STORY

added value of STORage in distribution sYstems

Deliverable 4.5
Overview of requirements for embedding measurements for services on ICT

Revision..... 1
Preparation date .. 2016-04-27 (m12)
Due date 2016-04-30 (m12)
Lead contractor.... BASEN
Dissemination level PU

Authors:
Topi Mikkola ..... BASEN
Olivier Hersent..... Actility
Pedro Da Silva..... Actility
Shmuel Solomon… Actility
Marjan Jerele… ... Elektro Gorenjska
Arnout Aertgeerts…Actility
Lode Van Halewyck….Actility

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

STORY

Deliverable administration										
No & name	**D4.5 Overview of requirements for embedding measurements for services on ICT**									
Status	Released		**Due**	M12	**Date**	2016-4-30				
Author(s)	Topi Mikkola (BASEN, ed.), Olivier Hersent (Actility), Pedro Da Silva (Actility), Shmuel Solomon (Actility), Marjan Jerele (Elektro Gorenjska), Arnout Aertgeerts (Actility), Lode Van Halewyck (Actility)									
Description of the related task and the deliverable in the DoA	Task 4.3.1 and 4.3.2 provide direct input, other wp4, 5 and 6 tasks provide background information. ICT requirements from installation sites are analysed for potential of embedding measurement and control to ICT equipment. These requirements are analysed and plan for actual embedding is proposed. D4.5 Overview of requirements for embedding measurements for services on ICT Overview of the typical requirements that measurement and data logging equipment poses on the ICT infrastructure.									
Planned resources PM	VTT	THNK	VITO	VLER	BASN	UL	BEN	EG	VIES	HAW
					1			1		
	B9	LOPT	JR	ACT	PROS	CEN	EXL	UCL		Total
				1						3
Comments										

V	Date	Authors	Description
0		BASN TM	Very initial draft
1		BASN TM	Coordinated with ACT
2	2016-3-22	BASN TM	Version merge
3	2016-3-28	BASN TM	Review comments included
4	2016-4-5	BASN TM	Second round of comments
5	2016-4-17	BASN TM	All comments answered, merged ACT version
6	2016-4-24	ACT AA	Final version for release

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

STORY

Table of contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

1 Publishable executive summary

This document details the STORY effort to integrate measurement and control instrumentation with ICT hardware equipment for the STORY demonstration sites. In the current world, end user consumer sites have a wide variety of sensors available, but their interoperability is a problem, whereas large industrial installations are usually operating under a SCADA system and adding new 3rd party devices is a major task. Thus the main focus of this task is in integrating instrumentation with ICT equipment that can be used in consumer sites and small/medium scale industrial installations, where new equipment is needed and SCADA is not available.

STORY project has eight demonstration sites, which can be characterised as six case studies as follows:

- Case studies 1 and 2 are related to single residential buildings and the microgrid where they are connected. These smaller private sites have very little existing instrumentation, so cost and ease of installation are of high importance. In addition, the technologies provided need to be robust and easy to maintain, which is a direct consequence of the lack of qualified on-premises personnel in this use case.
- Case study 3 is an industrial site in southern Europe. It is a self-sufficient site that has both embedded sensors and logic, plus local level computational resources for operation. Due to the local conditions and legislation, it does not feed power back to the grid.
- Case study 4 is a microgrid. Study 4 is not included in this deliverable due to site plans not being ready by the time of writing this deliverable. (Unexpected delay in starting the demonstration.)
- In Case study 5, a medium scale storage unit for the demo case will be connected to 20/0,4 kV MV/LV transformer station supplying a residential village. To enable system control and data acquisition, the demo site is fully ICT supported. The same storage system will also be used at two other sites, with the data characteristics and security requirements being the same.
- Case study 6 is related to an industrial installation, where storage will be used for peak shaving and added stability, with later a possibility for selling excess energy and completely isolated for security reasons, so all monitoring and control happens on site, with monitoring data being available as off-line batch dumps. The internal communication is via a local bus, with all the data gathered in a local SCADA installation. This installation will also handle the control processes, so the site has no requirements for external layer 3 access.

This document describes the data characteristics (both measurement and control) for all STORY demonstration sites and describes the common shared properties. These characteristics have been collected partly in connection with the demonstration and measurement related tasks, and are used here to give an overview of typical data, amount of network traffic, and required response times. The hard real time control (cutting breakers due to frequency drops etc.) is handled within the sites, as time requirements are typically under 10ms, whereas the control requirements for STORY are timewise mostly of short or medium term, where local storage is used to shave consumption peaks, optimize site energy availability and optimize energy consumption in regard to market price. Response time requirements for such control tasks are usually in the order of minutes.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

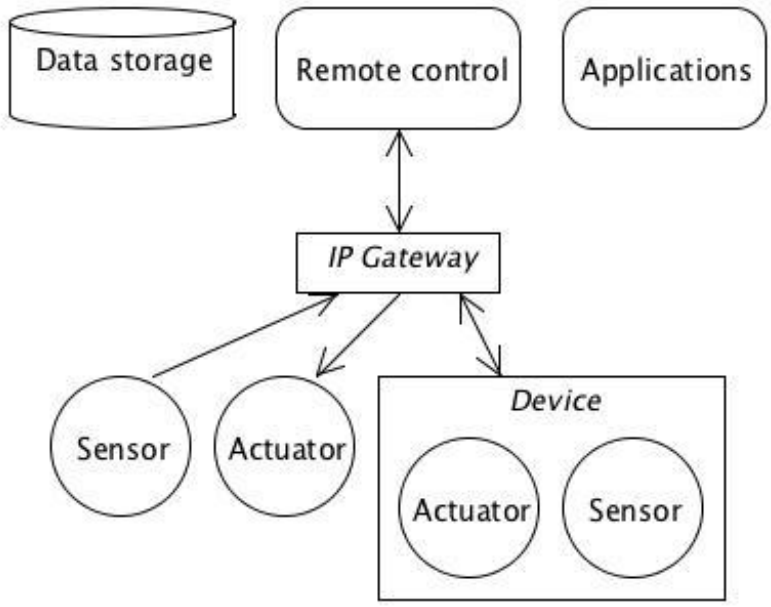
Project STORY - H2020-LCE-2014-3

Typical site security is also discussed. Most industrial sites are either completely isolated from the outside network or access is through a single point, whereas consumer sites are in public network and both measured data and control commands must be encrypted and authenticated. Similarly, a secure way of arranging a bi-directional access (for control) to the consumer sites has long been a problem, as these sites often do not have a public endpoint (e.g. a public IP address) but an address which either keeps changing or is behind a NAT or a similar arrangement.

From this overview data, high level requirements are extracted. These requirements are used to show how a modern wireless approach like the LoRaWAN long range radio based system can be used to provide data transport and bi-directional access in a secure way, while still allowing legacy equipment to be used as part of the installation due to an easy integration process.

We also show how the chosen approach maps to the STORY 3 layered model of functionalities and responsibilities (Table 1).

Table 1 The STORY 3 layered model

<table>
<tr>
<td rowspan="3"> 
</td>
<td>Layer 3: remote
• Long term optimization
• 3rd party access to data
• Forecasts, reports</td>
</tr>
<tr>
<td>Layer 2: site
• Local control
• Authenticated access to layer 1
• Site coordination
• Driver abstraction for layer 1 devices</td>
</tr>
<tr>
<td>Layer 1, device
• Embedded devices and actuators
• Device safety
• Fall back logic</td>
</tr>
</table>

Main problems encountered in this preliminary review were the lack of standardization on the low level sensors and very restricted budgets with which the house hold installations must be made. In larger sites the main challenge is the restricted nature of SCADA systems – it is very hard to install new components without a SCADA manufacturers' consultant help. STORY's proposed answer to this is to standardize the access above layer 1 and to provide a wireless LoRaWAN based approach for manufacturing new sensors and for integrating existing ones. Both the lack of standardization and vendor lock-in would be at least alleviated, if all systems supported standard south- and northbound APIs, whereas wireless approach makes sensor selection and installation easier.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

2 Introduction

The purpose of this document is to analyse the results of previous wp4 tasks and installation site documents from wp5 and 6, to find out what part of the required instrumentation (metering and control) could be embedded into the local ICT equipment. It is assumed that the reader is familiar with the earlier STORY document (D4.1[6]) giving a structured overview of current and emerging communication standards for smart grids, including the criteria for data exchanges and communications and the general description of the demo sites. This document gives a brief overview of each site as far as is needed to explain the requirements and peculiarities of each individual site. This deliverable mainly builds on top of the work done in tasks 4.3.1 *Measurement and data logging characteristics* and 4.3.2 *Potential for embedding measurements in ICT*. The first part of the document covers each individual site, the second part gathers the requirements and classifies the types of installation sites. Finally, the third part of the document covers the potential for embedding the needed functionality in ICT, details the chosen LoRa technology and discusses some of the problems and pitfalls. Interoperability guidelines (from D3.6) are also used for baseline requirements and recommendations on the pitfalls of system design.

