**FP7 Grant Agreement N° 607109**

***S*ecurity for smart *E*lectricity *GRID*s**

# D1.1 Architecture and design for use cases

Due date of deliverable: 31/03/2015
Actual submission date: 01/10/2016
Work package: WP1 Use Cases and Security Goals
Number of pages: 77
Revision: Version 1.2
Classification level: Public

| | |
|---|---|
| Project type: | Collaborative project – small or medium scale focused research project |
| Thematic Priority: | FP7-SEC-2013-1 |
| Start date of project: | October 1st, 2014 |
| Duration: | 36 months |

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 607109

# Management summary

This deliverable describes the selection of some highly relevant representative use cases with regard to the Smart Grid concept for further use in the SEGRID context. These use cases highlight relevant scenarios and functionalities to be developed within the emerging Smart Grids while taking full potential of the installation of the Smart Grid components in the customer premises, and in the primary and secondary substations.

First, a state-of-the-art analysis is performed. An overview on the Smart Grid architecture and representative use cases addressed in different European initiatives and projects is provided. The related work study focuses on adopted use cases in similar security related projects and on outcomes of the work done by international standard development organisations and other national and international research & development projects.

The five selected SEGRID use cases are outlined by providing a short description, identifying the actors, the stakeholders, the information flows as well as the assumptions and pre-conditions for the specific use case. From that, the use case requirements are derived for each specific use case with the aim to ensure that the basic properties and objectives of the use cases are not jeopardised throughout the SEGRID project research and development.

The SEGRID use cases are key to facilitate a thorough analysis of their potential cybersecurity and privacy vulnerabilities and to investigate and develop mitigation strategies. The use case descriptions will serve as a base for the demonstration of the vulnerabilities and their potential impact for the different stakeholders involved, if exploited, but also facilitate the implementation of the SEGRID test environment – the SITE.

# TABLE OF CONTENTS

1 INTRODUCTION ..... 4
1.1 The SEGRID project objectives ..... 4
1.2 Work Package 1 – Use Cases and Security Goals ..... 5
1.3 Deliverable D1.1 – Architecture and design for use cases ..... 5
1.4 The structure of Deliverable D1.1 ..... 6
2 RELATED WORK ..... 8
2.1 Smart Grid Information Security (SGIS) ..... 8
*2.1.1 Introduction ..... 8*
*2.1.2 Key elements of SGIS ..... 8*
*2.1.3 A historical approach: the SGIS toolbox ..... 9*
*2.1.4 The SGIS framework (former SGIS toolbox) ..... 10*
*2.1.5 Relevant base standards ..... 11*
2.2 Other initiatives ..... 11
*2.2.1 Europe ..... 11*
*2.2.2 United States ..... 16*
*2.2.3 Other national and international bodies ..... 18*
2.3 Security initiatives regarding Smart Metering ..... 20
3 SEGRID ARCHITECTURE ..... 21
3.1 Smart Grid Architecture Model ..... 21
3.2 Functional Architecture ..... 24
3.3 Component Architecture ..... 32
*3.3.1 Supervision and Control Systems for Electricity Distribution ..... 32*
*3.3.2 Smart metering ..... 35*
4 STAKEHOLDERS ..... 38
5 USE CASES ..... 39
5.1 Smart meter used for on-line reading of consumption and technical data ..... 39
5.2 Load balancing renewable energy centrally ..... 46
5.3 Dynamic power management for smart homes, smart offices, electric vehicles ..... 52
5.4 Load balancing renewable energy regionally (substation automation) ..... 59
5.5 Automatic reconfiguration of the power grid ..... 65
6 GLOSSARY ..... 73
7 REFERENCES ..... 75



**Classification level: Public**

# 1 Introduction

This section introduces the SEGRID project and defines the goals of this deliverable as well as explains the context for the use cases in this document.

## 1.1 The SEGRID project objectives

SEGRID's main objective is to enhance the protection of Smart Grids against cyber-attacks. In a Smart Grid, it is not sufficient to consider all the different components separately; they will together form a truly integrated system-of-systems. The Smart Grid will neither be completely owned, nor completely controlled, by a single power system operator. There will be many Smart Grid services and components that are operated by other organisations, such as public telecom networks and third party-delivered (outsourced) application services. There will potentially be many new methods for connecting with various Smart Grid applications using a diverse set of communication channels, such as local connection interfaces, distributed web access, and smart apps on smart phones.

This new utility-wide system (-of-systems) will not come into existence overnight. Therefore, the Smart Grid will be composed of a mix of old, even legacy, and new components. This is why we introduce the concept of a gradually evolving system in which new functionalities are added to accommodate new use cases with the challenge to maintain security, privacy and dependability of the Smart Grid as a whole.

We have selected five use cases that clearly demonstrate this gradual evolving system concept. The SEGRID use cases have been selected based on the work already done by ENISA along with the working parties involved in the EC Mandates M/441 [9] and M/490 [10] as well as based on the work and competence of the project partners.

The rationale for the five SEGRID use cases is based on:

- Relevance for new business, economic growth, and supporting the introduction of more sustainable and locally generated power;
- Addition of new functionality and components that inherently will introduce new vulnerabilities and a wider cyber-attack surface.

The five SEGRID use cases are:

1. Smart meter used for on-line reading of consumption and technical data;
2. Load balancing renewable energy centrally;
3. Dynamic power management for smart homes, smart offices, and electric vehicles;
4. Load balancing renewable energy regionally (substation automation);
5. Automatic reconfiguration of the power grid.



**Classification level: Public**

We believe that the SEGRID use cases reflect important steps of Smart Grid developments until 2020 and beyond (see the SEGRID storyline Figure 1). Moreover, the SEGRID use cases will cover the most relevant security and privacy issues that will arise from the increasing complexity of Smart Grids.

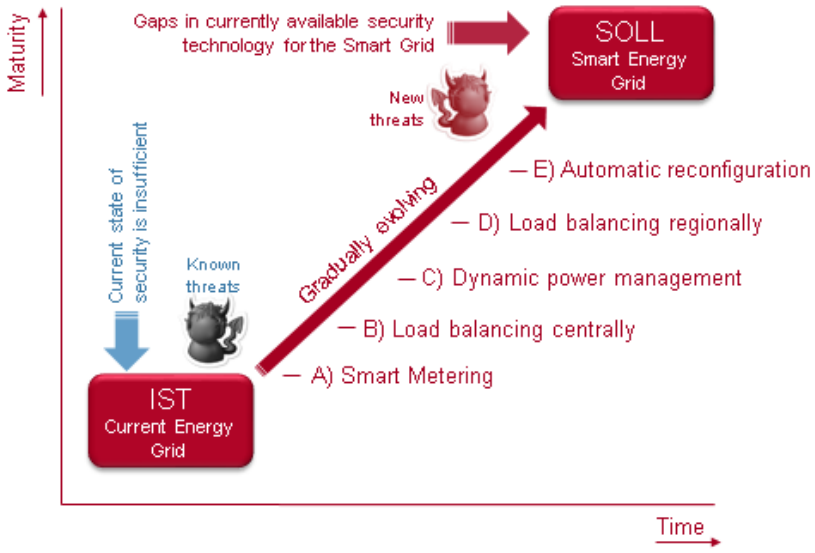


**Figure 1: SEGRID storyline**

## 1.2 Work Package 1 – Use Cases and Security Goals

Work Package 1 is a key building block for the SEGRID project, setting the basis for all activities within SEGRID.

The Work Package 1 main objectives are:

- Elaborate on the SEGRID reference architecture and describe the five use cases.
- Establish the security & privacy (S&P) goals for each of the SEGRID use cases.
- Identify points of improvement with respect to Smart Grid security and privacy in policies and regulations related to the identified SEGRID use cases.
- Assess the cost of implementing security and privacy protection technologies that are developed in WP4 for each of the Smart Grids use cases.

## 1.3 Deliverable D1.1 – Architecture and design for use cases

Deliverable D1.1 provides the detailed specification of the SEGRID Smart Grid architecture and the specific requirements for the different use cases to be analysed in the SEGRID project. D1.1 is an outcome of Task T1.1.



**Classification level: Public**

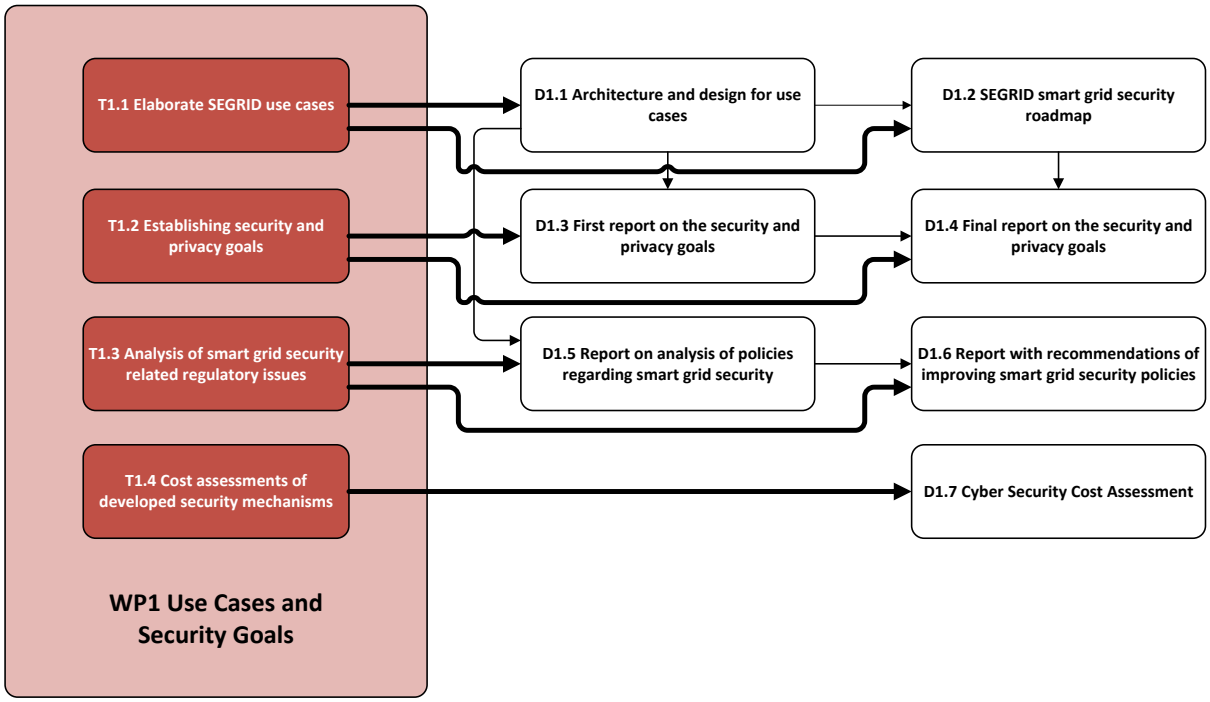


**Figure 2 - Dependencies in WP1**

D1.1's outcome relates to both D1.2 and D1.3 as shown in the task and deliverables dependency graph in Figure 2.

