



# STORY

added value of STORage in distribution sYstems

## Deliverable 4.1 Structured Overview of Communication Standards for Smart Grids



Revision .....	1.0
Preparation date ..	2015-12-31 (m08)
Due date .....	2016-01-31 (m09)
Lead contractor ....	VTT
Dissemination level	PU

### Authors:

Pekka T. Savolainen	VTT
Timo Kyntäjä .....	VTT
Heribert Vallant ....	JR
Stefan Marksteiner	JR
Arnout Aertgeerts.	ACT
Lode Van HaleWeyck	ACT
Paul Valckenaers.	UCL





# STORY

## Table of contents

<b>1</b>	<b>PUBLISHABLE EXECUTIVE SUMMARY .....</b>	<b>5</b>
<b>2</b>	<b>INTRODUCTION .....</b>	<b>6</b>
<b>3</b>	<b>SMART GRID COMMUNICATION .....</b>	<b>9</b>
3.1	STANDARDS & STANDARDISATION GROUPS.....	9
3.2	COMMUNICATION NETWORKS IN STORY.....	12
3.2.1	<i>Home Area Network (HAN) .....</i>	<i>16</i>
3.2.2	<i>Field Area Network (FAN) .....</i>	<i>16</i>
3.2.3	<i>Wide Area Networks (WAN) .....</i>	<i>17</i>
3.3	HIGHER LAYER COMMUNICATION PROTOCOLS.....	19
<b>4</b>	<b>INTRA LEVEL COMMUNICATION INSIDE OPERATIONS .....</b>	<b>20</b>
4.1	PREMISES AREA NETWORKING TECHNOLOGIES.....	21
<b>5</b>	<b>WIDE AREA NETWORK TECHNOLOGIES.....</b>	<b>25</b>
5.1	WIRELESS BROADBAND.....	25
5.2	PLC – POWERLINE COMMUNICATION .....	26
5.3	LOW POWER WIDE AREA NETWORKS (LPWAN).....	26
5.3.1	<i>LoRaWAN.....</i>	<i>27</i>
5.3.2	<i>Sigfox.....</i>	<i>27</i>
5.3.3	<i>Others .....</i>	<i>29</i>
<b>6</b>	<b>M2M PROTOCOLS .....</b>	<b>30</b>
6.1.1	<i>Legacy M2M Protocols.....</i>	<i>30</i>
6.1.2	<i>Upcoming M2M Protocols .....</i>	<i>30</i>
<b>7</b>	<b>SECURITY AND PRIVACY .....</b>	<b>36</b>
7.1	CURRENT SITUATION AT STORY DEMONSTRATION SITES.....	36
7.2	SECURITY ASPECTS.....	37
7.3	SECURITY ANALYSIS OF SELECTED COMMUNICATION STANDARDS.....	39
7.4	PRIVACY ASPECTS.....	41
7.4.1	<i>European General Data Protection Regulation.....</i>	<i>41</i>
7.4.2	<i>OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data .....</i>	<i>41</i>
7.4.3	<i>International Safe Harbor Privacy Principles.....</i>	<i>42</i>
7.4.4	<i>IPEN Initiative.....</i>	<i>42</i>
7.4.5	<i>Online Trust Alliance (OTA).....</i>	<i>42</i>
7.4.6	<i>OWASP Top 10 Privacy Risks Project.....</i>	<i>42</i>
7.4.7	<i>Privacy Recommendations for STORY Project.....</i>	<i>43</i>
<b>8</b>	<b>STORY COMMUNICATION GATEWAY REQUIREMENTS .....</b>	<b>44</b>
8.1	COMMON CHARACTERISTICS .....	44
8.1.1	<i>General.....</i>	<i>44</i>
8.1.2	<i>Application Layer.....</i>	<i>45</i>
8.1.3	<i>Security Layer .....</i>	<i>47</i>
8.1.4	<i>Data Exchange Layer.....</i>	<i>49</i>
8.1.5	<i>Communication Layer .....</i>	<i>50</i>
8.2	INSTALLATION SITE CHARACTERISTICS.....	51
8.2.1	<i>Specific Characteristics – Case Study 1-2.....</i>	<i>51</i>





# STORY

8.2.2	<i>Specific Characteristics – Case Study 3</i> .....	52
8.2.3	<i>Specific Characteristics – Case Study 4</i> .....	53
8.2.4	<i>Specific Characteristics – Case Study 5</i> .....	54
8.2.5	<i>Specific Characteristics – Case Study 6</i> .....	59
<b>9</b>	<b>CONCLUSIONS</b> .....	<b>61</b>
<b>10</b>	<b>ACRONYMS AND TERMS</b> .....	<b>63</b>
<b>11</b>	<b>REFERENCES</b> .....	<b>65</b>
<b>12</b>	<b>APPENDICES</b> .....	<b>67</b>
12.1	INTRODUCTION TO SGAM METHODOLOGY .....	67
12.2	ICT SECURITY QUESTIONNAIRE .....	71
12.3	GENERAL INFORMATION ON DEMONSTRATION SITES .....	74
12.4	CASE STUDY 6 .....	75

## Disclaimer

The information in this document is provided without guarantee or warranty that the content fits for any particular purpose. The user thereof uses the information at its sole risk and liability.

The document reflects only the author's views and the Community is not liable for any use that may be made of the information contained therein.



## **1 Publishable Executive Summary**

---

Communication systems and technologies are being standardised globally by various associations. Some of them have a viewpoint solely towards communications and some of them are more related to a selected application area, such as smart grids. This deliverable aims to provide information about the existing standards when considering energy storages related systems, and especially takes into account the selected demonstration use cases of the STORY project. Several international R&D projects have and are preparing comprehensive descriptions of different communication standards, thus that kind of information is not covered here.

The deliverable is divided in sections looking at the standards from different aspects of the system. Firstly, the overall system communication and its different levels are taken into account. The levels are divided into home/premises area networking (HAN), field area networking (FAN), and wide area networking (WAN). The different notable standards are considered and briefly explained.

Secondly, Machine-to-Machine (M2M) and security are currently the most discussed topics in communication systems and technology and are each presented in a dedicated chapter. The Machine-to-Machine (M2M) related protocols and standards are developing rapidly due to the Industrial Internet and the Internet of Things related efforts globally. The most common standards are presented here. Within STORY, security and privacy is taken very seriously to ensure a maximum of protection for the demonstration cases. Especially since some test sites already have some existing and operational systems and must remain trustworthy also during the demonstration case setups and after the extension with the STORY ICT architecture.

Finally, initial considerations towards the STORY Communication Gateway requirements are made based on the existing knowledge. The STORY Communication Gateway will be an opinionated best-practice gateway to implement storage in a smart-grid context. The work will continue in the following tasks and the gateway itself will be documented more precisely in upcoming project deliverables.

The deliverable concludes by stating out the most important communication and security standards related to the STORY project and its demonstrations. Since the demonstration sites and their systems differ significantly, only suggestions of the most valuable standards are given. The suggestions are divided into three different networking categories (HAN, FAN, WAN).

To unify the whole STORY demonstrations controlling and monitoring system, a gateway will be implemented for all demonstration sites. The initial requirements are presented here. Security and privacy issues are defined and will be implemented for all the demonstration sites, and especially taken into account with the gateway specifications and implementations.

## 2 Introduction

---

In the smart grid environment, communication and information technologies continue to evolve, possibly in a disruptive manner. Looking at other application domains, which already underwent such transition into smart systems earlier, lessons can be learned and should not be neglected. In fact, one should recognise that certain scientific laws or general principles apply, delineating what is (not) possible, analogous to Carnot's principles or laws of thermodynamics in the energy domain.

### 1) Telecommunications

Present-day telecommunication is characterized by a rapid shift toward data networks: e.g. voice over IP for telephony from fixed locations. In mobile systems, data traffic services are increasingly used to cover all others: voice, video conferencing, etc. Specialised communication services become applications over (IP) data networks.

### 2) Manufacturing automation

As manufacturing plants are controlled by a single organisation and capital-intensive, the research, development and deployment of smart manufacturing systems predate the smart grid by decades. Concerning communications, they learned what was possible (and what was impossible) the hard way.

Not impeded by any degree of modesty, the manufacturing community – led by high-level management of dominant players like GM – opted to design, develop and adopt their own solution: the Manufacturing Automation Protocol or MAP. This was justified by mainstream IT lacking essential functionality and the perception that mainstream could not be upgraded, extended to address the needs of manufacturing.

Today, the Wikipedia entry<sup>1</sup> for this Manufacturing Automation Protocol barely fills a single computer screen. It states: *“Although promoted and used by manufacturers such as General Motors, Boeing, and others, it lost market share to the contemporary Ethernet standard and was not widely adopted.”* Hubris in combination with a lack of understanding how complex man-made systems emerge and prevail (or not) resulted in this outcome.

The manufacturing community adopted IP/Ethernet, often in a high-performance variety (e.g. fully connected crossbar switches, hardened cabling, and hardware timestamping of packets). Hard real-time versions became available and are used. Ethernet offers many benefits over other existing solutions. For example, 10 Gbps Ethernet offers bandwidth that is almost 1000x faster than other traditional fieldbus networks.

### 3) De facto standards

---

<sup>1</sup> [en.wikipedia.org/wiki/Manufacturing\\_Automation\\_Protocol](https://en.wikipedia.org/wiki/Manufacturing_Automation_Protocol)



# STORY

Formal standards consistently underperform relative to de facto standards. E.g. REST will outperform, concerning development effort and time, so-called formally standardised alternatives (e.g. SOAP, RPC, CORBA, WSDL, and UDDI). Critical user mass within the software/system developers communities is decisive, not the number of large companies and organisation expressing / enforcing a (formal) standard.

The purpose of this deliverable is two-fold: Firstly, this deliverable strives to provide an overview of the communication standards and technologies that could be used specifically in the STORY project demonstrations. The focus of the study is on the coverage and operations of the different parts of the smart grids related to energy storages. Secondly, this deliverable presents the requirements for the STORY communication gateway. The project consortium will design and develop a gateway device to be used as part of each demonstration site. The gateway will be responsible for relaying data and control signals within demonstration sites, and for providing data security and privacy. It will also provide remote control capability and the ability to send and store demonstration data to the STORY cloud server for further analysis.

Extensive analysis of smart grid standards has been done in the past by numerous projects. One noteworthy effort in this regard was the STARGRID<sup>2</sup> project, supported by the 7<sup>th</sup> framework programme of the European Commission. Among the outcomes of the project were six recommendations regarding the standardisation process addressed to policy makers, regulation authorities (EU and national), industry and standardisation bodies. The final report of the STARGRID project was released in early 2015. As the STARGRID project was very thorough in their work, this deliverable is not meant to duplicate that work. Another notable European project was the FINSENY<sup>3</sup> project. In the FINSENY project, key actors from the ICT and energy sectors teamed-up to identify the ICT requirements of Smart Energy Systems. This leads to the definition of new solutions and standards, which were verified in a large scale pan-European Smart Energy trial. As part of the FI-PPP programme, FINSENY analysed energy-specific requirements and developed solutions to address these requirements.

The purpose of this deliverable is to look at communication standards and technologies most applicable for the STORY project demonstrations. In addition, this deliverable aims to give the reader a blueprint on how to replicate the data communication in STORY demonstrations.

Partners' contributions for the deliverable are:

- VTT Technical Research Centre of Finland (VTT) was the editor of the deliverable. Contributions include general communication network information for a modern electricity grid and smart grid standard and framework research.
- Actility (ACT) contributions include relevant smart grid standards, Wide Area Network (WAN) technologies and M2M protocols.
- UCLL Leuven (UCL) contributions consist of information about relevant communication protocols for the STORY project and premise area network technologies.

---

<sup>2</sup> <http://stargrid.eu>

<sup>3</sup> <http://www.fi-ppp-finseny.eu>





# STORY

- Joanneum Research (JR) contributions include the security and privacy chapter. In addition, JR was in charge of collecting the STORY communication gateway requirements and information about the specific characteristics of each demonstration site.
- University of Ljubljana (UL) contributed to the communication gateway requirements and provided information about the demonstration site setups.
- BaseN (BASN) contributed by providing expert information for the communication gateway requirements and to the demonstration site setups.
- In addition, all partners contributed to the STORY communication gateway requirements and collected information about the specific characteristics of each demonstration site.

The deliverable is organized in the following manner. Chapter 3 presents the smart grid standards and a general overview of the communication network types applicable to the STORY project demonstrations. Chapter 4 presents the candidate premise area network technologies. Chapter 5 presents the candidate Wide Area Network technologies. Chapter 6 presents the upcoming M2M standards or protocols and places them in a smart grid context. Chapter 7 discusses the security and privacy concerns in smart grids. Chapter 8 presents the STORY communication gateway requirements and the specific characteristics of demonstrations sites. Chapter 9 contains the conclusions of the deliverable.



### 3 Smart Grid Communication

---

A communication system can be abstracted using different levels. For communication systems, the most common level distribution is based on ISO standardized OSI (Open Systems Interconnection) model that originally contained seven different layers: physical, data link, network, transport, presentation, session, and application layer. For smart grid systems it is important to be able to model also other levels than just ICT related levels. These are the electricity grid related levels such as customer premises, DER, distribution, transmission and (bulk) generation. These levels are modelled with various architectures of which the most important are the SGAM (Smart Grid Architecture Model) and the SGCM (Smart Grid Conceptual Model), which will be discussed in the following chapter. The components and devices are also important as are the upper level communication technologies and information models, and finally towards the abstraction of the relations of different businesses and even markets. A common way in smart grid research is to divide communication networks into parts based on their application location. Typical communication network types are a Home (or premise) Area Networks (HAN), Field Area Networks (FAN), and Wide Area Networks (WAN). Different fixed, wireless, and mobile technologies can be applied for these.

In this chapter we will first present the most important smart grid standardisation efforts by various groups and then present the relevant standards for the STORY project. After this we will discuss how the communication networks in the STORY demonstration sites can be organized. The chapter concludes with an introduction to higher layer communication protocols for smart grid applications.

#### 3.1 Standards & Standardisation Groups

---

There are many applications, techniques and technological solutions for smart grid systems that have been developed or are still in the development phase. The key challenge is that the overall smart grid system is lacking widely accepted standards and this situation prevents the integration of advanced applications, smart meters, smart devices, and renewable energy sources and limits the interoperability between them. In fact, each metering company is using their own protocol and as most local area installations are relatively small, they do not have the financial incentives to push for a unified standard. However, the adoption of interoperability standards for the overall system is a critical prerequisite for making the smart grid system a reality. Seamless interoperability, robust information security, increased safety of new products and systems, compact set of protocols and communication exchange are some of the objectives that can be achieved with smart grid standardization efforts. There are many regional and national attempts towards achieving this goal. For example, the European Union Technology Platform organization's strategic energy technology plan is all about the development of a smart electricity system over the next 30 years. Also, Ontario Energy Board, Canada, has committed itself towards the completion of a smart meter installation. On the other hand, National Institute of Standards and Technology (NIST), the American National Standards Institute (ANSI), the International Electro technical Commission (IEC), the Institute of Electrical



# STORY

and Electronics Engineers (IEEE), the International Organization for Standardization (ISO), the International Telecommunication Union (ITU), the Internet Engineering Task Force (IETF), the Third Generation Partnership Project (3GPP) and on the regional level, the Korean Agency for Technology and Standards (KATS), and Joint Information Systems Committee (JISC) are the recognized standard development organizations that are noteworthy. In addition, CEN, CENELEC, and ETSI have formed a joint working group, called the Smart Grid Coordination Group (SG-CG), for smart grid standardization efforts and aim to achieve the European Commission's policy objectives regarding the smart grid. Their efforts focus on smart metering functionalities and communication interfaces for electric, water and heat sectors in Europe.

Some of the aforementioned organizations have developed architectural and conceptual models used in planning, evaluating and monitoring the progress of transforming the traditional electricity grid into the smart grid. Two popular models are the Smart Grid Conceptual Model (SGCM) formalized by the Smart Grid Interoperability Panel (SGIP) and the Smart Grid Architecture Model (SGAM) formalized by the CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG). SGIP is a consortium initiated by NIST to support in the coordination of standards development for the smart grid.

The SGCM [6] is a set of views (diagrams) and descriptions that are the basis for discussing the characteristics, uses, behaviour, interfaces, requirements and standards of the smart grid. The top level domains of the conceptual model are customers, markets, service providers, operations, bulk generation, transmission and distribution.

The SGAM [1] is a reference model to analyse and visualize smart grid use cases in a technology-neutral manner. It is divided into a three dimensional view with three axes: domains, zones, and interoperability layers. The SG-CG used the NIST Smart Grid Conceptual Model and the GWAC (GridWise Architecture Council) stack as a starting point and added a third dimension called zones to create the Smart Grid Architecture Model [7]. The GWAC stack consists of eight layers, which comprise a vertical cross-section of the degrees of interoperation necessary to enable various interactions on the smart grid [8]. An introduction to the SGAM is presented in the appendices (chapter 12.1).

An overview of the most relevant standards for the smart grid is given in paper [9] and is briefly reviewed here. The standards can be categorized into the following categories where for each category the most relevant are mentioned. A more detailed explanation of the use cases for these standards can be found in Table 1.

- Revenue Metering Information model
  - ANSI C12.19
  - M-Bus
  - ANSI C12.18
- Building Automation
  - BACnet
  - Others: KNX, Modbus, LonWorks, ZigBee



- Substation Automation
  - IEC 61850
- Powerline Networking
  - HomePlug
  - HomePlug Green PHY
  - PRIME
  - G3-PLC
- Home Area Network Device Communication Measurement and Control
  - U-SNAP
  - IEEE P1901
  - Z-Wave
- Application-level Energy Measurement System
  - IEC 61970 and IEC 61968 (especially IEC 61968-9 standard on meter reading & control)
  - OpenADR
  - DLMS/COSEM
- Inter-Control and Interoperability Center Communications
  - IEEE P2030
  - ANSI C12.22
  - ISA 100.11a
  - ITU-T G.9955 and G.9956
- Cyber Security
  - IEC 62351
- Other notable standards
  - OPC-UA
  - CAN
  - Profibus

There are also a lot of smart grid extension related actions for building automation related standards, e.g. BACnet<sup>4,5</sup> and ZigBee<sup>6,7</sup>.

Individual companies doing the overall installations are also using a method, where individual local devices use the abovementioned old protocols and access is via a local server providing SOAP/Webservice/HTTP+Rest interface.

<sup>4</sup> <http://www.bacnet.org/WG/SG/>

<sup>5</sup> <http://www.bacnet.org/WG/SG/> , <http://www.bacnet.org/WG/XML/>

<sup>6</sup> <http://www.zigbee.org/zigbee-for-developers/applicationstandards/zigbeesmartenergy/>

<sup>7</sup> <http://greentechadvocates.com/2013/04/04/zigbee-ip-smart-grid-meet-the-internet-of-things/>

**Table 1. Use cases for selected smart grid standards [9].**

Type/Name of Standards	Details	Application
<b>IEC 61970 and IEC 61969</b>	Providing Common Information Model (CIM): IEC 61970 works in the transmission domain and IEC 61969 works in the distribution domain	Energy management systems
<b>IEC61850</b>	Flexible, future proofing, open standard, communication between devices in transmission, distribution and substation automation systems	Substation Automation
<b>IEC 60870-6 /TASE.2</b>	Data exchange between utility control centers, utilities, power pools, regional control centers	Inter-control center communications
<b>IEC 62351 Parts 1-8</b>	Defining cyber security for the communication protocols	Information Security Systems
<b>IEEE P2030</b>	A Guide for smart grid inter-operability of energy technology and IT operation with the electric power system (EPS)	Customer-side applications
<b>IEEE P1901</b>	High speed power line communications	In-home multimedia, utility and smart grid applications
<b>ITU-T G.9955 and G.9956</b>	ITU-T G.9955 and G.9956 contain the physical layer specification and the data link layer specification	Distribution Automation, AMI
<b>OpenADR</b>	Dynamic pricing, Demand Response	Price Responsive and Load Control
<b>BACnet</b>	Scalable system communications at customer side	Building automation
<b>HomePlug</b>	Powerline technology to connect the smart appliances to HAN	HAN
<b>HomePlug Green PHY</b>	Specification developed as a low power, cost-optimized power line networking specification standard for smart grid applications	HAN
<b>U-SNAP</b>	Providing many communication protocols to connect HAN devices to smart meters	HAN
<b>ISA100.11a</b>	Open standard for wireless systems	Industrial Automation
<b>SAE J2293</b>	Standard for the electrical energy transfer from electric utility to EVs	Electric Vehicle Supply Equipment
<b>ANSI C12.22</b>	Data network communications are supported and C12.19 tables are transported	AMI
<b>ANSI C12.18</b>	Data structures transportation via the infrared optical port han	AMI
<b>ANSI C12.19</b>	Flexible metering model for common data structures and industry "vocabulary" for meter data communications	AMI
<b>Z-Wave</b>	Alternative solution to ZigBee that handles the interference with 802.11/b/g	HAN
<b>M-Bus</b>	European standard and providing the requirements for remotely reading all kinds of utility meters	AMI
<b>PRIME</b>	Open, global standard for multi-vendor interoperability	AMI
<b>G3-PLC</b>	Providing interoperability, cyber security, and robustness	AMI
<b>SAE J2836</b>	Supporting use cases for plug-in electric vehicles communication	Electric Vehicle
<b>SAE J2847</b>	Supports communication messages between PEVs and grid components	Electric Vehicle

## 3.2 Communication Networks in STORY

According to the SG-CG First Set of Standards [15], the following communication network types are defined for smart grids depending on the target application:

- **Subscriber Access Network**
- Neighbourhood Network
- **Field Area Network**
- Low-end Intra-substation Network
- Intra-substation Network
- Inter Substation Network
- Intra-Control Centre / Intra-Data Centre Network
- Enterprise Network

# STORY

- Balancing Network
- Interchange Network
- Trans-Regional / Trans-National Network
- **Wide and Metropolitan Area Network**
- Industrial Fieldbus Area Network

To avoid redundancy and minimize complexity we have selected three types from the above list to describe the communication networks at STORY demonstration sites. These are:

- Home Area Network (HAN), also called a Premises Area Network or a Subscriber Access Network
- Field Area Network (FAN), also called a Neighbourhood Area Network (NAN)
- Wide Area Network (WAN)

Figure 1 depicts the minimum requirements for the three network types, so that they can be considered applicable for the smart grid environment.