STORY is aiming for a cloud controlled solution where data is pushed to the cloud as quickly as possible. This means that the main function of the local ICT is to provide a stable and secure connection gateway using standard protocols. Furthermore, this approach means that when the connection to the local system is available, anyone supporting the communication standard can quickly build their own solution on top of that and these solutions can easily be switched, avoiding the normal vendor lock-in problem. This approach starts from the assumption that a site owner/data source owns their data, so relevant data can be sourced and used in higher level applications.

Regardless of the cloud/remote solutions, every site will still need physical sensors and often support for legacy systems, which can often only be communicated over a local bus solution. To this end, STORY introduces a 3 layer approach:

- Layer 1: Device Management System which handles the embedded layer.
- Layer 2: Site Management System which handles local site orchestration and logic, plus provides a fall back for cases where the network is unavailable.
- Layer 3: Remote layer which handles higher level optimization, provides remote control access.

These layers are described in particular in chapter 4.2.

Currently the big industrial sites already have the measurement equipment integrated with their SCADA-systems, so it is not feasible to introduce a new layer of ICT devices in those sites, as new devices must pass much more stringent evaluation and certification. The STORY ICT-integration is more geared to private HAN installations and small/medium commercial installations. The remote layer logic is also applicable to industrial sites but lies outside of the scope of this document.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

The STORY sites share the same problem as any commercial or research project: the plethora of sensors means that the integration to all the necessary sensors and actuators is a challenge and requires significant resources concerning interoperability. Presenting at least a partial solution for this is one of the main goals of this deliverable. We will categorize the available devices per communication method and propose an integration to the LoRa based communication to present the upper layers as a more unified interface.

LoRa has been chosen as the communication method between layers 1/2 and 3. The main advantages of LoRa are ease of installation, inbuilt secure transmissions and good wireless coverage both indoors and outdoors. Ability to share base station between installation sites also drives the costs down. LoRa is discussed in chapter 7.

3 Installation sites

This chapter briefly covers the STORY installation sites which are described in more detail in STORY deliverables D4.1 [6] and D4.3 [7] – here the main focus is on the interfaces supported, data characteristics, and security issues from the STORY point of view. For security and privacy reasons, site details and exact data cannot be revealed in all cases. Site 4 has been omitted, as site ICT structure was still in planning stage when this deliverable was written.

3.1 Case Study 1-2, private sites and microgrid

3.1.1 Overview

These smaller private sites have very little existing instrumentation, so cost and ease of installation are of high importance. In addition, the technologies provided need to be robust and easy to maintain, which is a direct consequence of the lack of qualified on-premises personnel in this use case.

As a consequence, the focus is placed on robustness of the communication layer, and also the cost of installation, which favours wireless technologies:

- Once the communication distance issues are addressed, star topology wireless technologies are extremely stable. Unlike wired technologies, no physical action can damage the established links. Furthermore, troubleshooting is also simple as it never requires inspection of the wired path, a well-known nightmare of installers in building automation. As new radio technologies now allow communication distances compatible with wide area deployments without a need for mesh in the ISM band, these technologies, such a LoRaWAN promoted by the LoRa alliance, provide the optimal characteristics for the use case.
- Cost of installation is obviously lower with wireless. In [1] the author mentions a wiring cost of 200USD per meter in “ordinary process plants” (p82). In typical residential buildings, a technician will typically install about 10 to 20m of wiring per sensor, and even with a much lower cost of wiring than mentioned above, the installation cost typically exceeds the cost of the sensor. On top of this, most building automation technologies require manual routing configuration, adding to the cost and requiring expertise.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

3.1.2 Data characteristics

Table 2 Site 1 and 2 data requirements

Measurement	CoV triggers	Latency requirements	Comments
Temperature	0.5°C 15mn minimum interval 4h maximum interval	None, may be batch compressed	For each main thermal zone requiring inverse thermal modelling
Electric cumulated energy (Active)	15mn intervals	None, may be batch compressed. Only exception is if local micro grid participates in fast reserve TSO program requiring real-time reporting.	For each modelled apartment or building. Separate meters may be required if aggregated loads do not belong to categories that may automatically be separated from aggregated load curve.
Electric cumulated energy (Reactive)	(optional)		
Electric power (Active)	100W 15mn maximum interval 10s minimum interval (optional if deaggregation not needed)		
Electric power (Reactive)	(optional)		
CO2	(optional) 15mn interval		Required only if occupancy is not known by profiling

If and when control actuators will be required, e.g. to control distributed storage, the reporting requirements will be detailed as a part of specification of such actuators.

3.1.3 Security requirements

There are no identified risks associated with the use case for sensors, except usual protection of data from eaves dropping. In cases where the network is also used to control actuators, it is important that attackers cannot feed the system fake commands or replay old ones.

For distributed radio networks, the main requirement is to avoid security flaw propagation. The system will leverage LoRaWAN standard security with a security key per device. Payload is secured by AES encryption with replay protection.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

3.2 Case Study 3, industrial site

Case study 3 is an industrial site in southern Europe. It is a self-sufficient site that has both embedded sensors and logic, plus local level computational resources for operation. Due to the local conditions and legislation, it does not feed power back to the grid.

3.2.1 Equipment used

The site has multiple PV inverters and connected power converters providing both measurement data about energy productions and a bi-directional control channel. In addition, standard power meters are installed in various key locations. The internal site connection is done via Modbus TCP/IP and the external connection is via web service.

3.2.2 Data characteristics

The internal site measurement cycle is 1 Hz and approximately 48kbits of data is generated in one cycle. This data will generate three primary KPIs based on four main measurements. The Sste will at least initially handle both layer 2 and 3 logic internally, so site measurements are collected externally, but no control interface is provided.

3.2.3 Security requirements

For security reasons, the site is isolated from the rest of the network and data collection access is provided through a dedicated server which is protected by firewalls. Connection to the server is encrypted and authenticated.

3.3 Case Study 5, industrial site

A medium scale storage unit for the demo case will be connected to 20/0,4 kV MV/LV transformer station supplying a residential village. To enable system control and data acquisition, the demo site is fully ICT supported. The same storage system will also be used at two other sites, with the data characteristics and security requirements being the same.

3.3.1 Equipment used

A Sipronika network control server (SNCS) acts as the heart of the control system and provides all control functionalities required. Besides typical local SCADA functionalities, it also serves as a powerful communication platform enabling communication between different distribution devices. Some basic SNCS functionalities provided for the site are:

- Connection to Power Quality server enables online network measurements readings by using standard OPC UA communication protocol
- Connection to RTU installed in TS, enables MV and LV equipment control using standardised DNP 3 protocol
- Connection to transformer AVR unit (PLC) enables transformer control using standardised DNP 3 protocol

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

- Connection to DCC SCADA provides all necessary data exchange with other internal systems and is based on IEC 104 standard protocol

Broadband WiMax radio provides an universal communication platform for remote control. The LV and MV networks use a WiMax communication and the HV network operates with a fibre connection. The communication and control will happen either over OPC UA when the SCADA is present, or over DNP 3 when communicating directly with the storage system.

