# Innovation Action


# inteGRIDy

integrated Smart GRID Cross-Functional Solutions for Optimized Synergetic Energy Distribution, Utilization & Storage Technologies

## H2020 Grant Agreement Number: 731268

## WP4 – inteGRIDy Distribution Grid Optimization Framework

## D4.1 - inteGRIDy Integration & Interconnection Plan and Report

| Document Info | |
|---|---|
| **Contractual Delivery Date:** | 31/03/2019 |
| **Actual Delivery Date:** | 29/03/2019 |
| **Responsible Beneficiary:** | VPS |
| **Contributing Beneficiaries:** | ATOS, SIEMENS, CERTH, UNEW, M7, ASM, NATURGY, AIGUASOL, INNED, TREK, UCY, PH, ENOVA, SIVECO |
| **Dissemination Level:** | Public |
| **Version:** | 1.0 |
| **Type:** | Final |

This project has received funding from the European Union's H2020 research and innovation programme under the grant agreement No **731268**. Any dissemination of results must indicate that it reflects only the author's view and that the Commission is not responsible for any use that may be made of the information it contains.

## Document Information

| | |
|---|---|
| **Document ID:** | **D4.1 inteGRIDy Integration & Interconnection Plan and Report** |
| **Version Date:** | 29/03/2019 |
| **Total Number of Pages:** | 55 |
| **Abstract:** | This deliverable offers a unified view of the Field Layer, the bottom layer or the inteGRIDy Reference Architecture that provides the basic interface with the physical world, and the integration mechanisms with the Cross-Functional Modular Platform (CMP) and the Reference Knowledge Warehouse (RKW) that incorporates the information collected from all pilots.<br>The proposed layered architecture brings to light the similarities between the diverse communication architectures and applications and can be used when planning the expansion of the current pilots or in the specification of new projects in accordance with the general inteGRIDy Framework.<br>A description of the implementation of field layer (devices and protocols) and test results at each pilot is presented.<br>Similarly, an assessment of the implementation of the data warehouse at each pilot is presented in the form of a survey whose returns are discussed in comparison with a baseline of minimum technological requirements defined as good practice guidelines in order to assure the compatibility, interoperability and interconnectivity that is a key requirement of the inteGRIDy Framework. |
| **Keywords:** | Field layer, smart grid communications, Home Area Networks (HAN), Neighbourhood Area Network (NAN), Wide Area Network (WAN), monitoring, sensing, data warehouse, API, cybersecurity |

## Authors

| Full Name | Beneficiary / Organisation | Role |
|---|---|---|
| Jorge Landeck | VPS | Overall Editor |
| Rita Carreira | VPS | Contributor |
| Javier Valiño | Atos | Section Editor |
| David Gómez | Atos | Contributor |
| Tom O'Reilly | SIEMENS | Contributor |
| Hamish Wilson | M7 | Contributor |
| Leonard Emaki | EMSc | Contributor |
| Adib Allahham | UNEW | Contributor |
| Marco Maccioni | UNIROMA1 | Contributor |
| Tommaso Bragatto | ASM | Contributor |
| Marco Merlo | POLIMI | Contributor |
| Davide Falabretti | POLIMI | Contributor |
| Lorenzo Corghi | UNE | Contributor |
| Julia Osoro | NATURGY | Contributor |
| Antonio Serrano | SIEMENS | Contributor |

| | | |
|---|---|---|
| Hatice Turner | TEES | Contributor |
| Huda Dawood | TEES | Contributor |
| Alberto Pérez | AIGUASOL | Contributor |
| Oscar Cámara | AIGUASOL | Contributor |
| Romain Chomaz | INNED | Contributor |
| Sotiris Tsakanikas | TREK | Contributor |
| Venizelos Efthymiou | UCY | Contributor |
| Carlos Raposo | ENOVA | Contributor |
| Vasco Abreu | ENOVA | Contributor |
| Aleksandra Krivoglazova | PH | Contributor |
| Dimitris Trigkas | CERTH/ CPERI | Contributor |
| Otilia Bularca | SIVECO | Contributor |
| Iacob Crucianu | SIVECO | Contributor |
| Paschalis Gkaidatzis | CERTH/ITI | Contributor |
| Lampros Zyglakis | CERTH/ITI | Contributor |
| Stelios Zikos | CERTH/ITI | Contributor |
| Alexandros Zerzelidis | CERTH/ITI | Contributor |

## Reviewers

| Full Name | Beneficiary / Organisation | Date |
|---|---|---|
| Marilena Lazzaro | ENG | 20/03/2019 |
| Thomas O'Reilly | SIEMENS | 27/03/2019 |
| Javier Valino | Atos | 29/03/2019 |
| Athanasios Tryferidis | CERTH | 29/03/2019 |

## Version history

| Version | Date | Comments |
|---|---|---|
| 0.1 | 23/01/2019 | TOC definition |
| 0.2 | 15/02/2019 | Feedback received from all 10 pilots |
| 0.3 | 12/03/2019 | Draft released for internal WP review (ENG) |
| 0.4 | 25/03/2019 | Draft released for Quality Control Board (SIEMENS) |
| 0.5 | 25/03/2019 | Final version for Coordination approval |
| 1.0 | 29/03/2019 | Final version to be released to the EC |

# Executive Summary

The Field Layer (FL) is bottom layer or the inteGRIDy Reference Architecture. This layer provides the basic interface with the physical world including sensing and actuation and is also responsible for data management including data acquisition, filtering, processing, aggregation and short and long term storage. As consequence this layer is heterogeneous in nature, from the disparate type of devices and systems used, from the different communication protocols and integration mechanisms deployed, and the varied scope of the project's pilots in terms of applications and geographical span.

The Reference Knowledge Warehouse (RKW) is a key element inside inteGRIDy framework of tools representing the glue that enables the interoperation and coordination of the tool set by sharing, using and storing the data produced from one another.

This deliverable offers a unified view of the FL and the integration mechanisms with the Cross-Functional Modular Platform (CMP) and the RKW that incorporates the information collected from all pilots. This effort brings to light the similarities between the diverse communication architectures and applications and resulted in the development of a layered model for the Field Layer (see Figure 1) that can be used when planning the expansion of the current pilots or in the specification of new projects in accordance with the general inteGRIDy Framework.

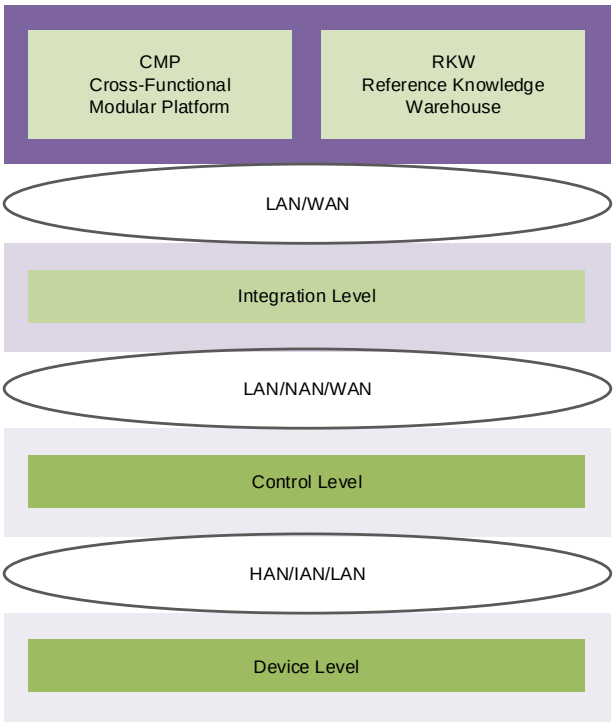


**Figure 1. Field layer general architecture**

Likewise, an assessment of the implementation of the data warehouse at each pilot is presented in the form of a survey whose returns are discussed in comparison with a baseline of minimum technological requirements defined as good practice guidelines in order to assure the compatibility, interoperability and interconnectivity that is a key requirement of the inteGRIDy Framework.

# Table of Contents

# Table of Figures

# Table of Tables

# List of Acronyms and Abbreviations

| Term | Description |
|---|---|
| ADSL | Asymmetric Digital Subscriber Line |
| AP | Access Point |
| API | Application Programming Interface |
| BESS | Battery Energy Storage Systems |
| BaMS | Battery Management System |
| BMS | Building Management System |
| BEMS | Building Energy Management Systems |
| CAN | Controller Area Network |
| CHP | Combined Heat and Power |
| CMP | Cross-Functional Modular Platform |
| DR | Demand Response |
| DSL | Digital Subscriber Line |
| DSO | Distribution System Operator |
| DSR | Demand Side Response |
| ESS | Energy Storage Systems |
| EV | Electrical Vehicle |
| FC | Fuel Cell |
| GFSK | Gaussian Frequency Shift Keying |
| HAN | Home Area Network |
| HP | Heat Pump |
| HVAC | Heating, Ventilation and Air Conditioning |
| IAN | Industrial Area Network |
| IEC | International Electrotechnical Commission |
| IP | Internet Protocol |
| IR | Infrared |
| IVP | Integrated Visualization Platform |
| JSON | JavaScript Object Notation |
| LV | Low Voltage |
| MAC | Medium Access Control |
| MPPT | Maximum Power Point Tracker |
| MQTT | Message Queue Telemetry Transport |
| MV | Medium Voltage |
| NAN | Neighbourhood Area Network |
| ODBC | Open Database Connectivity |
| OPC | Open Platform Communications |
| PHY | Physical layer |
| PLC | Programmable Logic Controller; Powerline Communication |
| PV | Photovoltaic |

| | |
|---|---|
| RES | Renewable Energy Source |
| REST | REpresentational State Transfer |
| RKW | Reference Knowledge Warehouse |
| RF | Radio Frequency |
| RTU | Remote Terminal Unit |
| SCADA | Supervisory Control and Data Acquisition |
| SOAP | Simple Object Access Protocol |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WG | Wind Generators |

# 1.Introduction

## 1.1 Scope and Objectives of the Deliverable

The main goal of this deliverable is to provide a detailed description of the integration and interconnection of the field level devices, equipment and systems. The field level corresponds to the lowest layer of the inteGRIDy Reference Architecture, described in D1.5/D1.6 [IND15][IND16], where the interaction (measurement and control) with the real world takes place. As consequence this layer is heterogeneous in nature, either from the type of devices and systems, either from the communication protocols and integration mechanisms deployed. This heterogeneity is further accentuated by the varied scope of the project's pilots in terms of applications and geographical span. Yet the integration of the different components assuring its compatibility, interoperability, and interconnectivity is key requirement for all inteGRIDy pilots, in particular, and a key feature of the inteGRIDy Reference Architecture.

This deliverable offers a unified view of the field layer and the communication mechanisms with the Cross-Functional Modular Platform (CMP) and the RKW that incorporates the information collected from all pilots. This effort brings to light the similarities between the diverse applications and proposes a layered model for this layer that can be used when planning the expansion of the current pilots or in the specification of new projects in accordance with the general inteGRIDy Framework.

Complementarily, an assessment of the implementation of the RKW by each pilot is provided since the integration mechanisms are similar or even the same. In fact, some of these mechanisms are even used by the top layer of the Reference Architecture, the Integrated Visualisation Platform (IVP).

## 1.2 Structure of the Deliverable

The structure of this report is as follows:

Section 2 presents an overview of the typical field architecture that is the bottom layer of the inteGRIDy reference architecture. Moreover, this section describes some of the standards mechanisms and protocols used to integrate and interconnect the field equipment and the CMP.

Section 3 introduces a survey to gather data regarding the implementation of the RKW by each pilot and that allows for benchmarking and double-check that at least the minimum technological requirements are met so as to guarantee that all the data used within the project is properly stored and secured.

Section 4 describes the field layer integration and interconnection protocols for each pilot using the model previously presented and provides a brief evaluation of the communication architecture in terms of quality of service attributes. Likewise, the implementation of the RKW of each pilot in terms of certain quality attributes is briefly presented and compared to a minimum baseline.

Section 5 provides some final remarks on the field layer integration and RKW implementation.

## 1.3 Relation to Other Tasks and Deliverables

Task 4.1 is one of the set of tasks that constitute the WP4 – inteGRIDy Distribution Grid Optimization Framework – the core development of the inteGRIDy Framework. In this sense T4.1 development methodology and management followed closely the other WP's tasks. On the other hand, the successful development of this task is fundamental for the success of the

other WP's tasks in the sense that it's related with the collection of data and the interaction with the physical world.

Task 4.1 uses to great extent the pilots' information collected and organized in D1.3 Pilot Sites Surveys, Use Case Requirements & Business Scenarios [IND13] and the architectural views presented in D1.5 inteGRIDy Architecture & Functional/Technical Specifications [IND15], updated in D1.6 [IND16] as well as the tools descriptions.

Furthermore, this report can be useful for the integration work of T5.1 Integration of inteGRIDy Framework Components & Iterative Testing, in particular, and with the evaluation and assessment work to be developed under WP6 and WP7.

# 2.Field devices and protocols

## 2.1 Overview

The Field Layer is bottom layer or the inteGRIDy Reference Architecture. The main functionality of this layer is to supply the upper layers with real-time measurements and to act on specific devices that interact with the physical world. In more detail, the Field Layer integration and interconnection services enable the CMP, the central and core layer that include the simulation and optimization tools, the RKW, the main data repository, and the IVP, that comprises the user interfaces, to access real world data from various sensors and meters and change the state of certain devices in response to automatic or user-originated actions. In fact, in the context of the inteGRIDy Framework real-time information from heterogeneous sources at various levels such as network, facility, building, distribution grid, and storage systems have to be considered.

The Field Layer provides the basic interface with the physical world including sensing and actuation and is also responsible for data management including data acquisition, filtering, processing, aggregation and short and long term storage. In other words, this layer provides service management and link to data storage. It is responsible for primary information processing, ubiquitous computation and automatic decision based on raw data [KHA12].

The equipment of this layer include sensors, actuators, meters, and power converters/inverters but also communication gateways, data concentrators, and controllers, usually connected to a supervisory system or integration platform (see Figure 2).

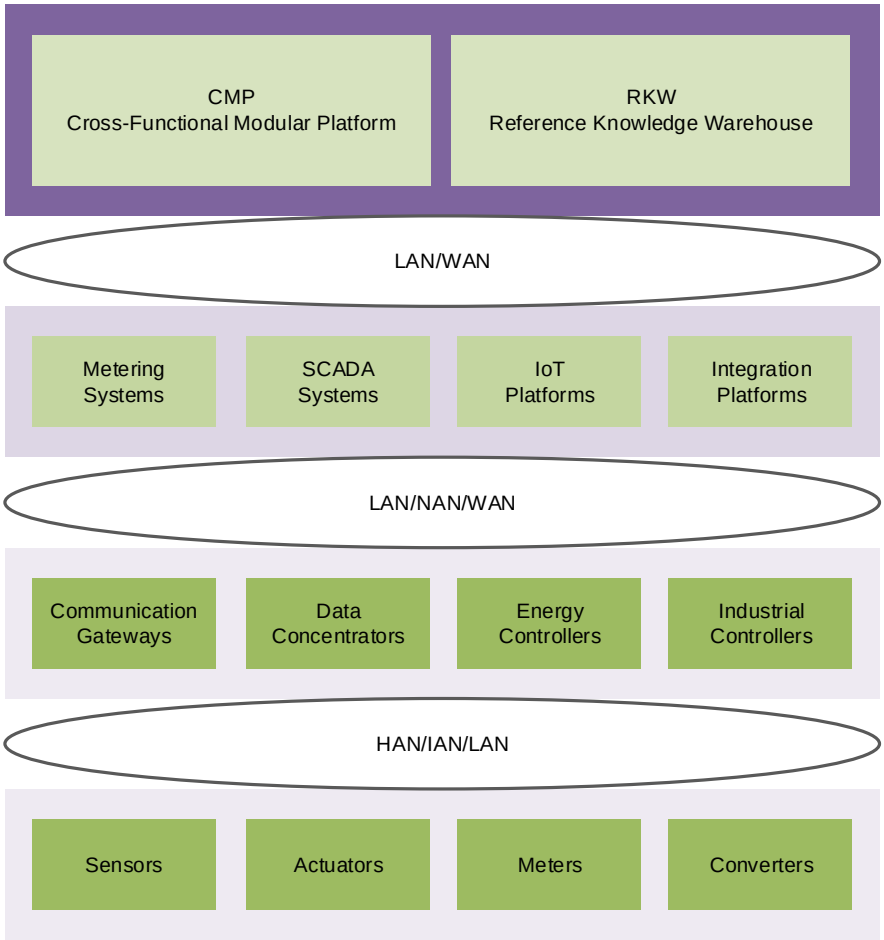


**Figure 2. Field layer architecture**

This layered high-level architecture of the Field Layer offers a unified, if simplified, view of a very heterogeneous environment in terms of devices, systems, and communication protocols that is the physical environment of the smart grid. As mentioned before, this heterogeneity derives from different factors and won't disappear in the near future. On the contrary, the current trend in terms of system integration and deployment tries to take advantage or at least deal with it.

The inteGRIDy Framework has as a key feature the integration of the different components ensuring its compatibility, interoperability, and interconnectivity. This feature is also shared by the recent Internet of Things (IoT) computing paradigm. Simplistically, IoT technology aims at interconnecting a large number of distinct devices, ranging from small sensors to complex management systems, using different communication technologies, such as fixed and mobile broadband access networks, Bluetooth, ZigBee, and Wi-Fi [KAB17]. The information is stored and processed centrally on a cloud-based datacentre which is another key aspect of this paradigm. In short, the high-level architecture presented for the Field Layer can also be seen as typical of IoT based data acquisition systems for energy metering and controlling applications [SAL17].