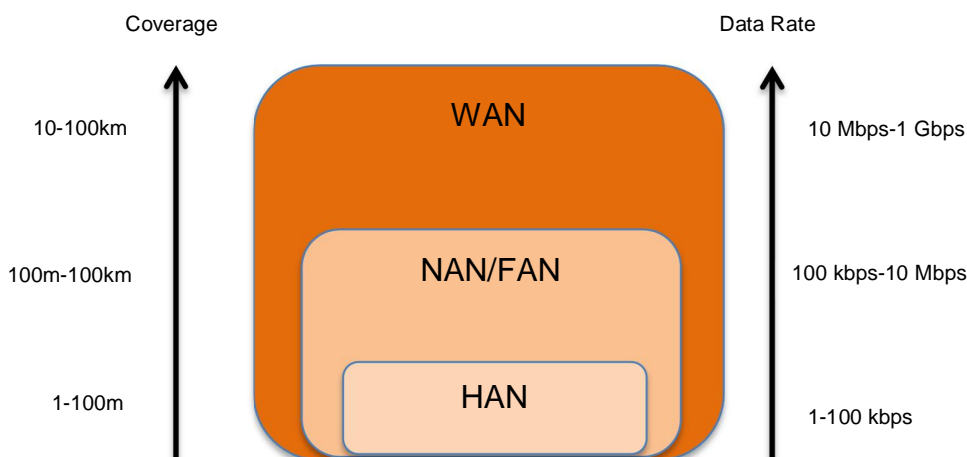







Figure 1. Coverage and data rate requirements for HAN, FAN and WAN networks [14].

Certain protocols do not always fit into abovementioned network types. For example, BACnet and OPC-UA are usually utilized in local networks but their coverage can be extended using Internet Protocol or virtual private network technologies.

Figure 2 depicts the STORY demonstration site communication network domains. Also in the figure are the SGAM and SGCM domains. Note that the SGAM and SGCM domains are not in a hierarchical order; the domains have electric or communication flows to several domains. On the right hand side of the figure are some example devices or entities that are or could be a member in the corresponding STORY domain. In the demonstrations, the WAN is usually the largest intra site network. WAN is connected to the STORY communication gateway, which arbitrates the uplink/downlink traffic to the enterprise and external network domains. Some sites have a legacy network run by the local DSO, which is depicted in Figure 2 as enterprise domain. The external domain is the Internet in all demonstrations.

# STORY

STORY Demonstration Domains	SGAM Domains	SGCM Domains	Example members
 External	(Bulk) Generation	Markets Service Providers	Retailers, Aggregators, Regulators, Providers
 Enterprise	Transmission	Bulk Generation Operations	MDMS, CIS/Billing, OMS, WMS, EMS/DMS
 WAN	Distribution	Transmission	Routers, Towers, Repeaters, Ground stations, Data aggregator unit
 FAN	DER	Distribution	Relays, Modems, Bridges, Access points
 HAN	Customer Premises (possibly incl. DER)	Customer	Thermostats, PCs, Smart meters, Field tools, Building automation(HEMS), Power generation, Power converters, Wattmeters

**Figure 2. Communication network hierarchy in STORY demonstration sites (left), SGAM domains, SGCM domains and example members.**

Figure 3 depicts the communication networks of STORY demonstration sites on a general level. Due to the different scale of demonstrations, not all sites need to have all three network layers (HAN, FAN & WAN) present. Common entities for all demonstrations are the STORY gateway device, energy storage device and a WAN network.

Figure 4 contains the demonstration sites of the STORY project. Demonstration site communication networks will be connected to the Internet via the STORY gateway device. This gives the opportunity to, for example, upload demonstration data to the central STORY database maintained by BaseN for further analysis. The data consists of e.g. measurements, faults, warnings, acknowledgements and control signals. The STORY gateway requirements are described in chapter 8.

# STORY

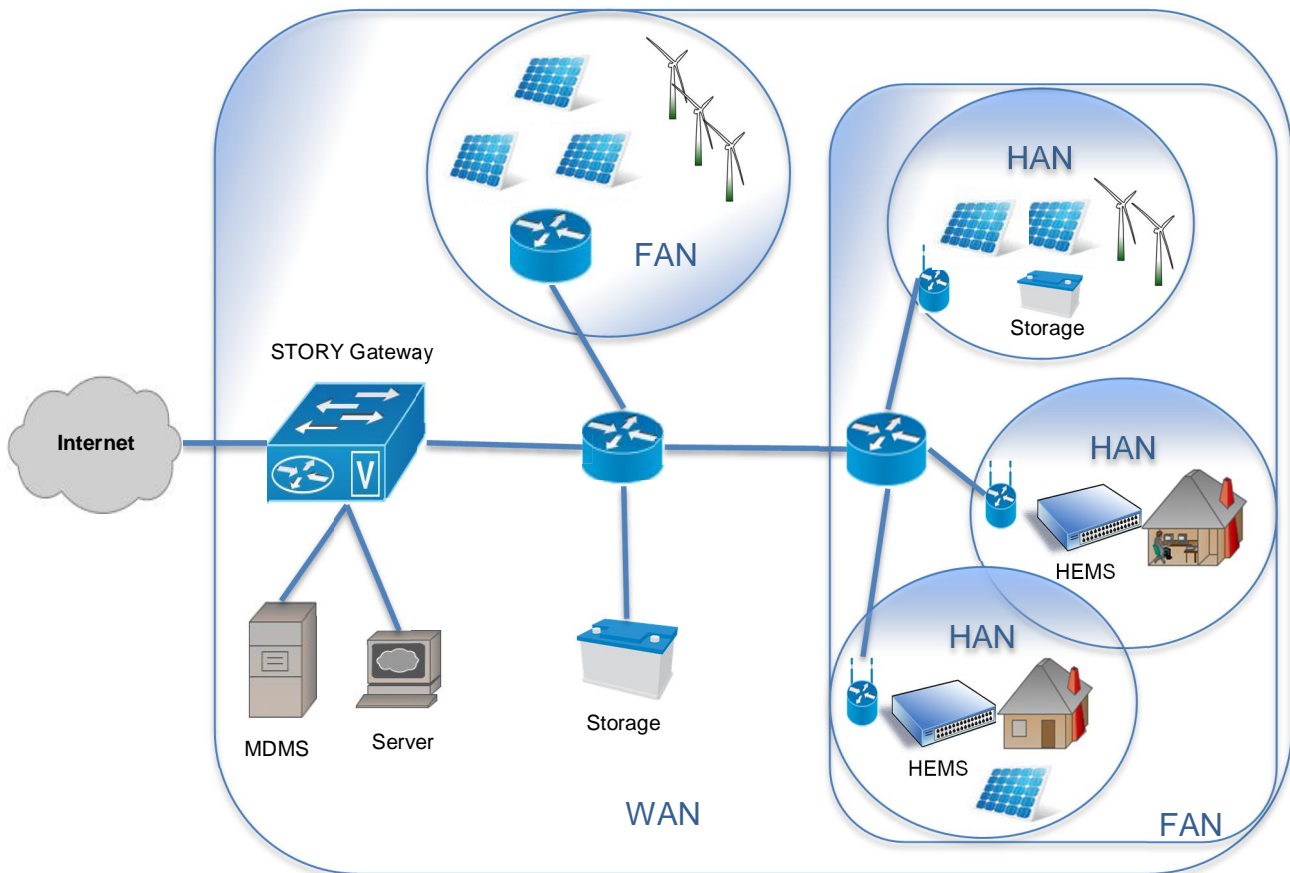


Figure 3. Overview of communication networks in demonstration sites.

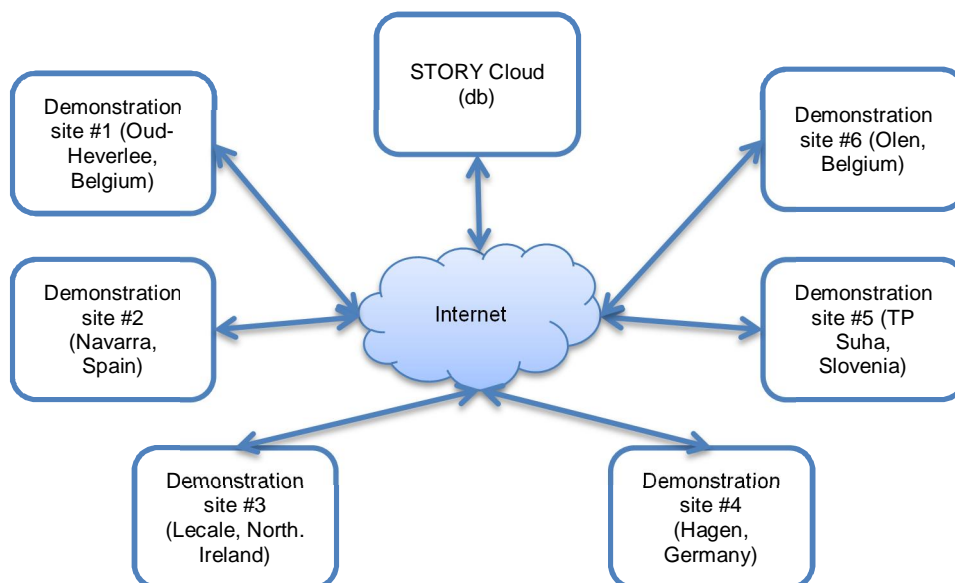


Figure 4. STORY demonstration sites.

Next three sub-chapters explain the HAN, FAN and WAN network types on a bit more detailed level. Chapters 4 and 5 discuss specific technologies and protocols pertaining to the STORY demonstration sites.

### **3.2.1 Home Area Network (HAN)**

A HAN (also referred to as a premise area network in this deliverable) is the smallest subsystem in the hierarchical chain of the smart grid [5]. HAN provides a dedicated demand-side management (DSM), including energy efficiency management and demand response by proactive involvement of power users and consumers. In STORY, HAN may also include industrial area and generation devices in some demonstration cases. The communication technologies discussed in this deliverable take no notice on the kind of data they are transmitting – whether it is generation or load data. HAN, in a residential setting, typically consists of smart devices with sensors and actuators, in-home displays, smart meters, and home energy-management systems (HEMS).

The HAN communicates with different smart devices using wired technologies including power-line communication (PLC), or BACnet protocol, and wireless technologies (e.g. Wi-Fi, and ZigBee). Wireless technology such as ZigBee is becoming a popular choice in contrast to wired technology due to its low installation cost and better control and flexibility. The term ZigBee is a registered trademark of the ZigBee Alliance. The relationship between IEEE 802.15.4 and ZigBee Alliance is similar to that between IEEE 802.11 and the Wi-Fi Alliance. They have published several application profiles applicable for smart grid development dealing with home automation (e.g. ZigBee Home Automation 1.2 and Smart Energy 1.1b), and automation (e.g. Building Automation 1.0). There are a number of interesting specifications under development. For example the ZigBee Smart Energy 2.0 specifications define an IP-based protocol to monitor, control, inform and automate the delivery and use of energy and water. Added services for the 2.0 version include plug-in electric vehicle (PEV) charging, installation, configuration, load control, demand response and application profile interfaces for wired and wireless networks.

HANs provide a general broadband access (including but not limited to the Internet) for the customer premises (homes, building, facilities). They are usually not part of the utility infrastructure and provided by communication service providers, but can be used to provide communication service for smart grid systems covering the customer premises like Smart Metering and Aggregated prosumers management [15].

Chapter 4.1 discusses HAN communication in the STORY project in more detail.

### **3.2.2 Field Area Network (FAN)**

FANs operate at the distribution level upper tier, which is a multi-services tier that integrates the various sub layer networks and provides backhaul connectivity in two ways: directly back to control centres via the WAN or directly to primary substations to facilitate substation level

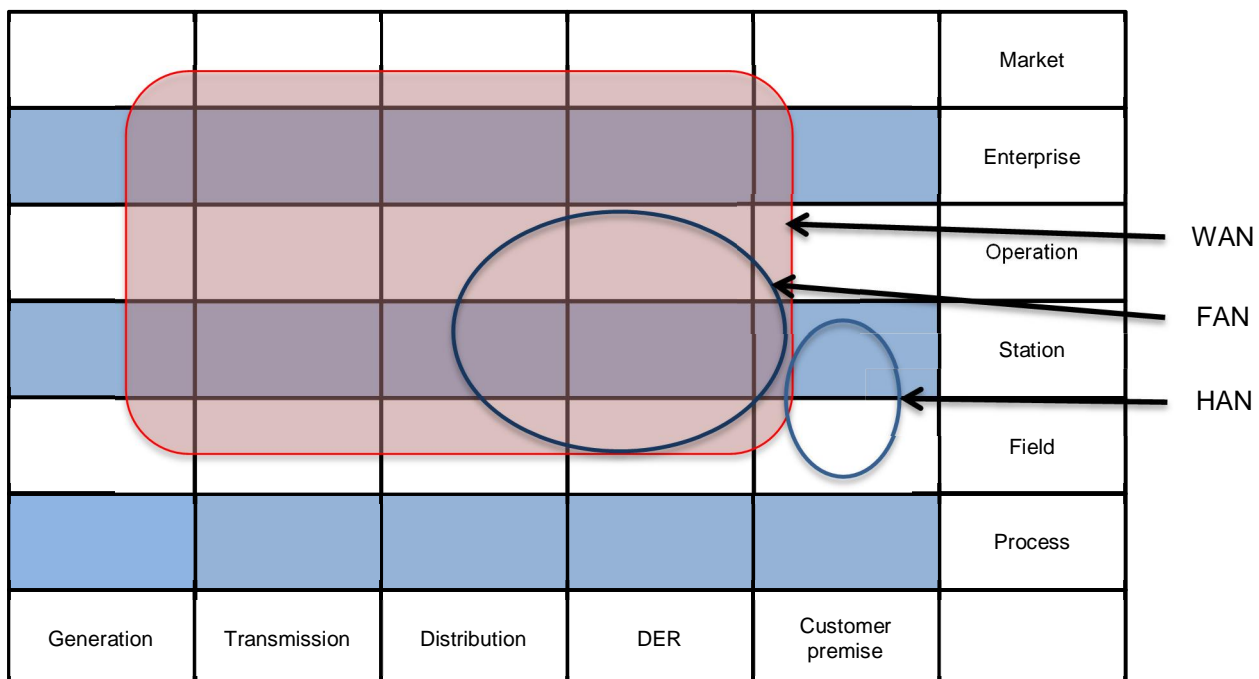
distributed intelligence. It also provides peer-to-peer connectivity or hub and spoke connectivity for distributed intelligence in the distribution level [15].

A Field Area Network fills the communication gap between the core Internet Protocol (IP) network and devices, as well as personnel, in the field. FANs are implemented most often with wireless networking technologies because of their large geographic coverage areas, many connected devices and the need to support mobile field-workers. If a wired network is preferred then fibre optic technology is a viable option, if the scale and economic realities are also taken into consideration.

Wireless networking technologies used in FANs include cellular, narrowband point-to-multipoint (PTMP), broadband PTMP and broadband wireless mesh networks.

### 3.2.3 Wide Area Networks (WAN)

A WAN is a data communication network that covers a relatively broad geographical area and that often uses transmission facilities provided by common carriers, such as telephone companies. It may be limited to an enterprise or an organization or it may be accessible to the public. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer. The main difference between WAN and LAN technology is scalability.



**Figure 5. Mapping of HAN, FAN & WAN networks on SGAM. Note: figure is according to SG-CG report guidelines [15] and is not meant to represent all STORY case studies.**

In a smart grid, a WAN can be used to connect multiple distribution systems together and act as a bridge between FANs, HANs and the utility network. WAN provides a backhaul for connecting



# STORY

the utility company to the customer premises. In this case, a backhaul can adopt a variety of technologies (e.g. Ethernet, cellular network, or broadband access) to transfer the information extracted from the HAN or FAN to the utility local offices.

A WAN gateway can use broadband connection or possibly an IP-based network (e.g. MPLS and DNP3.0) to provide an access for the utility offices to collect the required data [5]. A WAN can also be used to directly connect smart grid components without passing through a HAN or a FAN and still enable access to the same type of devices. Such a solution can provide easy implementation of new components and good scalability while the feasibility depends on the smart grid application. When the amount of traffic is low and latency requirements are not very strict, a LoRaWAN network could be used. This way, there is no need to install and maintain a HAN or FAN network. Figure 5 depicts the three network types mapped on SGAM (a modified figure from a SG-CG report [15]). Notice that the figure is according to SGAM guidelines and it is not meant to represent every communication network located in STORY demonstration sites. For example, in some demonstration sites, the HAN extends to the DER domain and in others it does not. Chapter 5 discusses candidate STORY WAN technologies in more detail. Table 2 provides selected communication standards in reference to their applicability as HAN, FAN or WAN networks.

**Table 2. HAN, FAN and WAN communication standards.**

	HAN	FAN	WAN
Narrowband PLC (med. & low voltage)	X	X	
Broadband PLC	X		
BACnet	X		
LonWorks	X		
KNX	X		
Modbus	X	X	
DNP3.0	X		X
CAN	X		
OPC-UA	X	X	
Profibus	X	X	
EN 14908		X	
EN 50090		X	
IEEE 802.15.4	X	X	
IEEE 802.11	X		
IEEE 802.16	X	X	
ETSI TS 102 887		X	
IPv4	X	X	X
IPv6	X	X	X
RPL / 6LoWPAN	X	X	
IEC 61850		X	X
IEC 60870-5			X

GSM/GPRS/EDGE	X		X
3G/WCDMA/UMTS/HSPA	X		X
LTE/LTE-A	X	X	X
SDH/OTN	X	X	X
IP MPLS/MPLS TP	X	X	X
DSL/PON	X		X
LPWAN			X
Satellite			X
ETSI M2M	X		X

### 3.3 Higher Layer Communication Protocols

Smart grid applications and standards rely heavily on Web Services for the higher layers protocols. Web Services are defined to be the methods to communicate between applications over communication networks, generally IP based. Two major classes of Web Services can be distinguished [15]:

- **RESTful Web Services (Representational State Transfer):** applications are fully defined via representations (e.g. XML) of resources that can be manipulated using a uniform interface that is composed of four basic interactions, i.e. CREATE, READ, UPDATE and DELETE. Each of these operations is composed of request and response messages. The most common implementation of REST is HTTP, whereby the REST operations are mapped into the HTTP methods: CREATE is mapped on HTTP POST, READ on HTTP GET, UPDATE on HTTP PUT, and DELETE on HTTP DELETE. However, other implementations are possible: CoAP (Constrained Application Protocol), XMPP (Extensible Messaging and Presence Protocol), etc. REST is a lightweight alternative to mechanisms like SOAP, RPC, WSDL, and CORBA.
- **SOAP/RPC based Web Services:** applications expose interfaces that are described in machine processable format, the Web Service Description Language (WSDL). It is also possible for applications to interact through SOAP interfaces which provide a means to describe message format. These message are often transported over HTTP and encoded using XML.