3.3.2 Data characteristics

The site will have both measurement and control data, with very high security and availability requirements. The hard real time control happens in-site and is outside of the STORY scope. Data includes, but is not limited to:

- Power quality meter data
- AMI metering data
- Transformer station remote control data
- OLTC remote setting
- Energy storage quality measurements

Each site will have multiple power quality analysers, which will provide upwards of 30 measurements per cycle. Initial reading cycle is 1 minute, but control algorithms might require higher granularity.

Using the 3-level approach, the level functionality is:
Layer 1, embedded in devices:

- Control
- Protection (overload, battery emptying)

Layer 2, site local:

- Real time status
- Scheduled operations

Layer 3, remote:

- Overall optimization
- Voltage profiles
- Market data
- Forecast data (weather, pricing, usage)

3.3.3 Security requirements

The site is isolated from the rest of the network, with access provided only via SCADA servers. Access to the SCADA is both restricted with firewalls/access control lists and requires user authentication over an encrypted channel. OPC UA security models will be used. Control messages must also be authorized and audited.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

3.4 Case Study 6, industrial site

The site is an industrial installation, where storage will be used for peak shaving and added stability, with later a possibility for selling excess energy and completely isolated for security reasons, so all monitoring and control happens on site, with monitoring data being available as off-line batch dumps.

The internal communication is via a local bus, with all the data gathered in a local SCADA installation. This installation will also handle the control processes, so the site has no requirements for external layer 3 access.

4 Summary of Site Equipment and requirements

4.1 Installation site types

The STORY installation sites can be divided in two categories, which have very different requirements. In reality these have some overlap, but from the point of view of embedding the sensors, they have to be separated.

4.1.1 Shared characteristics

The current hardware market is full of various sensors and actuators, but the level of standardization is very low, and from an end user's perspective, overall usability is also low. So this means that either sites use old and well known technology, or the owner takes a risk that each site will be using different connection and control logic, making maintenance very difficult. Private sites tend to use more modern (more market appeal) technologies, whereas industrial sites usually lean towards tried and well understood systems with a well-an established developer community.

Ease of installation must be relative to the level of user expertise and the requirements of the site. While it is permissible that for a big industrial site a team of technicians is needed, a private site installation must be doable by a non-educated layman to the extend allowed by the local laws. Similarly, the configuration and provisioning of sensors must be as easy as possible. In the perfect case no customer interaction would be needed, but an acceptable level is a configuration via a non-technical user oriented web application, with all the necessary services and models auto discovered from the devices. (So, the user does not need to install special software, or delve down to level of local bus communication parameters).

Safety and reliability are required by all sites. On private sites, this usually means high availability, ability to cope with situations where the network connectivity is lost, and good security against ICT threats. Industrial sites usually base their ICT security on a multi layered approach where access to the network is limited. Therefore, security is provided with auditing and validating control commands, having reasonable fall back logic fail safes, and near instant (millisecond level)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

response times to faults. On industrial sites, high availability usually means also battery back-up solutions which can survive power network irregularities (e.g. UPS).

4.1.2 Private installations

The smaller private sites and micro grids usually have little if any existing instrumentation, apart from the DSO supplied meters. Furthermore, usually the cost of integrating with the existing legacy equipment exceeds the cost of installing new equipment, as additional hardware and software converters are needed. These installations (households, very small area micro grids) are by nature very heterogeneous, in both available equipment and in optimization/control requirements. Most of them want to either optimize energy consumption or living comfort, while service stability and perceived safety are additional important factors.

In addition, the technologies provided need to be robust and easy to maintain, which is a direct consequence of the lack of technically qualified on-premises personnel in this use case.

Equipment varies from old home automatic (pumps, meters, HVAC) equipment to local smart home solutions and more modern IoT enabled white label goods (fridges, washing machines), so any central communication/control system must be able to cope with several interfaces – often a small (embedded) computer acting as a base station. All the usual local bus protocols and physical interfaces must be supported, and to provide a satisfactory customer experience, the system should in an optimal case also support 3rd party vendor locked protocols.

For optimization, each installation will usually have their own local optimization targets. These are usually related to shaving easy loads from normal usage (stand-by power, shutting down lights when no-one is home) or providing more comfortable living conditions (automated lights when residents arrive, making sure warm water is ready when tap is turned on, HVAC keeps temperature comfortable) – sometimes the goals can even be contradictory. More modern systems might also make local optimizations, e.g. using PV generated power for air pumps, storing heat in structures, or even advice residents when selling renewables production back to grid for monetary compensation.

STORY is also piloting a case where multiple private sites in the same area and on the same feeder are grouped together to create a small local micro grid – the idea could also be extended to create a virtual micro grid, connecting private sites from different locations and feeders. As loads and production of individual sites are relatively low, their use as a balancing load for a DSO or a backup in local power loss situation is limited. But when many sites are grouped together with even soft real time control available, several new options are opened.

Security in private sites is usually based on denying physical access to the devices or to the local communication network. In best cases, the local network is also protected by a consumer grade firewall, embedded into the modem or router. Sites also usually operate with only one public IP, so most IP enabled devices are behind a NAT, meaning that direct connection from outside is not feasible without prior arrangement.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

Control requirements for these sites are time wise relatively soft. Lights and similar immediate feedback giving devices are controlled locally, whereas most of the loads used for optimization, e.g. boilers, heaters and water storage, rarely need more than a few minute reaction time. (More complex systems like water controller by multiple valves might need quicker reaction time, but that is always case by case.) This means that the requirements for measurement frequency and latency/round trip time of the control channel are not very high. In most cases minute resolution is enough and even the hardest requirements are in second resolution, with no need for sub-second granularity in measurements or response times.

The Internet connection to private sites is usually via a consumer grade non-redundant Internet, so any local base station must also be able to cope with situations when the outside connection is lost for indeterminate time.

4.1.3 Industrial installations

The rest of the STORY sites can be classified as bigger industrial sites, either factories or larger micro grids. They are characterized by having a far higher potential for both load shaving and energy storage, and the optimization targets are usually purely economic or ecological.

The sites usually have industrial equipment using standard protocols, with an overall SCADA system handling monitoring and controlling. The interoperability requirements between SCADA and the installed devices means that the possibility for adding extra devices to the system is restricted, and the need for doing that is also much lower than with small sites, as most devices already contain all necessary interfaces.

Security is handled on several layers. Most of the devices operate in a network which is isolated from the rest of the world, with only access being through a central server (SCADA). The central server has limited access to outside world, usually protected with both encrypted and authenticated communication channels, and a dedicated firewall which can analyse incoming traffic for accepted connections. Most individual actuators will also contain embedded logic that will automatically handle fault situations and primitive safety checks on commands. Physical access to devices and SCADA is also limited, as it is a likely attack vector.

Control requirements for these sites are twofold. Physical security related control (islanding in case of frequency problems, lost phases, impeding blackout) has to happen in a few milliseconds, which limits the control to the local servers. Similarly, the best effort nature of Internet dictates that these sites either operate with a dedicated backup connection in addition to Internet, or a private dedicated network (dedicated optical network, WiMax or similar). Some of the less response speed reliant control (secondary power generation, energy dump facilities) can use remote control signals (DSO).

Industrial sites are standardized to far higher degree than private sites. Modbus, Profibus and DNP3 seem to be most common communication standards, with OPC (or OPC-UA) available for SCADA integration. Modbus, Profibus and other old local bus standards support only one

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

communication master on the bus, and therefore data collection and control by necessity goes through a dedicated master, which allocates bus time to different requests.

Optimization potential is obviously much higher than with private sites or small micro grids, with power consumption being in easily in the range of 10-100kW. Many sites also have the potential of using energy storages (ranging from simple water tanks to more complicated battery solutions), in order to buy energy when it is cheap and prioritize the usage of stored energy when buying is expensive.

The large industrial sites have their SCADA and monitoring equipment installed, so there is little potential for integrating STORY equipment, unless a significant market penetration is achieved. Main potential for the STORY wireless solution lies in the residential sites and private micro grids, which either need new equipment or integration with legacy installations.

4.2 Architecture

The previous generations of sensors and actuators were based on either a completely local approach with local bus communications and PLCs containing the control logic (most small/medium installations), or in approaches where the system was completely isolated from the world (large industrial installations). Both of these approaches have problems with flexibility and security existing mainly at the border of the installation.