## 1.4 The structure of Deliverable D1.1

The deliverable is structured in four main sections. It starts by performing a survey about the state of the art and related work concerning the Smart Grid use cases and its cybersecurity, providing a general overview of the work of standardisation bodies and national and international research and development projects in this domain. Then, it defines the SEGRID Smart Grid architecture, the main stakeholders involved and last, it addresses the five SEGRID use cases. In this deliverable we provide a brief use case description, followed by the identification of the involved actors, the identification of events and the flow that defines the behaviour in the use case.

Finally, it addresses the different requirements associated and imposed by each use case and point out the stakeholders involved.

Section 2 provides an overview on representative use cases addressed in other Smart Grid environments. The related work study focuses on adopted use cases in similar security related projects and on outcomes of the work done by international standard development organisations and other research & development projects in this domain.



**Classification level: Public**

Then, Section 3 describes the different SEGRID use cases by providing a short description, identifying the actors and the information flow, and finally the assumptions and pre-conditions for each of the use case.

Further, in Section 4 the use cases are specified, to ensure a solid basis for further research and development in the SEGRID project.

Finally, Section 5 describes the stakeholders in each of the use cases and provides further information about the different actors involved.



**Classification level: Public**

# 2 Related Work

In this section, the main initiatives regarding Information Security will be outlined. Also, it will include brief references of Smart Grid security implementations throughout Europe and other non-European countries, pointing out the current state of the art. This introduction is not intended to be exhaustive. The information about these methodologies and practical implementations could be completed in more detail following the corresponding references.

## 2.1 Smart Grid Information Security (SGIS)

### 2.1.1 Introduction

ISO/IEC 27002:2013 standard provides a definition of Information Security, which constitutes the protection of information from a wide range of threats in order to ensure business continuity, reduces business risks, and maximizes return of investments and business opportunities.

In particular, the Smart Grid Information Security (SGIS) activity refers to the technical and organizational needs for sustainable SGIS, as well as data protection and privacy (DPP), enabling the collection, collection, utilisation, processing, storage, transmission and erasure of all information to be protected for all participating players (as set out by the M/490 mandate.

There are three key elements to be considered and addressed by SGIS requirements, which are Confidentiality, Integrity and Availability. But the importance does not lie only in these elements by themselves; there are key concerns about the relative weight of each element and the prioritization rules between them, aspects that depend on the required security services for a given context. The essential security requirements may vary depending on the roles or activities performed by a given stakeholder in the Smart Grid value chain.

### 2.1.2 Key elements of SGIS

SGIS is composed by a number of main elements which are set out in the following subsections.

#### 2.1.2.1 Smart Grid Architecture Model (SGAM)

The SGAM is a high level conceptual model of the Smart Grid developed by the M/490 Reference Architecture WG, which describes the main agents in the Smart Grid and their interactions. The SGAM consists of five layers which represent business objectives and processes (SGAM-B, which includes uses cases describing several business needs), functions (SGAM-F, which includes use cases and logical functions which are platform-independent), information models (SGAM-I, which represents the data structures and objects which are needed to perform the specified functions, and are exchanged through the communication infrastructure), communication protocols (SGAM-C, which references the communication protocols for the exchange of information and commands between components), and components (again, SGAM-C, which represents the devices themselves). Each layer includes the Smart Grid plane, a 2-dimensional representation composed by Smart Grid domains of actions (Power Generation, Transmission, Distribution, Distributed Electrical Resources (DER) and end customer premises) and zones (hierarchical system aspect of each domain:



Classification level: Public

Process, Field, Station, Operation, Enterprise and Market). More detailed information about the SGAM and its application for SEGRID can be found in Section 3.

#### 2.1.2.2 SGIS Security Levels (SGIS-SL)

SGIS-SL defines five different security levels associated with different European grid stability scenarios. These levels have been defined from a global European perspective, and the disruption scenarios involve assets and power losses whose impact can be measured and put in relation with the overall European generation and installed capacity. The security levels start on level 1 (low), which implies a power loss under 1 MW, affecting a town or a neighbourhood; level 2 (medium), which implies a power loss from 1 MW to 100 MW, affecting a region or a town; level 3 (high), which implies a power loss from 100 MW to 1 GW, affecting a region or even a country; level 4 (critical), which implies a power loss from 1 GW to 10 GW, affecting a country and with a considerable impact at European level; and level 5 (highly critical), which implies a power loss above 10 GW and therefore it is considered as a severe pan-European incident. Several security measurements can be established for each Security Level. NISTIR 7628 provides security guidelines which address these measurement criteria.

#### 2.1.2.3 Smart Grid Data Protection Classes (SG-DPC)

The SG-DPC is a set of recommended classifications for information data models, which are exchanged by entities performing several Smart Grid Services throughout the complete domain/zone Smart Grid model. There are 2 different sets of information which need to be classified depending on their protection needs: these are personal data and other system information. The SG-DPC includes information on associated SGIS-SL for each use case and concerned agent. The information may need protection so as to preserve confidentiality, availability and integrity; to assure authenticity, accountability and non-repudiation; and to guarantee reliability.

### 2.1.3 A historical approach: the SGIS toolbox

The first approach to the SGIS toolbox was the way to integrate security in the general Smart Grid use case analysis framework. The main goal was to provide stakeholders a way to identify the security needs for concerned use cases.

The use of the SGIS toolbox was described in the following steps:

- First, the use cases ought to be collected and classified by domain and zone of application.
- Analysis of identified use cases so as to identify data, owners and agents.
- Determination of the SGIS risk impact levels for every data set.
- Identification of components which are intended to support the data set. These components ought to be grouped in term of likelihood.
- Determination of the SIGS security level for every data set after execution the corresponding risk analysis.
- Selection of the corresponding security standards in order to protect each data set depending on its security level.



Classification level: Public

- Establishment of the final set of security controls that had to be deployed to cope with the identified risks. This ought to be done in accordance with the security level, domain and zone.

These steps could be executed on a periodical basis in order to refine the use cases. The identification of new use cases, or the need to update security criteria could eventually drive to execute a new iteration of this process.

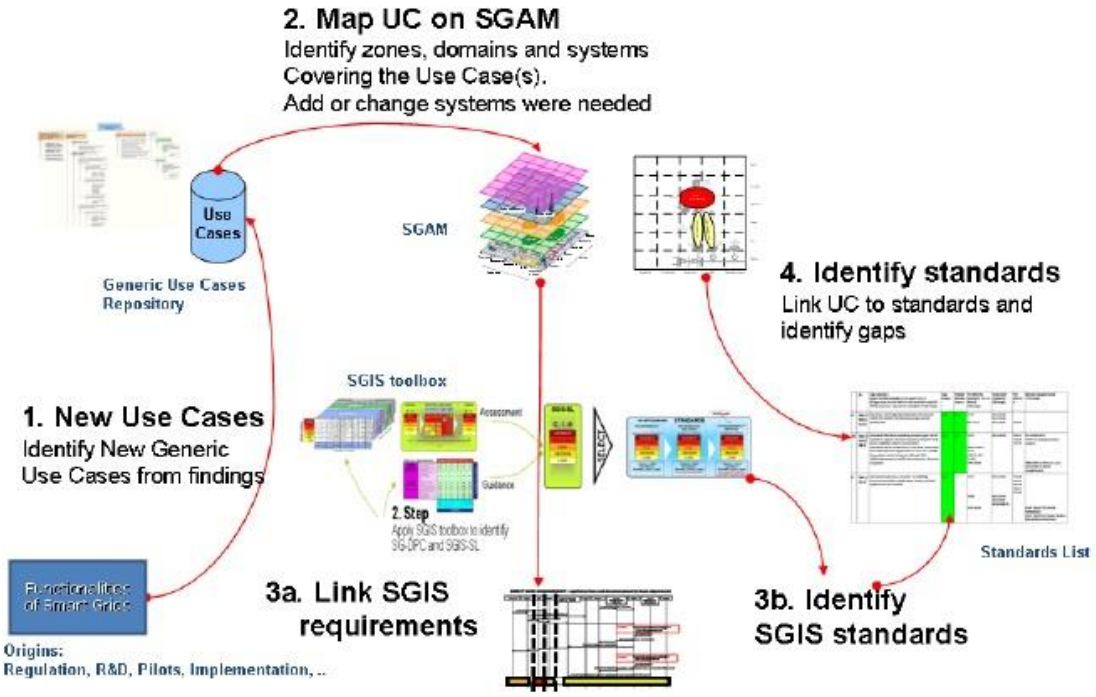


**Figure 3: SGIS toolbox overview**

### 2.1.4 The SGIS framework (former SGIS toolbox)

There is an update to the SGIS toolbox, an improved approach which puts the focus on the need for performing risk analysis, better than simply having a general framework for risk analysis. The SGIS toolbox has been redefined and renamed to avoid giving the feeling that it was a kind of tool or, in other words, a set of elements that anyone could use much like application programs, including calculated measures to mitigate threats and risks. The new approach changes the SGIS toolbox into a methodology to raise awareness of top management and decision makers. There's a clear need for managers to have a good view of the business, operational and technical risk and consequences prior to making decisions. The new steps that have been developed for this new approach are listed hereunder:

- Preliminary assessment: definition of scope, involving security experts and use case owners, and separate treatment of personal data if the use case in question includes them. In general terms, personal data protection is considered separately because an identical approach to security cannot be applied for data privacy.