## 4 Intra Level Communication Inside Operations

---

In STORY, existing and forthcoming equipment will be integrated into smart storage-centric installations. In other words, the project employs<sup>8</sup> (does not develop) this equipment. Therefore, it needs to cope with the existing and forthcoming smart grid reality while preparing for upcoming solutions – which are being developed elsewhere.

Importantly in view of the effective replicability of its solutions, STORY aims to avoid/minimize the ‘lock-in’ into legacy technologies that have issues in coping with current and future requirements. The unavoidable embedding of such legacy technologies (cf. below) needs to occur in manners that contain it, make it easy-to-replace, and block/counter any viral effects (i.e. induce to prefer it over more future-proof alternatives when expanding, upgrading, etc.).

Communication inside operations – from equipment toward the gateways providing access beyond the firewalls – has to account for the constraints, limitations and options offered by the equipment, which is available on the market and/or was already installed (possibly years ago).

For years to come, legacy communication technologies will remain a fact of life simply because of the installed base. In addition, equipment providers will serve existing markets first, if only because the necessary expertise is available, reputation/branding ensures customer confidence in the technology. In other words, the lowest layer in communications will include a significant portion of legacy technology simply because the selection of equipment is rarely decided by its communication technology but rather by energy and cost/price as well as reputation of the brand, familiarity, training, etc.

Typical shortcomings of legacy communication technologies are:

- Closed/own system model, e.g. having installation-specific addressing (i.e. not using IP). Note that it does not matter whether it is standardized or proprietary; closed means that it lacks the capabilities of IPv6. Containment strategies include:
  - Embed (many) small installations in an IP-based environment.
  - Keep the small installations choice-lean (to ensure low s/w maintenance).
- Security typically is addressed poorly (or not at all) in technologies that were developed when security was not an issue and efficiency was a primary concern. Containment strategies include:
  - Build a firewall around it, providing access solely through a limited number of gateways providing security.
  - Refrain from buying/using hardware from lesser-known sources. Only use equipment from providers that have the resources to address any security issues when they emerge (i.e. replace firmware, equipment) and that have a self-interest

---

<sup>8</sup> It is good practice to address only a single ‘stage’ in any given development activity. STORY therefore uses existing and forthcoming equipment and does not develop some next-gen equipment. Moreover, STORY uses and supports standards where opportune; it does not contribute to still-to-be-standards nor does it employ non-contributing or non-competitive standards (e.g. too complex for a limited value-adding potential).

in doing so (i.e. preserve the value of their brand/reputation). Indeed, the security attack may originate from firmware inside a sensor, actuator, etc.

- Install (all) the available security upgrades, add-ons, etc.
- Reliability can be substandard in (very) old equipment (e.g. RS232C). Containment strategies include:
  - Replace when possible by a more legacy technology (e.g. RS485).
  - Keep communication distances small/optimal. This reduces the chances of undetected errors.
  - Keep sources of errors away (stable power supply, shielding, etc.).
  - Add redundancy and error checking at a higher level.

The next section depicts the communication technologies and standards that are of interest in this context.

## 4.1 Premises Area Networking Technologies

---

Firstly, there exists a range of communication technologies distinguished by the manner in which data is transmitted. Applications may use dedicated communication wiring (e.g. Ethernet or serial communication links), powerline communication (cf. 6.1) or wireless communication. As stated above, the choice of communication mechanisms toward the devices, sensors and actuators will be constrained by the (energy) application and much less by ICT concerns.

Future-proof installations keep the niche technologies limited to small choice-lean implementations that are connected to an IPv6 solution in which the smart parts of the application reside. This will minimize the future need for software maintenance in these niche technologies (i.e. only when the connected hardware changes).

Among the above three categories, wireless technologies are of interest in this section on premises area networking because there is no “one size fits” all. Of interest are:

- NFC (Near Field Communication; [nfc-forum.org](http://nfc-forum.org)). This is an extremely short range technology (<10 cm, 100-420 kbps) aimed at ensuring security. Its niche is to provide contactless communication requiring strong prevention of intrusion (by means of its short range). It is widely supported on (recent designs of) smart phones and other portable equipment.
- Bluetooth 4.2, especially BLE (Bluetooth Low Power). This is a modest range technology (50+ m, 1Mbps) again widely supported on smart phones, tablets, portable computers.
- Wi-Fi is the de facto standard in wireless networking (50+ m, 150-600 Mbps). Widely supported on portable computers, tablets, smart phones, etc.
- ZigBee is an industry-standard (10-100 m, 250 kbps) offering advantages in low power operations. ZigBee also covers higher layers in the protocol stack (competing with Thread, the technology in Nest products). ZigBee is one of the main examples of a HAN network.
- Z-Wave (30 m, 9.6/40/100 kbps) is a low-power technology commonly used in home automation (e.g. lamp controllers). Simple and fast compared to other technologies.



# STORY

- LoRaWAN, SigFox, Neul, Weightless (multiple kilometres) are recent developments aiming at long range, low power, and low data rate communications for the Internet of things. Data rates range from a few bps to 50 kbps, depending on the density of the base station network. These are state-of-the-art technologies (security, reliability). User communities are emerging (too early to know which ones will succeed in attraction large numbers of users) but they have decisive advantages over established technologies; some will become widely available and used. The main advantage of these technologies is that they can make HAN obsolete for some smart grid cases and their high *plug-and-play* value.
- Cellular technologies (GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G)) offer longer range and higher data rates but at the expense of power consumption, subscription fees and hassle (i.e. internal discussion within a user organization to decide what services to acquire, paid from which budgets).

As said, the choice among the above depends often on other factors than the communication technology itself. Test cases start from e.g. existing installations and need/want to use equipment offering limited choices. Moreover, the less established technologies require adequate levels of expertise. In the STORY consortium, LoRaWAN (and oneM2M discussed below) enjoy this availability of knowhow. Its competitors are not in a position to be deployed in our test cases until they become more established and widely available/used.

Secondly, there exist a significant number of legacy technologies in the smart grid, both on industrial sites (often using SCADA systems and programmable logic controllers) and home automation (also using simple programmable logic controller but increasingly mainstream computers, often ARM-based favouring EU technology). In view of replicability for the STORY solutions, employing such legacy technologies is not considered a positive contribution but rather accounting for real-world constraints. Therefore, the discussion focuses on technologies that are present in one or more test cases.

In the home case in Oud-Heverlee (B), KNX is used. KNX is a protocol that is a convergence of three older standards, based on the communication stack of EIB (European Installation Bus) and supports multiple physical communication media (twisted pair wiring, powerline, radio, infrared and Ethernet). With native KNX support to ETSI TR 102 966, a REST API provides full access to the entire KNX ecosystem compliant with ETSI M2M. The 12 other houses in the neighbourhood are connected to the smart grid using LoRaWAN.

In industrial settings, Modbus and DNP3.0 is used. Modbus was designed in the late 1970s to communicate to programmable logic controllers. Versions exist for serial communication and Ethernet. The protocol itself provides little security. DNP3.0 is a protocol designed for usage in SCADA systems. Designed to be reliable, security features have been added to make it compliant with IEC 62351. DNP3.0 is a more recent design than Modbus, providing superior features but it is more complex.

In addition, other legacy technologies – BACnet, LonWorks, and ZigBee – exist. However, the purpose of this manuscript is to support developing future-proof installations while accounting





# STORY

for legacy as it presents itself. In-depth discussion of legacy technology not encountered in any test case is therefore out of scope.

Thirdly, the Internet of things and smart grid research and development have proposed and produced technologies that cope with hyper connectivity (IPv6) and are state-of-the-art software (REST). These developments have improved upon the internet by shedding/replacing a multitude of features that made the ordinary internet bloated and resource-hungry. For instance, for the following Internet technologies (on the left) more efficient counterparts have been developed:

HTTP	CoAP
TLS	DTLS
TCP	UDP
IPv6	6LoWPAN (cf. IEEE 802.15.4)

The OMA Lightweight M2M combines the above (supporting SMS next to UDP) to deliver services benefitting from lessons learned and knowhow acquired in the mobile communications industry. It provides banking class security, object and resource models. Lookup functionality for these objects and device management are defined. It is applicable to IP based devices and networks. Integration with ETSI M2M and support for oneM2M are planned.

CoAP, the Constrained Application Protocol from the CoRE (Constrained Resource Environments) IETF group is a document transfer protocol similar to HTTP. CoAP runs over UDP. Clients and servers communicate through connectionless datagrams. Retries and reordering are implemented in the application stack. CoAP follows a client/server model. Clients may GET, PUT, POST and DELETE resources (i.e. REST). CoAP is designed to interoperate with HTTP and the RESTful web using simple proxies. Because CoAP is datagram based, it may be used on top of packet based communications protocols such as SMS.

As CoAP is built on top of UDP, DTLS – Datagram Transport Layer Security – provides the assurances of TLS for transfers of data over UDP. Typically, DTLS capable CoAP devices will support RSA and AES or ECC and AES. In CoAP, a sensor node is typically a server, not a client (though it may be both). The sensor (or actuator) provides resources which can be accessed by clients to read or alter the state of the sensor.

An alternative protocol for small devices is MQTT. MQTT is a publish/subscribe messaging protocol. Every sensor is a client and connects to a server, known as a broker, over TCP. Messages are published to an address (a topic) and clients subscribe to (multiple) topics. It is less suited for very constrained devices, among other because it uses TCP/TLS instead of UDP/DTLS.

Fourthly, there are internet technologies that are relevant in view of a sustainable replicability of STORY developments. RESTful HTTP has become a de facto standard used in many





# STORY

applications. WS\* alternatives <sup>9</sup> cannot compete, especially in resource constrained environments. An upcoming technology is WebSockets (HTML5) allowing for two-way communication with a remote host (avoiding the need for work-arounds like long-polling); its adaptation remains an open issue today.

Next to the above relatively simple (= good) technologies, comprehensive middleware developments are ongoing (e.g. FI-WARE, AllSeen Alliance, etc.) which may become relevant when sufficient mature implementations become available. In view of the complexity of these developments, early adoption is not recommended. ETSI M2M, oneM2M enjoys expertise within the consortium and will take up responsibilities in this respect.

Finally, several standardization efforts aim at modelling from an energy/electrical/semantic perspective. In the power grid domain, EIC CIM (Common Information Model), IEC 61850, IEC 61970 and IEC 61968 standardize data representation in power grids. However, they originally focused on grid-internal matters. Other standardization bodies are active in adding application-aware semantic elements to their repertoire. This is work-in-progress and it is early days for the application of such standards (when it entails additional effort). In general, applications and test cases will not risk much whenever they stay to facts and elements that are necessary. Whenever some arbitrariness enters into a design (e.g. a performance indicator is a weighted sum), compliance with standards becomes relevant for future replicability and interoperability.

---

<sup>9</sup> <http://www.w3.org>



## 5 Wide Area Network Technologies

Within the smart grid context and thus STORY, WAN are used to communicate data and control actions over large distances. WANs allow for multiple components to be connected to the same gateway and are often easily scalable. Three main types of WAN exist: Wireless Broadband, Power Line Communication (PLC) and the more recent Low Power WANs (LPWAN).

### 5.1 Wireless Broadband

An overview of the characteristics of the most common wireless Broadband Wide Area Networks technologies is given in Table 3.

Table 3. Wireless broadband technologies.

	Down/Upstream Rate	Efficiency Range	Suitability	Future of the technology
<b>LTE</b>	100/30 Mbps	3-6 km	<ul style="list-style-type: none"> <li>• Coverage of remote areas</li> <li>• Quickly and easily implementable</li> <li>• Shared medium</li> <li>• Limited frequencies</li> </ul>	<ul style="list-style-type: none"> <li>• Commercial deployment of new standards with additional features (5G) and provision of more frequency spectrum blocks (490-700 MHz)</li> <li>• Meets future needs of mobility and bandwidth accessing NGA-Services</li> </ul>
<b>HSPA</b>	42.2 / 5.76 Mbps	3 km		
<b>Satellite</b>	20/6 Mbps	High	<ul style="list-style-type: none"> <li>• Coverage of remote areas</li> <li>• Quickly and easily implementable</li> <li>• Run time latency</li> <li>• Asymmetrically</li> </ul>	<ul style="list-style-type: none"> <li>• 30Mbps by 2020 based on next generation of high-throughput satellites</li> </ul>
<b>Wi-Fi</b>	300/300 Mbps	300 m	<ul style="list-style-type: none"> <li>• Inexpensive and proven</li> <li>• Quickly and easily implementable</li> <li>• Small efficiency range</li> <li>• Shared medium</li> </ul>	<ul style="list-style-type: none"> <li>• Increased use of hotspots at central places</li> <li>• Using directional antennas Wi-Fi can reach high bandwidth (+40Mbps) with range more than 10km.</li> </ul>
<b>WiMAX</b>	4/4 Mbps	60 km		<ul style="list-style-type: none"> <li>• Gets continually replaced by Wi-Fi and LTE</li> </ul>

These technologies are used by mobile devices to send and receive radio signals with any number of cell site base stations fitted with microwave antennas. These sites are then connected to a cabled communication network and switching system.

Advantages:

- Existing infrastructure (in case of 2G/3G/4G)

- High Bitrate (compared to LPWAN)
- Many devices support integration out of the box (either via dongle or internally)

Disadvantages:

- Power consumption (if this is a limitation)
- Cost: Module and Subscription

## 5.2 PLC – Powerline Communication

---

For decades, powerline communication technologies (PLC) have made it possible to use power lines to send and receive data. This “no-new-wire” approach makes PLC one of the best communication technology candidates for the Smart Grid, compared to other wired technologies. On the other hand, as PLC technologies use a media that was not specified for communication, they have faced a number of technical challenges limiting diffusion to niche indoor markets or dedicated ultralow rate applications.

Advantages:

- Use of Utility infrastructure (in case of 2G/3G/4G)
- Suited for HAN

Disadvantages:

- Sensitivity to disturbances (Harsh and Noisy environment)
- Relative low bitrate (20kb/s)

## 5.3 Low Power Wide Area Networks (LPWAN)

---

A number of low-power, wide-area networking (LP-WAN) solutions have arisen recently. These solutions have the following elements in common:

- Long range
- Low energy consumption
- Low cost (hardware module + subscription)
- Low bitrate
- Using license free spectrum in most cases (duty cycle to be respected)

Thanks to these characteristics, LPWAN solutions open up possibilities for whole new domains of solutions, such as smart parking solutions, people/asset/animal tracking and monitoring, utilities monitoring, environmental monitoring, etc.

The two main LPWAN solutions currently available in the market are LoRaWAN and Sigfox. A short introduction of both is given below.

## 5.3.1 LoRaWAN

LoRaWAN is a Low Power Wide Area Network (LPWAN) specification intended for wireless battery operated Things in regional, national or global network. The LoRaWAN is defined by the LoRa Alliance, a worldwide non-profit organization grouping all companies working on LoRa technology. LoRaWAN is being adopted by several telecom operators worldwide, i.e. Orange, Swisscom, KPN, Proximus, Singtel, etc.

LoRaWAN targets key requirements of internet of things such as secure bi-directional communication, mobility and localization services. These features are unique compared to Sigfox and other LPWAN solutions.

### Technical summary

- Using proprietary Semtech hardware
- Based on traditional network operators
- 125 KHz Spread Spectrum • SF12 SF6
- Class A, B, C:
  - A: Bi-directional end-devices
  - B: “+ scheduled receive slots
  - C: “+ maximal receive slots
- ACK Possible
- Mobility support
- Localization (future feature)
- Frequency band & channels: 863-870 MHZ
  - 3 125 KHz data channels
  - 125 KHz Join Request channels
- Data rate: 250 bps – 5470 bps
- Payload: 51-242 bytes max app payload

## 5.3.2 Sigfox

SIGFOX uses a UNB (Ultra Narrow Band) based radio technology to connect devices to its global network. The network operates - similar to LoRaWAN - in the globally available ISM bands (license-free frequency bands).

### Technical summary

- Ultra-Narrow Band
- SDR based gateways
- International network with national SNO's (Sigfox Network Operator)
- Payload:
  - Uplink: 12 bytes payload, total transmission  $\pm 6$  sec • Max transmission every  $\pm 12$  min (140/day) • 100 bps, BDPSK
  - Downlink • 8 byte payload • Requested with upload • Guaranteed 4/day

Technical capabilities	LoRaWAN	WAIVIOT	Neul	Low Power Wide Area Networks				Cellular	Short Range Networks				
				Nb-IoT	SigFox	Weightless - H	Weightless - P		BLE	WiFi	Thread	ZigBee	Z-Wave
Range (km/m)	2-5 urban, 15 suburban, 45km rural	up to 10km urban, 50+km rural	up to 10km	up to 10km	up to 10km urban, 50km rural	5km	2km	35km GSM, 200km 3G/4G	80m	50m	Mesh	100m mesh	30m mesh
Deep Indoor Performance	Yes	Yes	ISM yes, Whitespace no	Yes	Yes	Yes	Yes	No	No	No	No	-	-
Freq. Band	Variety, Sub-GHz	Frequency independent, 868/902/2400MHz	ISM or Whitespace	Sub-GHz	Frequency independent, 868/902/2400MHz	Sub-GHz	Sub-GHz	868/1000/1500/2100MHz	2.4GHz	2.4GHz	2.4GHz	915MHz/2.4GHz	900MHz
ISM?	Yes	Yes	Yes, depends on base-station	Yes	Yes	Yes	Yes	Depends	Yes	Yes	Yes	Yes	Yes
Fully Bi-Directional	Yes, depends on mode	Yes	Yes	No	No	Upstream only	Yes	Yes	Yes	Yes	-	Yes	Yes
Data Rate	0.3 - 50 kbps adaptive	60-100kbps	10-100kbps	100kbps	10-1000kbps	30kbps - 100kbps	up to 100kbps adaptive	35-170kbps GSM/ 3-10mbps LTE	< 1mbps	600mbps max		250kbps	10-100kbps
Power Profile	Low	Low	Low	Low	Low	Low	Low	Medium	High	High	Low	Low	Low
Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	High security, back by major telecoms	Trusted devices problematic	Yes	Yes	Yes	Yes
E2E Encryption	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Over the Air Software Upgrades	Yes	Yes		No	No	No	Yes	Yes	Yes	Yes		Yes	Yes
Supports sensors moving between beds	Yes	Yes		No	No	Yes	Yes	Yes	Yes	Yes	No	Yes, mesh-based	Yes, mesh-based
Location Aware	Yes	Yes	.	No	No	No	.	Yes	No	Yes	.	.	.
Operational Model	Public or private	Public or private	-	Public or private	Public	Public or private	Public or private	Public or private	Public or private	Public or private	Private/WiFi backbone	Public or private	Public or private
Standard	LoRaWAN	Nb-IoT (Narrowband Priority)	Weightless	Weightless	No	Weightless	Weightless	GSM, LTE etc	Bluetooth 4.0	IEEE802.11	Thread, based on 6LOWPAN IEEE802.15.4	ZigBee	Z-Wave
Scalability	Yes	Yes	Yes	Yes	Yes	Limited	Yes	Yes	Yes		Yes	Yes	Limited

### 5.3.3 Others

Several other (future) LPWAN solutions can be identified, but are not at the same level of performance, readiness or standardization as the two solutions mentioned above. A high level comparison is given in the table above. Note: An element that is not included in the table, but essential in the comparison of LPWAN solutions is the energy consumption of a device using one of the above technologies.

## 6 M2M Protocols

---

A Machine-to-Machine (M2M) protocol defines the way of communication between different devices of the same or different type. Many M2M protocols can be used both by wired and wireless technologies. This chapter will first start with a short overview of the legacy protocols in the M2M and smart grid domain. Secondly, the upcoming M2M protocols are elaborated more in detail.

### 6.1.1 Legacy M2M Protocols

The most common legacy protocols for Sensor Networks & Building automation used in the context of the smart grid or building automation and monitoring are listed below:

- BACnet
- LonWorks
- Modbus
- KNX
- ZigBee
- Z-Wave
- CAN
- OPC-UA
- Profibus

All these protocols require extensive expert knowledge to setup and the installation of a separate gateway on site. Furthermore, the protocols are heavily intertwined with their communication technology and do not have the critical mass to become the general standard for M2M. These are the main reasons why they are not widespread among residential customers and are mostly used for niche use cases. However, these protocols are well-known among industry, and have been used in industrial installations for years.

### 6.1.2 Upcoming M2M Protocols

#### ETSI M2M

While current M2M standards address the transport level, and client to server communication protocols, the future “Internet of Things” will require a system level architecture:

- Enabling application developers to focus on functionality, not lower-level tasks like network access control, authentication or routing;
- Enabling any application to read or control any sensor, under control of a horizontal security framework;
- Providing network-based services, such as data publication and subscription.