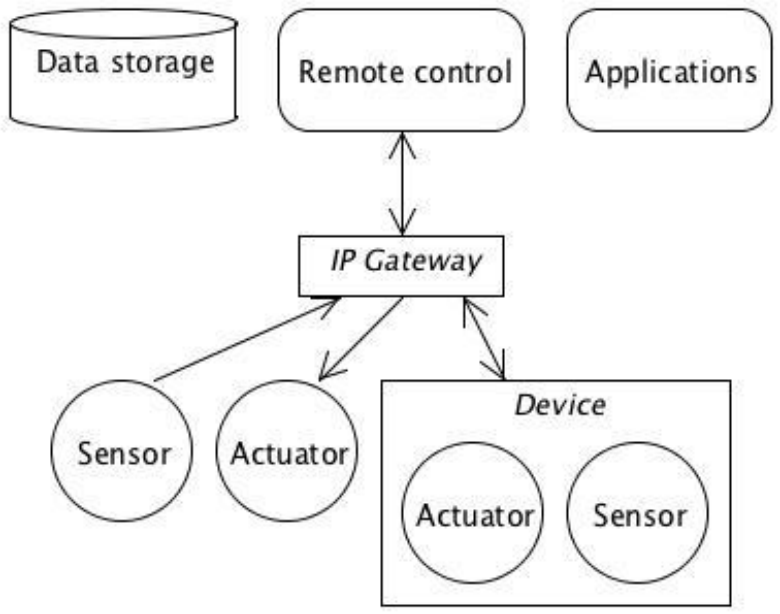
Modern systems exist in a world with distributed cloud based services, so systems can also utilize external measurements (price of electricity, expected breaks, weather forecasts, etc.) and do expensive calculations outside the local system. But in the power grid, some of the decisions need to happen with hard real time requirements (millisecond level), so control solely over internet, which by nature is only best effort, is not feasible. To this end, STORY introduces a 3-layer approach (Table 3), with all layers having separate requirements and responsibilities. This also makes it economically and technically more feasible to provide new solutions, as solution can access other layers via predefined APIs with needing to know the implementation details. This approach is used both for site modelling and for control strategies, even if in the chosen embedding strategies layer distinctions are somewhat blurred.

Each layer is responsible of its' own safety, in both functionality and data. For low level embedded sensor this might mean safety checking new parameters, environmental safety and local communications encryption, whereas for local layer this would mean both authenticating and authorizing control commands, ability to function when network connection is down etc.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

Table 3 The STORY 3 layered model

	Layer 3: remote • Long term optimization • 3rd party access to data • Forecasts, reports Layer 2: site • Local control • Authenticated access to layer 1 • Internet connectivity • Site coordination • Driver abstraction for layer 1 devices Layer 1: device • Embedded devices and actuators • Device safety • Fall back logic

4.2.1 Layer 1 Device management

Layer 1 deals with the actual embedded instrumentations: sensors, actuators and devices. This layer supplies most of the low level measurements and executes the actual device commands. Most of the devices on this layer have very little if any computational resources and will only check the command for immediate effects and single parameter validity. For legacy sensors security is mainly due to restricted access whereas more modern ip-based sensors may also either check source identification (shared secret) or can authenticate call via other methods. Layer 1 devices mostly contain intelligence about their own operations.

This is the layer where new ICT technologies have most to offer, so embedding effort will concentrate on layer 1 devices and the interface between layers 1 and 2. D3.6 Interoperability guidelines [8] list good and bad design practises for this level devices and interfaces.

4.2.2 Layer 2 Site management

Layer 2 is local, or site specific. It has access to all the instrumentation and local computation resources and data storage. With modern systems these resources are significant, so most of the logic can, when required, reside on this layer. This layer provides all the fall back logic and safety when internet connection is lost or when layer 1 systems unexpectedly signal an error. In normal operation, optimization parameters, scheduled operations etc. are provided by the layer 3.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

Layer 2 is responsible of providing an access to all the layer 1 resources and verifying the commands so that the combination of parameters stay within legal operational limits. Layer 2 also provides an interface towards layer 3 services – for security reasons, this access should be both encrypted and authenticated, in addition to having suitable traffic restrictions.

4.2.3 Layer 3 Remote

Layer 3 in STORY is the remote optimization and management layer, which can access external services (weather forecast, spot pricing, coming service breaks, etc.) and has the required computational resources to run overall models producing both short and long term optimization for a site. It also contains the facilities giving the user the ability to manage his installation.

- External APIs: external applications that want to connect to the system, accessing it via API at layer 3. In this way, a system only has one well defined and secure access point.
- Connection to external data systems: layer 3 provides the system with access to external data. These include but are not limited to: weather forecast, spot pricing, grid level events.
- Platform to run the site model and prediction software, which can be used to optimize both single and multiple sites.
- Layer 3 allows user to push both short and long term control logic down to layers 1 and 2. In this way, layers 1 and 2 can use cheaper hardware solutions, as the logic is mainly in the cloud and the local system just has the necessary failsafe logic.
- Layer 3 provides site and device managers, so users can control and manage their instances. This means that layer 3 is in charge of device identification, encryption keys etc.
- Billing and provisioning of new services is also provided in layer 3.
- Layer 3 also provides clearing house functionality, for cases where site owners want to either sell energy, or capacity to store/dump energy.

4.3 Current situation and future goals

In addition to requirements from individual sites, it must be taken into account that STORY does not happen in isolation. Adoption of smart grid and intelligent storage technologies is not a revolution but a slow and steady evolution, so any ICT solution must take into account both the already available hardware and control software for each site, and also the commercial feasibility of any new solution.

As the overview in previous chapters shows, most sites use old de facto standard technologies, where the original standards might be decades old. These standards have been updated several times but as they almost always need to be backwards compatible due to the amount of existing equipment, some of the old design principles cannot be changed. All these issues already have solutions in either modern or emerging technologies, so they are covered here from the point of view of currently desired end solution - all these are things that the STORY embedding should take into account and provide an answer for. The global transition in big commercial installations and thus developer communities will be slow, so the system must also have an intermediate answer.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

The main foreseen technological transitions that impact STORY are summarized below. These transitions won't happen immediately, but the STORY solution must have an intermediate answer and be compatible with the future.

Table 4 Foreseen technological transitions

Legacy technology	Future answer
Installation specific addressing	Hyperconnectivity and autodiscovery
Security based on physical access	Multilayer security
Local maintenance	Autodiscovery and self-description
Revalidation of elements	Separations of modules
Local bus access	Modular communications

4.3.1 Addressing

Most old standard technologies (particularly different fieldbus solutions) use installation site specific scaling, where the bus can support a predefined amount of unique addresses (often 255) which have to be manually configured to the devices. This means that the addressing scheme does not scale upwards and it is very hard to move sensors/actuators between sites without reconfiguration. This was partly mitigated by protocols using IPv4 addressing, but while individual sites could have, for practical purposes, an unlimited address space within IPv4 private blocks, devices could still not be globally identified by their address alone. The current solution for hyper connected IoT devices is IPv6, which offers both a large enough address space and the capability of having globally unique addresses for any connected device.

4.3.2 Security

While the old local bus solutions mainly relied in the physical security of a bus against eavesdropping and having authentication only in connection nodes, hyper connected devices must assume they are always connected to a wider network. Similarly, the current consumer grade devices make the assumption that security is "someone else's" problem, leading to world of open HVAC controls, publicly available cameras etc. Next generation devices must make the assumption that the network might be hostile, so every layer must be able to handle its' own security: ability to encrypt traffic, authenticate connections and authorize commands at the minimum, with the ability to also audit (log) the relevant commands and connections.

4.3.3 Configuration

In addition to the scaling problem, local configuration of devices also means that maintenance becomes very hard. Either a special software must be used (e.g. KNX) or anyone with the access to network can configure devices (modbus), meaning that the maintenance/configuration is easily locked behind one person and information is easily lost when she leaves the organization. The next generation systems must support both autodiscovery (ability to automatically detect and identify devices available in network subsection) and they must be able to provide self-description (what operations device supports, what measurements are available).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

4.3.4 Validation of elements

Currently, most industrial SCADA systems have very strict requirements for adding new devices or services. These must be certified, validated and afterwards the whole system might need a revalidation to see that computation and bandwidth requirements are still met. When the communication is moved to modern IP-based communication, all the validation can be moved to a conceptually higher level (as communication devices already handle the physical connection.) and standard communications tools are available for limiting network access (Quality of Service tools, giving higher network access priorities for critical services), process throttling (giving lower priority for less important processes) and software interfaces can be made software language independent and given a standard test/load packages.