In this layered perspective, communication gateways, data concentrators, energy controllers, and industrial controllers provide the interface between the sensing and actuation devices and the data processing platform (CMP and RKW) and user interface applications (IVP) through monitoring and supervisory systems or integration platforms. For the sake of simplicity the diagram splits components (functions) that in some cases are concentrated on a single physical device (e.g., grid smart meters usually include on the same device the meter and the gateway function). Moreover, in some cases even the integration service may be part of the same physical device in which case there is a direct connection between the data processing platform and the field device.

The communication protocols used in each layer are mainly distinguished by data rate and coverage. In the proposed model this distinction is "blurred" by the fact that it intends to represent large-scale (distribution grid, distributed set of residential and commercial buildings) and small-scale (single buildings and industrial facilities) deployments. In general terms, the typical protocols and characteristics of each level are [KUZ14].

- **Device level**: Home Area Network (HAN), Industrial Area Network (IAN), and Local Area Networks (LAN) with coverage up to 100 m and data rate up to 100 kbps; wired examples include powerline (PLC), Modbus-RTU over serial bus, BACnet; wireless examples include ZigBee, Z-Wave, Bluetooth Low Energy (BLE), and Wi-Fi.
- **Control level**: LAN, Neighbourhood Area Network (NAN), and Wide Area Network with coverage up to 10 km and data rate up to 10 Mbps; wired examples include PLC, Ethernet, and Digital Subscriber Line (DSL); wireless examples include mesh ZigBee, mesh Wi-Fi, WiMAX, and cellular.
- **Integration level**: LAN and WAN with coverage up to 100 km and data rate up to 1 Gbps; wired examples include Digital Subscriber Line (DSL); wireless examples include WiMAX, and cellular.

Since the lower layer components are usually physically installed in the end-users premises (homes, commercial and office buildings, factories and distribution grid facilities) diverse short range networks are used to interconnect the devices. Wireless networks are favoured in situations where there is no existing wired infrastructure or legacy monitoring and control system [ZHU12].

On the other hand, at the higher layers, the TCP/IP based networks are preferred for the diverse range of available solutions and tools, for the proven compatibility, and for the opportunity to build on existing (community) work.

## 2.2 Integration and interconnection mechanisms

In this section, a more detailed description of each layer/level of the architecture is presented having in mind the context of the pilot applications.

### *2.2.1 Device level*

The device level is populated with:

- **Sensors**: electronic components that convert environmental (e.g. indoor temperature and relative humidity, and solar irradiance) and process (e.g. open door and occupancy) variable into electrical signals;
- **Actuator**: electric or electronic components that convert an electrical signal into a physical action (e.g. power relays, power plugs);
- **Electrical meters**: particular kind of sensors that provide measurement of electrical variables (voltage, current, frequency, power factor, power and active and reactive energy);
- **Power converts/inverters**: modules that are necessary to connect batteries and RES to the grid or microgrid by adapting voltage and frequency levels.

These devices are usually equipped with one or more communication interfaces. The selection of the interface is dependent on some of the quality requirements of the application (like reliability, availability and determinism) but also on compatibility or legacy issues. The usual application or full-stack protocols are described below.

***Modbus***

The Modbus protocol was developed in 1979 by Modicon for its industrial automation systems and programmable controllers. It has since become a de facto industry standard and is now a widely-accepted, open, public-domain protocol.

Modbus uses a master-slave (client-server) logical topology in which only the master can initiate a request. The protocol defines a message structure regardless of the physical layer. Thus, Modbus-RTU is an application protocol over a serial line (usually RS485) and Modus-TCP is a similar application protocols over a TCP/IP connection (usually Ethernet) [THO08].

***BACnet***

Building Automation and Control Network (BACnet) is an open data communications protocol developed by ASHRAE (ANSI/ASHRAE 135-1995) and standardized as ISO 16484-5 in 2003.

BACnet provides a sophisticated object model for describing building controls (e.g. HVAC, lighting, security, fire, access control) and a message structure that assures wide interoperability. The protocol also specifies different transport networks over which the application messages can be exchanged [NEW15].

***CAN bus***

Controller Area Network (CAN or CAN bus) was developed by Bosch for the automotive industry as a vehicle bus but has since expanded to other applications (e.g. avionics, railway, and industrial automation) and, more recently, reached the burgeoning EES market as one of the preferred battery management systems communication interface.

CAN is a multi-master broadcast serial bus with specific bit signalling, encoding/decoding, and synchronization characteristics [COR02].

***ZigBee***

ZigBee standard was developed by the ZigBee Alliance, an industry consortium, as a cost-effective, low-power, wireless mesh network for monitoring and control applications in various areas, namely, home energy management systems, lighting, and metering.

ZigBee defines roles for each node of the network (coordinator, router or end device) and provides definitions for profiles that group data objects that support numbered endpoints (data and commands), data types, descriptors, frame formats, and a key value pair construction method. ZigBee also provide application binding link management and secure mechanism.

ZigBee like other low rate radio protocols use IEEE 802.15.4 physical (PHY) and medium access (MAC) layers [DAG14].

***Z-Wave***

Z-Wave is a wireless communication protocol used primarily in smart home networks, developed by Zen-Sys initially for lighting systems and now maintained by the Z-Wave Alliance that runs a certification program.

A typical Z-Wave network consists of a primary controller (home hub) and set of slaves (devices). The application layer is organized in terms of command classes that are groups of commands and responses associated with specific functions of the devices (e.g. Light on/off and Light dim). For interoperability reasons, each class must implement a basic set of commands.

The Z-Wave PHY and MAC layers are based on the ITU-T G.9959 global radio standard that uses GFSK modulation, Manchester encoding, and AES 128 encryption. A newer specification uses TCP/IP based networks for transport [ZWA19].

***Wi-Fi***

Wi-Fi is currently the most widely deployed wireless local area network (WLAN) in residential, commercial, and public buildings. For this reason, it is becoming popular communication interface for smart plugs and smart appliances.

Wi-Fi is the common name for a standard IEEE 802.11 suite of WLAN. In the most frequent Wi-Fi deployments (infrastructure mode), each individual device is radio connected to an Access Point (AP) which is suitable for static scenarios.

### *2.2.2 Control level*

The control level includes:

- **Communication gateways**: compact communication units that connect several devices to an aggregator or integration service or module converting from one protocol to another;
- **Data concentrators**: small computer units that collect data from (or send commands to) several devices and send this data to (or receive these commands from) an integration service or module;
- **Energy controllers**: systems developed for managing/optimizing the energy usage, production; storage in homes and buildings (e.g. HEMS – Home Energy Management System and BEMS – Building Energy Management System); EV charging stations;
- **Industrial controllers**: generic units that have a diversified set of input/outputs, communication interfaces, memory and that can be programmed (e.g. PLC – Programmable Logic Controllers and RTU – Remote Terminal Units).

The main functionality of these units is to forward data from the field devices to the integration layer and commands and/or settings on the reverse direction. The main functionalities are therefore secure communication management, short term data acquisition, alarm and event management, and command automation based on events or rules. Some application protocols used at this level beside others already mentioned are described below.

***OPC and OPC-UA***

Open Process Control (OPC) is the interoperability standard for the secure and reliable exchange of data in industrial automation applications. It is platform independent and ensures the seamless flow of information among devices from multiple vendors. The OPC Classic specifications are based on Microsoft Windows technology using COM/DCOM (Distributed Component Object Model) for the exchange of data between software components. A new version called OPC-Unified Architecture (OPC-UA) is specified using a standard web service and allows encryption and authentication. The specifications provide separate definitions for accessing process data, alarms and historical data [OPC17].

This interface is particularly suitable to read and write generic variables, states, alarms and events. Process variables can be sent to the server upon a change, on demand or when a given time elapsed.

***IEC 61850***

IEC 61850 is a multi-part standard that defines interoperable information exchanges between intelligent electronic devices (IED) from multiple vendors in electrical substations using TCP/IP. It is a reference architecture for electric power systems. The defined abstract data models can be mapped to a number of different protocols, like MMS (Manufacturing Message Specification), GOOSE (Generic Object-Oriented Substation Event), and SMV (Sampled Measured Values) [IEC50].

Although the scope of 61850 was originally focused on the communication inside the substation, recent advances had enabled its application to wide area substation-to-substation and substation-to-control centre communication. Multi-vendor interoperability has been demonstrated and compliance certification processes are in place.

This interface is well suited for application involving substation and control centres where it might already be implemented.

### *2.2.3 Integration level*

The integration level encompasses a large variety of systems that manage small and large, local and distributed resources including metering systems – developed to collect meter readings automatically and remotely (e.g. AMS – Advanced Metering System and AMR – Automatic Meter Reading), SCADA systems – customized supervisory control and data acquisition solutions developed to manage HVAC systems and distribution grid meters and switches, IoT platforms – that manage the connection with large number of devices/nodes and develop applications that follow the new computing paradigm, and integration platforms – mainly dedicated software modules that implement standard interfaces to proprietary or legacy systems.

Nowadays the great majority of these systems is either connected to the internet or is installed on a cloud server. For this reason, the employed application protocols use the TCP/IP stack or the web protocols as transport mechanisms. Likewise, the security features usually implemented are the same as the ones developed for the web applications because the threat landscape is similar.

***REST API***

A RESTful API is a web service designed in accordance with the Representational State Transfer (REST) paradigm. This paradigm is not directly linked with any particular platform or

technology, although HTTP is the preferred communication protocol due to its widespread use. For this reason this kind of APIs has been implemented extensively.

The functionality of an integration API designed or selected to interface the field layer and the CMP is not that extensive and has in essence to deal with reading inputs (registers, variables and parameters), writing outputs (registers, variables and settings), handling alarms and events and manage security features. Advanced features may include device configuration and firmware updates [INF18].

***MQTT***

MQTT – Message Queuing Telemetry Transport – is an M2M/IoT connectivity protocol. It was designed as an extremely lightweight publish/subscribe messaging mechanism over TCP/IP based networks.

This interface is particularly suitable for applications that have severe bandwidth limitations, intermittent connections, or mobility requirements. For these reasons, this protocol is gaining popularity in emergent IoT applications specially the ones involving small footprint mobile devices [MQT14].

***OpenADR***

OpenADR – Open Automated Demand Response – is an open and standardized way for electricity providers and system operators to communicate DR signals with each other and with their customers using a common language over any existing TCP/IP based communications network.

As the most comprehensive standard for Automated Demand Response, OpenADR has achieved widespread support throughout the industry. The open standard is maintained by the OpenADR Alliance formed by industry stakeholders.

This interface is interesting for applications that involve demand response requirement and, in particular, if a certification and interoperability is sought on [OAD17].

***IEEE 2030.5 (SEP 2.0)***

IEEE 2030.5 (SEP 2.0) is an industry effort to promote the interoperability between metering and home energy management systems, supporting device types like gateway, metering devices, thermostat and load control devices. The standard uses IEC 61968 (CIM) as a “dictionary” and a RESTful architecture [IEE30].

The Smart Energy Profile 2.0 is the result of the joint work of the ZigBee Alliance and the HomePlug Powerline Alliance. It has been developed to map directly the CIM defined on IEC 61968.

This protocol is intended to be used in applications such as metering and home energy management systems, supporting device types like gateway, metering devices, and thermostat and load control devices.

## 2.3 Quality requirements

Any particular implementation of the field layer communication architecture presented can be rigorously (designed and) assessed at each level or as a whole using well established quality requirements. For this type of smart grid related applications, the most important network attributes are:

- **Bandwidth**: Quantity of information that can be exchanged on a certain time interval; usually inferior to the nominal transfer rate.
- **Availability**: A measure of the percentage of time that the network/link is operational and data can be exchanged.

- **Latency**: The delay between a request and answer; in some (real-time) applications there might be required to have a maximum limit to this delay.
- **Reliability**: A measure that guarantees that "flawed" data exchanges are detected.
- **Security**: A measure that guarantees that "interfered" data exchanges are detected and "snooped" ones are protected.

A supplementary attribute that has gained relevance is interoperability. The use of standard protocols is in fact one of the best ways to assure interoperability that is the possibility at the lower layer to replace devices and at the higher layer to exchange data between applications (tools). On the other hand, the use of standard protocols is beneficial in terms of security features which are more widely mandatory, analysed and updated.

Table 1 adapted from [KUZ14] presents typical quality requirements for smart grid applications based on its geographical coverage.

**Table 1. Typical quality requirements**

| Network Coverage | Typical Applications | Latency | Reliability (%) |
|---|---|---|---|
| HAN | Home automation and energy management | seconds | >98 |
| | Building automation and energy management | seconds | >98 |
| NAN | Meter reading | seconds to hours | >98 |
| | Pricing (from utility to meter) | <1 minute | >98 |
| | EV Pricing (from utility to meter) and EV charging status (from meter to utility) | <15 seconds | >98 |
| | Demand Response | <1 minute | >99.5 |
| WAN | Predictive under frequency load shedding | <0.1 seconds | >99.9 |
| | Voltage stability control | <5 seconds | >99.9 |
| | Power oscillation monitoring and control | <0.1 seconds | >99.9 |
| | PMU-based and dynamic state estimation | <0.1 seconds | >99.9 |

# 3. Data warehouse

## 3.1 Overview

As described in D1.6 inteGRIDy final reference architecture, the Reference Knowledge Warehouse (RKW) is a key element inside inteGRIDy framework of tools.

This Warehouse represents the glue making it possible for tools to inter-operate and work in an integrated way by sharing, using and storing the data produced from one another. Therefore, the elicitation of appropriate guidelines (as done in D1.6 level) and the monitoring process so as to assure each and every pilot is implementing them is capital to the proper and smooth adoption of the framework.

This chapter takes D1.6 guidelines as starting point. Using that baseline, guidelines are extended, and a pilot implementation survey is introduced. The survey allows for benchmarking and double checks that at least the minimum technological requirements are met so as to guarantee that all the data used within the project is properly stored and secured, complying with the respective standards applicable to each pilot scenario.

## 3.2 Survey data collected from pilots

This section describes the needed information requested for each pilot in terms of the RKW data and the envisaged assessment.

First, the description of fields in the table template is provided, together with a short explanation of what is expected to be introduced in each of them.

Then, a set of minimum desirable options/technologies for the key fields is also provided. These minimum requirements will be used to assess the performance of the RKW guidelines implementation in each pilot.

Finally, the assessment criterium is introduced. This criterium comprises a set of ranking items for inteGRIDy to benchmark pilots and the performance of each solution with respect to the current state of the art for the aforementioned requirements.

### *3.2.1 Template fields and expected content*

The following list contains the expected content to be introduced.

- **Number of databases:** Pilot partners are asked to detail the number of different databases used in the project. By different databases it is meant those ones either implemented in different technologies, located in different sites (either different hardware or different virtual machines) or used by different partners. This is just the assessment of the number of different data base instances, the access to each one is analysed on the following API section.
- **API descriptions**
  - Access Technology: Though at the time of writing this document RESTful API is probably the most widespread technology/paradigm to expose the information, it is also true that there are also alternatives, such as SOAP, GraphQL, RPC, etc. Partners are asked to specify which of them they rely on. As extended information, some hints on the internals are welcome (e.g. ExpressJS, PHP, Python Flask, etc.)
  - Persistence/DB: As for the data exposed, it goes without saying that it should be stored somewhere. Unlike the previous point, here there is no clear dominant, hence a plethora of solutions can be found: SQL, MongoDB, PostgreSQL, Apache Cassandra, Apache Hadoop, CKAN and a long etcetera. If necessary, partners are asked to provide more technical details (e.g. version, etc.).

- Location: Here the goal is obtaining some hints on the deployment (hosted server, hosted server + VM, VM on an IaaS (Infrastructure as a Service) provider, like Amazon AWS…). Of course, if the API/service is split into several locations, this info must be included here too.
- Execution: In order to have a deeper vision on e.g. how to replicate a pilot's ecosystem elsewhere, it would be necessary to know more details on the particular execution setup. For instance, this is the place to indicate whether the pilot followed the guidelines and deployed the data base in a Docker-like container-based system to straightforwardly run the modules. Besides, traditional servlet containers are also a mainstream solution (Apache Tomcat, etc.).
- Authentication: Does the pilot support any kind of authentication technology? If so, partners are asked to specify it (Basic authentication, API Key…). For this and the following items (Authorization, User access and Security) it is important to note that there might be no strong need in some cases to implement such measures, so it is not imposed as a hard requirement.
- Authorization: Following the point above, does the authentication realm link to any authorization solution (e.g. OAuth 2.0)? In affirmative case, partners are asked to introduce the information here.
- User Access: On top AA (Authentication & Authorization), does the pilot support any kind of policies to distinguish among users and roles?
- Security: Concerning the previous three points, there are a number of off-the-shelf solutions on the market that offer a fully-fledged *Authentication* + *Authorization* + *User Access* framework within a single service. As introduced in D1.6, a handful of (open-source or freeware) solutions (e.g. OpeIAM, Forgerock, Gluu, etc.) are suggested, that could be leveraged by the pilots instead having the deal with the security by themselves. In case one of these options is used (or any other), they should be detailed in this field.

- **Dataset descriptions**
  - Encryption: One of the most popular ways to protect/secure an API is using HTTPS (instead of the legacy HTTP) at the top of the stack. This is a typical solution when it comes to encrypt the data exchanged between client and server. Pilot partners should state whether they use this or any other similar alternatives to encrypt data.
  - RE-Use: Is this dataset used by a single partner or is it commonly shared by a number of pilot partners in different tools? In affirmative case, partners are asked to detail the partners and the tools used. In addition, if the dataset is marked as Open Data, the potential use envisaged for third parties outside the project is specified.
  - API: If the dataset is exposed via any of the APIs previously described, this is the field where the reference to the proper API should be put.

### *3.2.2 Minimum requirements*

In order to assess the proper implementation of the RKW guidelines issued in D1.6 (inteGRIDy reference architecture), there are a number of the aforementioned fields that require pilots to, at least, comply by the identified minimum requirements.

Those requirements are listed below and will be used to review the implementation process of each and every pilot:

- **Technology minimum requirements**: Please confirm the database is accessible through an open API.
- **Authentication minimum requirements**: Basic authentication at least. API key preferred.