# STORY

In order to achieve these goals, common functions and network elements need to be identified and standardized as part of the M2M architecture: the ETSI M2M technical committee was created in January 2009 at the request of many telecom operators to create a standard system-level architecture for mass-scale M2M. ETSI TC M2M does not address one domain in particular; on the contrary, its ambition is to become the common backbone of all mass-scale M2M applications.

As for all recent automation protocols, the ETSI M2M architecture is resource centric and adopts the RESTful style. As usual, the 4 basic verbs of REST (create, read, update, delete) are complemented at the functional level by execute, subscribe and notify primitives, which are implemented, at a lower level, by helper resources manipulated by the CRUD verbs.

ETSI M2M does not aim at replacing existing standard or proprietary automation protocols, such as those listed above. It aims at integrating all of these protocols into a common architecture, facilitating access to any of these vertical protocols and networks from any hosted service, in an operator-controlled way.

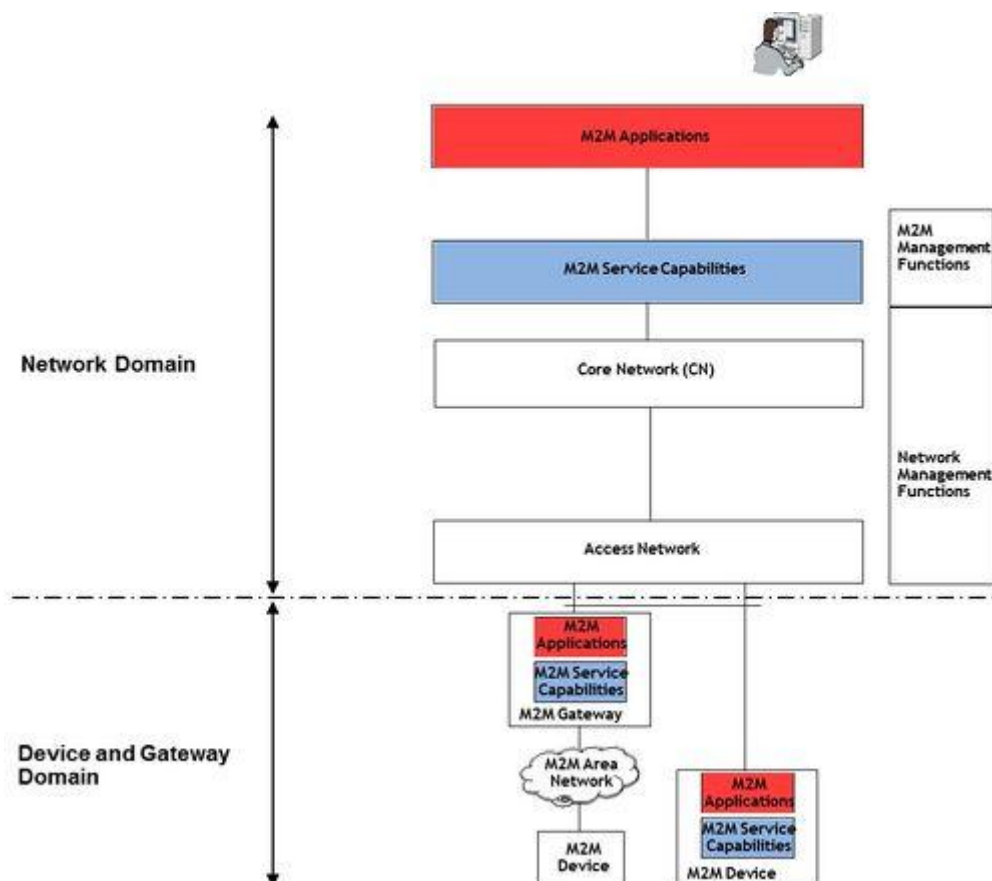


Figure 6. ETSI M2M Architecture.



# STORY

The ETSI M2M functional architecture is presented in ETSI TS 102 690<sup>10</sup> and separates the M2M device domain and the network and applications domain as shown in Figure 6.

- The device domain is composed of M2M Devices and M2M Gateways. ETSI M2M devices can connect to the M2M network domain directly or via M2M gateways acting as a network proxy. M2M gateways can be cascaded, or operate in parallel mode (e.g. for redundancy purposes).
- The Network and application domain comprises:
  - The access and transport network (e.g. an xDSL access network and an IP transport network)
  - The M2M Core, which itself is composed of:
    - a Core network (which provides IP connectivity, service and network control functions, network to network interconnect and roaming support); and
    - M2M service capabilities, the functional modules implementing the M2M functions shared by multiple applications through open interfaces.
  - The M2M Applications that run the M2M service logic and use the M2M service capabilities. The ETSI M2M architecture supports multi-agent applications, which can have components running in the end devices, in the gateways and in the network.

## One M2M

OneM2M is a global organization creating a scalable and interoperable standard for communication of devices and services used in M2M applications and the Internet of Things. OneM2M was formed in 2012 by seven of the world's preeminent standards development organizations: ARIB (Japan), ATIS (US), CCSA (China), ETSI (Europe), TTA (Korea) and TTC (Japan).

The One M2M functional architecture is presented in the OneM2M TS0001<sup>11</sup> and starts from a layered structure, with three layers:

- The Application layer (AE)
- The Common Services layer (CSE)
- The Network layer (NSE)

The overview of the functional architecture is given in Figure 7.

ETSI M2M/One M2M is not designed for the smart grid domain specifically. The added value will strongly depend on the use case. For example, ETSI M2M can be used for energy metering data management relatively straightforward but will be harder to use for more complex cases such as substation automation.

<sup>10</sup> [http://www.etsi.org/deliver/etsi\\_ts/102600\\_102699/102690/01.01.01\\_60/ts\\_102690v010101p.pdf](http://www.etsi.org/deliver/etsi_ts/102600_102699/102690/01.01.01_60/ts_102690v010101p.pdf)

<sup>11</sup> [ftp://ftp.onem2m.org/Deliverables/20140801\\_Candidate%20Release/TS-0001-oneM2M-Functional-Architecture-V-2014-08.pdf](ftp://ftp.onem2m.org/Deliverables/20140801_Candidate%20Release/TS-0001-oneM2M-Functional-Architecture-V-2014-08.pdf)



# STORY

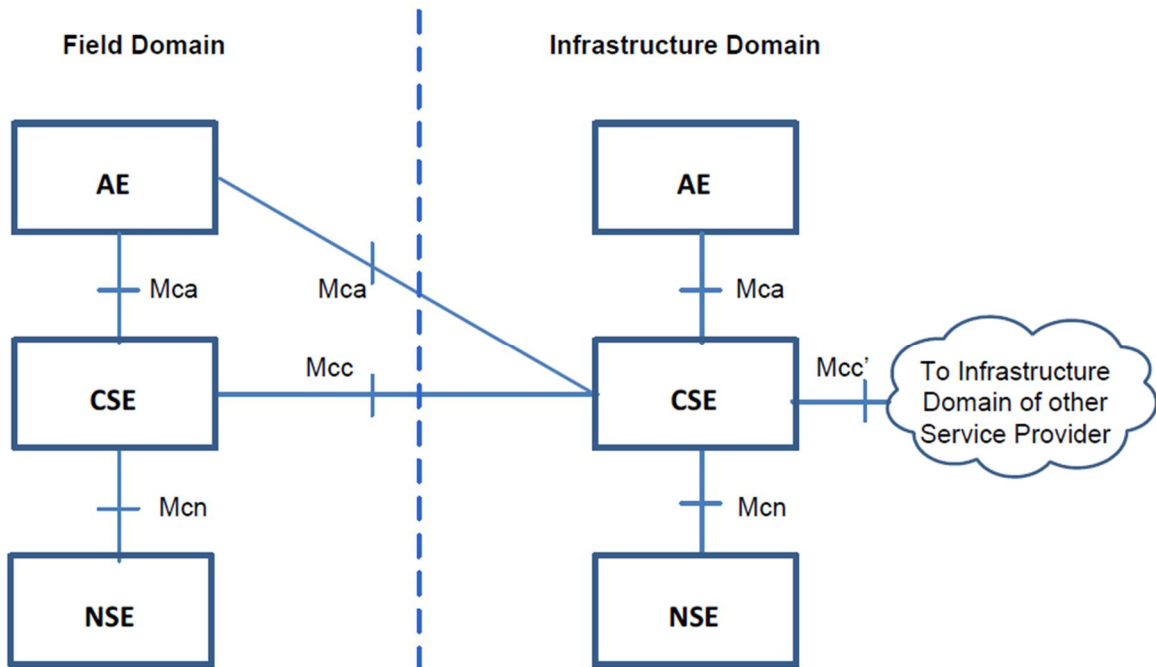


Figure 7. One M2M functional architecture.

The main benefit of ETSI M2M/One M2M is that they support multiple applications using data of one and the same device and vice versa (multiple devices/protocols supported by one application). This allows for easy integration of different devices/protocols/applications through the Common Services Layer. The main weakness of ETSI M2M lies in its generic character requiring a high level of customization for certain advanced smart grid use cases.

## OMA Lightweight M2M<sup>12</sup>

OMA Lightweight M2M is a protocol from the Open Mobile Alliance for M2M or IoT device management. Lightweight M2M enabler defines the application layer communication protocol between a LWM2M Server and a LWM2M Client, which is located in an LWM2M Device. The OMA Lightweight M2M enabler includes device management and service enablement for LWM2M Devices. The target LWM2M devices for this enabler are mainly resource constrained devices. Therefore, this enabler makes use of a light and compact protocol as well as an efficient resource data model. It provides a choice for the M2M Service Provider to deploy a M2M system to provide service to the M2M User.

OMA Lightweight M2M is designed to:

- Provide Device Management functionality over sensor or cellular networks
- Transfer service data from the network to devices

<sup>12</sup> [https://en.wikipedia.org/wiki/OMA\\_LWM2M](https://en.wikipedia.org/wiki/OMA_LWM2M), White Paper "Lightweight M2M": Enabling Device Management and Applications for the Internet of Things, [www.openmobilealliance.org](http://www.openmobilealliance.org)

# STORY

- Extend to meet the requirements of most any application

In Figure 8, the different deployment scenarios of OMA Lightweight M2M are given schematically.

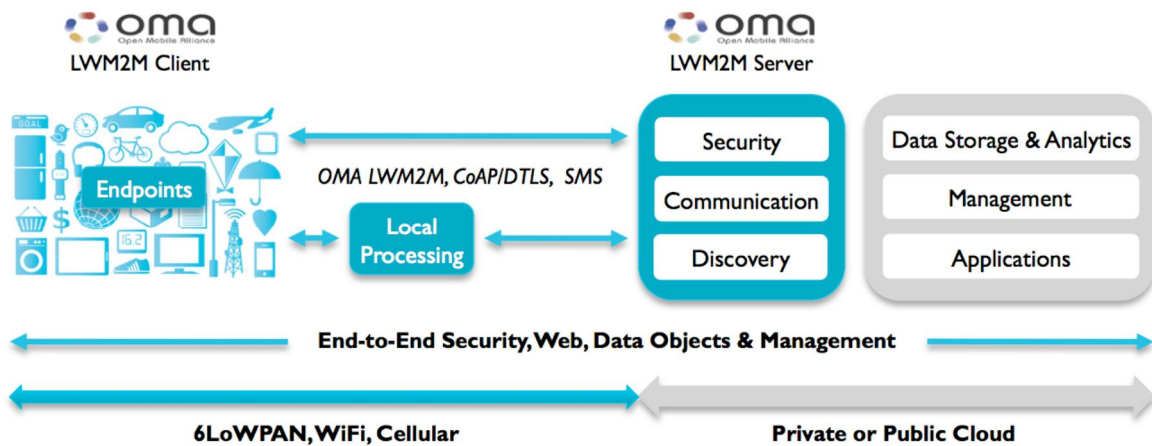


Figure 8. Deployment scenarios of OMA Lightweight M2M.

In essence, the OMA group on LWM2M has produced a client-server protocol specification that fits into the overall M2M architecture of oneM2M:

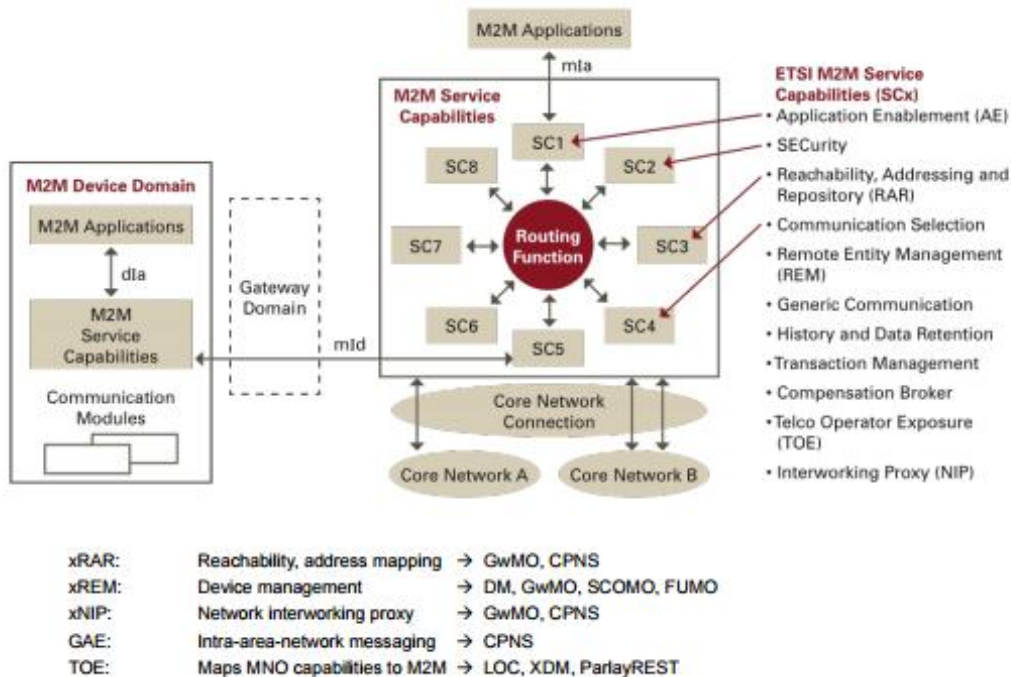


Figure 9. M2M Service Architecture.

- OMA collaborated with ETSI TC M2M during the specification of ETSI M2M Release 1
- OMA DM is natively included in the ETSI M2M R1 Functional Architecture and several OMA DM Management Objects have been specified.

- OMA is a oneM2M Partner Type 2 and actively participating in oneM2M activities

The M2M Service Architecture as defined within LWM2M can be mapped in Figure 9.

## 7 Security and Privacy

One major challenge for the management of STORY systems is that STORY energy requests and sensed measured data is reliably transferred both internally within the demo site and externally via network outside the territory of the company's network. This reliable transfer includes besides availability and robustness also additional security and privacy issues that arise when data is transferred outside the company's network.

It is important that secret or private information is kept undisclosed to unauthorized third parties since information about needed or deliverable amount of energy may be used to gain a financial benefit.

### 7.1 Current Situation at STORY Demonstration Sites

To gather information about ICT security practices at STORY demo sites, a questionnaire was created. The layout of this questionnaire is available in appendix 12.2. The following table reflects the information which was provided by the demonstration sites.

**Table 4. STORY demonstration site security practices (y=yes, n=no, p=planned).**

Question	Demonstration Sites (pseudonymised)					
	A	B	C	D	E	F
<b>Site identifier</b>						
<b>Certified according to 27.xxx standards</b>						
Waiting for the requirements of regulatory office				y		
<b>Security standards or guidelines</b>						
Waiting for the requirements of regulatory office				y		
<b>Separation between OT and IT</b>	y	y	n	y	n	n
<b>Risk management process established</b>	y	y	n	y	n	
<b>Tool support for assessment of your security situation</b>	y	y	y	y	y	
<b>Usage of tools to safeguard detect and manage cyber intrusions</b>						
Firewall	y	y	y	y	y	y



# STORY

Antivirus software	y	y	y	y	y	y
End-to-end cryptography	y	y	y	y	p	
Whitelisting approach for communication	y	y		p	p	y
Use of data diodes					p	
Intrusion detection system			y		y	
Intrusion prevention system			y	y	y	y
SIEM				p	p	
<b>Tools for recovery, correction of faults or restoration are introduced</b>	y	y	y	n	y	y
<b>Identity access management</b>						
Physical		p			p	
Authentication	y	p	y	y	p	
Authorization	y	p			y	
Role based (e.g. operator/administrator login)	y	p		y	p	
Identity based (individual user login)	y	p	y	y	y	

## 7.2 Security Aspects

In complex systems, connected via different communication systems and protocols, no 100% certainty regarding security is possible. There will always be residual risks that have to be managed. Security is a static but an ever evolving process adapted to changing threats and based on continuous development of the necessary processes and measures related to information security of the systems involved. Since security requirements depend on the components, machines and people involved, a threat catalogue, risk analysis and a suitable action plan build the basis for setting up adequate security measures which are in balance between effort, benefit and safety.

In the following sections relevant security measures, guidelines and standards for STORY are listed with a brief description and a linked reference.

**IEC 62443**<sup>13</sup> – The ISA/IEC 62443 is a series of technical specifications and related information that define procedures for implementing electronically cyberphysically secure Industrial Automation and Control Systems (IACS).

**IEC 62351**<sup>14</sup> – Is a standard developed for introducing different security objectives to protocols without information security measurements established for power system control operations. This includes [IEC 60870-5](#) series, [IEC 60870-6](#) series, [IEC 61850](#) series, [IEC 61970](#) series & [IEC 61968](#).

**BDEW White Paper**<sup>15</sup> – The BDEW White Paper “Requirements for Secure Control and Telecommunication Systems” is specifying essential security measures for control and telecommunication systems. It has been developed for power industry organizations.

**Smart Grid Information Security**<sup>16</sup> – The scope of the CEN-CENELEC-ETSI Smart Grid Information Security (SGIS) working group under the European Commission Smart Grid Mandate M/490 is to support European Smart Grid deployment. Within this context they provide a high level guidance on how standards can be used to develop Smart Grid information security. In this light it presents concepts and tools to help stakeholders to integrate information security into daily business.

**Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)**<sup>17</sup> – This Protection Profile defines the security objectives and corresponding requirements for a Gateway which is the central communication component of such a Smart Metering. The PP is directed to developers of Smart Meter Gateways and informs them about the requirements that have to be implemented. It is further directed to stakeholders being responsible for purchasing Smart Meter Gateways.

**NIST SP 800-53**<sup>18</sup> provides a catalogue of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors.

**NIST SP 800-82**<sup>19</sup> – This document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems,

<sup>13</sup> International Electrotechnical Commission (IEC). IEC 62443, <https://webstore.iec.ch/publication/7029>

<sup>14</sup> International Electrotechnical Commission (IEC). IEC 62351, <https://webstore.iec.ch/publication/6903>

<sup>15</sup> [https://www.bdew.de/internet.nsf/id/232E01B4E0C52139C1257A5D00429968/\\$file/OE-BDEW-Whitepaper\\_Secure\\_Systems%20V1.1%202015.pdf](https://www.bdew.de/internet.nsf/id/232E01B4E0C52139C1257A5D00429968/$file/OE-BDEW-Whitepaper_Secure_Systems%20V1.1%202015.pdf)

<sup>16</sup> [https://www.dke.de/de/std/informationssicherheit/documents/sgcg\\_sgis\\_report.pdf](https://www.dke.de/de/std/informationssicherheit/documents/sgcg_sgis_report.pdf)

<sup>17</sup>

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0073b\\_pdf.pdf;jsessionid=773BAF974E3B8474ED81298F60D70D9C.2\\_cid294?\\_\\_blob=publicationFile&v=1](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0073b_pdf.pdf;jsessionid=773BAF974E3B8474ED81298F60D70D9C.2_cid294?__blob=publicationFile&v=1)

<sup>18</sup> <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

<sup>19</sup> <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>

# STORY

Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

**NIST 7628<sup>20</sup>** – These Guidelines for Smart Grid Cybersecurity, present an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of smart grid-related characteristics, risks, and vulnerabilities.

**NERC CIP<sup>21</sup>** - This set of standards address the security of cyber assets essential to the reliable operation of electric utility operations and their assets. It covers the security of electronic perimeters, the protection of critical cyber assets, personnel and training, security management as well as disaster recovery planning.

**ISO/IEC TR 27019<sup>22</sup>** Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

## 7.3 Security Analysis of Selected Communication Standards

There are several possibilities to establish a secure connection. Generally for wired IP based networks TLS, IPsec and MACsec mechanism can be used to introduce security. Regarding OSI model, TLS is located at the application layer, IPsec is performed at the network layer, whereas MACsec is applied at the data link layer. For wireless networks WPA2/AES is used to secure the communication. The following table shows security concepts for different network types provided at OSI layer 1 to 3.