4.3.5 Communications

Each local bus communication protocol has its own physical bus requirements (voltage/current message levels, needed wiring etc.) meaning that for a big installation site, different sensors and actuators might require different wirings side by side, driving both costs and installation complexity up. Modern systems must be able to operate in IPv6 network with various communication modes being transparent to other layers: optical fibre for high performance and reliability, various wireless technologies for ease of access, twisted pair cabling for low economical cost etc.

5 Unified baseline requirements for embedded ICT services

With the three layered model and characteristics/requirements from various sites, it is quite clear that ICT embedding falls mainly to layer 1 and has most applicability in private and small scale industrial sites where SCADA is not a de facto industry standard. This chapter outlines the requirements for embedding ICT measurement and control functionality in existing equipment.

One of the biggest requirements from different sites is the ability to interface with various different existing interfaces. Usually required sensors and actuators are available, but setting up a working communication network is a major task. So this can be formulated as a requirement for an interface with various physical and legacy local bus interfaces, and present a single unified interface to higher layers.

Readily available connection to most sites is either 3G/4G or a consumer grade internet connection, with best effort availability. Combined with control requirements, this means that in smaller installations, layer 2 has the requirement to be self-sufficient in all situations. As hard real time is usually not a requirement for smaller sites, data per sensor is usually of either second or minute resolution. This means that if the normal size of a data packet is 3*8bytes (8 byte timestamp, 8 byte payload and 8 byte universal identifier), one data packet is 192 bits. Even with 1Hz data reading

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

resolution, the needed bandwidth for data alone is minuscule by modern standards. (The amount of monthly data at a 1Hz interval would amount to roughly 60 Mb.) So as long as the connection is available, neither bandwidth nor round trip time are major problems.

It is worth noting here that if data is sent forward every 1 second with TLS (as HTTPS does), or other algorithms using repeated handshakes, this is a significant overhead to the data traffic. Depending on the handshake protocol, keys, etc. this is easily a few kilobytes more per transaction. Meaning that a 28byte transaction suddenly has 2kb extra, resulting in an overhead 100 times the payload. For this reason, either the cryptography must be based on pre-shared keys, bandwidth requirements must accept this, or data must be sent with a lower frequency.

Control applications in small sites have either minute resolution time requirements (switch to battery, start charging etc.) or a few seconds' resolution (valve switching, alarms) with sub-second control being done on site (light switches). This means that the backchannel of the measurement sending suffices in most situations.

The data generated in the STORY installations is both security and privacy sensitive – sites can be controlled remotely and patterns (and deviations from patterns) can easily be identified from the data. So the system has a requirement for sending all data encrypted, and all connections must be both authenticated ("who am I communicating with"), authorized ("Is the requestor allowed to do this") and all major actions must be audited ("Who sent this command, who made these changes").

In the smaller sites, STORY is working with consumer grade internet connections, so remote availability is mostly set by the internet service provider and cannot be influenced by the project. For the internal system, high availability is a good thing, but more important is a capability of recovering from errors. (Internet down, power lost, human boots the system). This also means that necessary amount of sensor data and access to all actuators must always be available to the Site Management layer, even if outside access is lost.

One of the big obstacles with even modern systems is the need for an expert user. From system physical installation (modbus line termination, knx wiring, wlan authentication) to logical configuration (knx physical-logical mappings, firewalling local base station etc.) an expert is needed to set up a sensible and fault tolerant system. IoT means that every home will have more and more connected appliances and if human intervention is needed to set up each and every of these devices, the end result won't be secure. So there is a requirement for easy setup, preferably with no local configuration needed. This also means that the system must be wireless and able to join the network without expert human intervention.

For usability and user acceptance purposes, the system must be such that the end user can at any point add or remove sensors/actuators from the system, or restrict the data they are sending. It is also of importance that the user can define which devices are hers, so that adjacent sites cannot accidentally or intentionally listen to each other, without both users expressing their confirmation. The solution for this is not to limit the range of wireless network, as data transfer must be available despite heavy walls, some sensors being outside etc.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

Many of the local bus approaches expect that the main security comes from the fact that an intruder cannot access the physical network. With modern wireless systems, this aspect of security is moved to the communications layer. All embedded systems must be able to function normally in a hostile network, where other network elements cannot necessarily be trusted. Communication partners must be identified and communication must be encrypted between end points.

Sensors/actuators must work with minimal human interaction containing either a battery which allows at least a year of operation and the ability to signal low battery power, or energy harvesting.

6 Potential for embedding

Requirement for wireless access and data availability locally for a Site Management system means a wireless network and a supporting base station solution. From the hardware point of view, suitable base stations are readily available commercially as long as communication APIs are the same, base stations do not matter much to the embedding scheme. (This is covered in Deliverable 4.3 [7]) So here we concentrate more on the actual potential for embedding measurement/actuator control in ICT.

High end white label goods, programmable lights, etc. already have a wireless solution embedded and can often be interfaced by the base station directly leaving future products and the plethora of existing legacy devices as the focus of this report. These devices often have parts of the layer 1 functionality already embedded (simple failsafe logic, parameter sanity checks) and are mainly lacking communication options and security. So the obvious embedding strategy is to provide an easy way to add secure wireless communication capacity to these devices. In the STORY model, the sensors and communication are on layer 1, whereas the base station is on the layer 2 for most sites.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