Classification level: Public

- SGAM mapping: the use case must be evaluated and mapped to the general SGAM. Starting from this, associated SGIS-SL can be identified and used as reference.
- Threats mapping to the use case assets: threats must be identified, as well as vulnerabilities and risk factors as a first step prior to their comparison with the ENISA threat catalogue. The classification may take into account traditional risk analysis practices (the organisation doesn't need to change its approach in this sense; it only needs to take this guide into account), and includes: identification of most critical threats as well as critical and not-critical assets, taking advantage of the expertise acquired by the organisation regarding security.
- Definition of a risk mitigation plan: An identification of measures for mitigation must be performed, and then linked to the identified risk.
- Definition of traceability: The link established between the defined risk and a specific mitigation measure, performed in the stage above, must be justified. Documentation of all steps taken between identified risk factors and their corresponding mitigation measures must be complete and accurate, including personal interviews to document who each involved individual is and his or her role in the organisation, and subsequently, the use of an automated risk analysis system, which should include the capability of generating tracking or logging reports.
- Definition of a mitigation plan: Here, a comparison between incident costs and costs of mitigation measures must be performed.
- Definition of an action plan: the list of actions to be taken, with information on priority and budget for each one. This is the point in which ENISA and Data Protection Impact Assessment (DPIA) security recommendations, obtained in the aforementioned step 3, should be added.

### 2.1.5 Relevant base standards

There are several Smart Grid information security standards which constitute the basis of the investigation and developments regarding SGIS and associated elements. These are the main referenced standards are the following:

- ISO/IEC 27001.
- ISO/IEC 27002.
- IEC 62351.
- NERC CIP.
- NISTIR 7628.

## 2.2 Other initiatives

### 2.2.1 Europe

#### 2.2.1.1 ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the European Union, its Member States (MS), European citizens and private sector. ENISA develops recommendations on good practices regarding information security, and works in conjunction with those agents. ENISA also collaborates and provides assistance to concerned parties to implement EU legislation on this matter, and works to improve the resilience of EU's critical information infrastructure and networks.



Classification level: Public

ENISA has delivered a number of general recommendations addressed to the European Commission (EC), the MS and private and public stakeholders (including educational and R&D), all of them involved in the definition and implementation of Smart Grids and, in particular, their cybersecurity aspects. Main recommendations are the following:

- Concerned authorities from the EC and the MS should make the necessary efforts to improve the regulatory and policy framework on Smart Grid cybersecurity, at national and EU levels.
- The EC, along with ENISA and the MS, should enforce the creation of a Public-Private Partnership (PPP) to coordinate Smart Grid cybersecurity activities.
- ENISA and the EC should promote awareness raising and training initiatives, as well as dissemination activities.
- The EC, along with ENISA, the MS and the private sector, should implement a set of security measures based on existing standards and guidelines.
- The EC and the MS should work on the development of security certification schemes for Smart Grid hardware, software and concerned organizations, as well as the creation of necessary test environments and security assessments.
- Trying to avoid large scale severe pan-European cybersecurity incidents in power grids, the EC and the MS, with ENISA collaboration, should refine strategies addressed to coordinate necessary measures.
- The EC and the MS should cooperate with the R&D sector regarding further research in Smart Grid cybersecurity.

ENISA has developed several technical guidelines and other documents covering different aspects of Smart Grid cybersecurity, with corresponding links to current international standards on the matter:

- Guidelines on incident reporting.
- Resilience metrics.
- Guidelines on security measures.
- Guidelines for auditing security measures.
- Methodologies for the identification of critical information infrastructure assets and services.
- Analysis and implementation of National Cyber Security Strategies (NCSS), with the corresponding evaluation framework.
- Risk management and assessment, including inventories to existing methods and good practices.
- Confidentiality and privacy concerns.

#### 2.2.1.2 CEN/CENELEC/ETSI JWG and SGCG

The CEN/CENELEC/ETSI Joint Working Group was established as a way to avoid inconsistencies arising from the independent work of several standardisation bodies. The result of this JWG has been the development of new standards and the improvement of former ones, so as to establish detailed recommendations to selected standardisation bodies.

The M/490 mandate requested ESOs to develop a framework to aid ESOs to continuously enhance standards regarding Smart Grids. The CEN/CENELEC/ETSI Smart Grids Coordination Group (SGCG) is the response to M/490. The SGCG includes four WGs, which

are in charge of the reference architecture, the standards and processes, and security. The latter matter is the main subject of the Smart Grid Information Security WG (SGIS WG, whose main outcomes – the SGIS technical and organisational characteristics, structure and framework- have been briefly described at the beginning of this section 2).
The CEN/CENELEC/ETSI JWG final report on standards for Smart Grids includes recommendations for standardisation regarding information security.
The SGIS WG defines several security requirements for Smart Grids based on integrity, confidentiality, availability, reliability, privacy and interoperability criteria. Different security levels have been established to classify the concerned infrastructures. Reviewing of current European regulations and standards, as well as the definition of a set of tools and methodologies to classify assets and assess risk factors are also under the scope of this WG.
The CEN/CENELEC/ETSI Smart Meters Coordination Group (SMCG) is the answer to the Mandate M/441, which provides a specific focus on smart metering standardisation issues. The result of the activities carried out by SMCG is a functional reference architecture for communications relevant for smart metering systems. This addresses privacy and data security issues, all related specifically to smart meters.

#### 2.2.1.3 DG CONNECT

The EC created this Ad-hoc Expert Group to gain a major degree of understanding the objectives of the private and public sectors on the ICT security and resilience challenges for the Smart Grids. Communications on Critical Information Infrastructure Protection (CIIP) and Smart Grids constitute the basis for this initiative. This group has two main objectives: the identification of priority areas for which actions addressing security and resilience of communication networks and information systems must be taken first, and the identification of strategic security requirements, good practices and the proposal of means to make decision makers aware.
A work plan was defined to improve the cybersecurity of the Smart Grids. It focuses on the security and resilience of communication and information systems that are critical for the performance of the electricity infrastructure, and it is divided into main four main areas: treatment of risks, threats and vulnerabilities; identification of requirements and research on technologies; knowledge sharing; and awareness and training.

#### 2.2.1.4 SGTF

The Smart Grid Task Force (SGTF) is a public body set up by the EC to ease EU's concurrent Smart Grid implementation. It takes into account worldwide experiences, and integrates regulatory, technological and commercial vision on Smart Grids. The final goal of the SGTF is to produce a set of regulatory recommendations to ensure that the implementation of Smart Grids across the EU is consistent and cost-effective, and fulfils the network users' needs. The efforts are focused on the functionalities of smart meters, recommendations regarding data protection, and recommendations regarding roles and responsibilities of different parties involved in the Smart Grid development. There are four expert groups. EG2 is the expert group in charge of producing regulatory recommendations for data safety, handling and protection. Its main objectives are: identifying benefits and concerns of customers in relation with Smart Grids, as well as possible risk factors when managing data, ownership of data and access rights, and responsible agents for data protection and enforcement measures; providing an overview on European legislation on these matters; recommending the assumption of new



Classification level: Public

protective measures if necessary; and developing a framework in which way data can be managed.

#### 2.2.1.5 EU-US WG on cybersecurity and cybercrime

The EU-US Working Group on cybersecurity and cybercrime is devoted to cope with the new threats that arise and constitute a menace to the global networks. Its activities include: cooperation for incrementing incident management response capabilities, sharing good practices with industry, securing industrial control systems and Smart Grids and enhancing the resilience and stability of the networks.
Regarding Smart Grid security aspects, there are inputs coming from both US and EU sides of the collaborative organization: activities at European and MS levels, performing ENISA studies on industrial control systems, and activities regarding security and resilience of communication networks and information systems for Smart Grids, with DG CONNECT coordination, experiences in collaboration and coordination to acceptance of security standards, etc. The result of this collaboration is a strategy for EU and US public and private engagement on cybersecurity of industrial control systems and Smart Grids.

#### 2.2.1.6 European Network for Cyber Security (ENCS)

ENCS is an independent European not-for-profit organization. Its founding members are Alliander, City of The Hague, CPNI.NL, KEMA, KPN, Radboud University Nijmegen and TNO. ENCS forms a network between critical infrastructure owners, academia and standardization and working groups. It contributes to the task of cyber security for critical infrastructures by dedicated security research that forms a basis for security consulting, testing, education and training, and information and knowledge sharing. ENCS helps critical infrastructure owners to make accurate risk assessments and to take the adequate measures to ensure the continuity of systems operation.

#### 2.2.1.7 ESMIG

The European Smart Metering Industry Group (ESMIG) provides expertise and advice to European institutions and other organizations on key issues for the implementation of Smart Grid technologies across the EU.
ESMIG works with the SMCG in the definition of a functional reference architecture of advanced metering infrastructure (AMI), and the definition of functional requirements by use cases, which includes cybersecurity considerations. It is also working with the SGCG.

#### 2.2.1.8 PRIME Alliance

The PRIME Alliance is an organization responsible for the creation of an open, narrowband PLC communication protocol specification for Smart Grid devices, with special focus on interoperability and compatibility with open standards. The protocol includes several security profiles, which provide authentication, encryption, privacy and data integrity to upper layers (these security features are performed at MAC layer, and different security settings can be selected, depending on the scenario and the balance between required security and performance).