**Table 5. Security analysis of candidate communication technologies in STORY demonstrations.**

Network	Security concept
Ethernet	IPsec, MACsec
WLAN	WPA2 with /AES
WiMAX	Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) PKM-EAP (Extensible Authentication Protocol) together with AES-CCM for link-layer wireless encryption
GSM/GPRS/EDGE	A5/1 cryptography. Frequency hopping also gives some extra security Based on symmetric cryptography, the encryption algorithm has been broken, an

<sup>20</sup> <http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf>

<sup>21</sup> <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>

<sup>22</sup> <https://webstore.iec.ch/publication/11303#additionalinfo>





# STORY

	option might be the usage of EAP-SIM
3G/HSPA/HSPA+	Several cryptography technologies for user plane and for control plane can be used. KASUMI is one of the proposed block ciphers used in UMTS, GSM, and GPRS mobile communications systems. The KASUMI block cipher used as GEA/3 (GPRS Encryption Algorithm 3) is only based on a 64-bit key and was theoretically broken. The KASUMI block cipher used for GEA/4 is based on a 128-bit key and is considered to be secure. GEA/1 and GEA/2 are older proprietary stream ciphers, which are broken and should therefore not be used.
4G/LTE	Several cryptography technologies for user plane and for control plane can be used. KASUMI is one of the proposed block ciphers [see note on KASUMI for 3G (above)].
IEC 61158/61784-2 Profibus, Profinet, Modbus, cc link	IEC 61784-4 MACsec
WirelessHART	Based on CCM - a counter mode with CBC-MAC encryption and AES 128 block cipher to enable authenticated encryption mode
ISA100.11a	Based on CCM - a counter mode with CBC-MAC encryption and AES 128 block cipher to enable authenticated encryption mode Use of mode ENC-MIC-128 to enable both authentication and encryption best
ZigBee	Based on CCM - a counter mode with CBC-MAC encryption and AES 128 block cipher to enable authenticated encryption mode Unsafe due a weak key exchange mechanism when adding a new device
LoRaWAN	Based on CCM - a counter mode with CBC-MAC encryption and AES 128 block cipher to enable authenticated encryption mode AERO Authenticated Encryption with Replay protection might be an option
Sigfox	Frequency hopping
6LoWPAN	IPsec
Z-Wave	Uses cipher block chaining message authentication code technique (CBC-MAC) by using AES 128 as block cipher to construct the des message authentication code



	During initial setup or re-installation of a device the key exchange could be eavesdropped by using default values set at Z-Wave firmware
PLC	Usage of AES128 as encryption algorithms must be established

## 7.4 Privacy Aspects

Privacy aspects in STORY are not limited to confidentiality and access control. The sensors in use will generate a large amount of data and partly highly sensitive personal data about activities within the demonstration site. At residential building demonstrations the connection to smart household appliances or smart home functionality has to be considered, because such a connection has a huge impact on the privacy of a person. Such an amount of personal data can deliver a lot of information about the person's behaviour, location and actions, as well as health and finance status. In the area of industrial demo sites, the interconnection to other deployed systems may have serious impact regarding accessibility of confidential internal information (data protection) and processes. Therefore, measurements have to be undertaken to protect this information from unauthorized access.

The following subsection lists standards and initiatives, which have to be taken into account for future development.

### 7.4.1 European General Data Protection Regulation<sup>23</sup>

The European Commission plans to unify data protection within the European Union (EU) with a single law, the General Data Protection Regulation (GDPR). The current EU Data Protection Directive 95/46/EC does not consider important aspects like globalization and technological developments like social networks and cloud computing sufficiently and the Commission determined that new guidelines for data protection and privacy are required. The EU's European Council aims for adoption by the end of 2015/early 2016. In 2017, the Regulation is planned to take effect after a transition period of two years.

### 7.4.2 OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data<sup>24</sup>

In 1980, the OECD adopted the Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data ("1980 Guidelines") to address concerns arising from the increased use of personal data and the risk to global economies resulting from restrictions to the flow of information across borders. In 2013 an update was published to address innovations, particularly in modern information and communication technologies, which support global

<sup>23</sup> [https://en.wikipedia.org/wiki/General\\_Data\\_Protection\\_Regulation](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation)

<sup>24</sup> <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>

accessibility and wide range of analytics that can provide comprehensive insights into individuals' movements, interests, and activities.

### 7.4.3 International Safe Harbor Privacy Principles<sup>25</sup>

The international Safe Harbor Privacy Principles are principles which enable US companies to comply with privacy laws protecting European Union and Swiss citizens. In October 2015, the European Court of Justice held the Safe Harbour Principles to be invalid, as they did not require all organizations (US federal government agencies could use personal data under US law, but were not required to opt in) entitled to work with EU privacy-related data to comply with it, thus providing insufficient guarantees.

### 7.4.4 IPEN Initiative<sup>26</sup>

The IPEN initiative was founded in 2014 by EU Data Protection Supervisor's Head of Policy, with the goal to bring together privacy experts with developers. The objective of this is to integrate data protection and privacy into all phases of the development process, from the requirements phase to production, as it is most appropriate for the development model and the application environment.

### 7.4.5 Online Trust Alliance (OTA)<sup>27</sup>

The Online Trust Alliance was founded in 2005 as a non-profit organisation with the mission to enhance online trust and empower users, while promoting innovation and the vitality of the Internet. OTA provides a set of best practices, resources and guidance to help enhance online safety, data security, privacy and also brand protection. The IoT Trust Framework addresses the growing concerns and risk at the fast innovation of IoT and focuses on privacy, security and sustainability, including a defence-in-depth strategy for all systems.

### 7.4.6 OWASP Top 10 Privacy Risks Project<sup>28</sup>

The OWASP Top 10 Privacy Risk Project provides a top 10 list for privacy risks in web applications (2014) and related countermeasures (2015/2016). This list was obtained by 63 privacy and security experts, which rated 20 privacy violations for their frequency in web sites. It covers technological and organizational aspects that focus on real-life risks for users and providers. The aim of the project is to reach a common understanding of web application privacy and to support developers and web application providers to implement privacy by design web applications.

<sup>25</sup> [https://en.wikipedia.org/wiki/International\\_Safe\\_Harbor\\_Privacy\\_Principles](https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles)

<sup>26</sup> <https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/IPEN/cache/offonce>

<sup>27</sup> <https://otalliance.org/initiatives/internet-things>

<sup>28</sup> [https://www.owasp.org/index.php/OWASP\\_Top\\_10\\_Privacy\\_Risks\\_Project](https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project)

#### **7.4.7 Privacy Recommendations for STORY Project**

- All personally identifiable and sensible data must be encrypted using state of the art encryption standards
- Establish state of the art access control mechanism to all data
- Specify which personally identifiable and sensitive data types and attributes are collected and used and for what purposes
- If sensitive data is transferred outside the premises, only part of the data which is reasonably useful for the functionality have to be transferred
- If data is transferred outside the premise, personalized data has to be pseudonymized
- If data is transferred outside the operations, personalized data has to be anonymized
- During the transfer, all data has to be encrypted by using current generally accepted state of the art security standards
- In general, data must only be stored within storage devices located inside the EU
- Collected data is not shared with third party organisations
- Specify how long data will be stored
- Provide information about policies, terms and conditions to the user
- Provide information and control how the user can decline and personalized data is being removed.

## 8 STORY Communication Gateway Requirements

This chapter establishes the criteria for the STORY communication gateway for the range of actual installations envisaged in the project. These criteria are used for the selection of the actual communication solutions employed within these installations.

### 8.1 Common Characteristics

Besides some general cross section characteristics, the STORY communication gateway requirements are aligned to four layers:

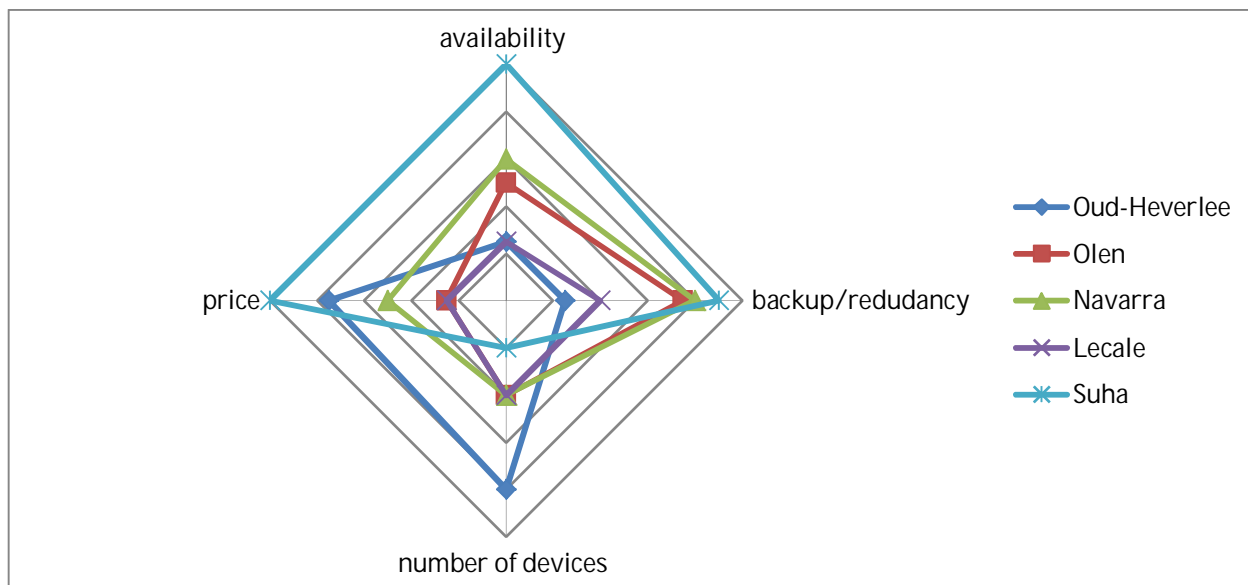
**Table 6. Layer structure of the communication gateway.**

STORY Layer	Local network	Distributed (WAN)
Application layer	application provided by demo-site	application provided by DSO
Security Layer	authentication, encryption, access control, privacy ....	authentication, encryption, access control, privacy ....
Data exchange layer	KNX, Modbus, ETSI-M2M	DNP3.0, OPC-UA, ETSI-M2M
Communication layer	Ethernet, LoRaWAN, RS232, RS485	Ethernet, WiMAX, LoRaWAN

#### 8.1.1 General

Some general gateway characteristics are derived from a questionnaire filled in by the different demo sites. The diagram below shows the connection between price, availability, backup/redundancy and the number of devices to control. In terms of costs two groups for gateways could be determined, an expensive one with the link to availability, redundancy and scalability and a cheaper version with a reduced availability, backup and scalability scope.

The gateway has to be available 24 hours a day (24/7), more precisely a 99.9% uptime is required for the equipment installed inside the STORY operations. To achieve this objective a backup solution for data and configuration information is required. In general, the gateway itself has to be linked to the power supply directly. Depending on the local operation mode at the STORY demo site an islanded mode without power from the grid might be required under such consideration a battery or UPS to enable such a mode is required.



**Figure 10. Relation between the gateway criteria price, availability, backup/redundancy and scalability for the different demo sites.**

The price of the GW installed at on single premises area shall not exceed the limit of 500€. In case of assembling multiple independent units inside one operation, the purchase costs shall not exceed 2.000€.

The standard GW must be capable to interact with at least 20 devices. In case of assembling multiple independent units inside one operation, the GW has to scale up to support 200 devices.

To guarantee an optimal system performance a keep-alive response, throughout the entire system, has to be performed within one second.

The gateway and associated devices and services must be easy to install and configure. Zero-touch configuration and plug and play are preferable when designing services and devices. Appropriate tools for end-users and operators must be available.

The gateway must support a remote management system to enable remote operations and management procedures.

The gateway must be supported for software management and updates. It must be possible to support software modules that can be upgraded remotely.

## 8.1.2 Application Layer

The application layer, being closest to the end user applications, heavily depends on the outcome of WP3 developments. Minimizing risk, this translates in gateway requirements that keep sufficient options open to cope with the range of possible needs to accommodate WP3.



# STORY

To be able to handle late-arriving requirements, the gateway needs to be a general-purpose platform enjoying a large and diverse user group (critical mass). Moreover, the project must avoid to be “penny-wise but pound-foolish” even for applications that are cost-sensitive. This translates into the following.

The processing unit needs to be a platform on which substantial software applications can execute. Minimally, it will be a 32 bit microprocessor with 512 MB RAM and 4GB persistent storage or (often much) more. Indeed, such capability fits within a smart watch, is present in entry-level smart phones and even in a credit card sized computer module sold at less than 10€.

In other words, the benefits of lowering this minimal requirement are extremely small (for developments aimed at future installations) where below this threshold software development will be hampered (slow, expensive, hard to maintain when forced to squeeze it into a sub-standard environment encountered e.g. in microcontrollers). Depending on the application, the hardware may be more powerful by a significant margin as long as it does not become a niche product lacking critical mass (e.g. only used in an industrial automation niche in some part of the world, which typically will be reflected in steep prices for the hardware and software).

Operating system is selected to be Linux (open source) as the gateway – typically communicating over the Internet – must not and will not support hard<sup>29</sup> real time services. Moreover, there is no compelling need to support a proprietary OS within the project, also not for the replicability of the results.

To guarantee the ability to execute software code as needed by the applications, the gateway needs to support ANSI-C in its software stack. Other languages may need to be supported, such as Java, Python and C++. Note that all programming languages, which the project might consider accommodating, are able to interact with ANSI-C. As the project uses mainstream computing platforms, supporting ANSI-C effectively allows the project to implement applications in any language of their own choice. The extent of support for other languages will depend on the test cases.

Concerning response times, the applications are expected to determine this. A wide range of response time requirements is expected from the test cases. The gateway provides swift response, e.g. suitable for interaction with humans over the Internet. However, no guaranteed response time will be provided. Any requirement for hard guarantees is to be provided locally within the application itself.

Clock synchronisation (NTP protocol) will be ensured within the demo-sites. Where needed, services will provide features like a heartbeat, publish-subscribe interface, etc. The gateway enables user interaction. Mainstream (web/Internet) protocols will be used (e.g. http, https, REST, web sockets) and M2M protocols that integrate well (e.g. CoAP). The gateway will support asynchronous execution (e.g. not restricted to RPC).

---

<sup>29</sup> *Hard* means that missing a deadline is a serious error.



# STORY

The gateway allows for remote management, updating (preferably within a given time frame) of data and applications (software) as needed. Finally, logging functionality is supported where the test cases and WP3 outcomes determine what needs to be logged (operation information, alerts, measurements, authorised intervention by whom, etc.). Both push and pull are to be supported.

### 8.1.3 Security Layer

Authentication and access control is one of the most crucial elements to secure the STORY infrastructure. Therefore, depending on the size of the storage production capacity and their integration into the grid, two categories are introduced:

- For demo sites with a storage capacity which are mainly for their own consumption identity based, individual user login/ password or eID are proposed.
- Demo sites, which are mainly under control by a DSO a more sophisticated authentication process including a combination of a certificate and role based authentication and access control process is planned. This two-way authentication needs more administrative interaction, but at the area of DSO such an expertise to manage is assumed. Therefore, the maintenance of certificates is pre-existing.

The roles defined in the authentication (and authorization) may also be used for alerting; the system **MUST** be capable to report certain safety and security relevant events to distinctive people or groups thereof. Reporting methods may include email and SMS. Furthermore the system may contain a security dashboard, displaying recent events on the management interface. We also propose four levels of alert classes to categorize these events and assign it to roles or groups to be alerted.

The access control also includes measurements to prevent unauthorized access. To achieve this, the device **MUST** be hardened (all unneeded services must be deactivated; a customized, reduced kernel is also recommended to provide a smaller target to adversaries). Also a host-based firewall and strict patch management **MUST** be in place.

Also, communication channels have to be secured. Due the limited resources normally available at embedded systems, a hybrid cryptosystem approach is used which combines the security benefit of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. During the communication establishment, the asymmetric key is used to exchange the symmetric key, which used afterwards for an efficient data throughput. Such a hybrid approach is part of various cipher suites and should be enabled.

In order to provide authentication and encryption, Transport Layer Security (TLS) **MUST** be used to provide communication security while traversing over foreign networks. For this implementation, TLS is chosen as requirement over alternatives (e.g.) IPsec for the following reasons [16]:

- TLS is easier to integrate between different vendors



- TLS needs less overhead
- TLS allows quicker handshakes
- TLS is easier to configure

In constrained environments such as STORY demo sites which mainly use their own consumption Datagram Transport Layer Security (DTLS) might be used as a lightweight alternative. For the remainder of this section, DTLS is treated the same way as TLS.

To fully utilize the security features of TLS, this protocol stack has to be configured properly. That means that encryption and authentication measures allowed in the standard, but regarded unsafe by now must not be used. The Internet Engineering Task Force (IETF) published a guideline for the secure use of TLS [19]. The gateway MUST support and implementers MUST comply to these recommendations with the following constrictions:

- Symmetric cipher with at least 128 bits (SHOULD NOT support < 128 bits changed to MUST NOT support)
- MUST NOT support static key assignments (RSA and PSK) instead of SHOULD NOT [p.11]
- MUST negotiate TLS 1.2 (exclusion of TLS 1.0 and 1.1 [p.6])
- MUST implement strict TLS (recommendation set to MUST [p.7])
- MUST disable TLS-level compression (changed from SHOULD [p.8])
- DH keys of at least 2048 bits or ECDH keys of at least 192 bits MUST be used (recommendation to MUST) [p.12f.]
- No anonymous suite MUST be used[3, p.92]

For simplicity, the allowed TLS cipher suites are restricted to the ones recommended in this IETF document [p.11]:

- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

One reason for changing the IETF recommendations to mandatory is that the gateway is regarded critical infrastructure and has therefore a higher demand of security than standard desktop machines or web browsers. Another reason is that generally industrial and energy systems have longer product life cycles and therefore the time period the security measures have to prevail are also longer. Because of this, the key size is restricted to 128 bits or greater, for they are recommended beyond 2031 by the National Institute of Standards and Technology (NIST) [20]. Another related issue is the block size of symmetric encryption algorithms. Block sizes of 64 bits are generally not recommended [17] and therefore prohibited for the gateway. Of the encryption algorithms currently standardized in TLS [21], only AES, SEED, CAMELLIA and ARIA fulfil this requirement. Of these four, SEED does not occur in a cipher suite in CCM/GCM mode and does therefore practically not fulfil these requirements. AES is strongly

recommended, for it is the most proliferated of these algorithms. CCM and GCM are generally recommended, because both of them offer a combined authentication and encryption algorithm.

In the same manner as in communications, data stored locally on the device has to be secured from unauthorized access. Apart from system access controls, this data has to be encrypted and integrity checked by the same algorithmic methods as communication lines. This is distinctively a requirement for security relevant data (explicitly logs that contain security events), which **MUST** be encrypted and integrity checked. Additionally, for privacy reasons, some sort of anonymization method has to be implemented, if personal data is to be processed. As it is a sensitive part, special focus on the key management is needed. A key derivation function that is deemed state of the art by current research **MUST** be used. A smart card-based key derivation function is recommended. To protect systems (i.e. ICS) in contact with the gateway, some sort of filtering (ICS intrusion protection or anomaly detection system) is also recommended.

#### 8.1.4 Data Exchange Layer

The objective of the data exchange layer is to ensure that all the information transferred by the data transport protocols are

- 1) conveyed between the systems parts,
- 2) there are no data losses nor errors with data transformations, and
- 3) the data packets are routed to the correct receiving entities of the system.

The most efficient way to handle this in the GW is to send all the data protocol packets/messages transparently using another protocol to encapsulate the whole data packets/messages. When this is possible no protocol transformations are required in the gateway. In addition, no implementations of the data exchange protocols are required within the GW and the licenses, which are often quite valuable, would not need to be acquired.

The transporting and encapsulating protocol could be for example the ETSI M2M proposed IETF CoAP protocol (Constrained Application Protocol, RFC 7252).

Another solution would be to map all the data exchange protocols to a common information model that is described then e.g., for CoAP. This still requires counter parts for these protocols and therefore also the licenses. The only benefit is that the GW itself would not be running them.

The conclusion is that all the legacy protocols must be conveyed through the gateway as is (DNP3.0, Modbus, OPC-UA, etc.), or optionally there must be implemented a suitable protocol transformation (e.g. Modbus, KNX => ETSI-M2M).

### 8.1.5 Communication Layer

The communication layer handles the different types of communication networks. To compare different communication network implementations, we will look at the communication layer as an incorporation of the three lowest OSI layers: The network, data link and physical layer. As such, the communication layer can be seen as a network solution to send data from a smart grid component to an Internet connected gateway using certain protocols. Examples of such communication layer networks are cellular networks such as 3G, low power radio networks such as LoRa, Ethernet and common Home Area Networks (HAN) such as ZigBee and KNX.