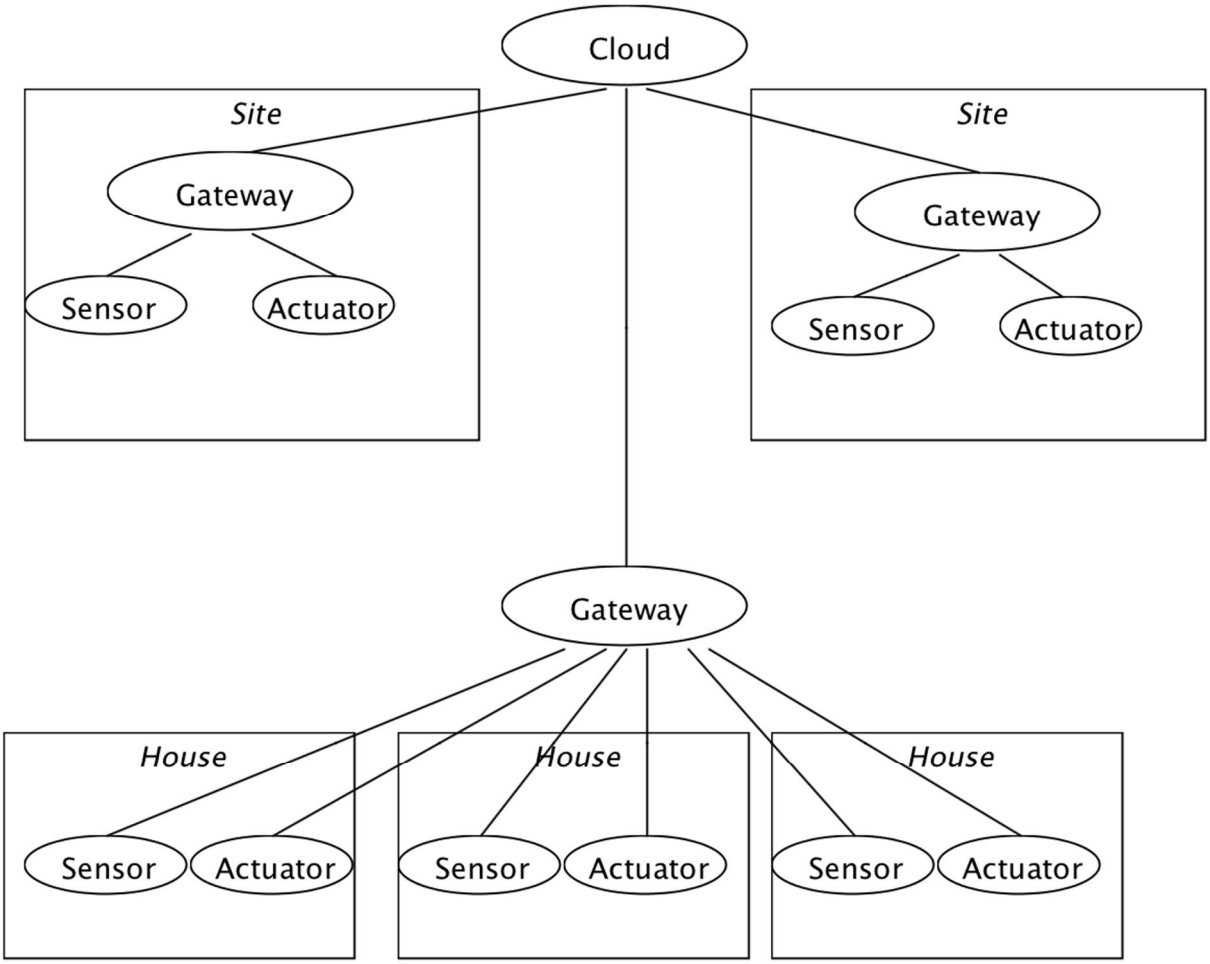


Figure 1: Different install options for sensor + base station

Figure 1 covers the main 2 use cases. In the first case each site has its' own base station controlling the local sensors and actuators. In the second one, there is a single base station serving multiple sensors/actuators. These sensors can belong either to multiple individual sites or sites which together form a bigger *virtual* site. In this case it is the base station's responsibility to make sure that each user sees only their own data. A base station can either be local, or when the base station covers wider ranges (10km+) it is shared by multiple virtual sites and is essentially a part of the 3rd layer.

In the chosen LoRa approach, the LoRaWAN network properties allow collaboration between all base stations. Therefore, regardless of the number of base stations, from a topology point of view, this will always be "the network" to the sensors. Gateways may be added dynamically without any network planning whenever link budget requires improved coverage, or when capacity increase is required. Indeed, any improvement in link budget is leveraged by the LoRaWAN standard to increase communication speed, and therefore reduce airtime and increase capacity.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

6.1 The sensor part

As outlined in D3.6 Interoperability Guidelines [8], a driver model is preferable for interfacing with legacy devices. This allows the upper layers to treat all the devices in the same way, with the necessary communication details abstracted away by the drivers. For most industrial legacy equipment, this is expected to be Modbus which does not support any form of security, and generally expects that the local wired network is protected. Note that as the ModBus drivers actually support ModBus TCP, any other serial Modbus device needs to interface via a controller ModBus TCP interface, or via a ModBus TCP bridge (Many sensors will be installed in the various use cases, and for the reasons exposed in section 3.1 are likely to use LPWAN technology.)

For new sensors, they may easily be developed by using:

- USB for any application that interfaces with a microcomputer (Raspberry Pi or any industrial computer)
- Communication Modules which are widely available commercially
- Open reference designs

As easy availability is required, a model like LoRaWAN where the whole communication stack is available as open source is desired.

Great care must be taken to keep any communication extremely compact, typically less than 50 bytes. This requires careful programming with binary payload format and compression (e.g. differential compression for time series).

As LPWAN solutions might share base stations and receivers, it is necessary that the sensor can both identify itself towards the network, encrypt the traffic and encrypt the payload so that the network elements themselves cannot sniff the details of the message. This can be achieved for example with two secrets as used in the LoRa model (one for the network and one for the application payload.)

6.2 The base station part

The traditional smart grid base station serves one installation, acting as an abstraction point for local devices and providing the upstream communication and security. It is a proven concept, but particularly in smaller sites, the financial cost of installing a separate base station to each site might be prohibitive. Furthermore, it adds one more device to be maintained, and a single point of failure for each site, as all traffic flows through it.

To this end, STORY embedding will at least partially skip the traditional base station and use LPWAN wireless base stations, which will be able to serve a much wider area by just relaying traffic between layers 1 and 3.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

Base stations in the LPWAN model are not involved in the end to end security concept: they just act as relays to the central controller. As a consequence:

- Base stations can be shared: sensor data can go via any base station without any implication of security
- Base stations compromised by an attacker do not give more access to the data to an attacker than wireless sniffing.

The back-end interface or "Tunnel interface" provides a REST based interface for uplink measurement data and downlink commands.

This model will also provide a simple service discovery as base stations have a list of registered devices which will then be able to provide information about their capabilities via drivers.

If extra resilience is required, this can be addressed with the base station topology and placement – having extra base stations using different internet connections means that sensors can always reach multiple base stations. Finally, base stations can also provide non-volatile data storage in the same way as traditional base stations.

7 Chosen approach for embedding

As presented above, a modern base station based wireless approach is probably both the most cost efficient and user friendliest way for embedding the required instrumentation for STORY-like purposes. For the STORY project, the selected wireless technology is LoRaWAN and the selected system architecture is ETSI M2M.

From the requirements it is clear that both the easiness and the cost of installations are major issues, resulting in a preferred wireless solution. The most common choices there are either ad hoc WLAN-based networks, Zigbee, or longer range radio solutions like LoRaWAN. Both Zigbee and WLAN ad hoc networks have a much more restricted range than long range radio solutions, which means that Zigbee and WLAN require more base stations and duplication of communication equipment.

7.1 Technology choice of embedment

LoRaWAN was chosen for several reasons:

a) Commercial Support:
Several nation-wide networks are currently being built in Europe, especially in the Benelux Region. The target of the operators in Belgium and the Netherlands is to have full coverage by the end of 2016. Furthermore, nation-wide or partial LoRaWAN deployments are being planned in the period 2016-2017 in France, Germany, Italy, Spain, Switzerland, Ireland, Denmark, Poland, etc.
The current coverage map for e.g. Belgium can be found in [2].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

b) Power Requirements:
The nodes in a LoRaWAN network are asynchronous and they communicate when they have data ready to send. This data can be both event-driven and scheduled. This type of protocol is typically referred to as the Aloha method. In a mesh network, or with a synchronous network, such as cellular, the nodes frequently have to 'wake up' in order to synchronize with the network and check for messages. This synchronization consumes a lot of energy and therefore, significantly reduces the battery lifetime. In a recent study and comparison done by GSMA of the various technologies addressing the LPWAN space, LoRaWAN™ showed a 3 to 5 times advantage compared to all other technology options.

c) Good range with decent latency and bandwidth:
The advantage of LoRa is in the technology's long range capability. A single gateway or a base station can cover entire cities, or hundreds of square kilometres. The range highly depends on the environment and the obstructions in a given location. Still, the LoRa® and LoRaWAN™ is claimed to have a link budget greater than any other standardized communication technology (See [3]).
LoRaWAN data rates range from 0.3kbps to 11kbps. In Europe, this is extended with a GFSK data rate at 50kbps. To maximize both battery life of the end-devices and overall network capacity, the LoRaWAN network server is managing the data rate and RF output for each end-device individually by means of an adaptive data rate (ADR) algorithm.

d) LoRa Alliance:
The LoRa Alliance is an open, non-profit organization whose members are actively sharing know-how and collaborating on the definition of the LoRaWAN protocol. The LoRaWAN protocol is positioned as the open global standard for secure, carrier-grade IoT LPWA connectivity.
Furthermore, a certification program will guarantee the interoperability to address the multiple IoT applications.

e) Open source software support with active developer base:
The LoRa Alliance also gathers and supports developers working on LoRaWAN solutions. This includes e.g. providing an open source software stack and proof of concept examples for LoRaWAN solutions on Github.

A comprehensive comparison of LPWAN technologies can be found in [4].