Classification level: Public

#### 2.2.1.9 DLMS UA

The DLMS User Association is a non-profit organization whose main goal is to develop, promote and maintain the DLMS/COSEM specification. The DLMS UA provides means to test compliance with the specification, standardization bodies and a forum for developers and system providers to gain knowledge about the DLMS/COSEM specification. It also provides a certification scheme for devices implementing the specification. The DLMS UA is linked with IEC TC 13 WG 14.
The DLMS/COSEM specification contains several sections dedicated to security (authentication, cryptography), privacy and non-repudiation for electrical, gas, water and heat metering communications.

#### 2.2.1.10 DECC

In the UK, the initiative to incorporate Smart Grid security to its network has been taken by the UK government, represented by the Department for Energy and Climate Change (DECC). The need to deploy new brand smart meters and to address all the security problems that arise when customers' personal data, consumption patterns, billing information and remote command deliveries led to the intensive application of a complete range of security features, involving the selected communication protocols (DLMS and Zigbee), the necessary Public Key Infrastructures (PKI) to manage cryptographic material at all levels and the Head End System, which is the entry point for all concerned partners to exchange data with the Smart Meters. Several organizations are involved in the work of turning security of Smart Grids into a reality: DCC, CESG, BEAMA, suppliers and end users associations, providers of communication infrastructure, etc. The complexity of the UK energy environment has had a considerable impact on the specifications of the system (not only for security issues), which are under revision and final refinement at the time of writing this document. Initial live operations are planned for late 2016, and final deployment is planned to be completed by 2020.

DECC is divided into several expert groups and task forces: perhaps the most relevant on the field of cybersecurity is the STEG (Smart Meter Design Security Technical Experts Group), which includes a wide range of Smart Grid agents, like energy suppliers, trade associations, governmental instances (CESG), technical security specialists, meter manufacturers, system integrators and telecommunications providers.

#### 2.2.1.11 DIN

DIN is the German Institute for Standardization, which offers stakeholders a platform for development of standards that meet market requirements. It is a non-profit association, and it is the national standards body that represents German interests in international standards organizations. Penetration of DIN in CEN working committees is high.
Regarding cybersecurity aspects, DIN has developed roadmap recommendations for standardization, which provides recommendations on information technology (IT) security and data protection.



Classification level: Public

### 2.2.2 United States

The following US entities are the main entities that cover cybersecurity for smart grids in the United States:

#### 2.2.2.1 NIST

References for this section are [24], [25] and [26].

##### 2.2.2.1.1 The organization

The NIST is an agency of the US Federal Government whose main goal is to improve US innovations and industrial competitiveness by advancing in standards and technology. It is one of the most important standardization organizations in the US, and it's been the developer of many standards regarding industrial control systems (ICS) security.

NIST has also defined an overall cybersecurity strategy for the Smart Grid, including a risk mitigation strategy to ensure interoperable solutions across different components of the infrastructure. As a result of this work, document NISTIR 7628, Guidelines for Smart Grid Cybersecurity stands as an important and strategic publication.

NIST collaborates with other groups on the field of cybersecurity so as to: develop system-level security requirements for Smart Grid applications (advanced metering, distribution automation, HAN, etc.); provide inputs on the Smart Grid standards, priorities and gaps, identifying issues and needs; finally carry out several activities regarding the development of a Smart Grid framework for interoperability and cybersecurity (the Smart Grid Interoperability Panel, SGIP). The SGIP has several working groups; of interest for this work package are:

- The Smart Grid Architecture Committee (SGAC), which is responsible for the creation, maintenance and refining of a conceptual reference model for the smart grid and also maintains the corresponding lists of standards and profiles. Finally, this group is responsible for the creation of a new reference framework for the smart grid.
- The Smart Grid Testing and Certification Committee (SGTCC), which is in charge of creating and supporting the environment for compliance, interoperability, and testing and certification for the recommended standards.
- The Cyber Security Working Group (CSWG) identifies and analyses security requirements and, on this basis, the group develops the risk mitigation strategy. This is the group responsible for document NISTIR 7628.

##### 2.2.2.1.2 The Framework

The Smart Grid Framework for interoperability and cybersecurity is technology agnostic, so as to address as many technological scenarios and environments as possible. The methodology is designed to provide guidance to ease risk management consistent with an organization's approach to cybersecurity, and tries to integrate both privacy and cybersecurity concepts. The Framework complements the organization's risk management strategy; it does not substitute it at all. Its main components are the following:

- The Framework Core, which is composed of five concurrent Functions: identify (understanding business context, critical functions and associated resources and cybersecurity risks), protect (limiting an eventual cybersecurity event), detect (developing the necessary activities to identify the occurrence of a security event), respond (developing the necessary activities to take actions as a result of the detection



Classification level: Public

of a cybersecurity event) and recover (developing the necessary activities to resume normal operation after the occurrence of a security event, trying to reduce its negative impact). Taken as a whole, these five functions provide a strategic view of the lifecycle of an organization's management of cybersecurity risk. It also defines key Categories and Subcategories for each function, and matches each of them with the corresponding standards, guidelines and practices, which constitute the Informative References.

- The Framework implementation Tiers: the Tiers characterize an organization's practices over a range, starting from "Partial" (Tier 1) to "Adaptive" (Tier 4), and reflecting a progression from informal responses to approaches that are risk-informed. There are 4 Tiers: Partial (in this stage, cybersecurity risk management practices are not formalized, and risk is managed on an *ad hoc* and reactive basis), Risk informed (in this stage, risk management practices are approved by management but may not be established as organizational-wide policy), Repeatable (in this stage, the organization's risk management practices are formally approved and expressed as policy) and Adaptive (in this case, the organization adapts its cybersecurity practices based on its experience and adopts predictive indicators derived from previous and current cybersecurity activities).
- A Framework Profile: a Profile represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories, and it can be described by means of the alignment of standards, guidelines and practices to the Framework Core in a particular scenario.

The Framework uses risk management processes to enable organizations to inform and prioritize decisions relative to cybersecurity. It is adaptive to provide a flexible, risk-based, implementation that can be applied to a broad set of cybersecurity risk management processes.

#### 2.2.2.2 ANSI

ANSI is a private, non-profit organization supported by both private and public entities. Its main line of action is the development of standards, which ensure consistency between products from different manufacturers in terms of characteristics and performance; and ensures that relevant terms and definitions are unique, and tests for products are carried out in a consistent way.

ANSI C12.19 series includes encryption, authentication and management of security credentials.

ANSI C12.22 relates to security and authentication services.

#### 2.2.2.3 NERC

The North American Electric Reliability Corporation (NERC) is an organisation composed of public and private partners, including manufacturers, integrators, service providers, operators, and public and standardization bodies. Its main objective is to ensure the reliability of the US bulk power system. NERC has developed a set of self-regulation documents on critical infrastructure protection of the power grid (NERC-CIP standards), all of them completely focused on both the physical security and the cybersecurity aspects of the bulk electric



Classification level: Public

system. As a result of this work, NERC provides guidelines and technical papers. Two main WGs are devoted to cybersecurity: NERC SGTF (Smart Grid Task Force), which is in charge of reviewing smart grid characteristics, identifying reliability concerns such as vulnerabilities, and providing recommendations as a result of its activity. The NERC SGWG (Smart Grid Working Group) reviews existing security guidelines and promotes awareness and application of such guides.

#### 2.2.2.4 NEMA

National Electrical Manufacturers Association (NEMA) is the trade association of choice for the electrical manufacturing industry. Regarding cybersecurity, NEMA's objectives consist on addressing the risk to business operations from security breaches and the risk to product development and marketing as the Federal Government adopts preventive measures. NEMA considers that security must be always part of the design considerations for any Smart Grid product.

#### 2.2.2.5 GridWise Alliance

The GridWise Alliance represents a wide range of various stakeholders, from utilities to large technological companies. Its work is specially focused on Smart Grids, and there is a specific cybersecurity division in charge of studying the security problems of US grid. They aim to involve all stakeholders and take full advantage of existent works regarding security. The Alliance uses a comprehensive risk management approach and provides clarity to stakeholders. Also, they implement a framework specifically dedicated to electric grid applications and create verification and test procedures for standards and guidelines.

### 2.2.3 Other national and international bodies

The following entities carry out a wide range of activities regarding cybersecurity for Smart Grids throughout the world. As long as they cannot be assigned to a specific country or geographical area, they are listed in this section.

#### 2.2.3.1 CIGRE

The International Council on Large Electric Systems (CIGRE) is an international, non-profit association. Its main objective is to develop and distribute technical knowledge regarding generation and HV transmission. There are several Study Committees (SCs) in charge of different aspects of the field the CIGRE is dedicated to. One of them, SC D2, includes security aspects of information systems and telecommunications for the Electric Power Infrastructure.

#### 2.2.3.2 ITU-T FG on Smart Grid

The International Telecommunication Union (ITU) is the United Nations agency for information and communication technologies, which established a Focus Group (FG) on Smart Grids in 2010. It is intended for collecting and documenting ideas for developing recommendations on Smart Grid issues from the perspective of telecommunications. Particularly, the FG Smart Grid group has identified security, privacy and reliability issues which could be reflected in the development of standards on these regards.



Classification level: Public

#### 2.2.3.3 IEC

The International Electrotechnical Commission (IEC) is the world's leading organization which develops international standards for electrical and related technologies. The IEC standards fulfil the needs of all stakeholders of every country which takes part in the IEC activities. IEC also works in cooperation with other standardization bodies like ISO. IEC includes several WGs which are in charge of implementing security measures in Smart Grid environments:
The IEC TC 8 WG AHG4 activities include Smart Grid requirements for electrical system reliability, communication security regarding metering, etc.
The IEC TC 57 WG 15 is in charge of developing standards for security of the communication protocols like the IEC 60870-5 series, the IEC 61850 series and the IEC 61968 series, among others.
The ISO/IEC JTC1/SC27 is devoted to the development of standards for the protection of information and ICT (methods, guidelines and techniques, all of them addressing both security and privacy issues).

