by any authorized LMVRCS. Each LMVRCS shall decide the priority

of the events and if they may be considered alarms. As examples, some possible events / alarms to be reported could be:

1. Critical malfunctions triggered by the SMs or the SSN
2. Critical deviations of the clock,
3. Indication of modification of critical parameters in the meter;
4. Software and firmware version.
5. Changes from Presence to absence of voltage.
6. Unauthorized access attempts/ any possible violation attempt.
7. Power control as threshold programming.
8. Switch-off of the disconnection element
9. Outage / planned interruptions.

6 High level security requirements

All applicable policies of the utility and its major business partners must be observed, as well as the relevant legislation and regulation. Non-Compliance may result in banning of the system [5].

The SSN should be implemented with security features to avoid

- Software intrusion: uploading of data from unauthorized parties. The measures adopted to address these risks will be implemented mainly at the communication protocol level. Encryption and use of certificates are methods that should be explored as part of the communication architecture design. Besides, if removable parts (SD cards of the like) are used to store sensible information, they should be encrypted.
- It is not foreseen to protect the SSN from DoS attacks by internal means. If this is deemed as necessary, some external measures should be adopted (e.g., an intrusion detection system at the gateway level, that could also help reduce some of the other intrusion risks.)
- Restricted access to corresponding actors to data recollected from the SMs and the SS devices, or elaborated from them.
- Access to operation services offered by the SSN that could be harmful (like issuing SS commands) or inadequate (like reprogramming SMs.)

Availability. Availability of Components and Data and use of existing standards must be ensured. In fact, security controls proposed should be based on existing standards as far as possible. In particular to secure most of the communication, e.g., for communication of the SSNs with the SMs. The system, all of its components (SMs, SSNs, Local Devices, MW), and its information assets must be sufficiently available (SLA) to authorized parties. The system and its components must function properly, reliably and robustly.

Confidentiality, non-repudiation. For data transmitted between security cells, and whenever crossing trust boundaries or sending data across open Networks (whenever technically feasible), confidentiality and integrity of the transmitted information must be ensured against outsiders and secure authentication of the communication parties.

If intermediate components are not trusted by the end components for some purpose, end-to-end security mechanisms must be used. Critical data must be sufficiently integrity and authenticity protected and kept confidential in processing, transmission, and when stored. Facts/data may not be falsely repudiated after having been issued / generated by the involved parties or components.

Authentication and authorization. Reliable authentication and authorization of communication partners (including administrators interacting with the system) are also necessary.

The various components shall only provide authorized administrators with functions for the management of the security features. It must be ensured, that only authorized parties are able to provide updates and that only fresh, authentic and entire updates are applied.

Especially for critical transactions as well as of other security relevant administration events and authorizations, log data must be integrity protected and available. Relevant actions must be accountable to the responsible parties and components with sufficient confidence. Consumer related log entries must be kept confidential.

Reliability, integrity, secrecy. The system shall provide reliable time stamps and update the internal clocks of the various components in regular intervals by retrieving reliable time information from a dedicated reliable source in the WAN.

The system shall implement functionality to protect its security functions against malfunctions and tampering. This specifically applies to exposed components like SMs, Devices and SSNs. These components shall only collect and buffer minimal data, and shall safely delete any information that is no longer required (data sparseness). This ensures that these data are not or no longer available via the external interfaces of the respective SMs, Devices, and SSNs. Critical Data buffered in these components must be stored encrypted to prevent unauthorized access on the containing storage device. We require a self-test and

a fail-safe design of these components. We must make any physical manipulation within the scope of the intended environment of the SM, Device or SSN detectable to consumers or administrators. To allow for reaction, in the case of intrusion detection, suitable alarms must be raised to make concerned parties aware of the security breach.

Privacy. Privacy sensitive data like billing relevant consumption data must remain access restricted for administrators, unless actually indispensable for the required task. Legally adequate privacy protection of personal identifiable information. Customer adequate privacy protection of sensitive information by the company. Failure to comply with the prescribed regulations may result in legal prosecution, substantial fines and loss of reputation, as well as banning of the non-compliant application.