In this project, legacy support for existing instrumentation is high on the list of requirements. This requires the system to offer a feasible way of integrating with existing devices while providing a driver-like abstraction for accessing them.
As reviewed in D4.1 ("Structured overview of current and emerging communication standards for smart grids"), modern IoT/Smart Grid protocols like ETSI M2M, OMA M2M and LWM2M all offer these capacities via drivers, management objects or similar, while being agnostic to actual transport protocols and offering REST-capability and others soft requirements from D3.6
Of the presented protocols, ETSI M2M was chosen, as it is commonly used with LoRaWAN and ready implementations exist.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426
Project STORY - H2020-LCE-2014-3

7.2 ETSI M2M

ETSI M2M architecture (Figure 2) is presented in [5] and covered here as an overview. The ETSI M2M system architecture separates the M2M Device domain and the Network and Applications domain (Figure 2).

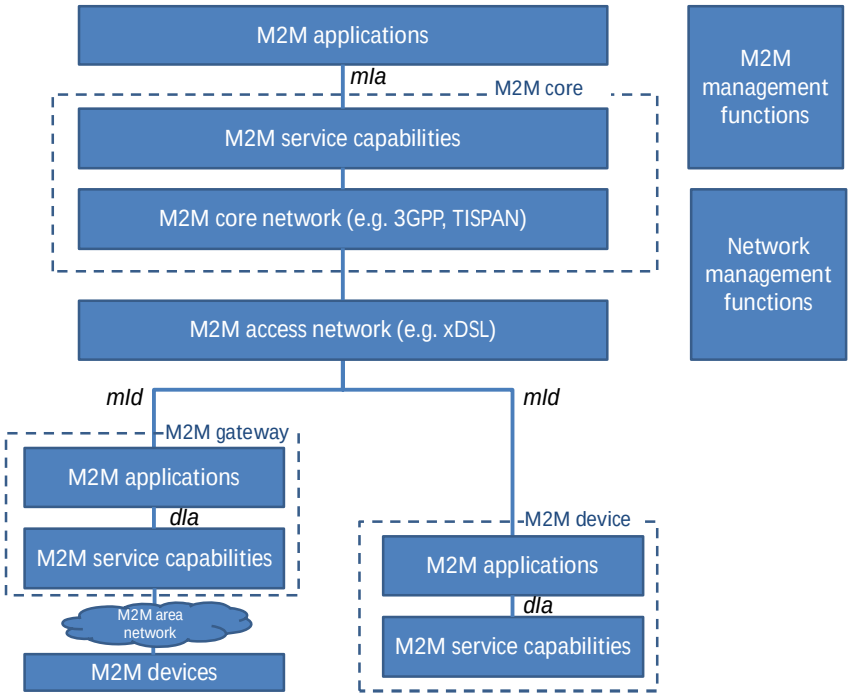


Figure 2 ETSI M2M high level architecture [5]

- 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.
- The *Network and Applications domain* comprises of:
    - the access and transport network (e.g. an xDSL access network and an IP transport network)
    - the *M2M core*. The M2M core 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,* providing M2M functionality over open APIs.
    - The *M2M applications* which run the M2M service logic and use the M2M service capabilities.
    - In addition, there are M2M and network management functions.

In the residential use case, the LoRaWAN network attaches to the ETSI M2M subsystem through a driver function which emulates an ETSI M2M gateway. The system gives resource access rights

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

based on the action issuer. These rights include read, write, delete, create, and discover, and can differ between the users.

7.3 The LoRaWAN Standard

LoRaWAN is a LPWAN implementation targeted for IoT applications. It provides secure bi-directional communication, while requiring low power to operate. Following the ETSI M2M model above, it connects LoRa-enabled devices via gateways to backend servers. The communication between devices and gateways happens over a wireless connection, while communication after gateways is IP-based. For more details on LoRa, see [4].

When optimally used (e.g. by LoRaWAN MAC), sensors always use the highest bitrate allowing communication with the nearest base station, conserving airtime and therefore battery. This also allows easy scalability: whenever the network is congested, adding a base station improves link budget and therefore decreases airtime and collisions. Both the data rates and frequency used can vary, based on range and message needs. This means that the same protocol can be adapted to different needs by different sensor and base station placements and configurations. Lora modulation allows data rates ranging from 33Kbps to 300bps by 30bps to 600bps with frequency varying from 868MHz to 169MHz. In addition, because of the spread spectrum, the range is increased compared to the existing solutions while obtaining a good resistance to interference.

Based on the application needs, LoRa devices support multiple different transmission schemes. For battery conservation reasons, most sensors adopt receiver initiated transmission: a window for downlink transmission is opened exactly one second after the last uplink transmission of any sensor. This allows the sensor to sleep most of the time. This strategy is called “class A”.

Devices that are permanently powered can afford to listen permanently and therefore may receive downlink messages at any moment: these devices are called “class C”.

An intermediary class “Class B” is being finalized. Class B devices open extra receive windows at scheduled times. In order for the End-device to open its receive window at the scheduled time it receives a time synchronized Beacon from the gateway. This allows the server to know when the end-device is listening and provides lower latency downlink communication at the expense of higher energy consumption.

For security reasons, LoRaWAN uses a model where the device has two keys, namely the integrity key (NwkSkey) and the payload key (AppSkey), which handle the traffic and payload encryption. This separation of keys means that even public LoRaWAN-networks can be used while keeping the payload (sensor readings and commands) safe from eavesdropping or replay attacks. The encryption used is AES 128 with 128-bit key.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

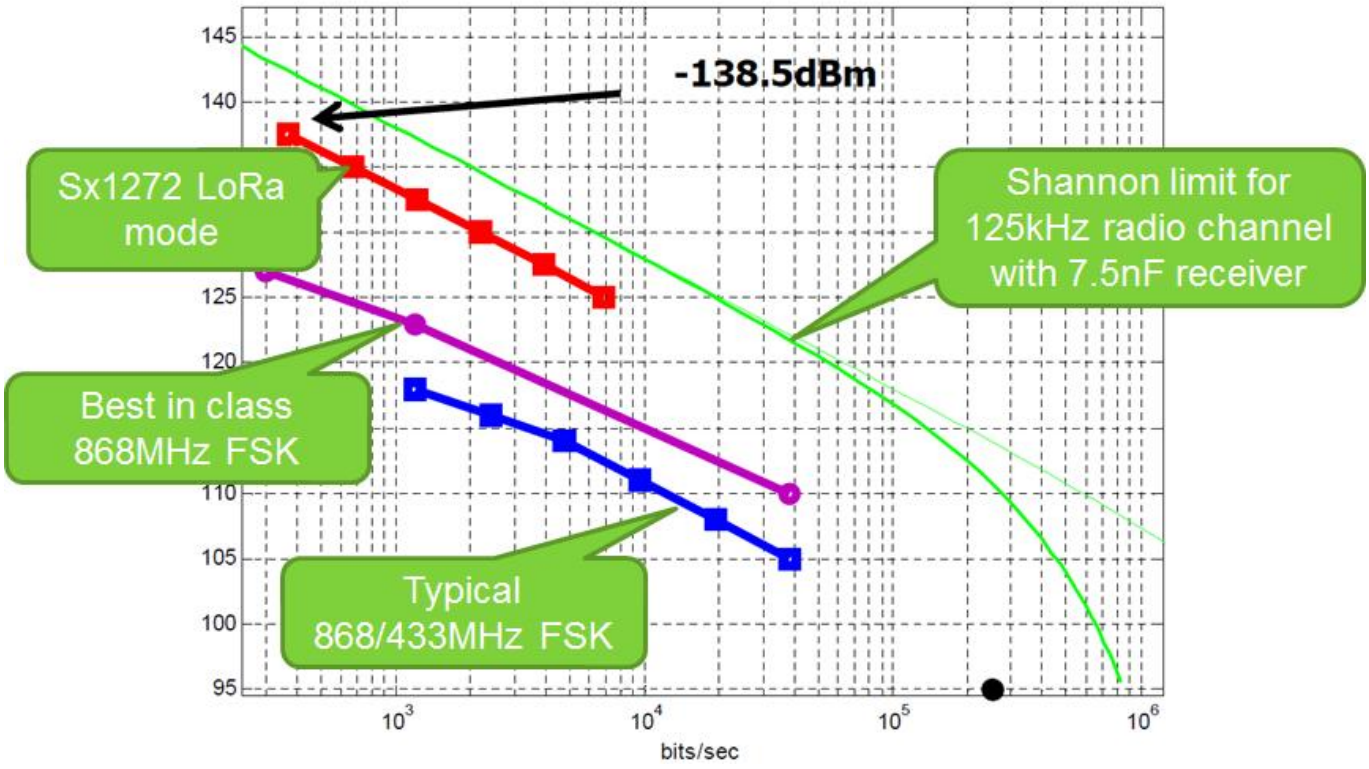


Figure 3 Sensitivity

7.4 Embedding LoRa

Embedding LoRaWAN in a device requires both a software stack and hardware.