- **Authorization minimum requirements**: OAuth or similar
- **User Access minimum requirements**: Up to pilots. Nothing requested.
- **Security minimum requirements**: One of Keyrock, Forgerock, Apache Syncope, Gluu, Keycloak, OpenIAM (or any other all-in-one security framework).
- **Encryption minimum requirements**: For those assets that are confidential or use sensitive data, please confirm if you use HTTPS (or similar).

These minimum requirements are mapped on the following table, corresponding to rank "1". Additionally, pilots can achieve rank "2" in case their solutions are technically exceeding the minimum requirements and "3" if they are using top solutions available currently. It is important to note that all pilots achieve the minimum requirements as detailed in D1.6, so this exercise is just to point out those pilots performing outstandingly on these RKW topics.

**Table 2. RKW assessment table**

| Guidelines | Implementation Rank | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| **APIs** | | | |
| **Access Technology** | Slightly used technologies | Websockets, MQTT | Mainstream Access Technology (e.g. REST API) |
| **Persistence DB** | No ranking (we could have also included a ranking in this category, classifying the different databases, in terms of e.g. performance, scalability, etc. Nonetheless, this analysis is out of the scope of RKW and would not have brought any added value to the studio) | | |
| **Location** | Local server (no backup) | Local Server + backup | Cloud Server (AWS, Azure) |
| **Execution** | "Manual" (e.g. Apache Tomcat, Python Flask...) | Docker/Container-based approach | Docker/Container-based approach + Service Orchestration (Kubernetes…) |
| **Authentication** | No authentication | Basic authentication/API Key | "Advanced" schema (OAuth2…)/CA Certificate |
| **User Access** | No user roles | Basic user access | Profile access (IDM) |
| **Authorization** | No authorization | Basic authorization | OAuth or similar/CA Certificate |
| **Security** | No restricted data | Based on user roles | Based on user roles and encryption |
| **Datasets** | | | |
| **Encryption** | None (HTTP) + CO | None (HTTP) + Open data | HTTPS/SSL |
| **Reuse** | No reuse | 2 partners | 3 or more partners |

Each pilot chapter will include a sub-paragraph for analysing the performance of the implemented RKW and assessing the implementation of guidelines. At the conclusions section, the overall assessment will be also provided and the big picture of RKW performance for pilots is analysed.

# 4. Pilot implementation

This section analyses the implementation and deployment of the field layer and data warehouse at each pilot.

The field layer devices are briefly described and an integration architecture diagram is presented and commented in terms of its quality attributes. The diagram was developed to match the general field architecture introduced on section 2. In this way it is possible to compare all the pilots and recognize a similar organization and even a similar choice of integration mechanisms as emphasised on the conclusions.

Still in relation with the field layer integration, a brief reference is made to the testing of the communication requirements that were carried out by the technological providers of each pilot. In general the testing procedures were defined by each partner to meet the defined requirements and performed without any major difficulty due to the extensive use of standard protocols.

The implementation of the data warehouse at each pilot is presented in the form of the survey introduced in section 3. The return from each pilot is discussed in comparison with a baseline of minimum technological requirements defined as good practice guidelines. Once again the collected results show a certain similarity between all the pilots that is expanded on the conclusions.

## 4.1 Isle of Wight

### *4.1.1 Introduction*

The Isle of Wight Pilot is deployed in three distinct and somewhat independent scenarios: a municipal leisure centre, a set of houses equipped with a HP, and an EV charging station. The sensing and metering devices include:

- A set of energy meters and sensors connected to a BMS in the municipal building;
- An energy meter, temperature sensors and on/off control on each HP installation;
- An EV charger, PV inverter, and battery management system on the charging station.

### *4.1.2 Field layer integration*

The field layer devices are connected through different REST APIs depending on the scenario. The devices on the municipal building are connected through a BMS services adaptor. The HP controllers are connected though a cloud portal, and the devices at EV charging station through an EMS (SCADA). These integration services or modules communicate using broadband accesses (DSL or 3G) using either proprietary protocols or MQTT over a VPN link.

At device level, the existing BMS communicates with the field controllers and sensors using BACnet; the HP controller is an integrated solution; Modbus-TCP and CAN bus are used to connect the EV charging devices to the SCADA (see Figure 3).

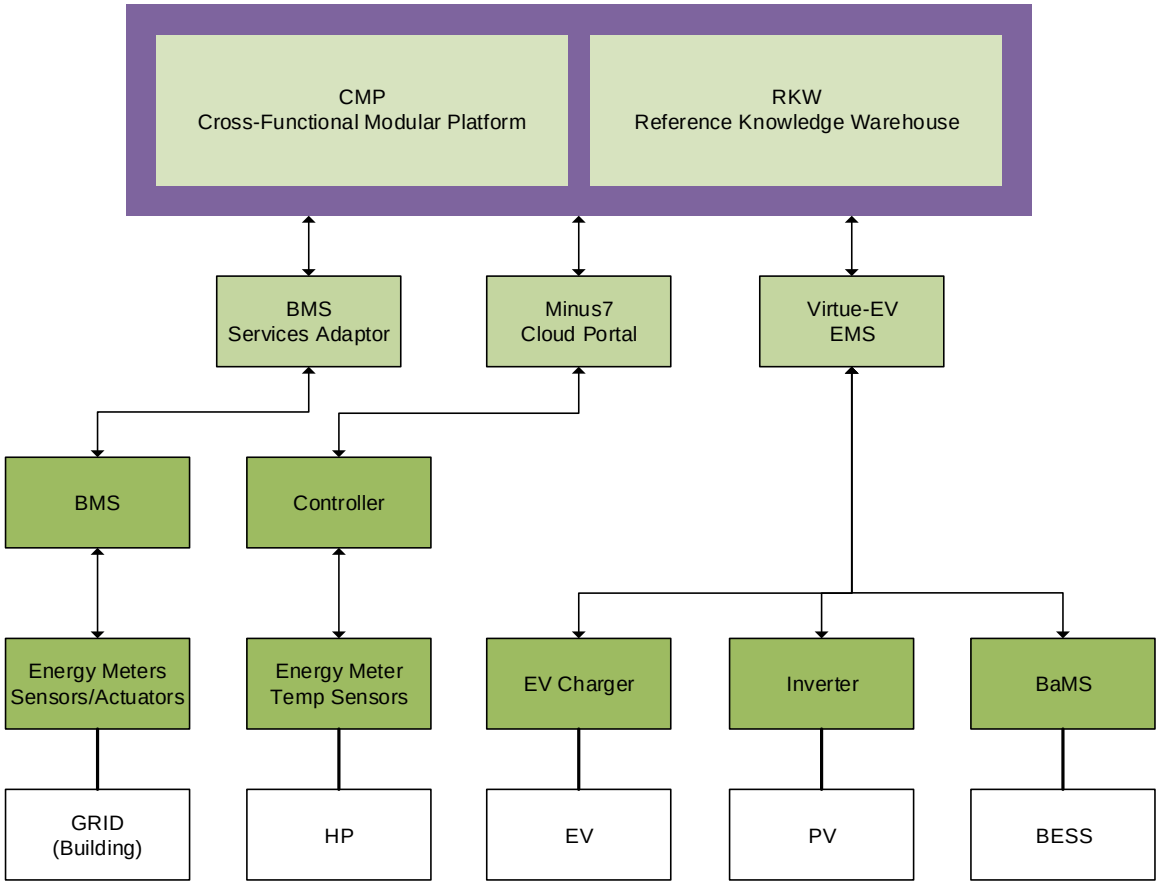


**Figure 3. IoW pilot field layer architecture**

The communication architecture is a good example of how to integrate different subsystems that originate from different market segments. The resulting solution is heterogeneous at field level but the integration mechanisms are similar which simplifies the development of advanced tools that combine data from the different sources. Individually, each solution is scalable, secure, and reliable being somewhat common in its area.

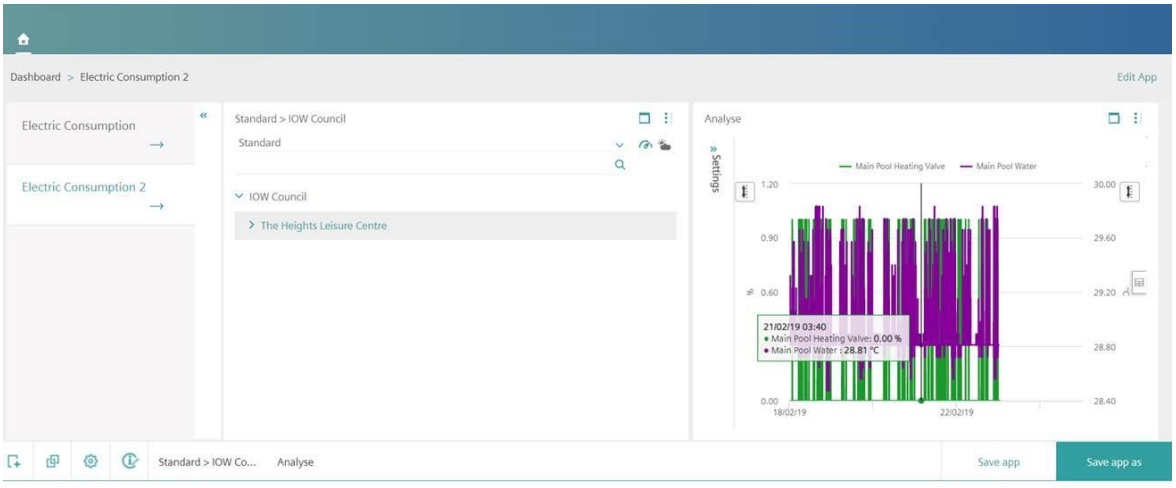


**Figure 4. IoW field data**

Figure 4 shows data collected (electricity consumption and indoor temperature) from the municipal building where field tests concerning the integration with the existing BMS were completed. The other systems of the pilot were also preliminary tested.

### *4.1.3 Data warehouse*

The Isle of Wight Pilot has reported the following information on the RKW survey.

**Table 3. IoW pilot RKW rank assessment per RKW item**

| Item | Description | Rank |
|---|---|---|
| Number of DBs/APIs | 4 | - |
| **API 1** | | |
| Access Technology | RESTful API | 3 |
| Persistence / DB | SQL | |
| Location | Amazon AWS | 3 |
| Execution | Docker | 2 |
| Authentication | API Key | 2 |
| Authorization | AUTHORIZATION DESK | 3 |
| User Access | Yes | 3 |
| Security | Custom solution | 3 |
| **API 2** | | |
| Access Technology | RESTful API | 3 |
| Persistence / DB | SQL | |
| Location | Cloud (Microsoft Azure) | 3 |
| Execution | Server (Tomcat) | 1 |
| Authentication | No | 1 |
| Authorization | | 1 |
| User Access | No user access needed – system admin only | 1 |
| Security | End/End encryption | 3 |
| **API 3** | | |
| Access Technology | RESTful API | 3 |
| Persistence / DB | SQL | |
| Location | Stored locally initially at Powerstar HQ | 2 |
| Execution | None yet for Pilot. Can be developed for future | 1 |
| Authentication | OpenVPN | 3 |
| Authorization | OpenVPN access level controlled | 3 |
| User Access | Yes | 3 |
| Security | None yet but for future | 3 |

**Table 4. IoW pilot datasets and RKW assessment**

| Dataset | Confidentiality | Encryption | | Reuse | Database |
|---|---|---|---|---|---|
| Asset Data | CO | HTTPS, OpenVPN | 3 | 3 | API1, API2, API3 |
| DR Points | RE | HTTPS | 3 | 2 | API1, API2 |
| Generation Profiles | CO | HTTPS, OpenVPN | 3 | 3 | API1, API2, API3 |
| Load/Consumption Data | CO | HTTPS, OpenVPN | 3 | 3 | API1, API2, API3 |
| Network Model | RE | OpenVPN | 3 | 1 | API3 |
| Simulation Environment | RE | Offline | 2 | 1 | API3 |
| Customer Data and Residential Profiles | CO | OpenVPN | 3 | 2 | API2, API3 |
| ESS Data | OP | OpenVPN | 3 | 1 | API3 |
| ESS Charge/Discharge Schedules | OP | OpenVPN | 3 | 1 | API3 |
| ESS and DR Set points | OP | OpenVPN | 3 | 1 | API3 |
| RES Set points and curtailment actions | OP | OpenVPN | 3 | 1 | API3 |

This pilot has RESTful interfaces with overall proper location layouts and security implementations. However, it is recommended to extend to the second API the satisfactory user authentication, authorization and control to resources achieved in the first and third APIs. Since the pilot has successfully achieved to use Docker on one of their interfaces, we believe that a good exercise, for the sake of a friendlier replicability, would be to Dockerize the other two deployment strategies.

## 4.2 Terni

### *4.2.1 Introduction*

Terni Pilot is deployed on a farm (microgrid powered by a PV panels and a CHP unit and including a storage system) and the local DSO infrastructures. The sensing and metering devices include:

- A set of power quality analyser at the microgrid's PV, CHP, and battery management systems;
- A power quality analyser at the LV/MV grid near the connection point of the microgrid.

### *4.2.2 Field layer integration*

The connection with all the field devices is realized through a dedicated monitoring tool module via MQTT. This module provides a MQTT broker and implements the required proprietary protocol to communicate with the field devices (that are all similar) through a broadband connection (DSL or 3G) using the HTTP protocol (see Figure 5).

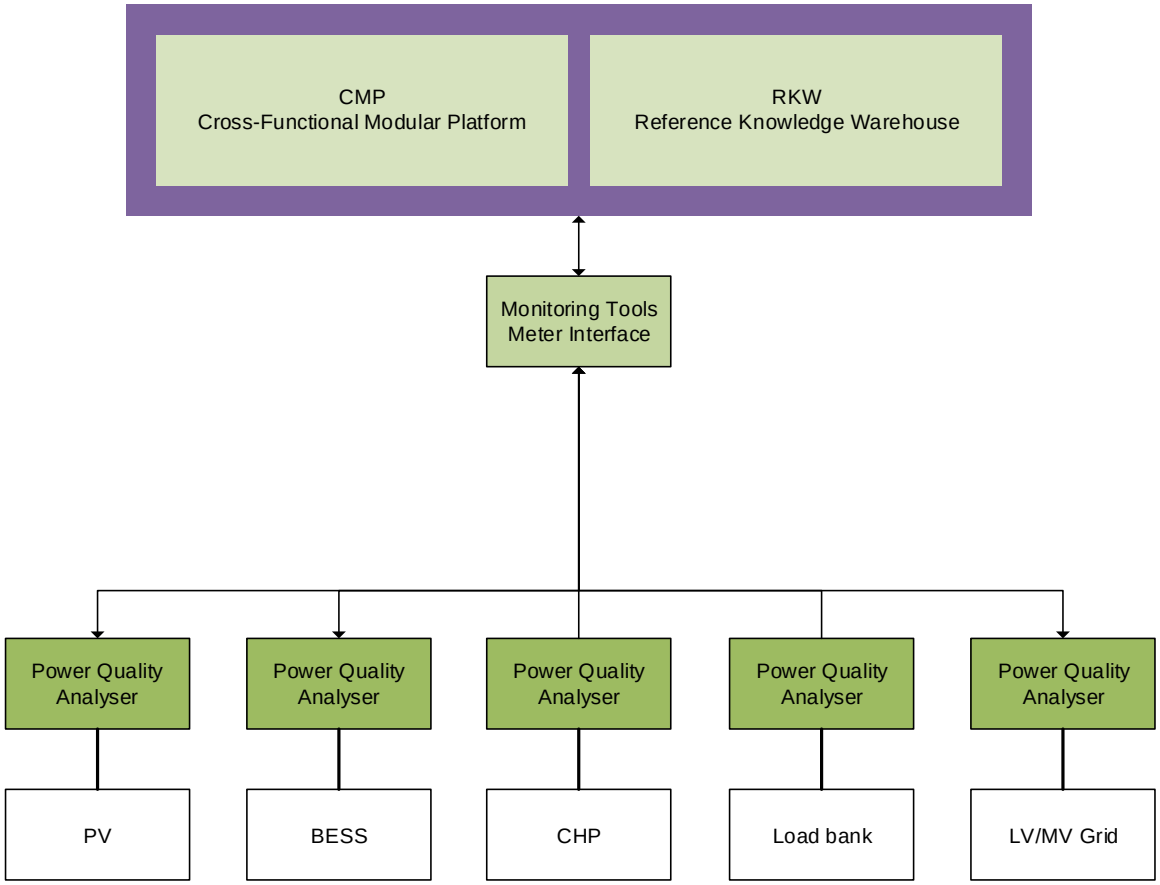


**Figure 5. Terni pilot field layer architecture**

The communication architecture is very simple and homogeneous. It is becoming widely used with the broad coverage of broadband networks. The solution is scalable, secure (if appropriate measures are taken) and reliable.

Preliminary communication tests were carried out regarding the MQTT protocol. Figure 6 shows data collected from the micro grid where field tests were performed.