#### 2.2.3.4 IEEE

The IEEE is probably the world's largest professional association devoted to technological improvement in many areas. IEEE develops standards, technical reports and publications. Some of them are addressed directly to cybersecurity aspects. IEEE also organizes conferences and training, educational and professional activities.
The IEEE is divided into technical committees, the standardization one perhaps being the most important. This committee includes several working groups which are in charge of defining security measures for Smart Grid environments: IEEE WGC1, responsible for the standard for substation intelligent electronic devices with active cybersecurity capabilities; IEEE WGC6, responsible for the trial use standard for cryptographic protocol for cybersecurity in substation serial links; the WG IEES PSACE CAMS (Power System Analysis, Computing and Economics; Computing and Analytical Subcommittee), which is in charge of analyzing the cybersecurity of the electric power infrastructure; and others.

#### 2.2.3.5 ISA

ISA (International Society of Automation) is a global, non-profit organization whose main mission is to become the standard for automation globally through certification of professionals, supply of education and training (e.g. workforce development on ICS cybersecurity), publishing technical articles and developing standards and guidelines for good practices for industry.
Secure practices and assessment of electronic security performance are their main purposes. ISA67 16WG5 is in charge of investigation and management of cybersecurity issues.

#### 2.2.3.6 Zigbee Alliance

The Zigbee Alliance is a non-profit consortium of semiconductor manufacturers, technology providers and end users worldwide. It has defined a global specification for interoperable, low-power and cost-effective wireless communications based on the IEEE 802.15.4 standard.



Classification level: Public

The specification defines mesh and tree network topologies for wireless control and metering systems. The Zigbee Alliance has got the necessary infrastructure to test and certificate devices as Zigbee compliant. The Alliance has defined several application profiles for device control (Home Automation, HA) and metering (Smart Energy Profile, SEP), with built-in security features, based on either symmetric or asymmetric schemes and well-known cryptographic algorithms and industry standards.
The Zigbee Alliance has produced a complete set of norms and standards which describe in full detail the particularities of the Zigbee protocol and profiles, including cybersecurity features.

## 2.3 Security initiatives regarding Smart Metering

In general terms, there are many countries with AMI systems under development and/or deployment. There are also many variants in the topology and specifications of the system, although most solutions are based on the existence of a kind of Head End System (HES), which is in charge of managing all the metering information retrieved from smart meters, as well as personal, billing and security information. This element is also the source of any kind of commands to be delivered to meters, e.g. connection/disconnection of the subscriber to/from the network, change of settings, other commands and firmware upgrades. This HES is linked with meters through one or more intermediate devices, which provide connectivity and eventual adaptation of communication protocols to the metering protocols which implement final communication with the meters. These intermediate devices can be the boundary of segments with different physical transmission media, and therefore different protocol specifications.

Examples of countries that already have ongoing AMI initiatives are UK (with plans to end deployment by 2020), France (with end of deployment expected by 2020, with about 35 million devices), Portugal, Spain (with expected end of deployment in 2019), The Netherlands, Germany, Italy (with the world's major smart meter deployment, about 30 million devices), Denmark, Sweden, Norway, the British Columbia and Ontario in Canada, several states of the US like California, Texas, Florida, Maryland, the State of Victoria in Australia, Iran, Lebanon, Saudi Arabia and Japan. Cybersecurity is a common concern for all these deployments, which is usually implemented at application level (for both the smart meter and HES communication segments, taking advantage of currently operative communication technologies and protocols).



Classification level: Public

# 3 SEGRID Architecture

Most Smart Grid architectures are structured *vertically* in three interacting levels. The top level is the electrical network infrastructure, providing metering and energy management services through a service-oriented architecture. The mid-level is the primary and secondary substations that provide metering and concentration of information, automation, fault detection, event reporting, and quality of supply monitoring. The lower level is at the customer's premises, where the Smart meter provides metering and contractual functions, and enables micro-generation integration and control. Through a wireless Home Area Network (HAN), the Smart meter can monitor and control energy devices inside a house; whereas the customer (consumer/prosumer) can interact with the HAN services through a local interaction interface, and remotely, through the Internet.

In the SEGRID architecture, we take a dual view

- The *functional architecture* focuses on the data-flows necessary to implement the functionality of the SEGRID use cases, including the corresponding data sources and targets. Rather than seeing the grid as a hierarchical structure, the assets are sorted by the roles of the asset owner or location. The functional architecture provides one overarching architecture picture for all use cases.
- The *component architecture* focuses on physical components, and sticks to the vertical view. For this architecture, selected use cases are analysed, and the necessary components and protocols are described in more detail.

All described architectures are *technology-agnostic*, meaning that they do not depend on a specific system or technology.

Before defining the SEGRID architecture, basic notations are introduced in relation to the Smart Grid Architecture Model (SGAM) framework established under mandate M/490 by the European Commission.

## 3.1 Smart Grid Architecture Model

The SEGRID architecture is based on the Smart Grid Architecture Model (SGAM) developed by the Smart Grid Coordination Group (SG-CG) formed by the European standardization organizations CEN, CENELEC, and ETSI [16], [17], [18], [19]. As depicted in Figure 4, the SGAM framework is three-dimensional involving *domains*, *zones*, and *interoperability layers*.



**Classification level: Public**

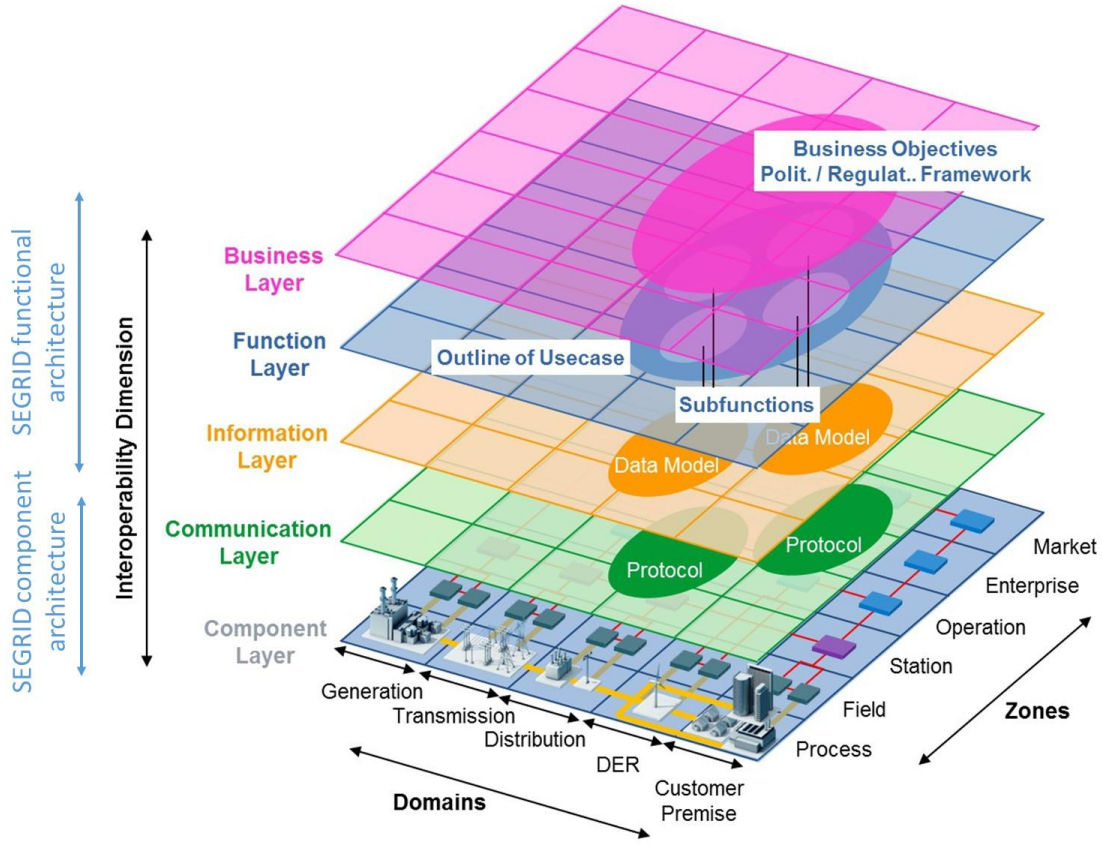


**Figure 4: M/490 Smart Grid Architecture Model (SGAM)**

The domain of energy distribution is the centre of the SEGRID use cases. The logically connected *domains* in SEGRID involve transmission, producers of distributed energy resources (DERs), and consumers ranging from large factories to standard private households.

To establish a hierarchy on the smart-grid plane, SEGRID security solutions are devised per *zone*: the process, field, station, operation, enterprise, and market. As a reminder, Table 1 lists the definitions of each zone from the SGAM Reference Architecture.

**Table 1: Domains and zones together form the Smart Grid plane**

| Zones | Description |
|---|---|
| **Process** | Including the physical, chemical or spatial transformations of energy (electricity, solar, heat, water, wind …) and the physical equipment directly involved. (e.g. generators, transformers, circuit breakers, overhead lines, cables, electrical loads any kind of sensors and actuators which are part or directly connected to the process,…). |
| **Field** | Including equipment to protect, control and monitor the process of the power system, e.g. protection relays, bay controller, any kind of intelligent electronic devices which acquire and use process data from the power system. |
| **Station** | Representing the areal aggregation level for field level, e.g. for data |



Classification level: Public

| | |
|---|---|
| | concentration, functional aggregation, substation automation, local SCADA systems, plant supervision… |
| **Operation** | Hosting power system control operation in the respective domain, e.g. distribution management systems (DMS), energy management systems (EMS) in generation and transmission systems, microgrid management systems, virtual power plant management systems (aggregating several DER), electric vehicle (EV) fleet charging management systems. |
| **Enterprise** | Includes commercial and organizational processes, services and infrastructures for enterprises (utilities, service providers, energy traders …), e.g. asset management, logistics, work force management, staff training, customer relation management, billing and procurement… |
| **Market** | Reflecting the market operations possible along the energy conversion chain, e.g. energy trading, mass market, retail market. |

Security is defined with respect to the third dimension in the SGAM, the five *interoperability layers*. Use cases are defined on the *function layer*, while policies and standardization efforts relate to the *business layer* and the *information layer*. Risk assessments and implementations of security solutions in SEGRID will focus on the *communication layer* and the *component layer*.