As smart grid applications can have significantly different requirements, STORY will not try to promote a single ideal communication network to fit all applications. However, the ambition of this chapter is to give guidance to the reader on which communication network is most suited for his application. Four types of generalised communication networks are compared:

- 1) **Cellular networks.** Wide area communication network using the mobile network such as GPRS and 3G. These networks are mostly operated by a telecom provider and require a subscription to send data.
- 2) **Low Power Wide Area Networks (LPWAN).** Wide area radio networks which often operate in the free frequency bands and which require minimal power to transmit messages but have limited response time and bandwidth.
- 3) **HAN.** Residential installed networks to which smart grid components can be connected. Examples here are Wi-Fi, ZigBee and KNX
- 4) **Ethernet.** A direct Ethernet connection using a cable.

The list of different network possibilities is kept limited on purpose to give a general understanding of the capabilities and differences of these networks. The networks are evaluated qualitatively using the following criteria.

- 1) **Range.** The range of a communication network determines the allowed distance of the smart grid component to the communication gateway connected to the internet. Communication networks with an extended range allow for an easier implementation of new components to the network without installing additional gateways.
- 2) **Cost.** The cost of connecting a smart grid component to the Internet via the communication network. This cost includes the gateway costs as well as possible subscription rates.
- 3) **Autonomy.** The possibility of smart grid components to be battery powered for a reasonable period (more than a year) while sending messages over the communication network
- 4) **Speed.** Possible speed of the communication from the component to an application. This includes bandwidth, frequency and latency.

Note again that we try to stay as general as possible and partly neglect influencing factors between different criteria. E.g. the autonomy of a component will decline if the frequency of messages is increased.



# STORY

The following table gives a comparison between the different communication network possibilities using the four criteria.

**Table 7. Comparison of candidate technologies.**

	Range	Autonomy	Cost	Speed
<b>Cellular</b>	++	-	0	++
<b>Ethernet</b>	--	-	+	+++
<b>LPWAN</b>	++	++	++	0
<b>HAN</b>	0	0	+	+

An Ethernet or Cellular communication network can be used when high bitrates and fast communication is required but are often costly and consume a lot of power making battery powered components difficult.

An LPWAN network has several advantages such as low subscription rates, battery powered components and a high *plug-and-play* potential for non-industrial customers making the roll-out of smart grid components in the residential sector possible. However the speed of the network is limited and can be a bottleneck for some applications.

## 8.2 Installation Site Characteristics

This section contains the relevant characteristics of the installations/case studies that have an impact on this task (i.e. establish the criteria).

### 8.2.1 Specific Characteristics – Case Study 1-2

The demonstration cases in Oud-Heverlee, Belgium consist of 13 houses. In one of these houses, Think HQ, the goal is to monitor every detail and control all possible components posing additional requirements on the ICT architecture. The other 12 houses are normal residential houses where the implementation of smart grid components should be as general and easy as possible.

The smart grid components inside the houses in the neighbourhood are directly connected to the Belgian national LoRa network making a HAN obsolete and thus significantly reducing the costs. Only for the Think HQ, STORY chose to deploy a HAN KNX network due to a multitude of sensors placed inside the building, the thermal storage tanks and other components.

Communication between applications and the STORY gateway will be over ETSI M2M. The Actility LoRa platform directly enables this communication whereas a translation gateway from KNX is placed in Think HQ.

A LoRaWAN network connects the different sensors and actuators in the OHL demo making the implementation of an expensive local HAN for each house obsolete.

# STORY

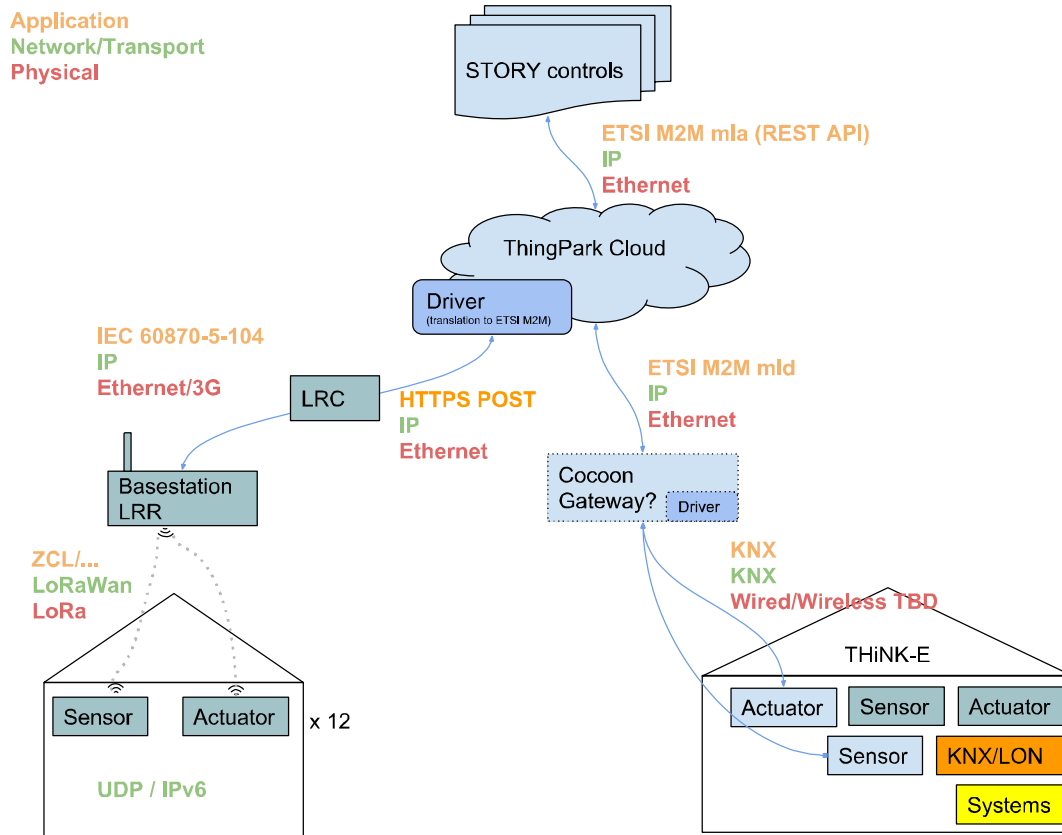


Figure 11. Communication infrastructure at the Oud-Heverlee, Belgium site.

## 8.2.2 Specific Characteristics – Case Study 3

The installation in Navarra, Spain, will be a small industrial site, where power produced by a PV system will be used to feed a battery to help shaving peak power consumption.

The communication inside the site will be Modbus over TCP/IP with estimated bandwidth requirements 60kb/s with 10Hz (100ms) measurement and control cycle. The system is bidirectional, with the general controller handling setting the control variables (write registers) on the actual devices. All in all, the site will consist of 6-10 separate devices, all of which support bi-directional data flow.

The external access from the system to both STORY data store (BaseN Platform) and DSO is over Internet. Estimated reachability SLA for site is 99.9% (8.75h downtime/year) with the system providing a local backup logic for safe operation during communications downtime.

# STORY

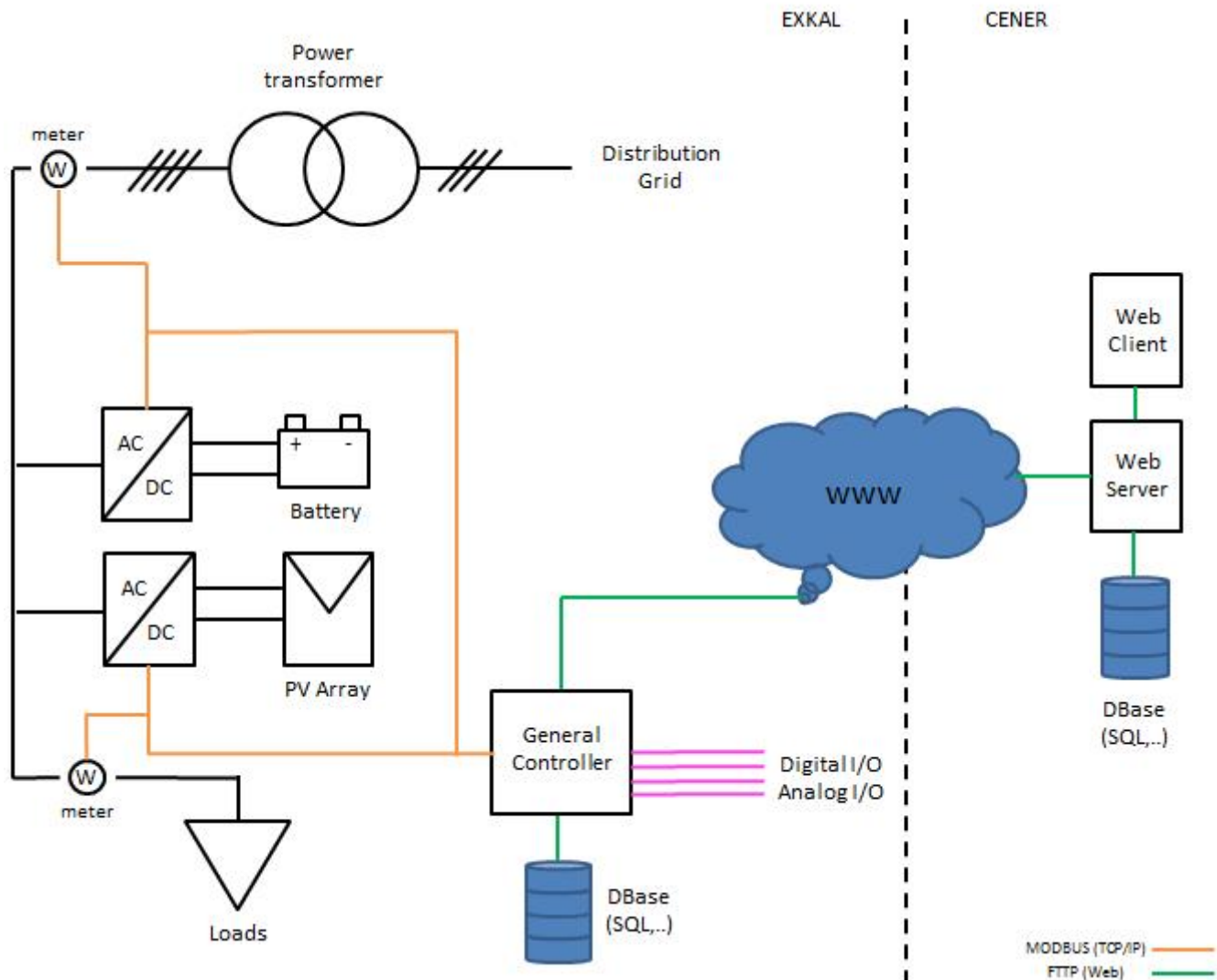


Figure 12. Navarra, Spain site setup.

## 8.2.3 Specific Characteristics – Case Study 4

### Lecale, Northern Ireland

In site communication is over 434MHz radio (EN-ETSI 300220-1, 300220-2) between sensors and bridge. Northbound communication (BaseN Platform and DSO) is Wi-Fi/Ethernet, with the communication protocol still open, probably one of the M2M protocols outlined in this document. Near real-time power sensors will be attached to various devices and radio link will be user to communicate the values – necessary measuring interval and bandwidth are still unknown.

The microgrid in Lecale is planned to be coupled to the main grid operated by Northern Ireland Electricity (NIE). Negotiations for this are ongoing. The Point of Common Coupling (PCC) would be located on a 33 kW substation. If this is realized, it would provide stability and services to the

microgrid and also provide support for the reduction of the microgrid's electrical consumption (curtailment) during peak usage hours.

Generation:

- 250 kW of PV
- 2 x 2.5 MW wind turbines (onshore)
- 500 kW anaerobic digestion unit

Load:

- 300 residential buildings (microgrid)

Storage:

- 250 kW and 2 MWh Compressed Air Energy Storage (CAES)

## 8.2.4 Specific Characteristics – Case Study 5

Two demonstrations are carried out in Slovenia:

- Medium scale storage unit connected in low voltage substation in residential grid (TS Suha demo case), WP5, Task 5.6, Subtask 5.6.2.
- Medium scale storage unit connected in low voltage substation in industrial grid (EG headquarters demo case), WP5, Task 5.6, Subtask 5.6.3.

### Residential grid case

Medium scale storage unit will be connected to 20/0.4 kV MV/LV transformer station supplying Suha village residential grid. To enable system control and data acquisition, demo site is fully ICT supported.

WiMAX network is used to efficiently connect different components of the distribution grid, providing a nearly real-time monitoring and control network. Broadband wireless IP network enables the use of single communication paths to share same network resources for multiple applications.

# STORY

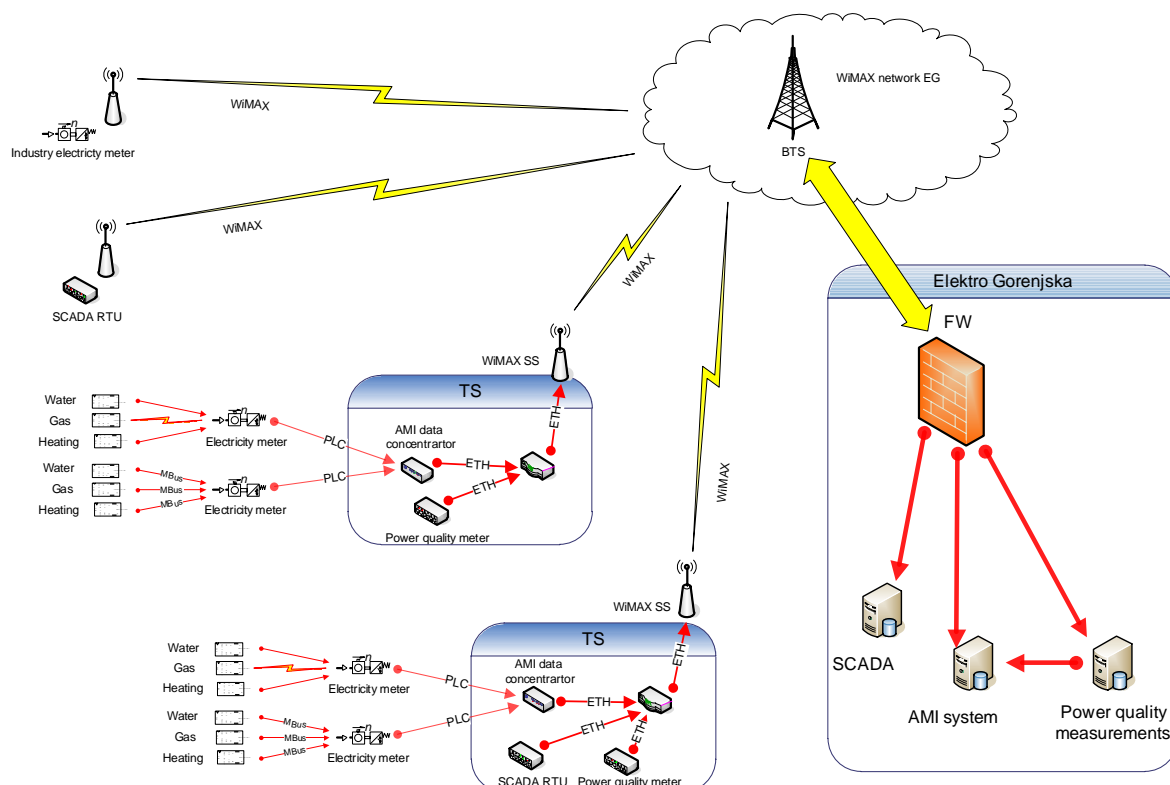
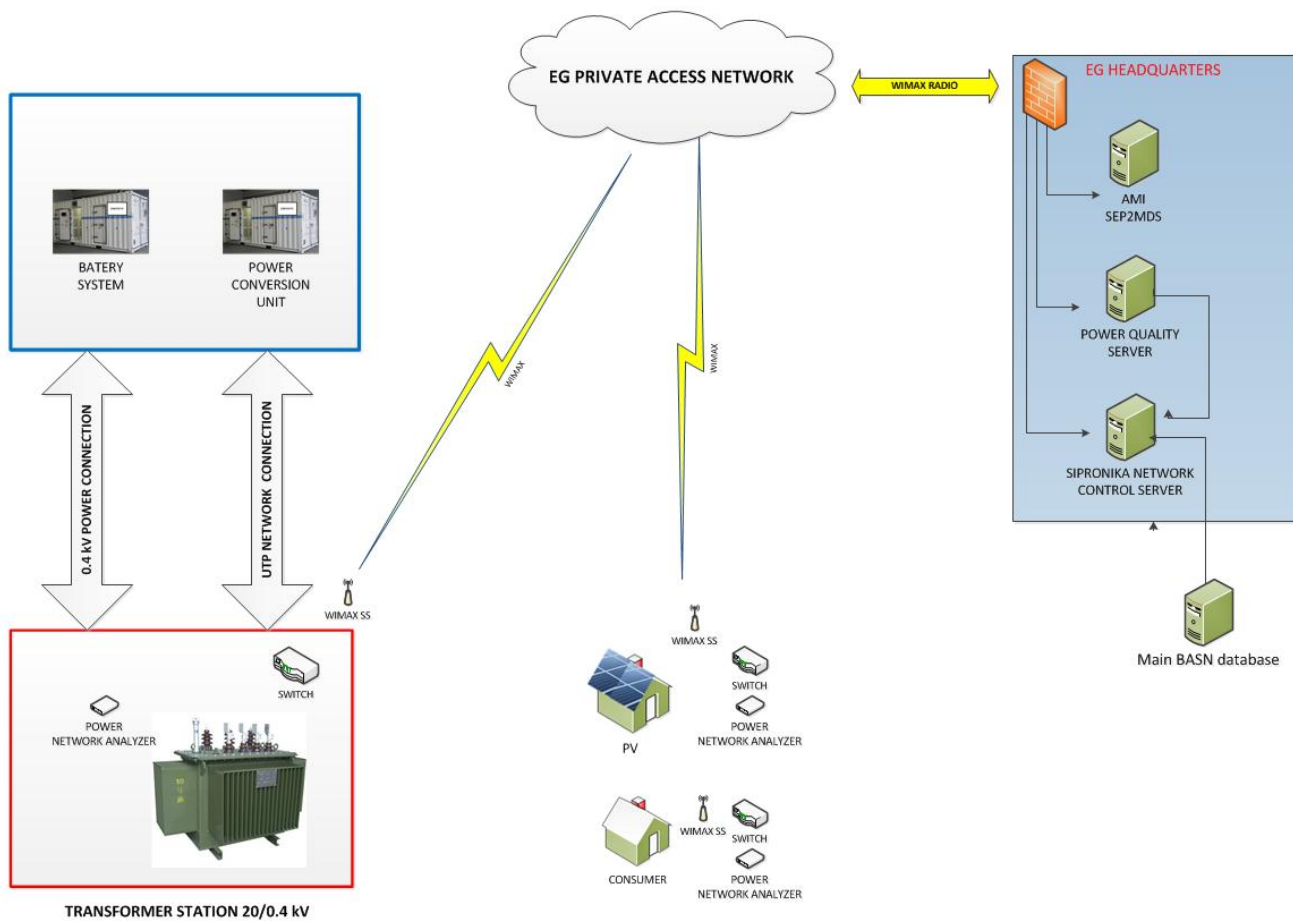


Figure 13: WiMAX as common EG communication platform.

In MV/LV transformer stations data from AMI concentrators, power quality meters, SCADA RTUs, industry electricity meters and other sensors are transferred through single communication path. WiMAX through its support for standardized quality levels enables configuration of different profiles of different data flows.

Suha demonstration site general communication setup is depicted in Figure 14.

# STORY



**Figure 14. Proposed Suha demonstration site setup.**

For the communication between different demo site equipment (Battery Storage PLC, SNCS, BASN server) only standard communication protocols are foreseen. For the purpose of TS Suha remote control, EG has already implemented some protocols as follows:

- DNP 3.0 protocol
- OPC-UA protocol
- IEC 60870 – 5-104
- Modbus

Proposed communication solution is depicted in Figure 15.