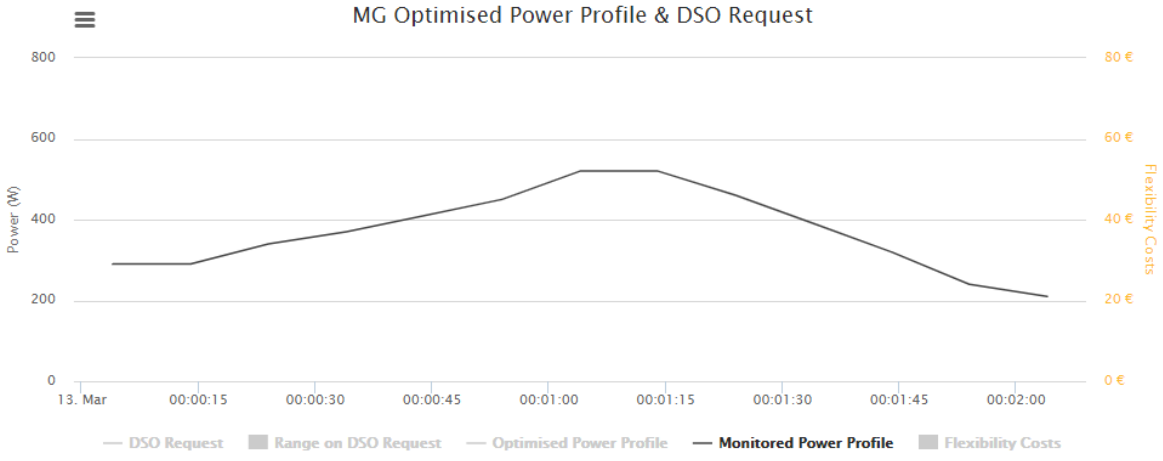


**Figure 6 Terni pilot field layer architecture**

### 4.2.3 Data warehouse

The Terni Pilot has reported the following information on the RKW survey.

**Table 5. Terni pilot RKW rank assessment per RKW item**

| Item | Description | Rank |
|---|---|---|
| Number of DBs/APIs | 1 | - |
| **API 1** | | |
| Access Technology | JPA | 1 |
| Persistence / DB | PostgreSQL | |
| Location | Terni pilot server + Backup | 2 |
| Execution | Docker container | 2 |
| Authentication | No, since all tools can be used only from the local private network that is accessible by authorised personnel only | 2 |
| Authorization | No, as per previous point | 2 |
| User Access | No difference between users has been identified | 2 |
| Security | No, as per previous point | 2 |

**Table 6. Terni pilot datasets and RKW assessment**

| Dataset | Confidentiality | Encryption | | Reuse | Database |
|---|---|---|---|---|---|
| Setpoints & DR commands | RE | No | 2 | 1 | API1 |
| Power flexibility | RE | No | 2 | 1 | API1 |
| DSO request | RE | No | 2 | 1 | API1 |
| Monitoring Data | RE | No | 2 | 1 | API1 |
| Device parameters & rated values | RE | No | 2 | 1 | API1 |
| Generation Data | RE | No | 2 | 1 | API1 |
| Consumption Data | RE | No | 2 | 1 | API1 |
| Weather Data | OP | No | 2 | 1 | API1 |
| Energy Prices | OP | No | 2 | 1 | API1 |
| Simulated Data | OP | No | 2 | 1 | API1 |

Regarding this pilot, it is worth mentioning the fact that their approach is rather orthogonal to the others since the access to the information is not foreseen to be open or shared with anyone. This has led to the utilization of a less-known interface (JPA) and the lack of encryption on the datasets (since everything is “hidden” behind a local private network).

## 4.3 San Severino

### *4.3.1 Introduction*

The San Severino Pilot is deployed on the area covered by the local DSO and includes the installation of some energy storage systems at small-medium users' premises. The sensing and metering devices include:

- Access the MV distribution grid measurement data from the existing DSO SCADA;
- An energy meter, a PV inverter (and MPPT controller), and a battery management system on each residential unit.

### *4.3.2 Field layer integration*

The connection with the MV field layer devices (power meters and switches) uses the ODBC protocol to access the DSO database server. Since this connection is highly sensitive for obvious reasons, only a replica of part of the database is accessible.

The connection with the LV field layer devices is carried out through a web server via a REST API. This server manages the connection with the field layer units that communicate with the server using an encrypted Modbus-TCP protocol over a broadband link (DSL or 3G). Locally, at each control unit, Modbus-RTU is used to connect the various devices including an energy meter, a sodium battery management system, and a custom PV inverter and a MPPT controller (see Figure 7).

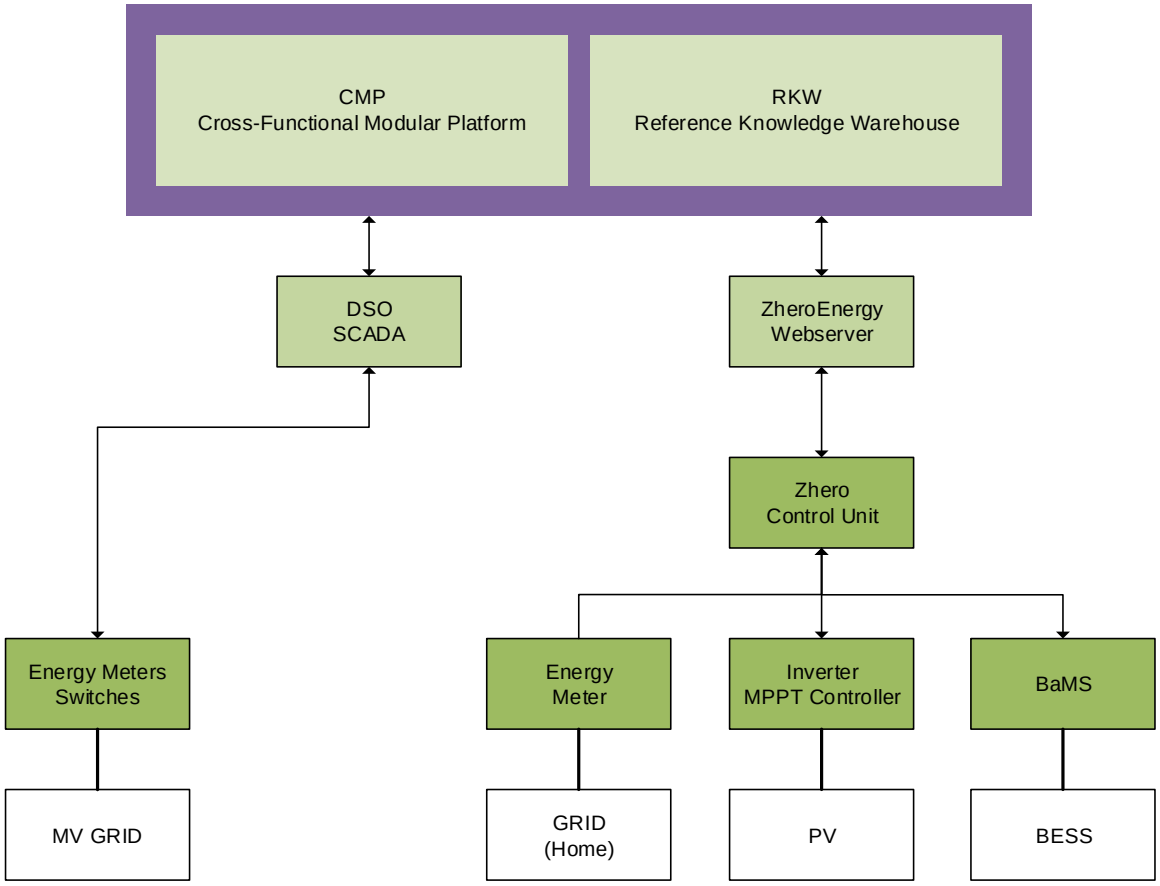


**Figure 7. San Severino pilot field layer architecture**

The communication architecture is adequate for the intended integration, MV grid information and LV grid storage capacity information. The solution is scalable, secure, and reliable.

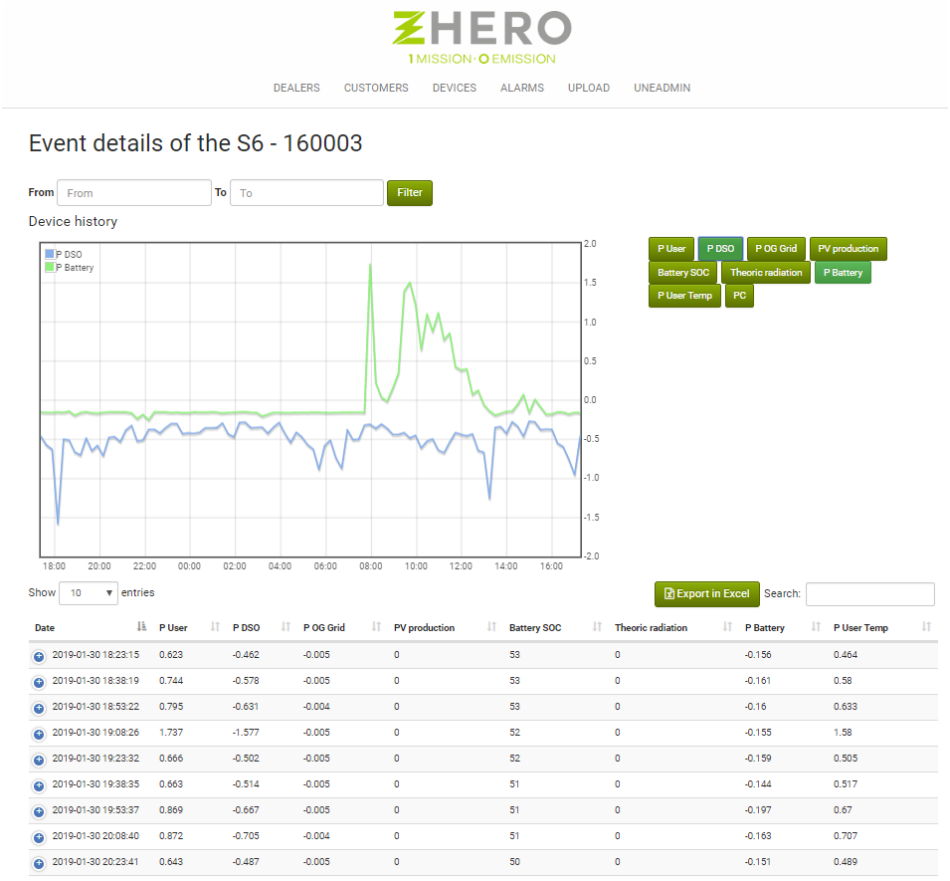


**Figure 8. San Severino pilot field data**

Figure 8 shows data collected from residential user where field tests were performed. Preliminary integration tests with the DSO SCADA were also carried out.

### *4.3.3 Data warehouse*

The San Severino Pilot has reported the following information on the RKW survey.

**Table 7. San Severino pilot RKW rank assessment per RKW item**

| Item | Description | Rank |
|---|---|---|
| Number of DBs/APIs | 2 | - |
| **API 1** | | |
| Access Technology | RESTful API | 3 |
| Persistence / DB | SQL database deployed in the UNE Cloud. | |
| Location | Remote Cloud | 3 |
| Execution | Application server and webserver: Tomcat | 1 |
| Authentication | DB server: MySQL | 2 |
| Authorization | DB server: MySQL | 2 |
| User Access | API catalogue implemented; it manages setpoints and data (HTTPS REST/JSON with an authentication header signature generated using the HMAC-SHA512 algorithm on the request parameters and a pre-shared API-key, a cryptographically random generated byte array converted to base64 string. | 2 |

| | | |
|---|---|---|
| Security | Endpoints use the HTTP POST method for both read operations and command actions to avoid issues with parameter sizing in the URL query, parameter spoofing, intermediate caching exploits and stale data | 2 |
| **API 2** | | |
| Access Technology | RESTful APIs | 3 |
| Persistence / DB | Oracle Database | |
| Location | Workstation is directly connected to the local (private) LAN of the DSO Control Center | 2 |
| Execution | Custom, no dockerized | 1 |
| Authentication | Admin access only | 3 |
| Authorization | SW with access rights is scheduled with a predefined timing (that is, each procedure is activated periodically, without user's intervention). | 3 |
| User Access | On the workstation, there is also a servlet (nginx), able to expose to an external module the set of RESTful APIs, and interact with a specific front end (deployed externally to the workstation itself). | 3 |
| Security | Authentication is handled through standard OAuth 2.0 authentication mechanisms exploiting the functionalities provided by specific OAuth Authentication Server. | 3 |

**Table 8. San Severino pilot datasets and RKW assessment**

| Dataset | Confidentiality | Encryption | | Reuse | Database |
|---|---|---|---|---|---|
| Customer Data | RE | HTTPS | 3 | 1 | API1 |
| ESS Data | RE | HTTPS | 3 | 1 | API1 |
| ESS Power/Energy Profiles | RE | HTTPS | 3 | 2 | API1 |
| ESS Setpoints | RE | No | 2 | 1 | API2 |
| Forecasted Algorithm Parameters | OP | HTTPS | 3 | 2 | API1 |
| Forecasted Load/Gen Profiles | RE | No | 2 | 1 | API2 |
| Freq. Reg. Signal | OP | HTTPS | 3 | 1 | API2 |
| Generation Profiles | RE | HTTPS | 3 | 1 | API2 |
| Grid Measurements | RE | HTTPS | 3 | 1 | API1 |
| Grid State Estimation | RE | HTTPS | 3 | 1 | API2 |
| Load / Consumption Profiles | RE | HTTPS | 3 | 1 | API2 |
| Market Data | OP | HTTPS | 3 | 1 | API2 |
| MV Network Data | RE | HTTPS | 3 | 1 | API2 |
| Optimal Grid Topology | OP | HTTPS | 3 | 1 | API2 |
| Weather Data | OP | HTTPS | 3 | 1 | API2 |

This pilot follows very well the given recommendations. It uses RESTful APIs with rightful location mechanisms and authentication/authorization/user control schemes, and the proper security level with encrypted communications for all the datasets. All the same, we suggest using a deployment strategy that involves containerization to boost compatibility and maintainability.

## 4.4 Barcelona

### *4.4.1 Introduction*

The Barcelona Pilot is deployed on a refurbished sports centre (Claror). The sensing and metering devices include:

- A set of status information and setpoints related mainly with the HVAC and dehumidifier systems that are connected to the BEMS (SCADA);
- A PV inverter and a battery that will be installed.

### *4.4.2 Field layer integration*

The connection with the field layer devices is realized through the NEMO tool that will be installed on the premises through a set of REST APIs. Moreover, the tool also supports the standard IEC 60870-5-104 and OpenADR protocols as data integration mechanisms, in particular, NEMO will also integrate with DEMS tool for the management and exchange of information related to Demand Response events. This tool implements the communication with the existing SCADA system via a proprietary protocol and with the inverter and the battery management system via Modbus-TCP, via LAN connections.

The SCADA communicates with the devices that include the HVAC and the dehumidifier using standard Modbus-RTU and KNX over serial links (see Figure 9).

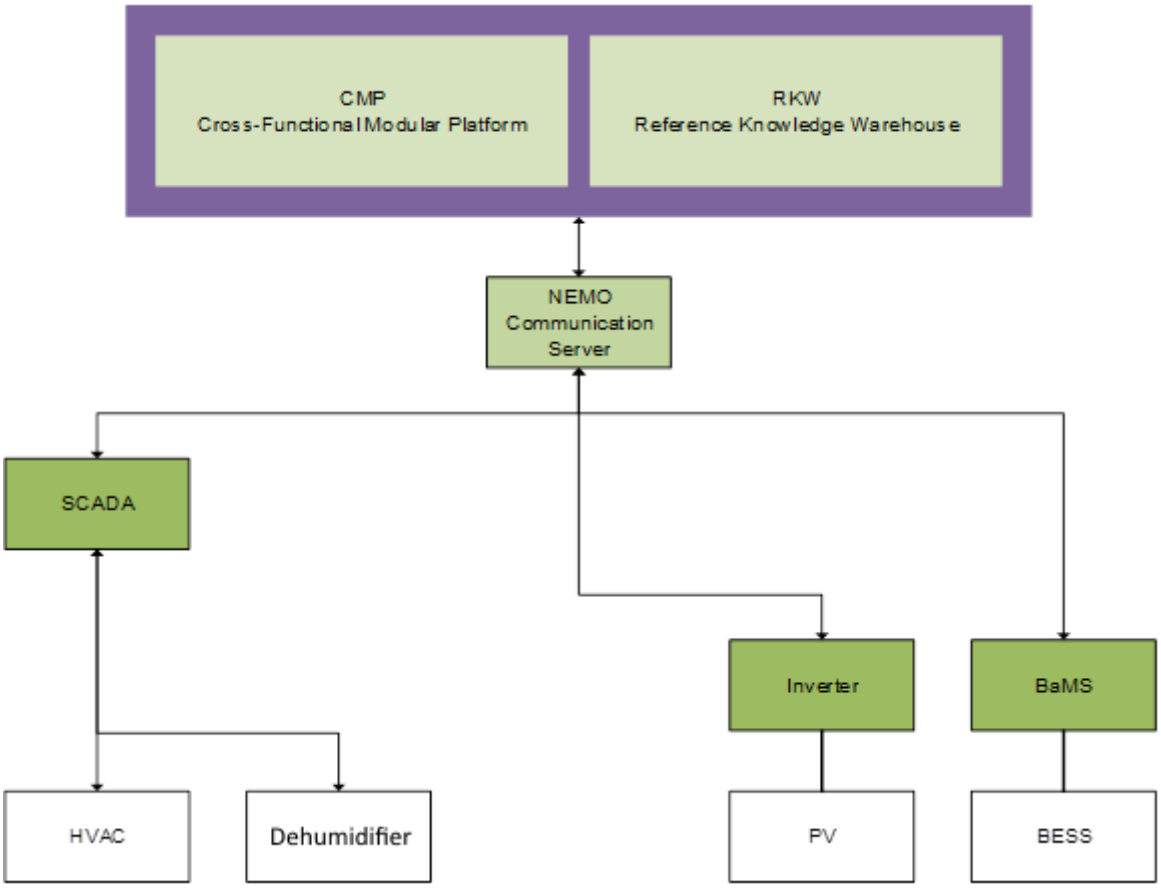


**Figure 9. Barcelona pilot field layer architecture**

The communication architecture is appropriate for the integration requirements. The protocols used are exclusively wired and use the existing network infrastructure (LAN). The solution is scalable, secure, and reliable.

### 4.4.3 Data warehouse

The Barcelona Pilot has reported the following information on the RKW survey.