As shown in Figure 4, the SEGRID functional architecture is described with respect to the three upper layers while the SEGRID component architecture focuses on the two lower layers.

Table 2 lists the definitions of each layer from the SGAM/SGIS final report.

**Table 2: Definitions of the SGAM/SGIS interoperability layers**

| Interoperability Layers | Description |
|---|---|
| **Business** | Represents business cases which describe and justify a perceived business need. |
| **Function** | Represents use cases including logical functions or services independent from physical implementations. |
| **Information** | Represents information objects or data models required to fulfill functions and to be exchanged by communication |
| **Communication** | Represents protocols and mechanisms for the exchange of information between components |
| **Component** | Represents physical components which host functions, information and communication means |



**Classification level: Public**

## 3.2 Functional Architecture

The SEGRID functional architecture is based on the functional interoperability layer in the SGAM. In this, the functional architecture focuses on the information flow required to implement the desired functionality, including as assets the data source, communication channels, and data recipient. All assets described in this view are also assigned to the corresponding market roles, i.e., DSO, Household, etc. The functional architecture shows an overarching picture of the entire Smart Grid as relevant for the purposes of the SEGRID use cases, and thus also allows mapping the use cases onto roles and the corresponding assets and information flows. It also allows to see how the individual use cases interact on a functional level, and where assets are shared between use cases. By identifying where what data is needed, this part of the architecture will be used to identify where the SEGRID architecture needs to add resilience against attacks.

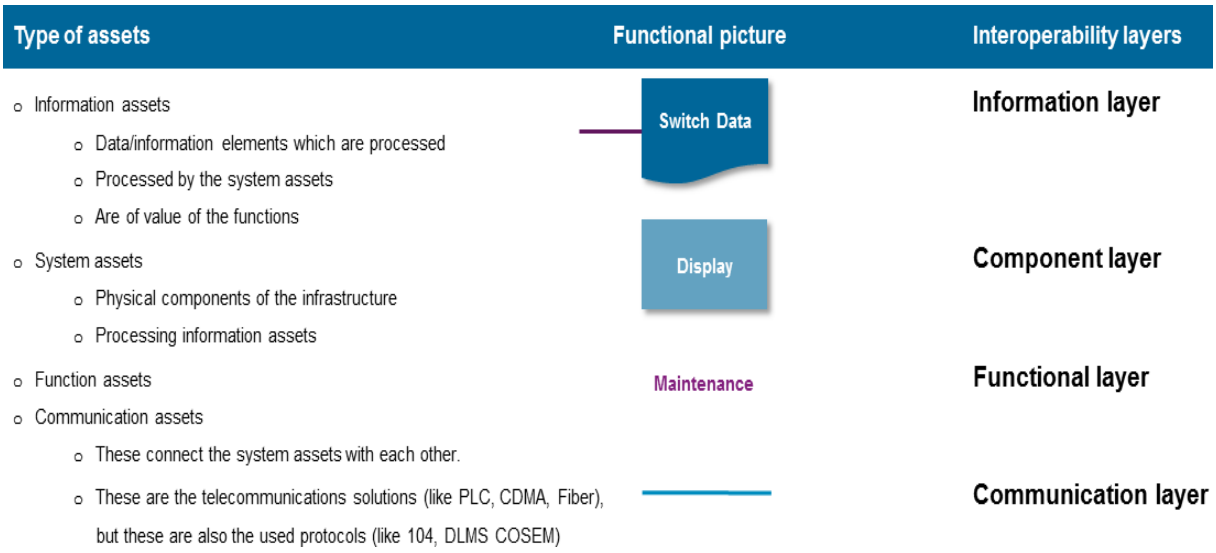


**Figure 5 – Identification of information and system assets**

Functional framework according to interoperability layers of Smart Grid Architecture Model (SGAM):



Classification level: Public

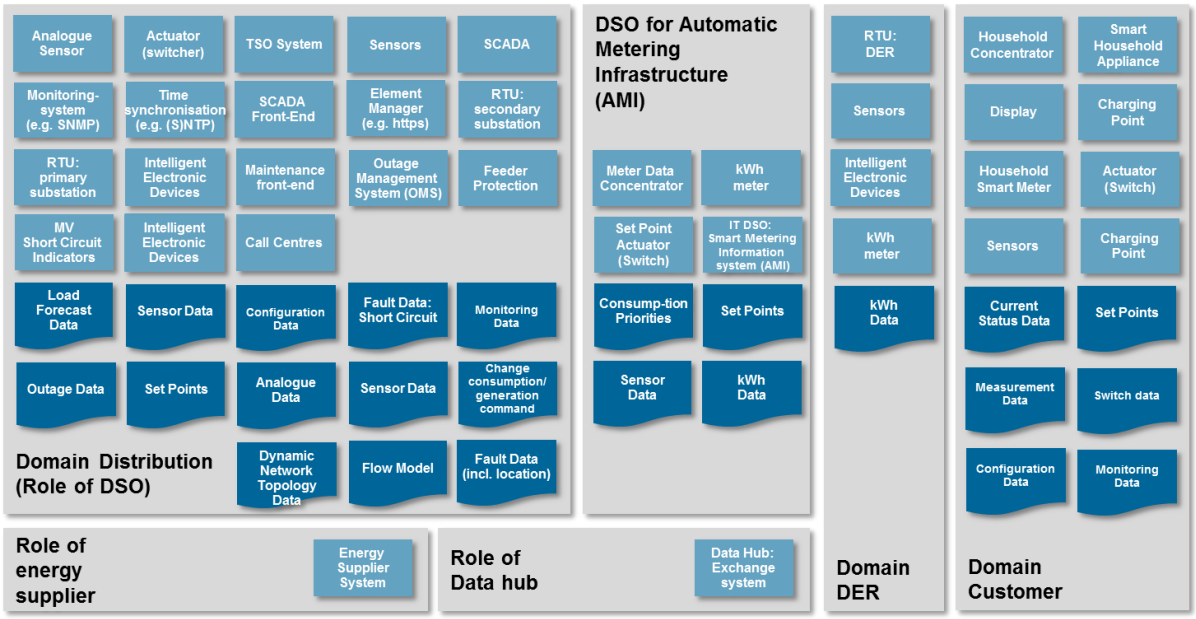


**Figure 6 - Distribution of information and system assets by domain**

To ensure a common interpretation of all the system and information assets throughout the remaining of the document, especially for the use case section, the following tables will clarify all the concepts that were introduced in the above figures:

**Table 3: List of SEGRID System Assets.**

| System Asset | Description |
|---|---|
| **SCADA** | **SCADA** stands for Supervisory Control and Data Acquisition and is a central placed control system that communicates with RTUs to get process information and send command signals to supervise and control the grid. SCADA system has several Human-Machine workstations for the grid operators and include functions for event and alarm handling, calculations, historical archiving, reporting, etc. |
| **SCADA Front-End** | **SCADA Front-Ends** are responsible for the communication with the RTUs. They collect process data and send it to the SCADA system, and they also issue commands to the RTUs from the SCADA workstations. Normally the SCADA Front-Ends are placed in connection the SCADA systems.<br>SCADA Front-Ends use various medias and specially designed communication protocols to communicate with the RTUs. Protocols can be both standard and proprietary. Examples of standard protocols commonly used are; IEC |



Classification level: Public

| | |
|---|---|
| | 60870-5-101 and -104, DNP 3.0, Modbus. |
| **Remote Terminal Unit (RTU)** | **RTUs** are devices placed in substations to collect process data and execute commands. They are equipped with binary and analogue input channels connected to sensors and to Intelligent Electronic devices (IED). They also include output channels for commands and setpoints connected to analogue and binary actuators. RTUs communicate with the SCADA Front-Ends to send process data to SCADA and receive commands using RTU protocols. In Smart Grids peer-to-peer communication between RTUs will be used.<br>The same type of RTUs is placed in both primary (HV/MV) and secondary (MV/LV) substations. Typically only the amount of input/outputs and packaging differs between these two types.<br>RTU are also placed at bigger distributed generation facilities. They are used to collect information about power generated, e.g. in a wind park, and to control generation via setpoints.<br>Modern RTUs can include a Human-Machine Interface and have substantial calculation power. They are used in Smart Grids for a higher degree of autonomous and self-healing functionalities. |
| **Intelligent Electronic Device (IED)** | **Intelligent Electronic Devices (IEDs)** are self-contained units with embedded software system for used for protection devices, bay controllers, etc. They work independent of the SCADA/RTUs and have the task to protect primary equipment and protect humans against incidents by disconnecting faulty equipment. IEDs are normally connected to a station bus using IEC 60850 or older types of protocols to communicate with other IEDs, RTUs, gateways and Substation Control System. They can be used as sensors by the RTUs when collecting Measurements (process information) or executing commands. |
| **Actuator** | **Actuators** are devices that execute commands, e.g. open a breaker, received from the central SCADA system or a local RTU. Both binary and analogue actuators exist, analogue actuators are typically used by generation regulators to controls the energy production. Binary actuators open and close breakers and isolators. |
| **Sensor** | **Sensors** are measuring devices that measures currents, voltages and power, etc. in the grid and convert it to a signal that can be connected to the RTUs input boards. Examples of sensors are current and voltage transformers |
| **Short Circuit Indicators** | **Short Circuit Indicators** are devices specially designed to detect short circuits on a medium voltage feeder. Both directional and non-directional Short Circuit Indicators exist. |