The LoRaWAN stack is available as open source from GitHub, with a reference/example gateway, a base station, and sensor implementations also available as open source resulting in fast implementation and testing.

Several hardware options exist for sensor integration of which 3 options are listed below, in increasing order of complexity of the hardware integration:

- MAC level Modem: these modems integrate an AT command set and the LoRaWAN stack. They allow extremely simple integration into any Linux or windows type operating system over USB (e.g. USB key from Nemeus). For more embedded solutions, MicroChip has produced a small module, RN2483, which interfaces through a serial connection.
- Physical level modem: these modems integrate the RF hardware and filters, but not the MAC layer, they require external MCU, e.g. ARM M3 core. The stack may be compiled from GitHub or Embed open source. Such modems may be purchased from many companies, e.g. IMST of Germany.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

- SX12xx transceiver. For high volume production equipment, the LoRa RF subsystem is highly integrated in the SX12xx transceiver series from Semtech.

Application level integration (Raspberry Pi or similar running local software) can also use USB-dongle based LoRa integration during prototyping phase.

Given the volumes and timing of the Story project, modem level integration will be used for new sensors and actuators. In addition of a range of readily available LoRa-enabled sensors, such a thermometers and pulse sensors will be used as required. Deliverable D4.6 ("Demonstrated embedment in 3 different components of storage equipment") will cover the actual embedding process and results.

8 Challenges

This document has been written before the actual embedding tasks have been finished, so it covers mainly challenges identified in the analysis process.

Secure identification of all the parts of the system is one of the main challenges – particularly in a wireless environment where base stations have multiple sites covered, it is of utmost importance that users can access only their own data. This concerns not only the hardware components (sensor, base station, layer 3), but also human operators. Normal best practices for designing secure distributed systems can be applied here (unique identifiers, key based encryption, actor identification and authentication on each layer), but the process must be as easy as possible for the end user. Security vs. usability is a common problem, and particularly vendor proprietary solutions which have completely in-house developed security are often lacking in security to provide a user friendly system.

Physical interfaces for sensors and actuators vary a lot, so while interfacing a wireless transceiver is possible, it remains to be seen to what degree this is possible while keeping the device economically feasible. This is one of the main topics for the rest of the STORY work package 4 tasks.

With the three layer approach, each layer is tasked with relevant authorization and backup fail safe logic, while control signals are pushed down from upper layers. If this system can be compromised, the central approach opens every system below for malicious attacks. The other choice is to push the security down to the individual sites, but as local devices are usually user maintained, this leaves the system too vulnerable to attacks based on old systems.

The current metering infrastructure for small sites is mainly electricity, water and gas. These meters are owned by the DSOs and the customer either does not have access to the data provided, or data is delayed and inaccurate (1h average being common) for Smart Grid purposes. When the users do not have an access to their own real time data, either metering infrastructure must be built anew for each project/service wishing to use such data, or access must be negotiated with each DSO. In this way, building one economically feasible system that has an open external API and

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

clearing house system for data is one of the major aspect of STORY and the only way to make instrumentation economically feasible.

The market is currently fragmented and many similar systems exist. So to be feasible, the embedded system must support all the relevant standards, and the cost must be low enough for the end user. This is one of the reasons why LoRa was chosen, as it seems to be the wide area communication protocol with the most potential.

9 Conclusions

These are the preliminary conclusions, as the actual embedding work is still ongoing. The results of STORY tasks (in WP4) later in the project will validate the choices done in this deliverable.

From the overview with various STORY sites, integration for small sites is feasible, as they are usually highly customized and use a large variety of sensors. Larger industrial sites have usually much more standardized equipment, which must pass a required security check, provide standard interfaces, and have support from leading SCADA vendors. Large sites are usually also mostly isolated from the network, and therefore site communication cannot pass through 3rd party systems. Thus, the STORY ICT embedding effort concentrates more on the requirements of small sites, starting with general use meters like energy, pulse counter, environmental (temperature, CO_2), and also demonstrates how to do embedding with a more complicated device like a battery storage.

LoRa radio technology was chosen for transport, for both security and ease of installation reasons. LoRa seems to be gaining commercial support, particularly in the Benelux countries and it seems to be a better choice than commonly used short range solutions like ZigBee. The data protocol to be used has several options as discussed in previous deliverables, and of those ETSI M2M was chosen, mainly because it is already in use in the LoRa community.

The embedding itself can happen on two levels, either sensors themselves are made LoRa aware by installing a radio chip, or a local base station handling the local bus communication is provided with a LoRa transceiver.

We also presented a communication architecture based on three layers and detailed the requirements and functionality for each layer. This high level view can be used as a modelling tool for future sites.

Main problems encountered in this preliminary review were the lack of standardization on the low level sensors and very restricted budgets with which the house hold installations must be made. In larger sites the main challenge is the restricted nature of SCADA systems – it is very hard to install new components without a SCADA manufacturers' consultant help. Both the lack of standardization and vendor lock-in would be at least alleviated, if all systems supported standard south- and northbound APIs.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

10 Acronyms and terms

HVAC	Heating, ventilation, and air conditioning
IoT	Internet of Things
NAT	Network Address Translation
LoRaWAN,LoRa	Low Power Wide Area Network
6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks
SCADA	Supervisory control and data acquisition.
RPL	IPv6 Routing Protocol for Low-Power and Lossy Networks
PV	Photovoltaic
OLTC	On Load Tap Changer, power transformer voltage regulation system
RTU	Remote terminal unit
TS	Transformer station
M2M	Machine 2 machine communication
DNP3	Industrial m2m communication protocol
OPC UA	Industrial m2m communication protocol
AMI	Automated metering infrastructure
UPS	Uninterrupted power supply

11 References

1 Çağrı, V; Güngör, G. and Hancke, P. 2014. Industrial Wireless Sensor Networks: Applications, Protocols, and Standards. CRC Press.

2 Proximus. 2016. Internet of Things (IoT); Data exchange between machines, applications and objects. [Available at: http://www.proximus.be/en/id_cl_iot/large-companies-and-public-sector/solutions/internet-and-networks/internet-of-things.html?ac_chn=google&ac_src=google-adwords&ac_aid=generic&ac_caid=Mecor-iot-en&ac_cid=proximus+iot&ac_cp=Mecor-iot&gclid=Cj0KEQjw8u23BRCg6YnzmJmPqYgBEiQALf_XzaJ4K4ALxUH8HCZGUBdnGKtKL_eNrLV_80qqTUVVzXoaAr558P8HAQ]

3 Moyer, Bryon. 2015. Low Power, Wide Area; A Survey of Longer-Range IoT Wireless Protocols. [Available at: http://www.eejournal.com/archives/articles/20150907-lpwa/]

4 Lora Alliance 2016. LoRa® Technology. [Available at: https://www.lora-alliance.org/What-Is-LoRa/Technology]

5 ETSI 2016. Main page with links to material presenting the ETSI M2M architecture. [Available at: http://www.etsi.org]

6 Savolainen, P.T.; Kyntäjä, T.; Vallant, H.; Marksteiner, S.; Aertgeerts, A.; Van HaleWeyck, L. and Valckenaers, P. 2016. Structured overview of communication standards for smart grids. STORY Deliverable 4.1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3

7 STORY consortium. 2016. Requirements definition of the hardware to be deployed. STORY Deliverable 4.3, in preparation, available in Oct 2016.

8 Valckenaers, Paul. 2016. Report on interoperability guidelines. STORY Deliverable 3.6

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646426

Project STORY - H2020-LCE-2014-3