**Table 9. Barcelona pilot RKW rank assessment per RKW item**

| Item | Description | Rank |
|---|---|---|
| Number of DBs/APIs | 5 | - |
| **API 1** | | |
| Access Technology | AWS REST API Gateway, OpenAPI 3.0 compatible | 3 |
| Persistence / DB | Persistence in logs from AWS CloudWatch and data from AWS RDS. | |
| Location | AWS, region Ireland | 3 |
| Execution | API Gateway (AWS) | 2 |
| Authentication | Not available | 1 |
| Authorization | Not available | 1 |
| User Access | Not available | 1 |
| Security | There's no confidential data, but all information is shared by HTTPS | 3 |
| **API 2** | | |
| Access Technology | Internal API under API 1 | 3 |
| Persistence / DB | Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 | |
| Location | Virtual Machine in Siemens Data Center | 2 |
| Execution | Physical server | 2 |
| Authentication | All EnergyIP specific database users and roles are created automatically while running the Installer. During installation you will be required to provide the password of either a user with DBA privileges or the EIP_DBA user. | 3 |
| Authorization | Access to the data requires that you provide credentials for a user with permissions sufficient to perform schema installation and upgrades. | 3 |
| User Access | Database users will need to provide the username and password for the corresponding database schema. | 3 |
| Security | A comprehensive model of user roles linked to permission groups, which are subsequently linked to permissions on data and functions, is shipped with EnergyIP. | 3 |
| **API 3** | | |
| Access Technology | REST based APIs | 3 |
| Persistence / DB | Apache Cassandra 3.9 | |
| Location | Virtual Machine in Siemens Data Center | 2 |
| Execution | Physical server | 2 |
| Authentication | DEMS provides a simple set of functionality for authentication and permissions. User authentication is managed using JSON Web Token (JWT). | 3 |
| Authorization | Permissions are managed by the EnergyIP permission model. There are permission group to read and write in common time series tables. | 3 |
| User Access | This API is used to retrieve time series data. | 3 |

| | | |
|---|---|---|
| Security | A comprehensive model of user roles linked to permission groups, which are subsequently linked to permissions on data and functions, is shipped with EnergyIP. | 3 |
| **API 4** | | |
| Access Technology | REST based APIs (ASP.NET) | 3 |
| Persistence / DB | Data persistent only in access logs | |
| Location | Virtual Machine in Claror Data Center (physical server) | 1 |
| Execution | Docker container | 2 |
| Authentication | Not available | 1 |
| Authorization | API Key | 2 |
| User Access | Not available | 1 |
| Security | There's no confidential data, but all information is shared by HTTPS | 3 |
| **API 5** | | |
| Access Technology | REST based APIs | 3 |
| Persistence / DB | | |
| Location | NEMO Tool | 2 |
| Execution | Physical server | 1 |
| Authentication | Not available | 1 |
| Authorization | Not available | 1 |
| User Access | Not available | 1 |
| Security | There's no confidential data | 2 |

**Table 10. Barcelona pilot datasets and RKW assessment**

| Dataset | Confidentiality | Encryption | | Reuse | Database |
|---|---|---|---|---|---|
| Accounts Data | RE | NO | 2 | 2 | 2 |
| Baseline | RE | NO | 2 | 2 | 3 |
| Battery Data (including Capacity) | RE | NO | 2 | 2 | 5 |
| Common Time Series | RE | NO | 2 | 2 | 3 |
| Customer Data | RE | NO | 2 | 2 | 2 |
| Demand Response Events | RE | NO | 3 | 3 | 3 |
| Assets Data | RE | NO | 2 | 2 | 2 |
| Distribution Grid Congestion data | RE | NO | 2 | 2 | 1 |
| Equipment Status | RE | NO | 2 | 2 | 3 |
| Forecasted Data | RE | NO | 2 | 2 | 2 |
| Forecasted Electricity Price Data | RE | HTTPS | 3 | 3 | 1 |
| Forecasted Weather Data | RE | HTTPS | 3 | 3 | 1 |
| Current conditions (Indoor data) | RE | NO | 2 | 3 | 5 |
| Proposed setpoint per asset | RE | NO | 2 | 3 | 5 |
| Market emulator (including Services | RE | HTTPS | 3 | 2 | 1 |

| | | | | | |
|---|---|---|---|---|---|
| Data) | | | | | |
| Load / Consumption Data | RE | HTTPS | 3 | 3 | 1 |
| Predicted Shed | RE | NO | 2 | 2 | 1 |
| Premises Data | RE | NO | 2 | 2 | 1 |

There have been some slight changes on the datasets and confidentiality levels with respect to D1.6. First of all, each and every dataset is now market as restricted. There were some labelled as Confidential in D1.6 but, after a thorough review, no personal/sensitive data is finally expected to be included there, so they were re-assessed in terms of confidentiality.

In addition, 2 datasets have been absorbed by bigger ones. That is the case of Capacity, which is now stored inside Battery Data dataset, and Services Data, whose information can be now retrieved from Market emulator dataset.

Barcelona's pilot is the one with more APIs and most of them follow the recommendations very well. All of them expose their information by using mainstream access technologies (RESTful and SQL), have recovery possibilities in case of hardware or communication failure, and have an adequate security handling. It is recommended, though, to extend the high-quality authentication/authorization/user access methods of APIs 2 and 3 to the rest of the interfaces.

Regarding the encryption of the communication with the datasets, it is highly advisable to include encryption in those datasets for which the confidentiality level has been set to confidential/restricted.

## 4.5 St. Jean

### *4.5.1 Introduction*

The St. Jean Pilot is deployed in a set of residential/commercial end users of the local DSO. The sensing and metering devices, at each location, include:

- An energy meter, smart-plugs, smart-switches, smart-lights (DALI LEDs) and an indoor multisensory (temperature, humidity, and illuminance) with Z-Wave communication interface;
- Smart light bulbs with a ZigBee communication interface.

### *4.5.2 Field layer integration*

The connection with the field layer is realized through a software communication module via a REST API. This module manages the connection with the field gateways and implements the required proprietary communication protocol. Each gateway is connected through broadband access via an Ethernet port.

At field level, each gateway communicates with the sensors using the mentioned wireless standard protocols (see Figure 10).

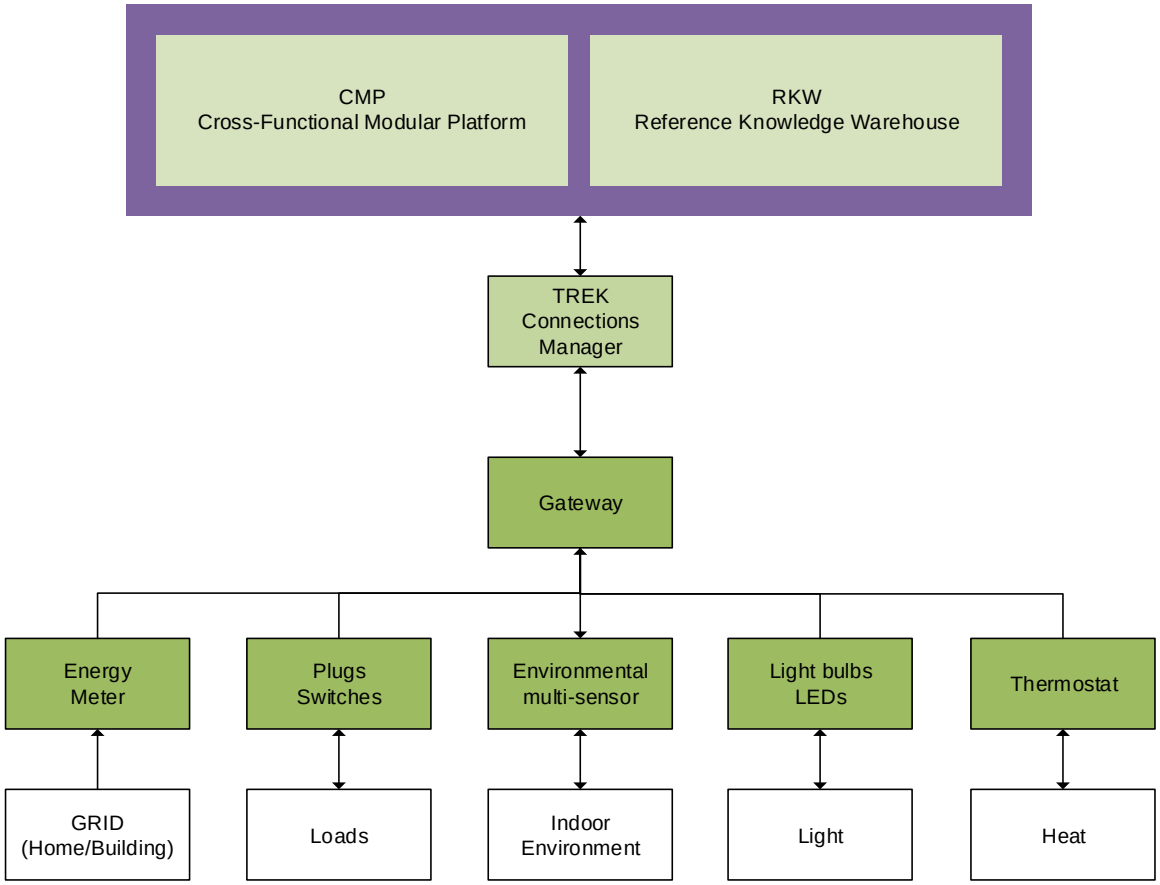


**Figure 10. St. Jean pilot field layer architecture**

The communication architecture is widely used in comparable applications and has proved to be effective if the deployment and maintenance of the wireless devices is carefully planned and executed. Apart from this the solution is scalable, secure, and reliable.


**Figure 11. St. Jean pilot field data**

Figure 11 shows data collected from a residential building. The complete field devices communication protocols were fully tested.

### *4.5.3 Data warehouse*

The St. Jean Pilot has reported the following information on the RKW survey.

**Table 11. St. Jean pilot RKW rank assessment per RKW item**

| Item | Description | Rank |
|---|---|---|
| Number of DBs/APIs | 1 | - |
| **API 1** | | |
| Access Technology | RESTful API (no service available though) | 3 |
| Persistence / DB | MySQL | |
| Location | TREK premises | 2 |
| Execution | MySQL server | 1 |
| Authentication | Through a module that manages the RKW | 2 |
| Authorization | Through a module that manages the RKW | 2 |
| User Access | Through a module that manages the RKW | 2 |
| Security | Through a module that manages the RKW | 2 |

**Table 12. St. Jean pilot datasets and RKW assessment**

| Dataset | Confidentiality | Encryption | | Reuse | Database |
|---|---|---|---|---|---|
| Asset Address | CO | Yes | 3 | 1 | API1 |
| Asset Flexibility | RE | No | 2 | 2 | API1 |
| Asset Location | RE | Yes | 3 | 1 | API1 |
| Environmental Data | RE | No | 2 | 1 | API1 |
| KPIs | RE | No | 2 | 2 | API1 |
| Load / Consumption Data | RE | No | 2 | 1 | API1 |
| Operational Data | RE | No | 2 | 1 | API1 |
| Thermal Profile | RE | No | 2 | 1 | API1 |
| Visual Profile | RE | No | 2 | 1 | API1 |

St-Jean's pilot relies on a mainstream RESTful API to expose their information, following the current trends. By virtue of potential replicability, the use of a container-based approach would have been more preferable over a straightforward MySQL environment (and even more preferable if that container-based approach is complemented with an orchestration tool for a complete control of the platform). Nonetheless, the pilot follows the recommendations given on the security plane, guaranteeing the correct use of a fully-fledged authentication/authorization/user control framework. Besides, the only confidential dataset is protected by means of encryption, which also satisfies the suggestions regarding the RKW.

## 4.6 Nicosia

### *4.6.1 Introduction*

The Nicosia Pilot is deployed on the campus of the University of Cyprus (microgrid powered by a PV panels and including a storage system) and group of selected dispersed prosumers. The sensing and metering devices include:

- A set of energy meters and sensors connected to existing BEMSs (SCADAs) on different campus' buildings;
- A PV inverter and a battery management system installed on the campus;
- A smart meter and a PV inverter installed at each prosumer location.

### *4.6.2 Field layer integration*

The connection with the microgrid field layer devices is realized through a pair of tools via REST APIs. These tools implement the required standard and proprietary protocols to communicate with the distinct commercial BEMSs, PV inverter and battery management system via the existing network infrastructure (LAN).

The connection with the dispersed prosumer units is realized through a DSO data server using also a REST API. These units measure electricity consumption and production (PV) and communicate with the DSO data server using a proprietary protocol via a cellular broadband connection.

Locally, each BEMS uses various protocols including Modbus-RTU and Modbus-TCP to communicate with the meters, sensors and actuators (see Figure 12).

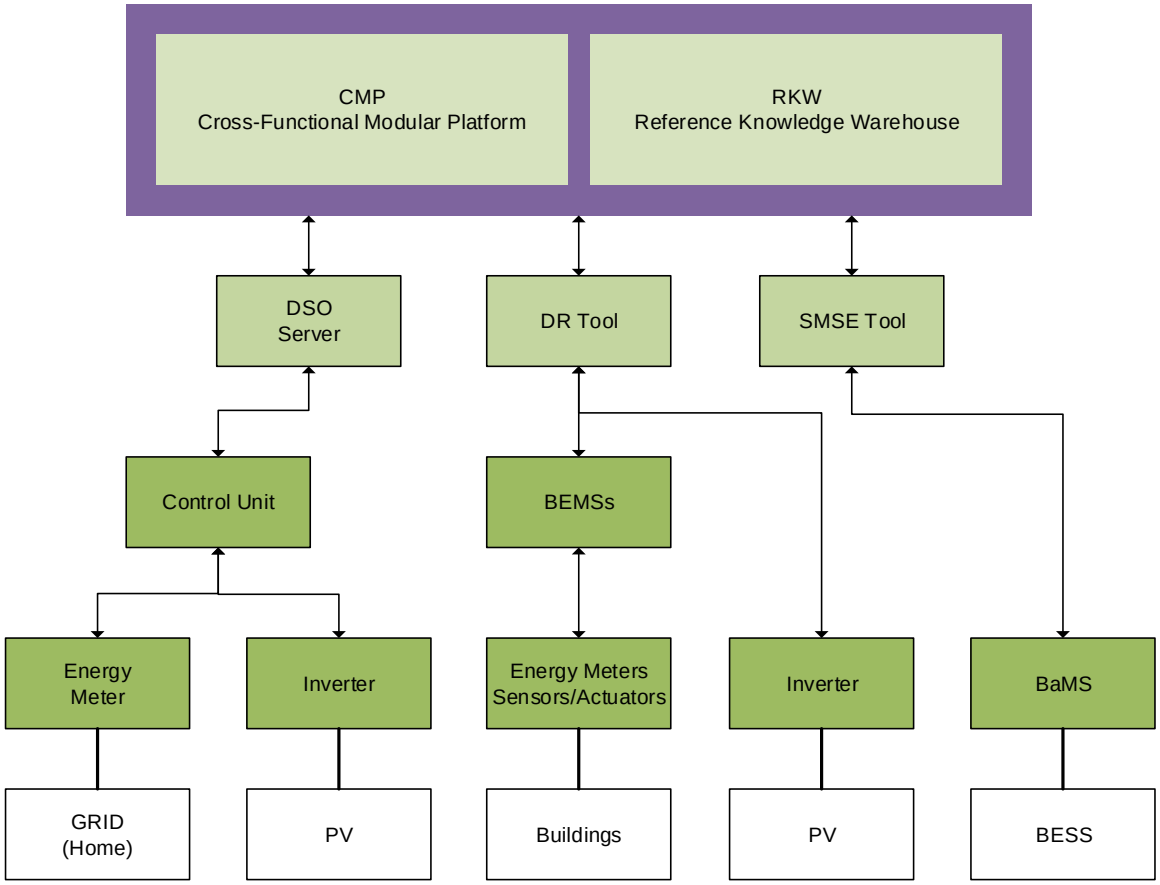


**Figure 12. Nicosia pilot field layer architecture**

The communication architecture for the microgrid scenario is a good example of the integration of existing building energy management systems and RES management systems. The integration effort in implementing distinct protocols is required to develop advanced analytical tools. The integration of the dispersed prosumers' information via the DSO infrastructure is also a good example of integration of an existing system. Overall, the solution is scalable, secure, and reliable.

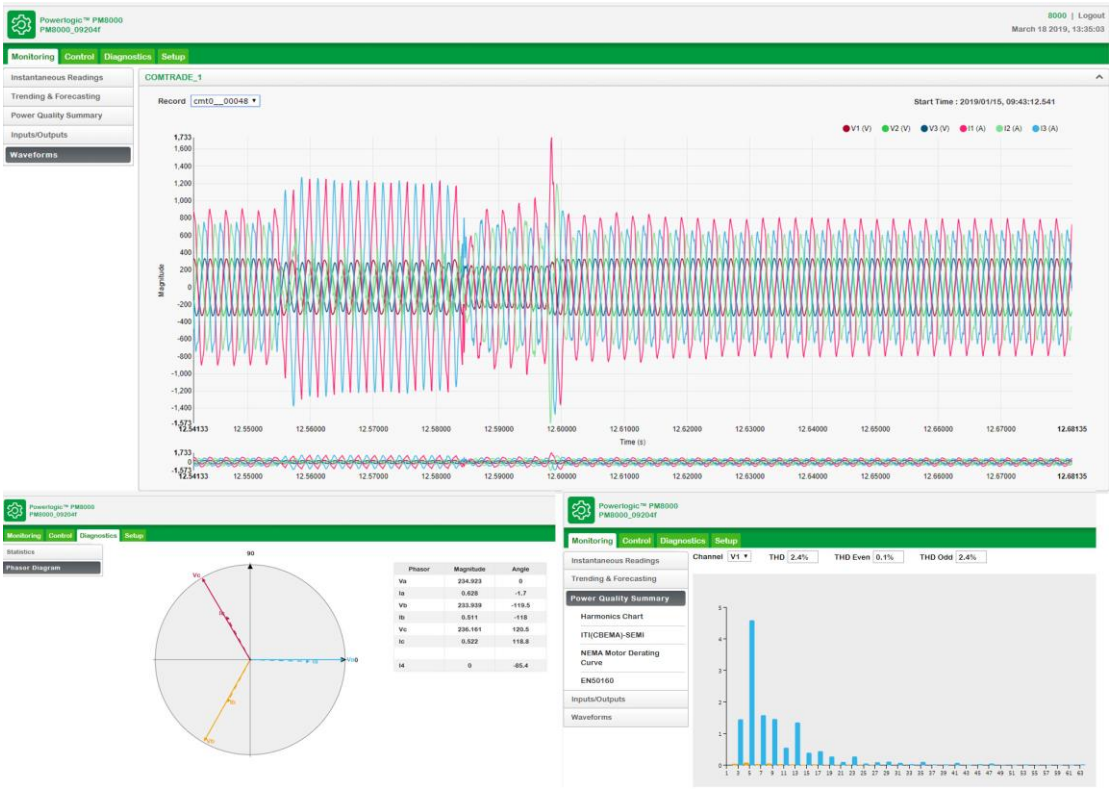


**Figure 13. Nicosia pilot field data**

Figure 13 shows data collected from various BEMS. Testing the full range of field devices communications is under way.