# STORY

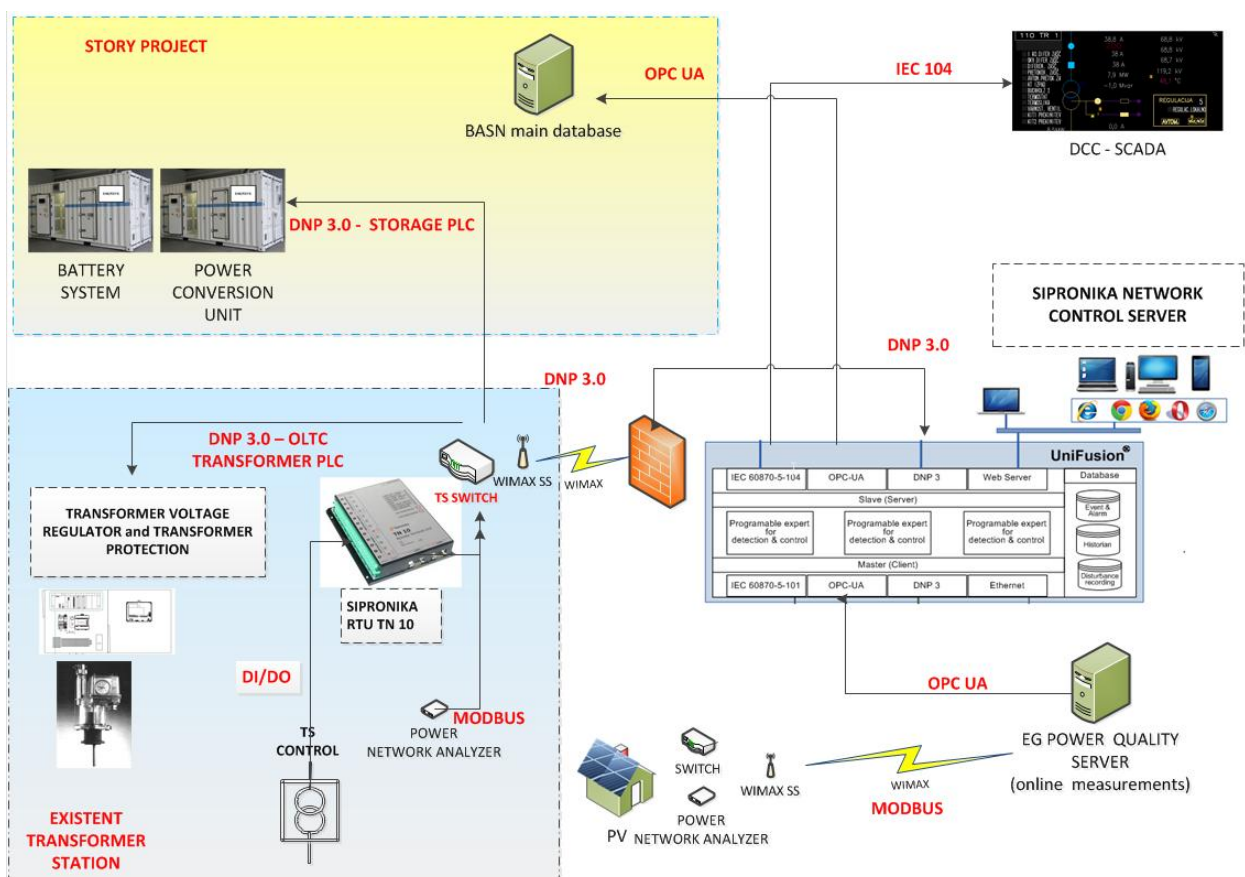


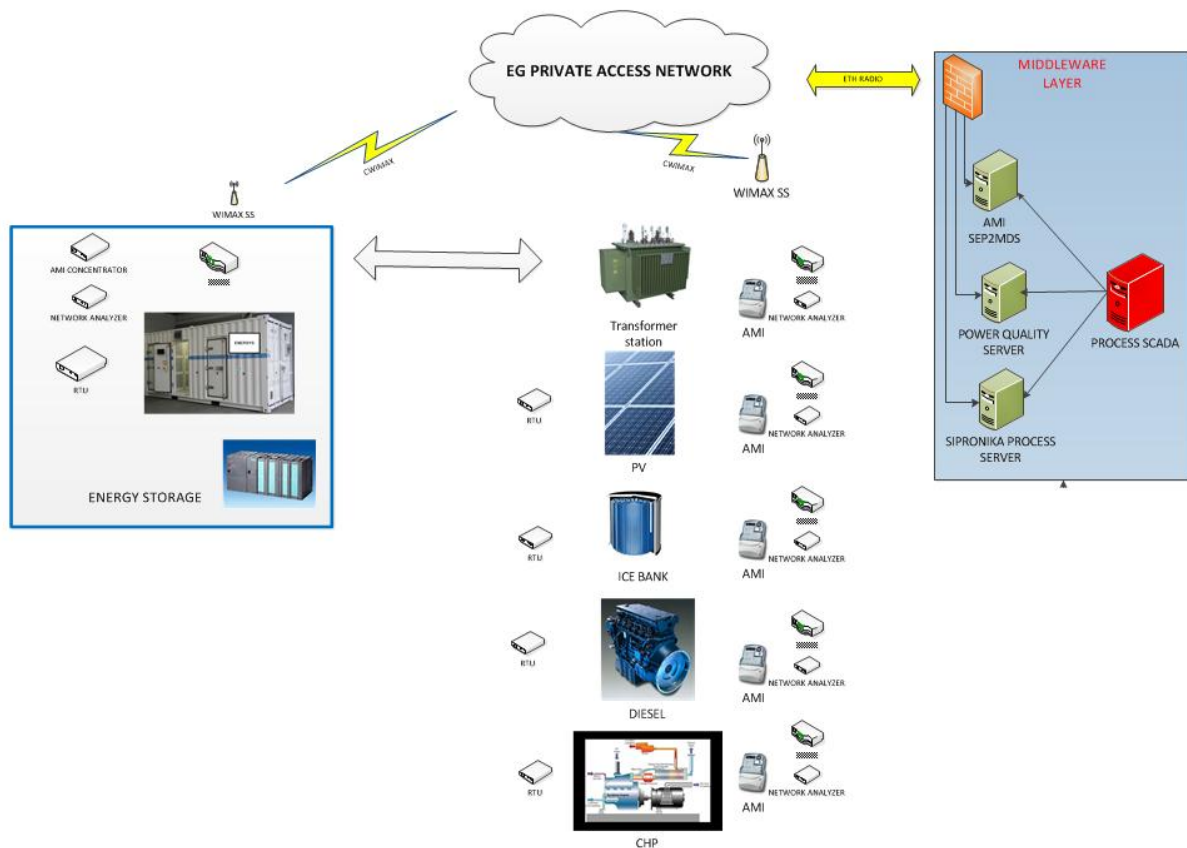
Figure 15. Proposed Suha demonstration site communication diagram.

## Industrial grid case

Medium scale storage unit for the second demo case will be connected to 20/0,4 kV MV/LV transformer station supplying Elektro Gorenjska headquarters industrial grid on Mirka Vadnova 3a street, Kranj.

Proposed demonstration site setup is depicted in the following Figure.

# STORY



**Figure 16 - Proposed EG headquarters demonstration site setup**

In the compound, the following devices are installed:

- 2 x 630 kVA transformer station
- 35 kW photovoltaic power plant
- 27 kW combined heat and power unit
- 80 kW diesel generator with network synchronization capabilities and the possibility of adjusting the amount of emitted power
- Ice storage within the heating / cooling facility

For the purpose of the industrial demo case, the same type of equipment as in TS Suha demo will be used as well as communication protocols.

# STORY

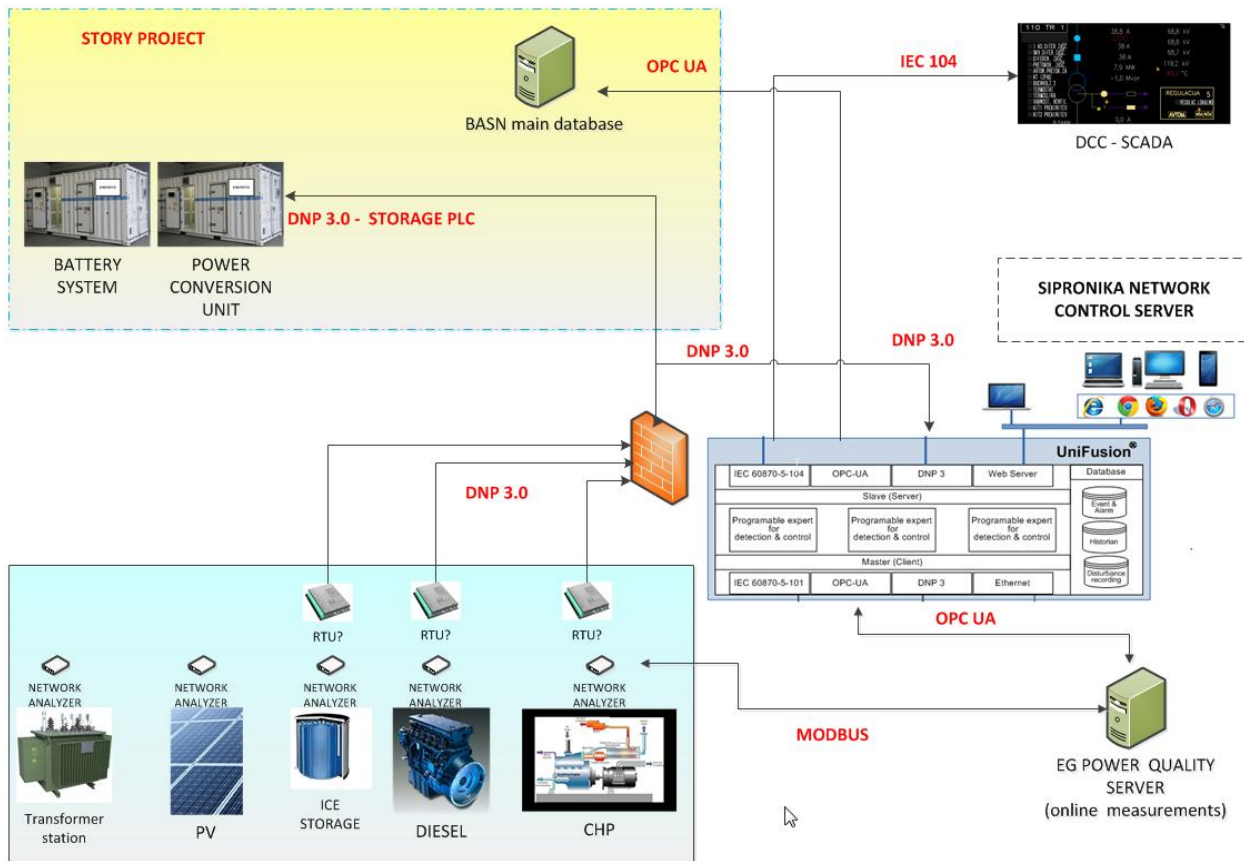


Figure 17. Proposed EG Headquarters demonstration site communication diagram.

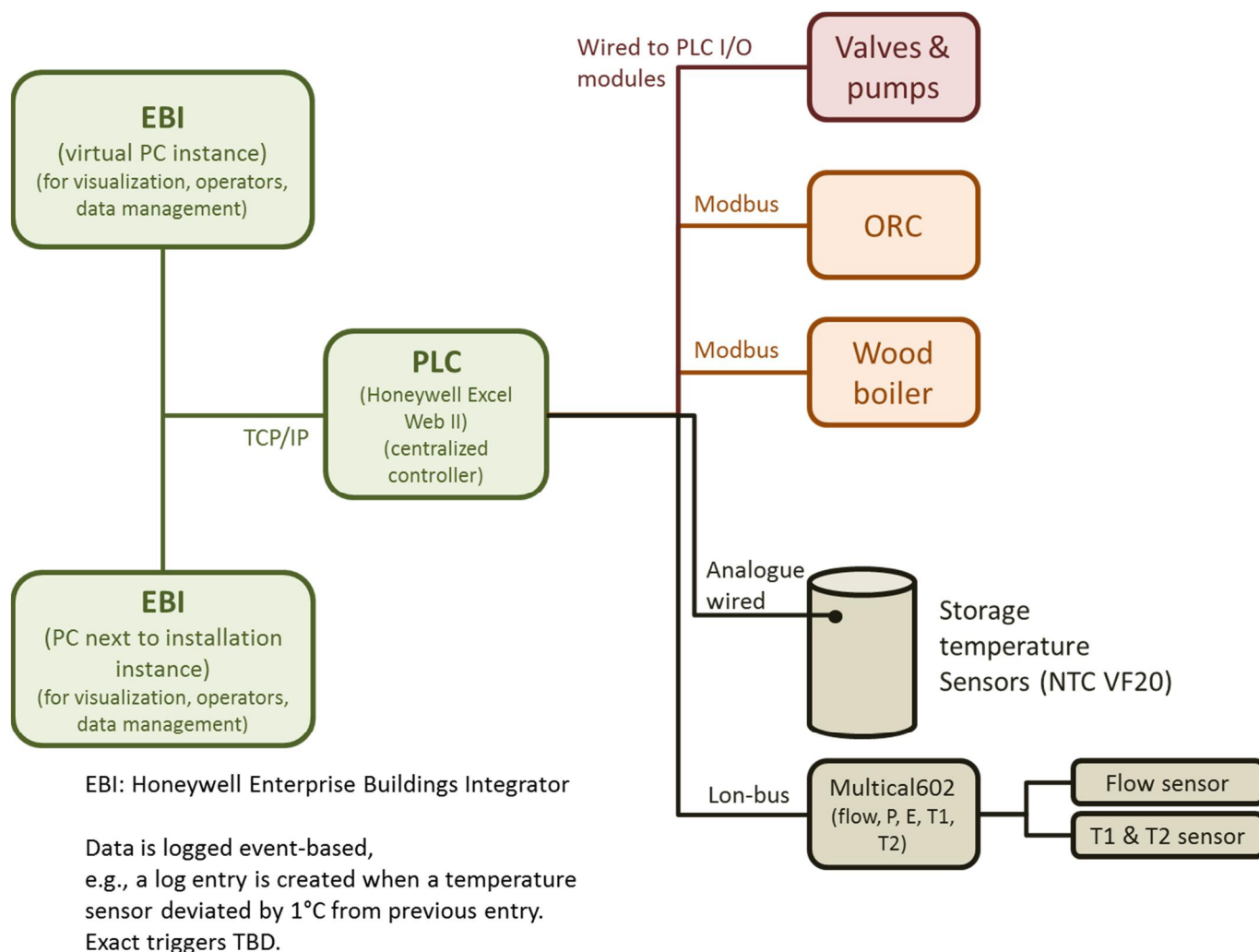
## 8.2.5 Specific Characteristics – Case Study 6

The demonstration site in Olen, Belgium, is a heating system, as depicted in figure 16. Its main components are:

- 1.6MW waste wood fired boiler
- an ORC generator (1MW thermal power in/900kW thermal power out, 100kW electrical power production)
- 2 large buffers of 20m<sup>3</sup> and 50 m<sup>3</sup> respectively.
- 1 900kW cooler
- Various heat lines to provide heat to the industrial facilities and to heat the office buildings

There is a detailed figure in appendix 12.4 indicating the location of the various temperature sensors, colorie meters, valves and pumps.

# STORY



**Figure 18. ICT infrastructure at the Olen, Belgium site.**

The entire system is controlled centrally from a PLC (Honeywell Excel Web II system). Figure 18 illustrates how the various actuators, measurements and operator interfaces are connected to the central PLC:

- Operator access is via either an EBI (Honeywell Enterprise Buildings Integrator) instance on a PC installed at the site, or via an EBI instance on a virtual PC.
- Valves, pumps and temperature sensors have a wired analogue connection to the PLC.
- The ORC and wood boiler are connected through Modbus
- The calorific meters are connected to the PLC using Lon-bus.

## 9 Conclusions

---

Extensive analysis of smart grid standards has been done previously by many organizations and groups. The most notable efforts in Europe were done in the STARGRID and FINSENY projects. In this deliverable we presented an overview of the most relevant smart grid communication and security standards for the STORY project demonstrations. These included e.g. building automation standards such as BACnet, KNX and LonWorks and home area network device communication measurement and control technologies such as ZigBee. The complete list of relevant standards can be found in chapter 3.1.

A suggestion was given on how the communication networks at demonstration sites can be organized (separation into Home Area (HAN), Field Area (FAN) and Wide Area (WAN) Networks). Many options for each network type were given. For example, HAN can be realized by using PLC, BACnet, LonWorks or KNX communications, FAN can be realized using e.g. Narrowband PLC or SDN/OTN communications and WAN can be realized using e.g. DNP3.0, Satellite, UMTS/HSPA, or LTE cellular technologies. The complete list can be found in chapter 3.2.3. If data rate requirements in a demonstration are modest, the whole intra demonstration communication can be handled with a single communication network technology, the LPWAN. These technologies include e.g. LoRaWAN, LTE-MTC, NWave and Sigfox. At the moment LoRaWAN and Sigfox are the forerunners in this category, due to their readiness, affordability and their active and growing user base.

In addition to the traditional HAN and WAN technologies, Machine-to-Machine (M2M) protocols were presented as possible communication technologies inside demonstration sites. Three upcoming M2M protocols were presented: ETSI M2M, OneM2M and OMA Lightweight M2M. For example, the Oud-Heverlee, Belgium, case is envisioned to use ETSI M2M for communication inside the demonstration site between applications and the STORY gateway device.

Most of the communication technologies discussed in this deliverable operate on the lower three layers of the OSI model. In addition, the most popular higher layer communication protocols for smart grids were introduced. Smart grid applications and standards rely heavily on Web Services, which are defined to be the methods to communicate between applications over (generally IP based) communication networks. Two major classes of Web Services were presented: RESTful and SOAP/RPC. REST has become a de facto standard and it generally outperforms its competition.

Security and privacy standards for smart grids were discussed in chapter 7. The most crucial elements in securing the STORY infrastructure; authentication, access control, encryption, reporting and communication security, were addressed and explained how they have to be configured. Transport Layer Security and Datagram Transport Layer Security were chosen to provide communication security while traversing over foreign networks. The most important privacy recommendations for the STORY project are:



# STORY

- All personally identifiable and sensible data must be encrypted using state of the art encryption standards
- Establish state of the art access control mechanism to all data
- All data transferred must be considered from the viewpoint of insuring privacy
- During the transfer, all data has to be encrypted by using current generally accepted state of the art security standards
- In general, data must only be stored within storage devices located inside the EU
- Collected data is not shared with third party organisations
- Specify how long data will be stored
- Provide information about policies, terms and conditions to the user

At time of writing, the communication infrastructures in demonstration sites are in different stages of completion. Some sites are maintained by utilities (such as the EG site in Slovenia) and already have a communication infrastructure in place, which has been tested and used in practice. Other sites do not have an up and running communication infrastructure in place but are in the process of building them or are still planning the upcoming networks. It is not meaningful to switch the available networks into new ones but to use the existing infrastructure as much as possible in the demonstrations. We cannot give universally applicable recommendations on what communication standards and technologies to use in the demonstrations. We must look at each demonstration site separately and decide, what are the most suitable and secure standards and protocols considering each site's requirements.

STORY gateway device is aimed to be incorporated into all demonstration sites. The device gives the ability to monitor, manage and control demonstrations sites, while maintaining data security, privacy and authenticity. In addition, it will provide the ability to send and store demonstration data to the STORY cloud. The requirements for the STORY gateway device are divided into five categories: general, application, security, data exchange and communication. These can be found in chapter 8.