**Classification level: Public**

| | |
|---|---|
| | Directional indicators can show in which direction on the feeder the short circuit has occurred. |
| **Feeder Protection** | **Feeder Protection** is a protection device placed at the feeder in the primary substations. It will discover a short circuit on the feeder and disconnect the feeder in this case in order to protect equipment and human lives. Typically feeder protection has a recloser automatic that tries to reconnect the feeder to see if the fault was temporary. If the fault remains the feeder will be permanently disconnected. |
| **HMI** | **HMI** is the Human Machine Interface to make it possible for human operators to interact with SCADA and RTUs. Typically HMIs consist of a workstation where the operators can request various views of the supervised process and initiate manual operations like commands.<br>Two types of HMI exist. One is a permanent workstation which is normally used by SCADA system and Substation Automation Systems at bigger substation. The second is a temporary workstation which could be laptop connected to an interface in a substation without permanent workstations. Temporary workstation are typically used by visiting service engineers to the substations |
| **Outage Management System (OMS)** | **Outage Management System (OMS)** is a software system that analyses Fault Data and calculate location of outages. OMS systems are normally also responsible for Crew Management, i.e. to send repair crews to the correct location of fault.<br>An important part of any OMS system is to handle planned extensions and maintenance of the distribution grid. This is the main task for any OMS system since planned maintenance activities significantly outnumber unplanned outages. |
| **Access to TSO Data (ICCP)** | Exchange system for data of DSO and TSO. Relevant for the risk analysis of WP2.<br>**The TSO Systems** are Transmission operators' SCADA and EMS system. EMS stands for Energy Management System, which include long lists of advanced mathematical applications for transmission grid, security and optimization. These systems are of little interest in the SEGRID project. |
| **Call Centre** | **Call Centre** is where customers can call for various complaints and questions to the distribution system operator (DSO). In the case of SEGRID the most interesting part of a Call Centre is when a customer calls to report power outages. This is used by the OMS to find fault locations in the same way as automatic fault reports. |
| **Energy Supplier** | **Energy Supplier** is the company or organization that generates electrical energy. Typically end users, like |



**Classification level: Public**

| | |
|---|---|
| | households, have a contract with the energy supplier to provide them with electrical power. The Energy Supplier uses the electrical grid to transport energy to the customers. |
| **Element Manager** | **Element Managers or maintenance systems** are used to enter all relevant parameters that are used by SCADA, RTU, AMI and Meters to operate. Parameters include information both about the electrical process and the control system execution. Examples of process parameters are device identifiers, static topology, operational limits, etc. Examples of control system parameters are communication parameters, alarm handling parameters, execution control, etc.<br>Normally the Maintenance system is a separate system only used for maintenance with an advanced database system to store all parameters and to handle maintenance versions. Data is downloaded to different control system assets like SCADA, AMI, RTUs, Protection and Meters. It is common that AMI and Meters have their own Maintenance System.<br>It should be understood that Maintenance is a big part of the DSO activities. Distribution grids are continuously undergoing changes and extensions and the process descriptions must be updated. |
| **Monitoring System** | **Monitoring Systems** collects information from other system assets about power quality, execution times, logging, communication statistics, etc. Monitoring systems are used to analyse the behaviour of other system assets.<br>They can use various protocols for their tasks but one common protocol is SNMP. |
| **Time Synchronization** | **Time Synchronization** systems are used to synchronize time between different system assets. Sometimes time synchronization is an integral part of SCADA. |
| **Smart Meter** | A **Smart Meter** is an electronic device that records the consumption and generation of electricity and communicates periodically that information to the utility, both for monitoring and billing purposes. The Smart Meter also facilitates a number of other services both for the utility (e.g., remote switching, tariff changes) and the customer (e.g., efficiency services, consumption levels). |
| **Smart Meter Display** | The **Smart Meter Display** is the interactive display of the Smart Meter which presents generation or consumption data from the smart meter in real time and other service related information. |
| **Data Concentrator** | A **Data Concentrator** is an electronic device that acts as a local hub for meters in a neighbourhood and that facilitates the connection to the head-end system. The data concentrator locally collects and aggregates data from multiple meters and |



Classification level: Public

| | |
|---|---|
| | sends it to the utility servers. |
| **AMI System** | The **Advanced metering infrastructure (AMI)** is an integrated system of smart meters, communications networks, and data management systems that enables two-way communication between utilities and customers. The AMI is also responsible to provide customer data to the Data Hub Exchange System. The AMI also enables several other utility capabilities such as Meter-level voltage monitoring and Distribution Automation. |
| **Data Hub Exchange System** | The **Data Hub Exchange System** securely collects information about customer loads and distributed production from the utilities and facilitates this resource (ensuring data minimization) to any third party that requires such data for several market or regulation related services. |
| **Household Concentrator** | The **household concentrator** collects the information of the Smart Household appliances and executes the change consumption/generation command. |
| **Smart Household appliances** | The **Smart Household appliances** are electronic devices that communicate through LAN protocols with the Smart Meters and facilitate the interaction of the customer with the smart meter and the utility. Customers can have real-time access to more accurate data and knowledge about electricity consumption and generation, electricity pricing, helping them save money and lower their environmental footprint. |
| **Charging Point** | The **Charging Point** is an element in an infrastructure that supplies electric energy for the recharging of plug-in electric vehicles. |
| **Set Point Actuator** | The **Set Point Actuator** is a process device with continuous regulation used for generation units. This can limit the supply of DER in emergency situations. |
| **kWh Meter** | **The KWH meter is a** company meter on the MV-level that provides information about the energy consumption or energy production at a certain load/generation point. kWh data is a special case of Measurements but useful to distinguish in the SEGRID use cases. |
| **SCADA Vendor access** | The **SCADA Vendor Access** provides access of the SCADA vendor to the operational SCADA system of the DSO. Relevant for the risk analysis of WP2. |
| **DSO IT** | The **DSO IT** is the back end system that uses Smart Grid data, but is outside the operation technology (OT) domain. Relevant for the risk analysis of WP2. |



**Classification level: Public**

**Table 4: List of SEGRID Information Assets.**

| Information Asset | Description |
|---|---|
| **Analogue Data** | **Analogue Data** are (smart) grid measurements about the state of the electrical grid like currents, voltage, active and reactive power (i.e., measurement with continuous values) |
| **Sensor Data** | **Sensor Data** are (smart) grid measurements about the binary states of breaker and isolator. |
| **Measurement data** | **Measurement data** are smart household meter measurements give information about the energy consumption or energy production at a connection on the LV-level. |
| **kWh data** | **kWh Data** are company meter measurements on the MV-level about the energy consumption or energy production at a certain load/generation point. kWh data is a special case of Measurements but useful to distinguish in the SEGRID use cases. |
| **Current status data** | **Current status data** is a special case of Binary measurements to indicate the state of a Smart Household Appliance. |
| **Switch data** | **Switch Data** are the commands from the control systems in order to switch on-off a device. |
| **Set points** | **Set points** are used to control process devices with continuous regulation like generation units. This can limit the supply of DER in emergency situations. |
| **Dynamic Network Topology Data** | **Dynamic Network Topology Data** is a real-time model of the distribution grid state represented as a bus-branch model but without power flow. The Dynamic topology model is built by the SCADA or RTU system based on the static topology from Configuration Data and from the real time states of binary devices like breakers and isolators, i.e. open or closed. |
| **Flow model** | The **Flow model** represents the power flows in the distribution grid. It is calculated by a Power Flow calculation in the SCADA or RTU systems using real-time analogue measurements, the bus-branch model from the dynamic topology and line parameters from Configuration Data. |
| **Load Forecast Data** | **Load forecasts** are a predication of future loads in the distribution system. It is calculated based on historical data and other parameters like weather data, special days (e.g., holidays), etc. |
| **Fault Data** | **Fault Data** is information from special equipment in the grid about faults in the distribution grid. The most |



**Classification level: Public**

| | |
|---|---|
| | common is fault indicators that show the existence of a short circuit and the direction of the fault and feeder head protection that open the feeder breaker in the primary substation in case of a fault. The feeder head protection can disconnect the feeder to protect primary equipment and human life.<br>Another type of Fault Data are **Error reports** from customer calling Call Centre and reporting that they lack power. Smart Meter and give Fault Data automatically to the AMI system using the last gasp functionality of the Smart Meter. |
| **Outage Data** | **Outage Data** is information calculated by the Outage Management System (OMS) to localize a fault in the grid. The OMS uses Fault Data from various sources to decide the probable location of a fault to enable a quick repair. |
| **Change consumption/generation command** | **Change consumption/generation command** is a special type of command to give instructions to Smart Meters and Household Appliances to start, reduce consumption or to increase/decrease generation.<br>This command type is used in the SEGRID user cases for clarification. |
| **Configuration Data** | **Configuration Data** incorporates a lot of parameters to describe the electrical grid but also parameters to control the execution of the control systems. Examples of the first category are device identity, static topology, i.e. how devices are statically connected, line impedances, operational limits, etc. Examples of the second category are communication parameters, RTU connections, execution periods, cryptographic keys, etc. etc.<br>Configuration Data is defined at Maintenance system and downloaded to different types of control system and meters lie SCADA, RTU, Smart Meters, etc. |
| **Consumption Priorities** | **Consumption Priorities** is a special case of Configuration Data where the customers can set priorities to their household devices which could be switched off or reduce loads in case the household receives a Change consumption/generation command.<br>Consumption Priorities is also be used to communicate to the DSO that a particular smart household appliance is ready to be started by the DSO within certain time frame. |
| **Monitoring Data** | **Monitoring Data** includes information stored in devices like Smart Meters concerning logging, power quality, outage times, etc. Monitoring Data can be collected by Monitoring system to build reports about process |



**Classification level: Public**

| | |
|---|---|
| | behaviour, device- and the total system behaviour. |

## 3.3 Component Architecture

The SEGRID component architecture is keyed to the component interoperability layer in the SGAM. As opposed to the functional architecture, the component architecture focuses on individual use cases, and provides a vertical view of the interaction in the Smart Grid zones[1]. Where necessary we also provide information on the information interoperability layer and the communication interoperability layer. While focusing on the individual use cases, the component view allows for a more detailed view on component properties and requirements, and thus will be used to determine how the SEGRID security functionality has to be designed to add resilience.