### *4.6.3 Data warehouse*

The Nicosia Pilot has reported the following information on the RKW survey.

**Table 13. Nicosia pilot RKW rank assessment per RKW item**

| Item | Description | Rank |
|---|---|---|
| Number of DBs/APIs | 1 | - |
| **API 1** | | |
| Access Technology | RESTful API | 3 |
| Persistence / DB | MySQL | |
| Location | Self-hosted server + VM | 1 |
| Execution | Standard installation; dockerization of some modules is possible | 2 |
| Authentication | basic username/password authentication | 2 |

| | | |
|---|---|---|
| Authorization | not available | 2 |
| User Access | role based only | 3 |
| Security | proprietary | 2 |

**Table 14. Nicosia pilot datasets and RKW assessment**

| Dataset | Confidentiality | Encryption | | Reuse | Database |
|---|---|---|---|---|---|
| Customer Data | CO | open VPN | 2 | 3 | API1 |
| DR Points | RE | HTTPS | 3 | 3 | API1 |
| Energy Prices | OP | HTTPS | 3 | 3 | API1 |
| Forecasted Data | OP | open VPN | 2 | 3 | API1 |
| Generation Data | RE | open VPN | 2 | 3 | API1 |
| Microgrid Load Profile | RE | HTTPS | 3 | 3 | API1 |
| Residential Load Profile | RE | HTTPS | 3 | 3 | API1 |

It is worth highlighting that all the datasets of the Nicosia pilot can be reused by 3 or more tools. With the possibility of dockerization/containerization, a role-based user access and respectable encrypted communication (not only on confidential or restricted datasets, but also on open data), most of the recommendations can be considered as followed. The only suggestion that is left would be the addition of a more robust deployment (e.g. backup, IaaS, etc.) that would save the system in case the legacy server/VM suffers a connection outage (or any other critical issue).

## 4.7 Lisbon

### *4.7.1 Introduction*

The Lisbon Pilot is deployed on one large municipal building (Campo Grande 25). The sensing and metering devices include:

- A set of energy meters on a main distribution board that monitor total income and partial consumptions (e.g. chillers and elevators);
- A set of standard EV chargers located in the basement;
- A pair of fast EV chargers also located in the basement that are managed by an external company responsible for the national network;
- A set of sensors (e.g. level and temperature) and meters (e.g. flow) related mainly with the HVAC system that are connected to the BMS (SCADA);
- A PV inverter that will be installed on the roof.

### *4.7.2 Field layer integration*

The connection with the field layer is realized through a software communication manager (service) via a REST API. This module manages the connection with the field layer devices and implements the required set of standards (with the fast EV chargers management platform and the BMS) and proprietary (with the data hubs or data concentrators) protocols.

The building energy meters, standard EV chargers and PV inverter are connected to its own data concentrator via Modbus-RTU while each concentrator is accessed via a broadband connection from an Ethernet interface. Similarly, the integration of the fast EV charger and the BMS is done via specific REST APIs over an Ethernet connection (see Figure 14).

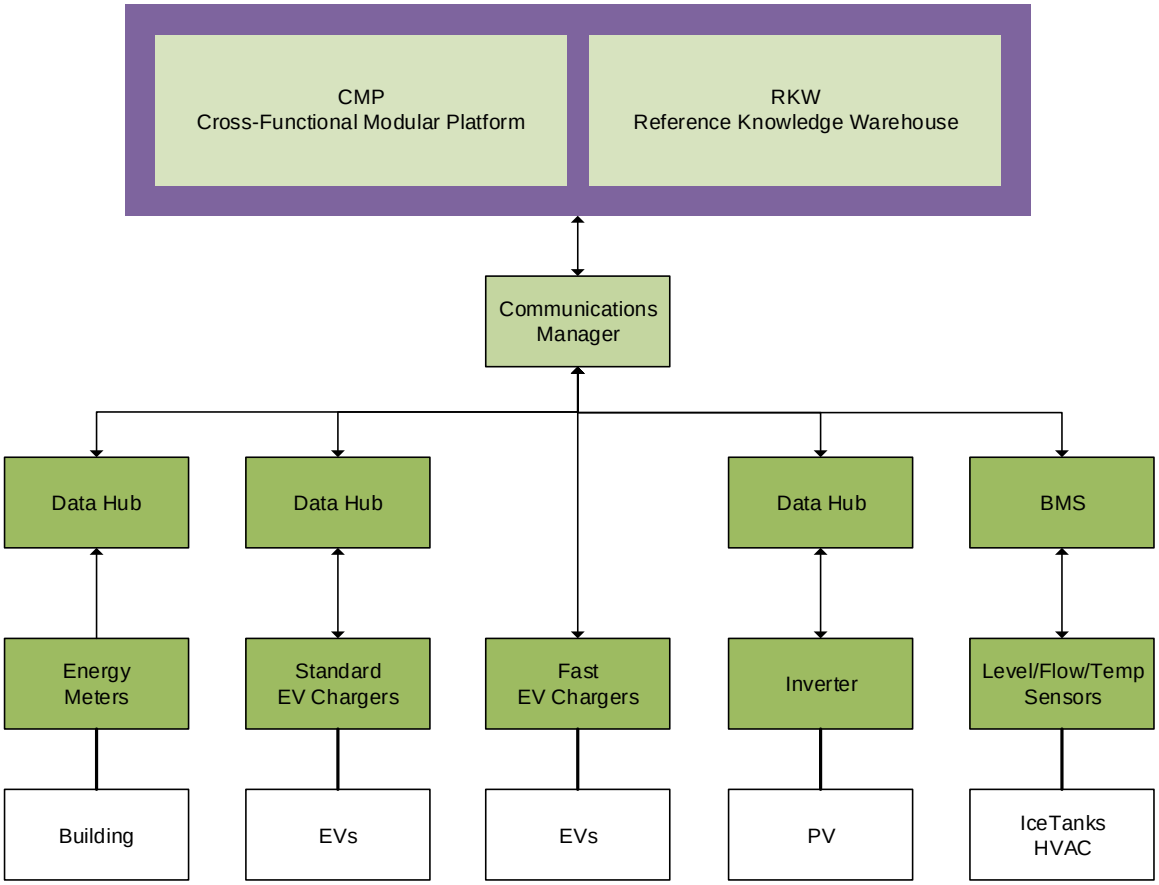


**Figure 14. Lisbon pilot field layer architecture**

The communication architecture is adequate for the implementation scenario that is a single building. The protocols used are exclusively wired and use the existing network infrastructure (LAN). This architecture is also a good example of how heterogeneous systems can be effectively integrated and explored. The solution is scalable, secure, and reliable.

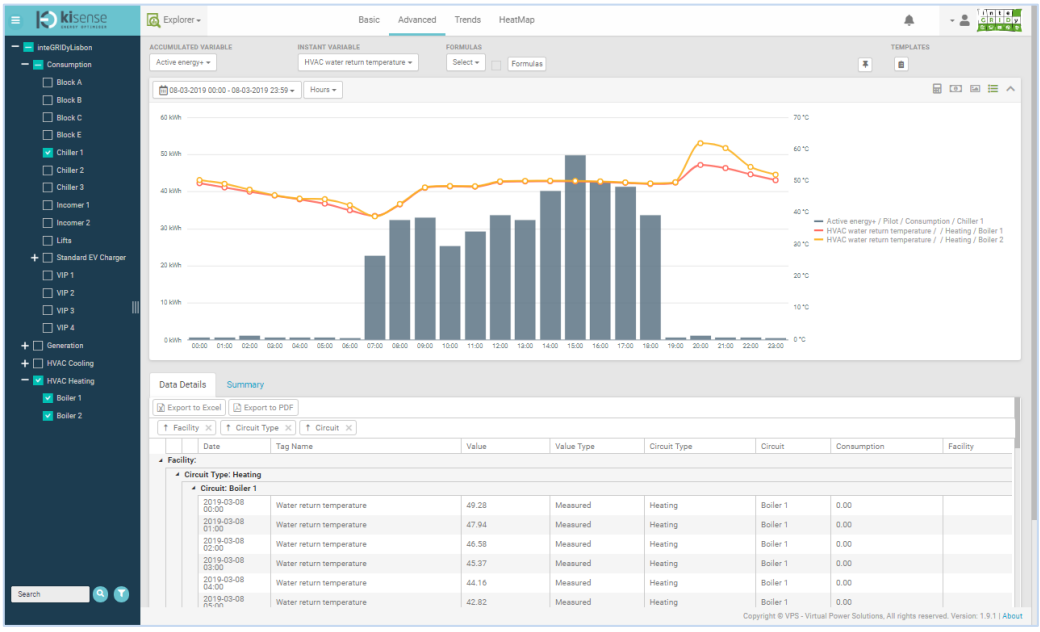


**Figure 15. Lisbon pilot field data**

Figure 15 shows data collected from the pilot building. The communication with all the field devices was fully tested including the integration mechanisms that are used to collect data from existing systems.

### *4.7.3 Data warehouse*

The Lisbon Pilot has reported the following information on the RKW survey.

**Table 15. Lisbon pilot RKW rank assessment per RKW item**

| Item | Description | Rank |
|---|---|---|
| Number of DBs/APIs | 1 | - |
| **API 1** | | |
| Access Technology | RESTful API | 3 |
| Persistence / DB | Microsoft SQL Server | |
| Location | Virtual datacentre | 3 |
| Execution | Standard installation; dockerization of some modules is possible | 2 |
| Authentication | Basic username/password authentication | 2 |
| Authorization | Token based authorization | 2 |
| User Access | Role-based and facility based | 3 |
| Security | HTTPS | 2 |

**Table 16. Lisbon pilot datasets and RKW assessment**

| Dataset | Confidentiality | Encryption | | Reuse | Database |
|---|---|---|---|---|---|
| DR Schedules | RE | HTTPS | 3 | 1 | API1 |
| Energy Prices | OP | HTTPS | 3 | 2 | API1 |
| EV Charging Data | RE | HTTPS | 3 | 1 | API1 |
| EV Charging Profiles | RE | HTTPS | 3 | 1 | API1 |
| ICE Tanks Data | RE | HTTPS | 3 | 1 | API1 |
| Load / Consumption Data | RE | HTTPS | 3 | 1 | API1 |
| Load / Consumption Forecast | RE | HTTPS | 3 | 1 | API1 |
| Load / Consumption Profiles | RE | HTTPS | 3 | 1 | API1 |
| Production Forecast | RE | HTTPS | 3 | 2 | API1 |
| Weather Data | OP | HTTPS | 3 | 1 | API1 |

Given this information, the result of the assessment is very positive overall. It uses virtual machines in the cloud with proper backup plans and the possibility of dockerization, which makes it potentially suitable for rapid deployment. Furthermore, it provides a good combination of authentication, authorization and user access based in roles and token exchange, not to mention that all the communications with the datasets are encrypted.

## 4.8 Xanthi

### *4.8.1 Introduction*

The Xanthi Pilot is deployed on an islanded microgrid facility (Sunlight RES Park) with three distinct test cases. The sensing and metering devices include:

- Energy meters, DC-DC converters, AC-DC inverters, AC-DC inverters, chargers distributed over the infrastructure to monitor production (from a diesel and wind generators) and load consumption;
- A diesel generator with start and stop controls;
- A fuel cell (FC) and an electrolyzer cell power production and status.

### *4.8.2 Field layer integration*

The connection with the field layer devices is implemented through the Data Exchange Tool via MQTT over a broadband connection. On field side, the tool communicates with a commercial SCADA that manages the connection with the devices using an OPC interface.

Proprietary serial (RS485) and TCP/IP protocols and the standard CAN bus are used to connect the devices to the SCADA system (see Figure 16).

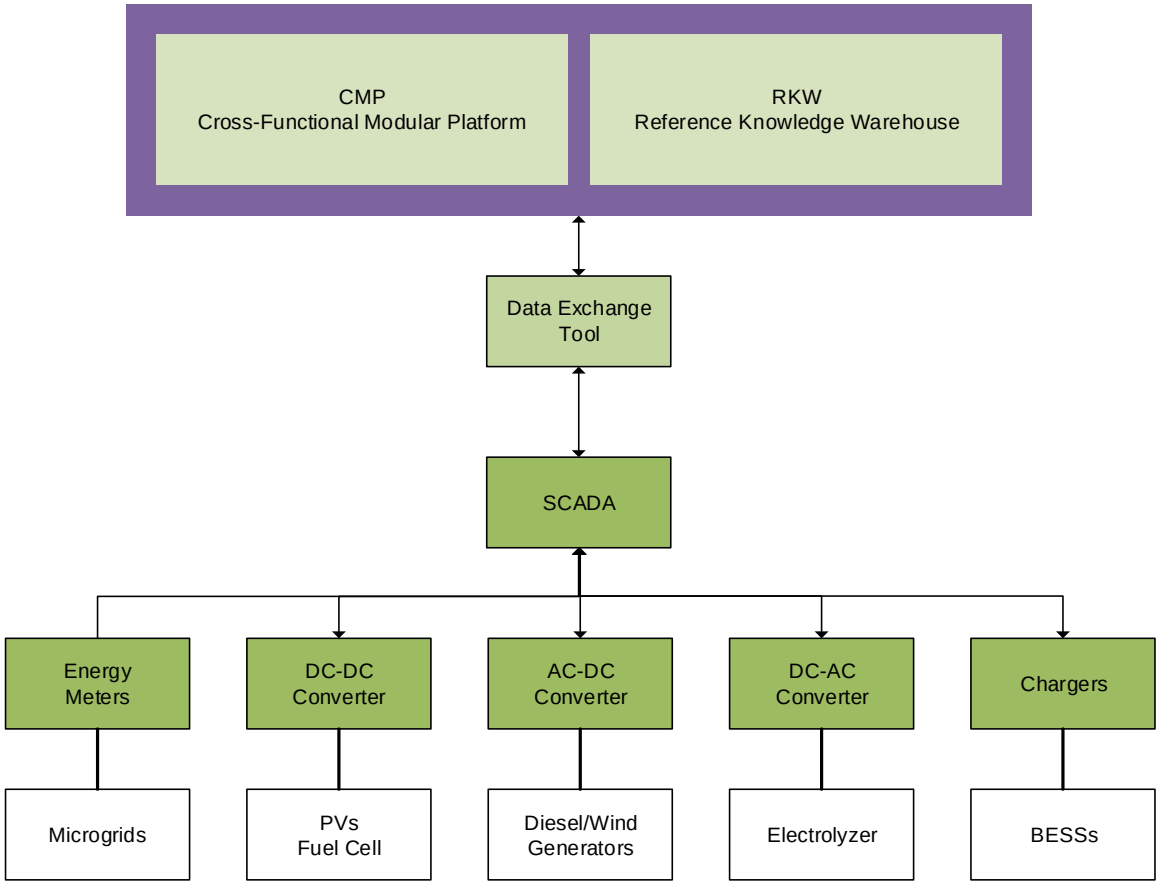


**Figure 16. Xanthi pilot field layer architecture**

The communication architecture is in our opinion adequate for the implementation scenario that is a localized power facility. The protocols used are exclusively wired and common on this kind of application. The integration mechanism that is based on OPC is also widely used in industrial applications. The solution is scalable, secure, and reliable.