## 10 Acronyms and Terms

---

AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
AMM	Advanced Metering Management
BAN	Building Area Network
CAES	Compressed Air Energy Storage
CAN	Controller Area Network
CORBA	Common Object Request Broker Architecture
DCC	Distribution Control Centre
DER	Distributed Energy Resources
DNP	Distributed Network Protocol
DSM	Demand-side Management
FAN	Field Area Network
GWAC	GridWise Architecture Council
HAN	Home Area Network
HEMS	Home Energy Management System
IP	Internet Protocol
ISO	International Organization for Standardization
M2M	Machine-to-Machine
MDMS	Metering Data Management System
MG	Microgrid
MGCC	Microgrid Control Centre
MPLS	Multiprotocol Label Switching
MV	Medium Voltage
NAN	Neighbourhood Area Network
NIST	National Institute of Standards and Technology
OPC-UA	Open Platform Communications – Unified Architecture
OSI	Open Systems Interconnection
PCC	Point-of-Common Coupling
PEV	Plug-in Electric Vehicle
PLC	Powerline Communications
PROFIBUS	Process Field Bus
REST	Representational State Transfer
RP	Report
RPC	Remote Procedure Call



# STORY

SG-CG	Smart Grid Coordination Group
SGAM	Smart Grid Architecture Model
SGCM	Smart Grid Conceptual Model
SGIP	Smart Grid Interoperability Panel
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SS	Substation
UDDI	Universal Description Discovery and Integration
WAN	Wide Area Network
WPA	Wi-Fi Protected Access
WSDL	Web Service Description Language



## 11 References

---

- [1] CEN/CENELEC website.  
<http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx>. Link checked 14.09.2015.
- [2] CEN-CENELEC-ETSI Smart Grid Coordination Group. "SGAM User Manual – Applying, testing & refining the Smart Grid Architecture Model (SGAM) [SG-CG/K]". Version 3.0.  
[ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG\\_Methodology\\_SGAMUserManual.pdf](ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_Methodology_SGAMUserManual.pdf). Link checked 14.09.2015.
- [3] CEN-CENELEC-ETSI Smart Grid Coordination Group. "Overview of SG-CG Methodologies [SG-CG/F]". Version 3.0.  
[ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG\\_Methodology\\_Overview.pdf](ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_Methodology_Overview.pdf). Link checked 18.11.2015.
- [4] CEN-CENELEC-ETSI Smart Grid Reference Architecture,  
[http://ec.europa.eu/energy/sites/ener/files/documents/xpert\\_group1\\_reference\\_architecture.pdf](http://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf). Link checked 18.11.2015.
- [5] Ekram Hossain, Zhu Han & H. Vincent Poor (Editors). "Smart Grid Communications and Networking" Cambridge University Press, 2012.
- [6] Smart Grid Interoperability Panel (SGIP) website. <http://sgip.org>. Link checked 17.11.2015.
- [7] JD Taft & A Becker-Dippmann. "Grid Architecture – QER Analysis". Pacific Northwest National Laboratory. January 2015.  
[http://energy.gov/sites/prod/files/2015/04/f22/QER%20Analysis%20-%20Grid%20Architecture\\_0.pdf](http://energy.gov/sites/prod/files/2015/04/f22/QER%20Analysis%20-%20Grid%20Architecture_0.pdf). Page 101-102/115. Link checked 19.11.2015.
- [8] SGIP website. <http://sgip.org/Interoperability-and-the-GWAC-Stack>. Link checked 19.11.2015.
- [9] Güngör, Vehbi C, Sahin, Dilan, Kocak, Taskin. "Smart Grid Technologies: Communication Technologies and Standards". Industrial informatics, IEEE transactions on 7.4 (2011): 529-539.
- [10] "The internet of Things, key applications and protocols"; Olivier Hersent, David Boswarthick, Omar Elloumi; Wiley 2012
- [11] [www.EDN.com](http://www.EDN.com)
- [12] Analysis Mason, 2012 "Policy orientations to reach the European Digital Agenda targets"



# STORY

- [13] [www.onem2m.org](http://www.onem2m.org)
- [14] M. Kuzlu, M. Pipattanasomporn & S. Rahman. "Communication network requirements for major smart grid applications in HAN, NAN and WAN". Computer Networks, Vol. 67, Pages 74-88, July 2014.
- [15] CEN-CENELEC-ETSI Smart Grid Coordination Group "First Set of Standards" Version 2.0. November 2012.  
<ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/First%20Set%20of%20Standards.pdf>. Link checked 3.12.2015.
- [16] AbdelNasir Alshamsi, Takamichi Saito. "A Technical Comparison of IPsec and SSL". 2005. Proceedings of the 19th International Conference on Advanced Information Networking and Applications. AINA, 2005.
- [17] McGrew, D. A. (2012). "Impossible plaintext cryptanalysis and probable-plaintext collision attacks of 64-bit block cipher modes". IACR Cryptology ePrint Archive, 2012.
- [18] Dierks, T., Rescorla, E. "RFC5246: The Transport Layer Security (TLS) Protocol Version 1.2. Internet Engineering Task Force", 2008.
- [19] Sheffer, Y., Holz, R., Saint-Andre, P. "RFC7525: Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Internet Engineering Task Force", 2015.
- [20] Barker, E., Barker, W., Burr, W., Polk, W., & Smid, M. "Recommendation for Key Management – Part 1: General" (Revision 3 - NIST Special Publication 800-57). National Institute of Standards and Technology, 2012.
- [21] Internet Assigned Numbers Authority. TLS Cipher Suite Registry. Online:  
<http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4>. Retrieved: 15.12.2015.



## 12 Appendices

---

### 12.1 Introduction to SGAM Methodology

---

In 2011, the European commission and EFTA issued the Smart Grid Mandate M/490 which was accepted by the three European Standards Organizations (ESOs), CEN, CENELEC and ETSI. M/490 requested CEN, CENELEC and ETSI to develop a framework to enable ESOs to perform continuous standard enhancement and development in the smart grid field. In order to perform the requested work, the ESOs together with the relevant stakeholders established the CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG) [1]. In the end of 2014, the CEN-CENELEC-ETSI Smart Grid Coordination Group finalized a number of reports. One outcome of these reports is the Smart Grid Architecture Model (SGAM). The SGAM user manual [2] recognizes a number of uses for the SGAM but the most relevant for this document are the following:

- To enable a structured analysis of Smart Grid use cases
- To provide a guide to analyse potential implementation scenarios
- To ensure a common understanding between different stakeholders

The SGAM, depicted in Figure 19, in short is a reference model to analyse and visualize smart grid use cases in a technology-neutral manner.

The SGAM spans three dimensions:

- Domains
- Zones (or levels)
- Interoperability layers

The plane spanned by Domains and Zones is called the SGAM Smart Grid Plane. The five domains ((Bulk) Generation, Transmission, Distribution, DER and Customer Premises) represent the complete electrical energy conversion chain. The six zones (Process, Field, Station, Operation, Enterprise and Market) represent the hierarchical levels of power system management. The smart grid plane enables the representation of the levels in which power system management interactions between domains or inside a single domain take place. The interoperability layers allow modelling of different views from business as well as technical nature.

# STORY

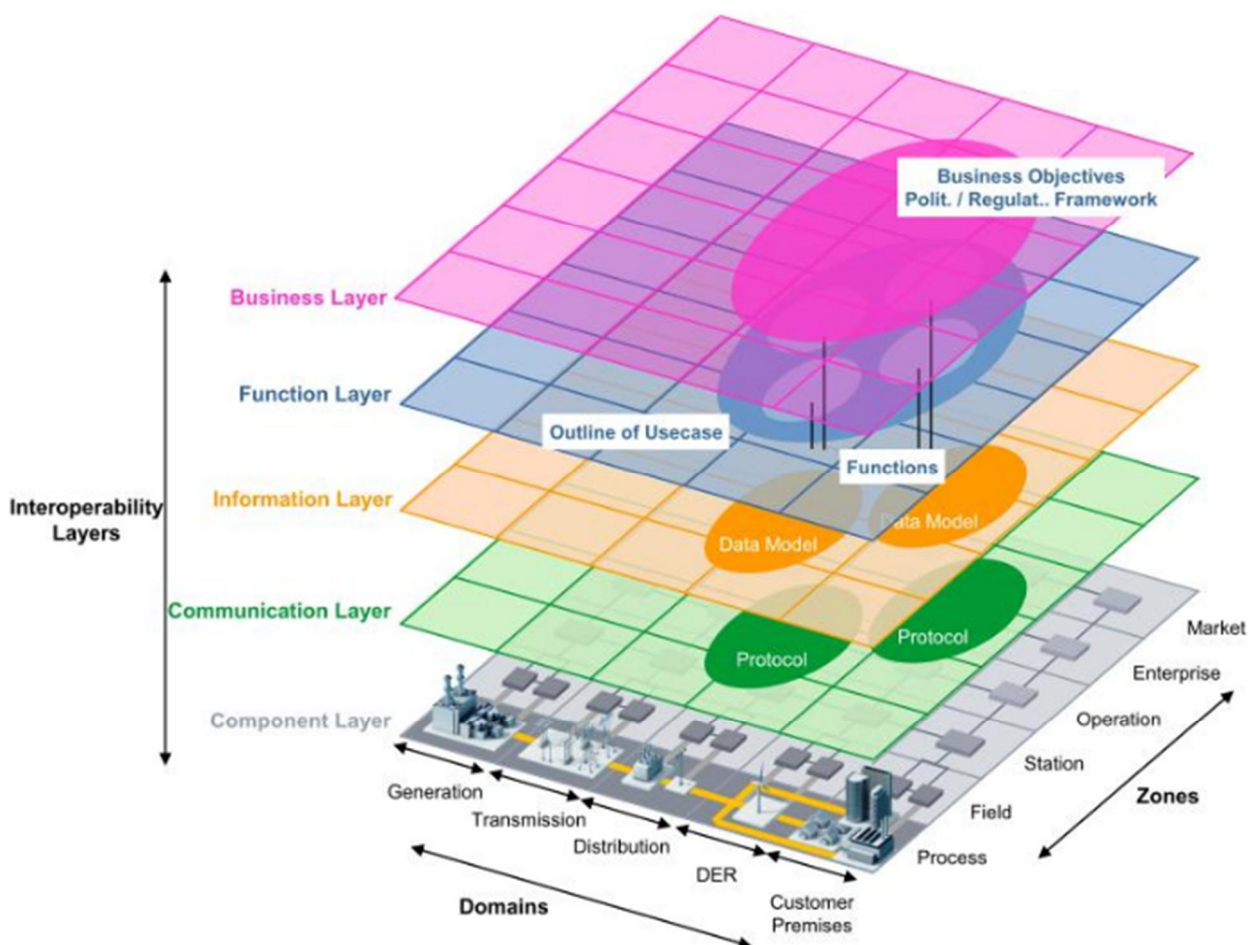


Figure 19. The SGAM Model [2].

SGAM domains:

- (Bulk) Generation: Represents generation of electrical energy in bulk quantities e.g. fossil, nuclear, hydro power plants, off-shore wind farms and large scale solar power plants
- Transmission: Represents the infrastructure which transports electricity over long distances
- Distribution: Represents the infrastructure which distributes electricity to customers
- DER: Represents distributed electrical resources directly connected to the public distribution grid. Applies to small-scale power generation and consumption technologies (typ. in the range of 3 kW to 10000 kW). Includes processes and any kind of DERs which **have** the objective of contributing to the electricity grid as primary business goal.
- Customer premises: End users of electricity and local producers of electricity. Includes industrial, commercial and home facilities. Generation in form of e.g. PV, EV storage, batteries and micro turbines. Includes processes which **do not have** the objective of contributing to the electricity grid as primary business goal.

# STORY

SGAM zones/levels:

- **Process:** Physical, chemical, or spatial transformations of energy and the physical equipment directly involved (e.g. generators, transformers, circuit breakers, cables)
- **Field:** Represents the equipment that protects, controls and monitors the process of the power system (e.g. protection relays, bay controllers, any kind of IEDs, which acquire and use process data from the power system)
- **Station:** Represents the areal aggregation level for field level, e.g. data concentration, functional aggregation, substation automation, local SCADA systems, plant supervision etc.
- **Operation:** Hosting power system control operation in the respective domain, e.g. distribution management system (DMS), energy management systems (EMS) in generation and transmission systems, microgrid management system, virtual power plant management systems, EV fleet charging management systems
- **Enterprise:** Includes commercial and organizational processes, services and infrastructures for enterprises (utilities, service providers, energy traders etc.) e.g. asset management, billing and procurement
- **Market:** Reflects the market operations possible along the energy conversion chain, e.g. energy trading, retail market

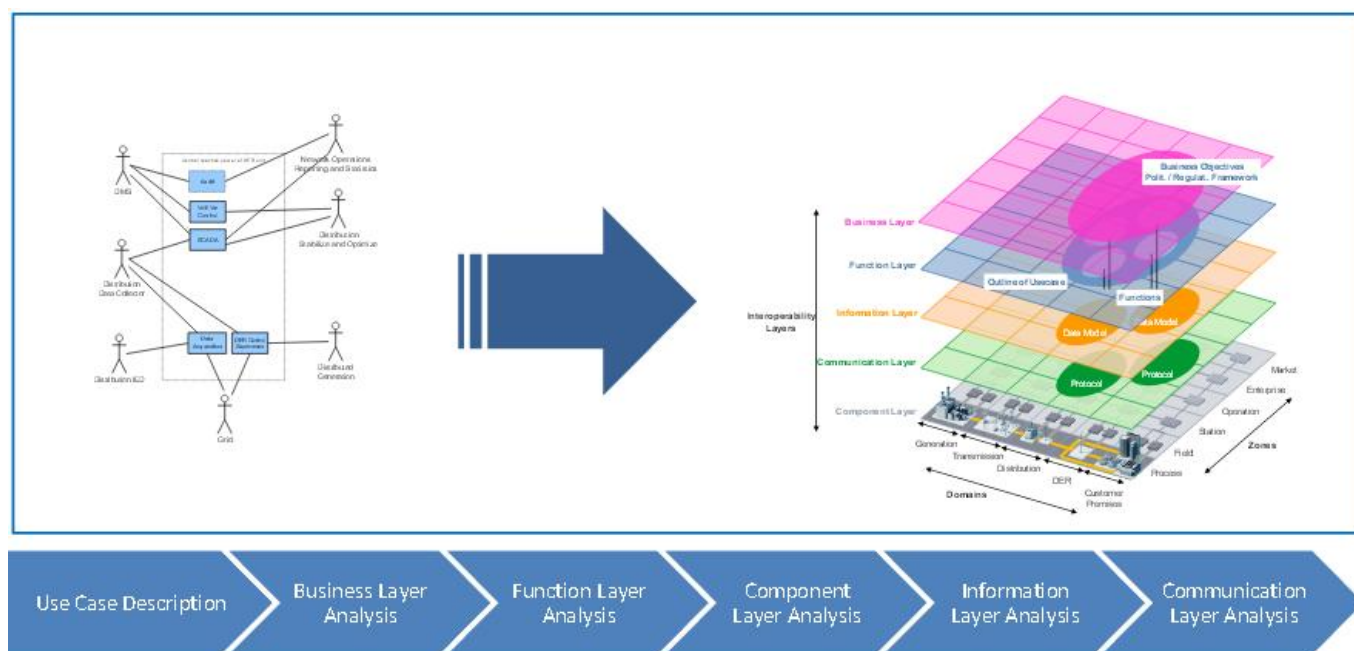


Figure 20. Use Case analysis example with SGAM.

Figure 20 depicts a use case analysis process using SGAM. In this document we shall formulate the demonstrations as use cases and then map these into the SGAM. We shall concentrate on the three lowest interoperability layers in the SGAM model; the information, the communication and the component layers. The information layer describes the information that is being used and exchanged between functions, services and components. It contains



# STORY

information objects and the underlying data models. The emphasis of the communication layer is to describe protocols and mechanisms for the interoperable exchange of information between components in the context of the underlying use case, function or service and related information objects or data models. The emphasis of the component layer is the physical distribution of all participating components in the smart grid context. This includes system & device actors, power system equipment (typically located at process and field level), protection and tele-control devices, network infrastructure (wired / wireless communication connections, routers, switches, servers) and any kind of computers. All layers cover the whole smart grid plane, which is spanned by electrical domains and information management zones.

The three lower layers in the SGAM provide a technical view of system use cases. The use cases can be detailed by defining function groups, functions and their internal behaviour e.g. as flow charts. On the information and communication layer we can derive further details by identifying the information & communication flows between functions and provide references to standards that could be applied. This gives an indication on which standards are relevant for the particular use case and which technologies could be relevant for the particular demonstration. In the next step we can define the information objects exchanged on the information layer and the communication services required on the communication layer. This detailing is followed by the definition of the information syntax and the mapping on protocols for the information and communication layers respectively. On the component layer we can identify the systems involved and in the following step of detailing the devices also.



## 12.2 ICT Security Questionnaire



### Questionnaire to gather ICT security related practices at STORY demo sites

1. Is your organization certified according to 27.xxx standards (software, hardware level and in terms of general security policies)?				
27xxx Standard	Certified	Planned	Note	
ISO/IEC 27001	<input type="checkbox"/>	<input type="checkbox"/>		
ISO/IEC 27019	<input type="checkbox"/>	<input type="checkbox"/>		
.....	<input type="checkbox"/>	<input type="checkbox"/>		
.....	<input type="checkbox"/>	<input type="checkbox"/>		

**Comments:** .....

2. Does your organization support other security standards or guidelines?				
Standard/Guideline	Supported	Planned	Note	
IEC 62443	<input type="checkbox"/>	<input type="checkbox"/>		
IEC 62351	<input type="checkbox"/>	<input type="checkbox"/>		
NIST SP 800-53	<input type="checkbox"/>	<input type="checkbox"/>		
NIST SP 800-82	<input type="checkbox"/>	<input type="checkbox"/>		
NERC CIP	<input type="checkbox"/>	<input type="checkbox"/>		
SGCG/M490/H Smart Grid Information Security	<input type="checkbox"/>	<input type="checkbox"/>		
BSI-CC-PP-0073 Common Criteria Protection profile	<input type="checkbox"/>	<input type="checkbox"/>		
DIN SPEC 27009	<input type="checkbox"/>	<input type="checkbox"/>		
BDEW White Paper - Requirements for Secure Control and Telecommunication Systems	<input type="checkbox"/>	<input type="checkbox"/>		
.....	<input type="checkbox"/>	<input type="checkbox"/>		
.....	<input type="checkbox"/>	<input type="checkbox"/>		

**Comments:** .....

3. Does your organization support a separation between the information technology (IT public) network and the operational technology network?				
---	--	--	--	--



# STORY

<input type="checkbox"/> Yes <span style="margin-left: 200px;"><input type="checkbox"/> No</span>
<b>Comments:</b> .....

<b>4. Does your organization have established a risk management process?</b> <small>Please state also whether standards (e.g. ISO 31000) are used or if your company imposes its own risk management model</small>	
<input type="checkbox"/> Yes <span style="margin-left: 200px;"><input type="checkbox"/> No</span>	
<b>Comments:</b> .....	

<b>5. Do you use tools that support you in the assessment of your security situation, so that potential risks and promptly counter measures can be initiated?</b>	
<input type="checkbox"/> Yes <span style="margin-left: 200px;"><input type="checkbox"/> No</span>	
<b>Tools in use:</b> .....	

<b>6. Does your organization use tools to safeguard, detect and manage cyber intrusions?</b>				
Tool	In use	Planned	Note	
Firewall	<input type="checkbox"/>	<input type="checkbox"/>		
Antivirus software	<input type="checkbox"/>	<input type="checkbox"/>		
End-to-end cryptography	<input type="checkbox"/>	<input type="checkbox"/>		
Whitelisting approach for communication	<input type="checkbox"/>	<input type="checkbox"/>		
Use of data diodes	<input type="checkbox"/>	<input type="checkbox"/>		
Intrusion detection system	<input type="checkbox"/>	<input type="checkbox"/>		
Intrusion prevention system	<input type="checkbox"/>	<input type="checkbox"/>		
SIEM	<input type="checkbox"/>	<input type="checkbox"/>		
.....	<input type="checkbox"/>	<input type="checkbox"/>		
.....	<input type="checkbox"/>	<input type="checkbox"/>		
<b>Comments:</b> .....				

<b>7. Does your organization use tools for recovery, correction of faults or restoration?</b>	
<input type="checkbox"/> Yes <span style="margin-left: 200px;"><input type="checkbox"/> No</span>	
<b>Tools in use:</b> .....	

<b>8. Does your organization have established identity access management at the demonstrator side?</b>			
Type	Established	Planned	Note
Physical	<input type="checkbox"/>	<input type="checkbox"/>	
Authentication	<input type="checkbox"/>	<input type="checkbox"/>	
Authorization	<input type="checkbox"/>	<input type="checkbox"/>	





# STORY

	Role based (e.g. operator/administrator login)	<input type="checkbox"/>	<input type="checkbox"/>	
	Identity based (individual user login)	<input type="checkbox"/>	<input type="checkbox"/>	
	.....	<input type="checkbox"/>	<input type="checkbox"/>	
	.....	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Comments:</b> .....				



## 12.3 General information on demonstration sites

Nr.	Task	Deliverable	Name	Location	Scale
1	5.2	D5.1	Demo. In residential building	Oud-Heverlee, Belgium	Residential Building
2	5.3	D5.2	Demonstrating the roll out of a neighbourhood	Oud-Heverlee, Belgium	Residential Neighbourhood
3	5.4	D5.3	Demo. of storage in factory	Navarra, Spain	Industrial building
4	5.5	D5.4	Demo. of storage In residential district	Lecale, Northern Ireland (UK)	Residential district
5	5.6.1	D5.5	Medium scale unit in Enersys factory	Hagen, Germany	Industrial building (Enersys-Hwaker factory)
6	5.6.2	D5.6	Medium scale unit connected to low voltage substation in residential grid	Slovenia, (TP Suha)	LV network in residential urban area
7	5.6.3	D5.7	Medium scale unit in low voltage industrial grid	Slovenia, (TP Suha)	LV network in Industrial zone
8	5.7	D5.8	Demo. of roll out of private multi-energy grid in industrial area	Olen, Belgium	Industrial zone

# STORY

## 12.4 Case Study 6