A Smart Meter data structure (simplified, partial)

The data structure outlined next is based on and oversimplifies [6] since the project OpenNode reuses the results for smart meters from the OpenMeter project [2]. There are different contracts that can be issued with a user: to import energy, to export energy, or both. All of them are managed by the same meter. Notice that measurements taken by a meter are always discrete measurements. Some of the typical records stored in the internal database of the SM are:

- Current date, time in sync with a clock in terms of year, month, day, hour, minute.
- Time and date of last sync.
- Initial date, time when SM started to measure (initial value).
- Status of meter reading: Import, import and export, export, disabled.
- Power limit, Power tariff, Customer name, User id number, Type of contract, Flag of disconnectivity, Start, end date.
- Time bands per day: weekly tarrif (Monday to Friday), Saturday and Sunday tariff, Power available to be supplied in each tariff (there can be 3 different types of tariffs: flat, daylight, night).
- Voltage interruptions during the last billing period (period of time expressed in intervals of 15 minutes). Save threshold for voltage interruption and cumulative totalizer of voltage interruptions. Counter of voltage interruptions in seconds during the current and the previous billing period.
- Same parameters to store meter power fails.

- Duration of time intervals in which meter has to calculate the average of voltage values to evaluate the voltage variations in day period.
- Time period in days in which voltage variations have to be observed.
- Upper threshold for voltage.
- Lower threshold for voltage.
- Instantaneous value of voltage measured.
- Minimum/max voltage in current and previous period.
- Number of failed authentication attemps.
- Alarms: meter without correct date and time info, alarm on communication if it is unable to connect, clock is not alligned, if there has been voltage interruption, or if internal corruption can damage data collected at end of billing period.

Regarding access to SM information:

- Users can access information from billing company by a web service but only for reading purposes, the information contained in their profile (RW), and billing information (RO), namely, tariff information, power consumption, power excess (for which a special tariff is exceed) when the user crossed the upper voltage limit. The bill will depend on the type of contract agreed: day, night or flat rate.
- Billing company can update tariffs and type of contract.
- DMS can update voltage and power limits and access any incidency that has to do with voltage interruption and failed authentication attemps.
- SSN may access different SM to check that the obtained information is correct by checking confirmation by redundancy checks from different SMs.
- SCADA system is the only actor that can configure parameters to update, read and store meter power fails, duration of time intervals in which meter has to calculate the average of voltage values to evaluate the voltage variations in day period, time period in days in which voltage variations have to be observed, Upper/Lower threshold for voltage, Lower threshold for voltage. Alarms are managed by the SCADA system although DMS has also access to the information. The SCADA system should report to billing company any problem that may affect customer(s)' bills.

Type of Access to information:

- – not readable, not readable
- RO, WO: Readable only, writable only
- RW: Readable and writable
- E: Executable

References

[1] OpenNode – Open Architecture for Secondary Nodes of the Electricity SmartGrid, *D1.1 General Requirements, Overall Architecture and Interfaces*, 2010.

[2] OpenNode – Open Architecture for Secondary Nodes of the Electricity SmartGrid, *D1.2 Evaluation of general requirements according state of the art*, 2010.

[3] OpenNode – Open Architecture for Secondary Nodes of the Electricity SmartGrid, *D1.3 Functional Use Cases*, 2010.

[4] OpenNode – Open Architecture for Secondary Nodes of the Electricity SmartGrid, *D2.1 Hardware and Software Reference Architecture*, 2010.

[5] OpenNode – Open Architecture for Secondary Nodes of the Electricity SmartGrid, *D4.3 Analysis of security architecture*, 2011.

[6] OpenMeter – Open public extended network metering, *D5.1.3.1 Database and Data Structure for the Meters and More Suite*, 2011.

[7] NESSoS – Network of Excellence on Engineering Secure Software and Systems *D11.2 Selection and documentation of the two major case studies*, 2011.

[8] CEN, CENELEC, ETSI, *SGCG Report on Reference Architecture for the Smart Grid – Draft*, 2012.