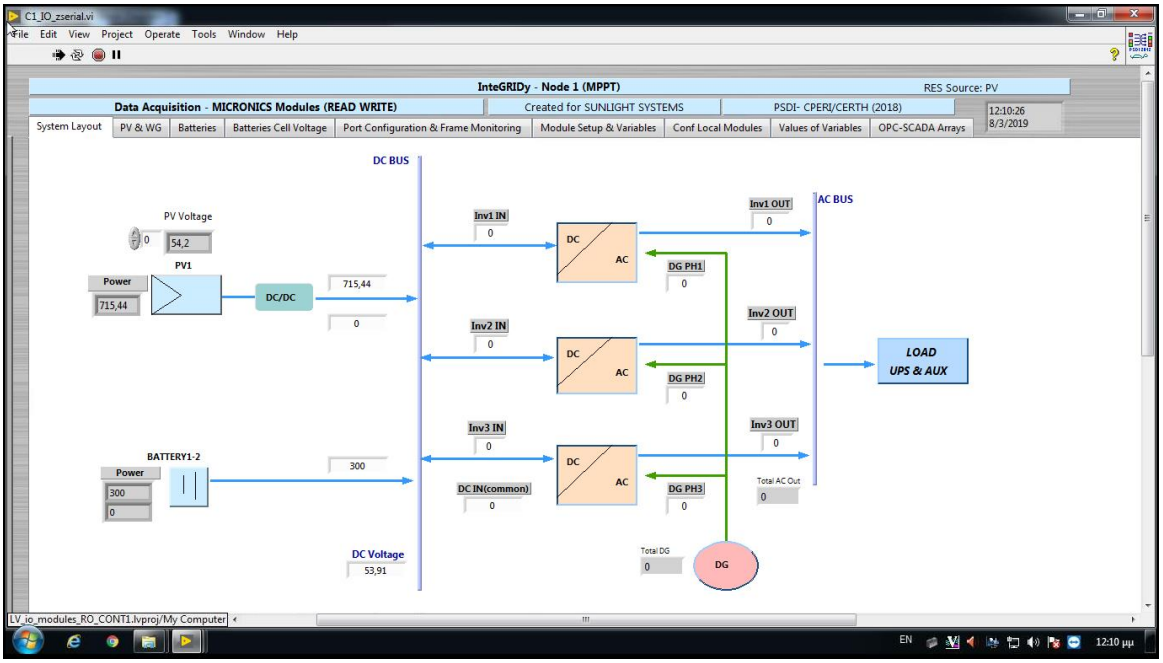


**Figure 17. Xanthi pilot field data**

Figure 17 shows data collected from one node of the pilot facilities. The communication will all the field devices was fully tested.

### *4.8.3 Data warehouse*

The Xanthi Pilot has reported the following information on the RKW survey.

**Table 17. Xanthi pilot RKW rank assessment per RKW item**

| Item | Description | Rank |
|---|---|---|
| Number of DBs/APIs | 1 | - |
| **API 1** | | |
| Access Technology | MQTT API through a MATLAB executable | 2 |
| Persistence / DB | Process DB SCADA Database | |
| Location | DET tool uses MQTT API through MATLAB Software. The DET tool will be installed in the control room, at the same machine as the SCADA database. The MQTT Server (Broker) is installed at CERTH/CPERI premises | 2 |
| Execution | The DET application is accessing the database using OPC protocol. The MQTT API transforms the data retrieved into JSON strings and publishes them to the Broker using the MQTT protocol. | 1 |
| Authentication | CA Certificate for MQTT Broker communications | 3 |
| Authorization | CA Certificate Key | 3 |
| User Access | Not needed. Ongoing user access update. | 1 |
| Security | TLS security for data transmission | 3 |

**Table 18. Xanthi pilot datasets and RKW assessment**

| Dataset | Confidentiality | Encryption | | Reuse | Database |
|---|---|---|---|---|---|
| Battery Data | RE | MQTT/TLS | 3 | 1 | API1 |
| Control Data | RE | MQTT/TLS | 3 | 1 | API1 |
| FC/ELEC Data | RE | MQTT/TLS | 3 | 1 | API1 |
| Forecasted Data | RE | MQTT/TLS | 3 | 1 | API1 |
| Hydrogen Storage | RE | MQTT/TLS | 3 | 1 | API1 |
| Load / Consumption Data | RE | MQTT/TLS | 3 | 1 | API1 |
| Load / Consumption Profiles | RE | MQTT/TLS | 3 | 1 | API1 |
| RES Data | RE | MQTT/TLS | 3 | 1 | API1 |
| RES Profile | RE | MQTT/TLS | 3 | 1 | API1 |
| Set Points | RE | MQTT/TLS | 3 | 1 | API1 |
| Weather Data | OP | MQTT/TLS | 3 | 1 | API1 |

Due to the particular requirements and tools used underneath the Xanthi pilot, they have opted for a tailored MQTT interface instead of a REST-based one. Besides, the use of CA certificates for authentication & authorization makes this pilot a rather different approach to the rest of the pilots analysed in this deliverable. Nonetheless, the overall evaluation dictates that the behaviour of both mechanisms are actually alike. Focusing on the recommendations, the handling of certificates leads to a lack of an explicit and automated user control-based on the resources/datasets (based on computational means), hence system operators must handle this physically.

## 4.9 Ploiesti

### *4.9.1 Introduction*

The Ploiesti Pilot is deployed on three ten-store apartment buildings. The sensing and metering devices include:

- A smart meter per flat.

### *4.9.2 Field layer integration*

The connection with the field layer devices is implemented through the Data Exchange Tool via a MQTT broker API. The tool communicates with the meters using MQTT over a wireless broadband (DSL or 3G) connection (see Figure 18).

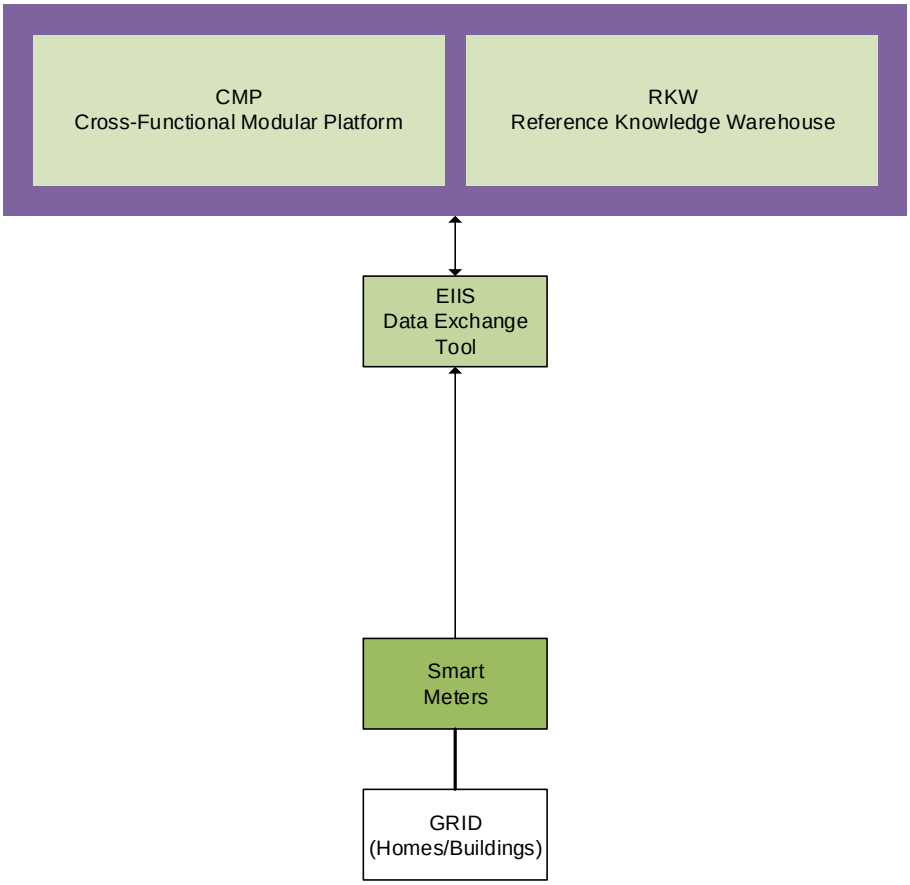


**Figure 18. Ploiesti pilot field layer architecture**

The communication architecture is widely used in similar deployment scenarios and for this reason verifiably scalable and secure. It is not clear yet if the sub-metering and other sensors will be installed later.

### *4.9.3 Data warehouse*

The Ploiesti Pilot has reported the following information on the RKW survey.

**Table 19. Ploiesti pilot RKW rank assessment per RKW item**

| Item | Description | Rank |
|---|---|---|
| Number of DBs/APIs | 1 | - |
| **API 1** | | |
| Access Technology | RESTful API | 3 |
| Persistence / DB | PostgreSQL | |
| Location | VM on pilot site or Amazon EC2 | 3 |
| Execution | Deployed as standalone and Docker container. | 2 |
| Authentication | Basic Authentication | 2 |
| Authorization | OAuth 2.0 | 3 |
| User Access | Role based only | 2 |
| Security | HTTPS | 2 |

**Table 20. Ploiesti pilot datasets and RKW assessment**

| Dataset | Confidentiality | Encryption | | Reuse | Database |
|---|---|---|---|---|---|
| Consumer Profile | RE | HTTPS | 3 | 1 | API1 |
| Consumption Prognosis | RE | HTTPS | 3 | 1 | API1 |
| Consumption Scenario Simulation | RE | HTTPS | 3 | 1 | API1 |
| DR Points | RE | HTTPS | 3 | 1 | API1 |
| Energy Consumption | OP | HTTPS | 3 | 1 | API1 |
| Energy Prices | OP | HTTPS | 3 | 1 | API1 |
| Energy Production | OP | HTTPS | 3 | 1 | API1 |
| Forecasted Data | RE | HTTPS | 3 | 1 | API1 |
| Indoors Data | RE | HTTPS | 3 | 1 | API1 |
| KPIs | RE | HTTPS | 3 | 1 | API1 |
| Load / Consumption Data | RE | HTTPS | 3 | 1 | API1 |
| Weather Data | OP | HTTPS | 3 | 1 | API1 |

The Ploiesti pilot is the one that best follows the given recommendations by implementing a RESTful API on a virtual machine on Amazon E2C, using OAuth 2.0 as Authorization method and HTTPS at the top of the API stack. To complement this, all the datasets are properly encrypted, thus leading to an extremely recommendable environment.

## 4.10 Thessaloniki

### *4.10.1 Introduction*

The Thessaloniki Pilot is deployed on residential and commercial buildings in city's metropolitan area. Three distinct scenarios are considered: residential buildings (with only metering), residential and commercial buildings (with metering and a BESS), and a commercial building (with metering, sub-metering, and sensing and control). The sensing and metering devices include:

- A smart meter on each residential and commercial buildings (first and second scenarios);
- A compact battery management system on some residential and commercial buildings (second scenario);
- Energy meters, HVAC IR control units, smart plugs and indoor environmental sensors (temperature and motion) on a commercial building (third scenario).

### *4.10.2 Field layer integration*

The connection with the field layer is realized through two central webservers via distinct REST APIs. Each webserver manages the connection with its particular gateways (data-loggers) using a proprietary protocol.

At each building an RF link is used to connect the smart meters with the gateway. Likewise the smart plugs and environmental sensors are connected to the gateway using a wireless ZigBee link. Furthermore, in the commercial building the HVAC IR control units are also connected to the gateway using a wireless Wi-Fi link while the energy meters are connected via wired Modbus-RTU. In all cases, the gateways use an Ethernet interface to access a broadband connection to the webservers.

Similarly, the connection with the business buildings devices is realized through a central web server via a REST API. The main difference is that ZigBee is used to connect a set of sensors to the gateway (see Figure 19).

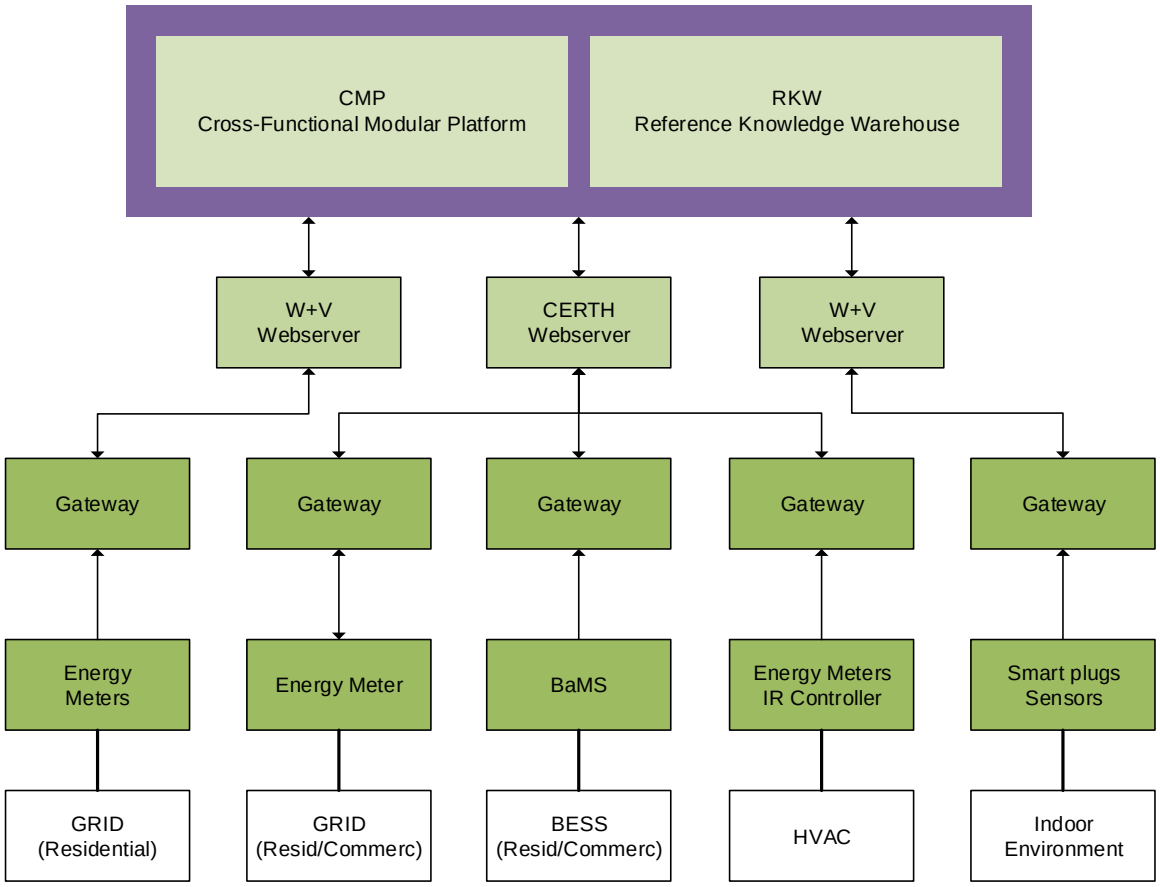


**Figure 19. Thessaloniki field layer architecture**

The communication architecture is a good example of how to integrate different subsystems, taking advantage of previously installed equipment. The resulting solution is somewhat heterogeneous but becoming ever more common. The use of wireless protocols for monitoring in existing buildings is also widely used due to the lower installation cost although it can in some situations impact the availability of the system. With a careful installation the solution is scalable, secure, and reliable.

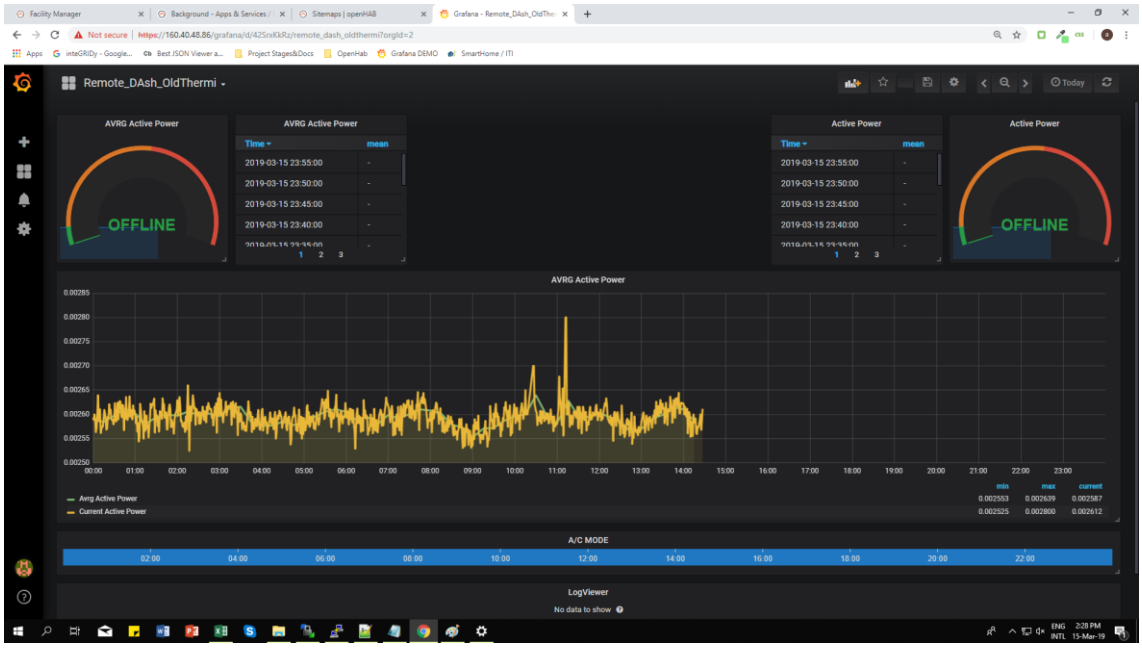


**Figure 20. Thessaloniki field layer data**

Figure 20 shows data collected from a testing installation of the HVAC power consumption. The other communication interfaces were also preliminarily tested.

### *4.10.3 Data warehouse*

The Thessaloniki pilot has reported the following information on the RKW survey.

**Table 21. Thessaloniki pilot RKW rank assessment per RKW item**

| Item | Description | Rank |
|---|---|---|
| Number of DBs/APIs | 3 | - |
| **API 1** | | |
| Access Technology | RESTful API | 3 |
| Persistence / DB | mongoDB+mySQL | |
| Location | Hosted Server | 2 |
| Execution | APACHE/mySQL | 1 |
| Authentication | Basic Authentication | 2 |
| Authorization | OAUth 2.0 | 3 |
| User Access | Role-based only | 2 |
| Security | proprietary | 3 |
| **API 2** | | |
| Access Technology | RESTful API | 3 |
| Persistence / DB | influxDB+rr4dj | |
| Location | Hosted Server on pilot site | 2 |
| Execution | Hosted Server | 2 |
| Authentication | influxDB Authentication+Basic Authentication | 2 |

| | | |
|---|---|---|
| Authorization | OAUth 2.0 | 3 |
| User Access | User-based only | 2 |
| Security | N/A | 1 |
| **API 3** | | |
| Access Technology | RESTful API + SSH | 3 |
| Persistence / DB | influxDB | |
| Location | Hosted Server+VM | 2 |
| Execution | N/A | 2 |
| Authentication | influxDB Authentication + RDP authentication | 2 |
| Authorization | OAUth 2.0 | 3 |
| User Access | User-based only | 2 |
| Security | N/A | 1 |

**Table 22. Thessaloniki pilot datasets and RKW assessment**

| Dataset | Confidentiality | Encryption | | Reuse | Database |
|---|---|---|---|---|---|
| BESS Dis-/Charge Schedules | RE | HTTPS | 3 | 2 | API2, API3 |
| Commercial User Measurements | RE | HTTPS | 3 | 2 | API2, API3 |
| Commercial User Profile | CO | HTTPS | 3 | 2 | API2, API3 |
| Demand Response Point System | RE | No | 2 | 1 | API3 |
| Demand Response Schedules | RE | HTTPS | 3 | 1 | API3 |
| Energy Prices | OP | No | 2 | 2 | API2, API3 |
| Facility/Residential Profile | CO | HTTPS | 3 | 2 | API2, API3 |
| Forecasted Data | OP | No | 2 | 1 | API3 |
| Residential User Measurements | RE | HTTPS | 3 | 2 | API1, API3 |
| User Data | CO | HTTPS | 3 | 2 | API1, API3 |
| Weather Data | OP | No | 2 | 1 | API3 |

This pilot is the most diverse when it comes to the usage of different technologies. Thus, we can say that the interoperability challenge overcame by Thessaloniki is worth mentioning given that 7 out of 11 of its datasets can be reused between tools. Moreover, it uses RESTful interfaces, pertinent authentication/authorization/user access methods, and the use of a time series database such as influxDB for time-based Datasets (e.g. Commercial User Measurements) makes it an excellent choice regarding performance. One of the action points that might be undertaken in this pilot is the encryption of all the confidential/restricted datasets, thus following one of the most critical recommendations.

# 5. Conclusions

## 5.1 Field layer integration and interconnection

The previous analysis of the field devices and protocols confirms that the proposed layered model for the communication architecture is a tool with the necessary flexibility and comprehensiveness. Table 23 summarizes the protocols used in each pilot and the following conclusions can be drawn:

- There is a general similarity between the various pilots in terms of protocols used which means that a certain number of solutions is gaining widespread acceptance;
- Some pilots still use proprietary protocols although not at the integration level;
- The REST API is the most frequent integration protocol provided.

**Table 23. Used communication protocols**

| Pilot | Device Level | Control Level | Integration Level |
|---|---|---|---|
| Isle of Wight | BACnet<br>CAN bus<br>Modbus-TCP\LAN | Proprietary\LAN<br>MQTT\WAN (VPN) | API\WAN |
| Terni | N/A | Proprietary (HTTP)\WAN | MQTT\WAN |
| San Severino | Modbus-RTU | Modbus-TCP\WAN | ODBC\LAN<br>API\WAN |
| Barcelona | Modbus-RTU<br>KNX | Modbus-TCP\LAN | API\WAN<br>OpenADR |
| St. Jean | Z-Wave<br>ZigBee | Proprietary\WAN | API\WAN |
| Nicosia | Modbus-RTU<br>Modbus-TCP\LAN | Modbus-TCP\LAN<br>Proprietary\LAN<br>Proprietary\WAN | API\WAN |
| Lisbon | Modbus-RTU | Proprietary\WAN | API\WAN |
| Xanthi | Proprietary\Serial<br>CAN bus<br>Modbus-TCP\LAN | OPC\LAN | MQTT\WAN |
| Ploiesti | N/A | Proprietary\WAN | MQTT\WAN |
| Thessaloniki | Modbus-RTU<br>Proprietary\RF<br>ZigBee | Proprietary\WAN | API\WAN |

The overall conclusion from the information collected is that the field layer heterogeneity is hidden at the integration level by the use of a standard mechanism which is in agreement with the general inteGRIDy Framework. Another overall conclusion is that all the pilots deploy well known and widespread communication architectures for specific types of applications which means that they have proven to be reliable and secure.

## 5.2 RKW

The analysis of the RKW guideline implementation shows that each and every pilot is currently enforcing at least the minimum requirements, which will make them able to:

- Be interoperable with any other inteGRIDy-based tool at framework level;
- Secure and protect all stored data, depending on the confidentiality policy;
- Smooth the potential integration of new tools or replication in other projects.

The overall benchmarking of inteGRIDy solutions with respect to the RKW is shown in the figures below.

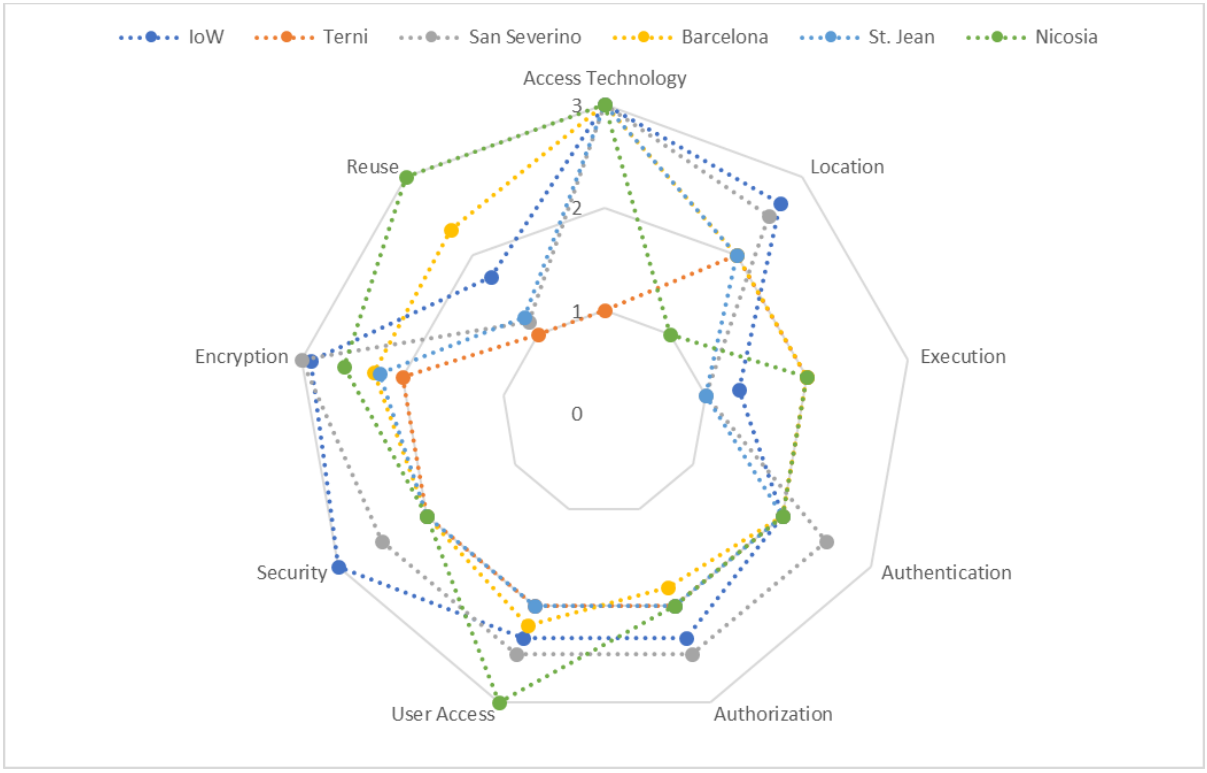


**Figure 21. Large scale pilot RKW assessment**

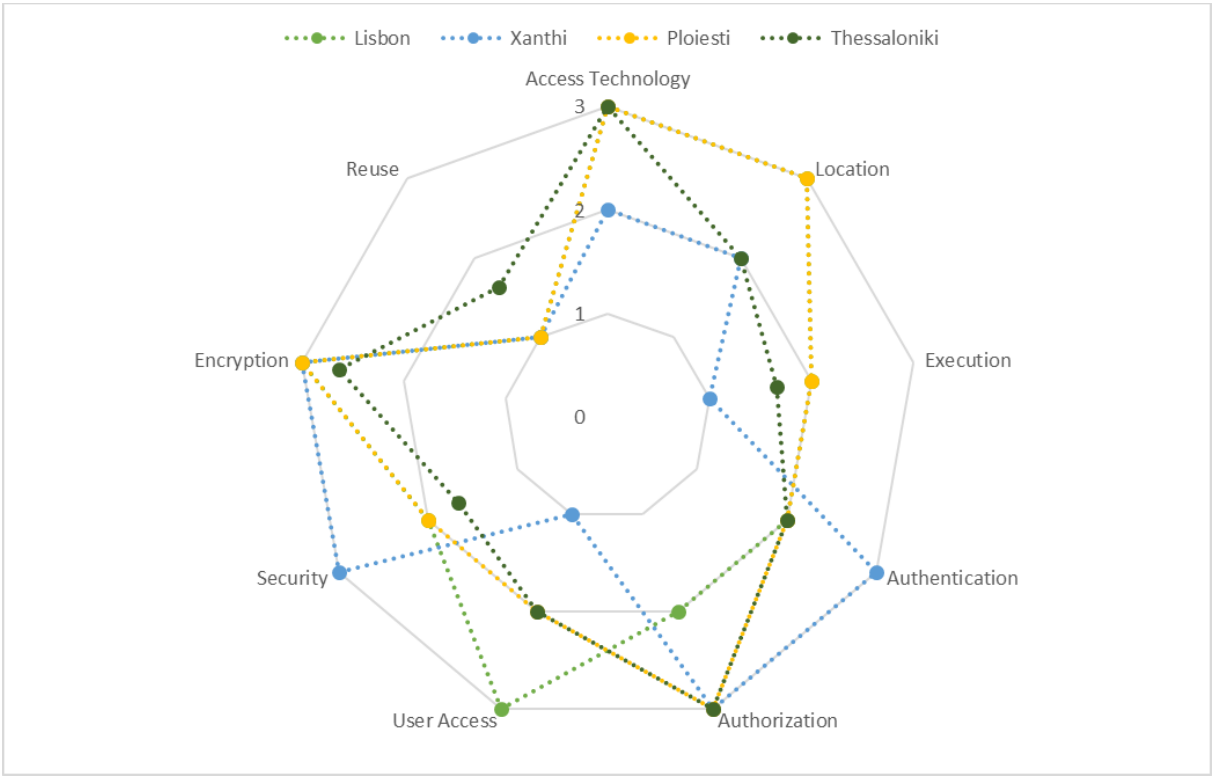


**Figure 22. Small scale pilot RKW assessment**

As shown in the figures above, we can conclude that most of the pilots follow a REST philosophy for their interfaces. Concerning the two pilots that do not use a RESTful API, we understand that their choices are more comfortable for internal use and that those APIs are not planned to be open to external networks.

With respect to the location of the services, note that there is an inclination to the use of privately-owned servers, though there are some pilots that trust in IaaS solutions to host their services. However, we understand that for most of the cases, the actual owners of the data (e.g. Distribution Service Operator) may have imposed restrictions due to internal policies.

Regarding the deployment strategies, we observed that most of the pilots use the classic deployment paradigm by executing their solutions natively. Nonetheless, it is worth mentioning that some of the pilots started using containerization (Docker) for a rapid, more compatible deployment.

Concerning the security realm, all the pilots provide an adequate level of security to access their data either using the recommended schemes or other alternatives (VPN, servers with administrator-only-access, etc.) that, for practical purposes, provide a similar functionality. Moreover, all the pilots follow the recommendations regarding encryption of their confidential data and, is worth mentioning, some of them use encrypted communication by default even in their non-confidential data. This demonstrate the simplicity to stablish an additional protection level on the data.

Regarding the reuse metric, we value the predisposition on behalf of the pilots with more than one tool to use their datasets in a transversal way.

Although we did not rank the persistence technology used, one can also note a predominance in the use of relational databases for persistence strategies. However, it has not escaped our note that some pilots use interesting alternatives like Cassandra or MongoDB for a more efficient management of massive amounts of data.

In addition, a number of technologies and standards are used in inteGRIDy pilots. This gives an overview of the diversity and heterogeneity of proposed scenarios. With this diversity in mind, the proven interoperability corroborates itself to be an even more outstanding achievement of the project.

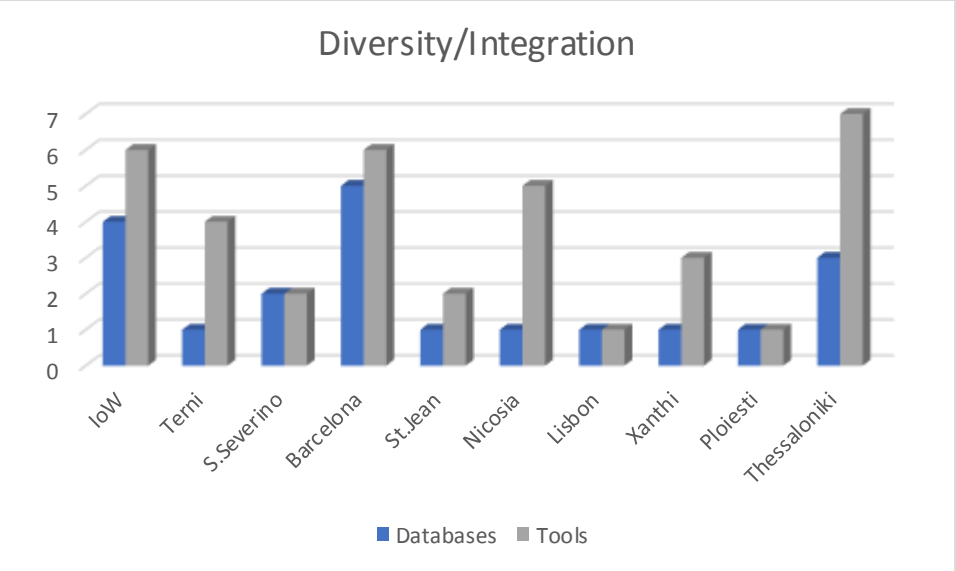


**Figure 23. Database/Number of tools per pilot relationship**


**Figure 24. Data base technologies (top) and hosting services (bottom) used.**

The implementation of inteGRIDy compliant RKW structures has proven to be a very effective way to pave the way for the integration process.

# 6.References

[COR02] S. Corrigan - Introduction to the Controller Area Network (CAN). Accessed Mar-2018. http://www.rpi.edu/dept/ecse/mps/sloa101.pdf

[DAG14] R. Dagher - ZigBee and IEEE 802.15.4. A (tiny) introduction. Accessed Mar-2018. https://team.inria.fr/fun/files/2014/04/fun-Seminar-intro-zigbee.pdf

[IEC50] International Electrotechnical Commission. Power Utility Automation (IEC 61850). Accessed Sept-2017. https://webstore.iec.ch/publication/6028

[IEE30] IEEE 2030.5-2018 Standard for Smart Energy Profile Application Protocol. Accessed Aug-2018. https://standards.ieee.org/findstds/standard/2030.5-2018.html

[IND13] inteGRIDy project D1.3 “Pilot Sites Surveys, Use Case Requirements & Business Scenarios” August 2017. http://www.integridy.eu/sites/default/files/integridy/public/content-files/deliverables/inteGRIDy_D1.3_Pilot_Surveys_requirements_%20business_scenarios_v1.0.pdf

[IND15] inteGRIDy project D1.5 “inteGRIDy Architecture and Functional/Technical Specifications” December 2017. http://www.integridy.eu/sites/default/files/integridy/public/content-files/deliverables/inteGRIDy_D1.5_Architecture_Functional_Technical_Specificationsv1.0.pdf

[IND16] inteGRIDy project D1.6 “inteGRIDy Architecture and Functional/Technical Specifications (Updated)” December 2018. http://www.integridy.eu/sites/default/files/integridy/public/content-files/deliverables/inteGRIDy_D1.6_Architecture_Functional_Technical_Specifications_update_v1.0.pdf

[INF18] Infosys. Best Practices for Building RESTFul Web Services. 2018. Accessed Nov-2018. https://www.infosys.com/digital/insights/Documents/restful-web-services.pdf

[KAB16] Y. Kabalci – A survey on smart metering and smart grid communication. Renewable and Sustainable Energy Reviews, 57, 2016.

[KHA12] R. Khan, S. Khan, R. Zaheer & S. Khan - Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, 10th International Conference on Frontiers of Information Technology, 2012.

[KUZ14] M. kuzlu, M. Pipattanasomporn & S. Rahman - Communication network requirements for major smart grid applications in HAN, NAN and WAN. Computer Networks, 67, 74-88, 2014.

[MQT14] Message Queuing Telemetry Transport. Accessed on Aug-2018. http://mqtt.org/

[NEW15] M. Newman - BACnet Celebrates 20 Years. Accessed Mar-2018. http://www.bacnet.org/Bibliography/HMN-2015-06.pdf

[OAD17] Open Automated Demand Response (OpenADR). Accessed Sep-2017. http://www.openadr.org

[OPC17] Open Platform Communications (OPC), Classic Specification. Accessed Sep-2017. https://opcfoundation.org/about/opc-technologies/opc-classic/

[SAL17] Y. Saleem, N. Crespi, M. Rehmani & R. Copeland - Internet of things-aided Smart Grid: technologies, architectures, applications, prototypes, and future research directions. arXiv:1704.08977, 2017.

[THO08] G. Thomas – Introduction to the Modbus Protocol. Accessed Mar-2018. https://ccontrols.com/pdf/Extv9n4.pdf

[ZHU12] Z. Zhu, S. Lambotharan, W. Hau & Z. Fan – Overview of Demand Management in Smart Grid and Enabling Wireless Communication Technologies. IEEE Wireless Communications, 19, 3, 2012.

[ZWA19] About Z-Wave Technology. Accessed Mar-2019. https://z-wavealliance.org/about_z-wave_technology

http://www.integridy.eu