Due to the more detailed analysis required for the component architecture, for this deliverable the focus lies on

- the distribution domain: components in a (secondary) substation and
- the customer premises: components for Smart metering

### 3.3.1 Supervision and Control Systems for Electricity Distribution

Transformer stations are the central points of the distribution grid. In primary substations high voltage (HV) is transformed into medium voltage (MV). In secondary substations medium voltage is converted into low voltage (LV). One often speaks of HV/MV or MV/LV stations, respectively. Apart from the voltage levels, primary and secondary substations differ in size and thus also in the amount of involved components.

The system assets of a transformer station include, amongst others, equipment such as circuit breakers, voltage and current transformers, control equipment and equipment to measure power quality measurement. One task of the smart electricity grid is to automate the tasks of a substation, to reduce the need of manning such a station or to send people whenever there is a need for local action. Distribution system operators (DSOs) normally use a SCADA (Supervisory Control and Data Acquisition) system to connect substation and field equipment via a telecommunication network to a central control system to be able to monitor and control power grid in real-time, i.e. to transfer the controls from a control room to the substation, and to collect information about loads, power quality, state of circuit breaker and isolators.

Substations exchange data with operations and the central control system (enterprise) over point-to-point networks using power line communication (PLC) or mesh radio as well as over wide area networks (WAN) using GPRS, UMTS, LTE, CDMA, 3G, or optical fiber.

[1] For better recognition zones are underlined in the text.



Classification level: Public

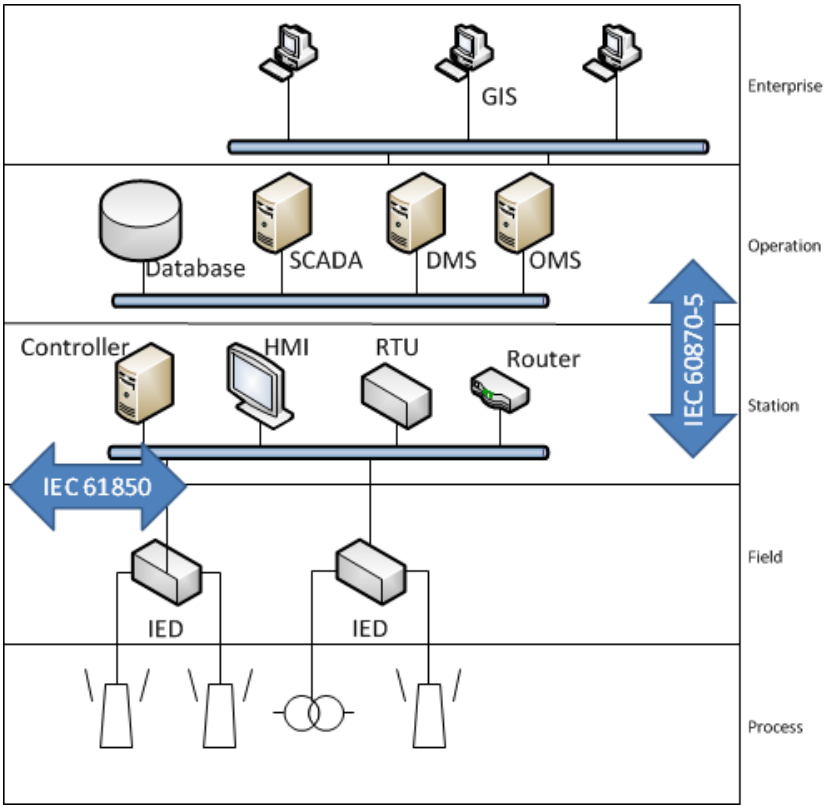


**Figure 7: Component architecture for the supervision and control system.**

Figure 7 shows the component architecture of a supervision and control system for distribution networks. The individual components are described in the following table.

**Table 5: Components of a supervision and control system for distribution networks.**

| Physical locations / SGAM Zones | Supervision and Control System for Distribution Networks |
|---|---|
| **Station Level** | The components for substation control, information gathering, control and communication in a substation ranging from (i) primary equipment over (ii) field devices to (iii) station equipment. |
| **Process Field Station** | Primary equipment comprises of switches, breakers transformers, cables etc. that make up the electrical grid.<br>Field devices are Intelligent Electronic Devices (IEDs) that interact directly with the primary equipment and include amongst others sensors, protection, bay controllers.<br>At the highest level in the substation, the station zone, a local control system connects to the protection system and automation system. Moreover, the local control system communicates with operations, |



Classification level: Public

| | |
|---|---|
| | gathers information from the field devices, and interacts with other components in the station. Such a local system can range from a large Substation Automation System including Human Machine Interfaces (HMI) and local intelligence to smaller devices like Remote Terminal Units (RTUs).<br>The RTUs are devices for the collection of data and for the control of actuators that are often used in substation where a full Substation Automation Systems is not required. The RTUs collects measured values and status via analogue and binary input cards and control actuators over output cards. The RTUs communicates to SCADA system using RTU communication protocols. Many RTUs have simple logics installed, e.g. for interlocking.<br>In secondary substations, a data concentrator (DC) often gathers meter data from connected households. Data concentrators can include some RTU functionality; these will be discussed in more detail in the Section 3.3.2. |
| **Control Room and Back Offices** | In the central control room a SCADA system (Supervisory Control and Data Acquisition) is placed which communicates with the substation system. Also systems for planning, statistics, billing are included in a back office environment. The control room and back offices are physically separated from the substation.<br>SCADA systems communicate with the substation using wide area network with both TCP/IP and point-to-point communication. Several different types of communication media are used, like Power Line Carrier, fiber and radio. Both propriety and standard protocols, like DNP 3.0 and IEC 80670-5-104, exist. |
| **Operations**<br><br>**Enterprise** | In operations, SCADA systems collect data from the substation, analyze it for important events and alarms, and send it to application servers called Distribution Management System (DMS) for further analysis and optimization. The SCADA systems are also used to control the distribution network by opening and closing circuit breakers and setting transformer tap changers<br>In the enterprise zone (back office) several other types of planning and data maintenance systems are included, e.g. Geographical Information Systems (GIS) which are used in the more or less continuous maintenance activities of a distribution network.<br>Further connected systems include Outage Management System (OMS) and Crew Management Systems to analyse automatic and manual trouble calls and to identify faults in the network in order to send maintenance crews. OMS systems normally include a connection to Call Centres so that Trouble Call operators can give accurate information to callers. |



**Classification level: Public**

The main standard defining the information model for substations is set in the IEC 61850 standard [5].

It is common to distinguish between horizontal communication inside the station and vertical communication between the station and operations. Horizontal communication nowadays often relies on the IEC 61850 communication protocols. Communication to operations relies on IEC 60870-5-101 for point-to-point communication or its extension IEC 60870-5-104 for TCP/IP based communication.

None of these standards provide security. For vertical communication the IEC 62351 [29] standard can be used as a wrapper around IEC-60870-5 traffic to provide entity authentication (digital signatures), message authentication and encryption.

### 3.3.2 Smart metering

A meter is used to record the consumption of electricity, gas, heat, or water. Using a multi-utility interface, it is possible to turn the electricity meter into a hub for measuring the consumption of other utility consumables. Other than a classical meter the smart meter provides direct access to this consumption data in short intervals. This data about consumption and reverse feeding by a prosumer is collected for various purposes including billing and grid management. In SEGRID, meters are mainly studied as part of private households.

Smart meters can communicate in different ways with the enterprise level. The European standardization organizations CEN, CENELEC, and ETSI have defined the M/441 Smart meter reference architecture as shown in Figure 8 [16] which captures all European Smart metering systems currently in use.

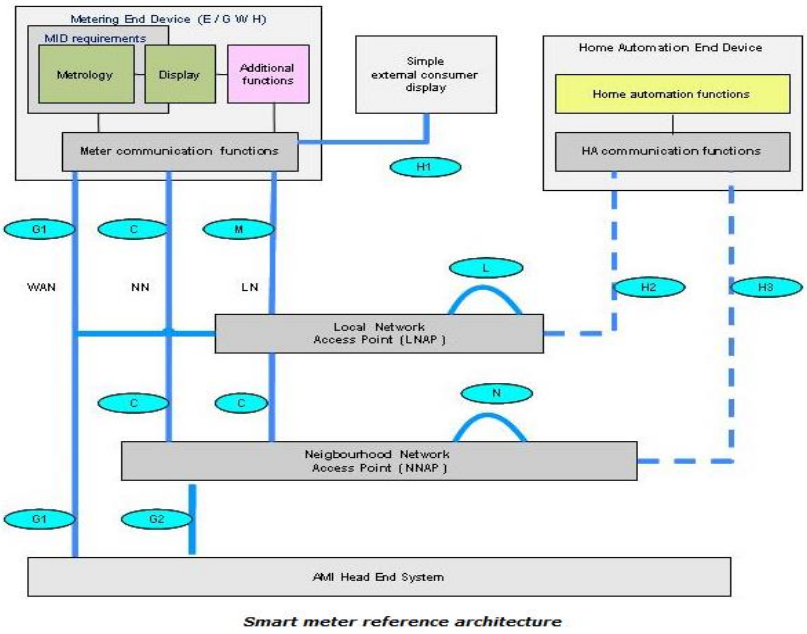


**Figure 8: M/441 smart metering reference architecture.**



Classification level: Public

Figure 9 shows the component architecture of a Smart meter system. It is important to note that the only the meter and HAN controller are part of the customer premises.

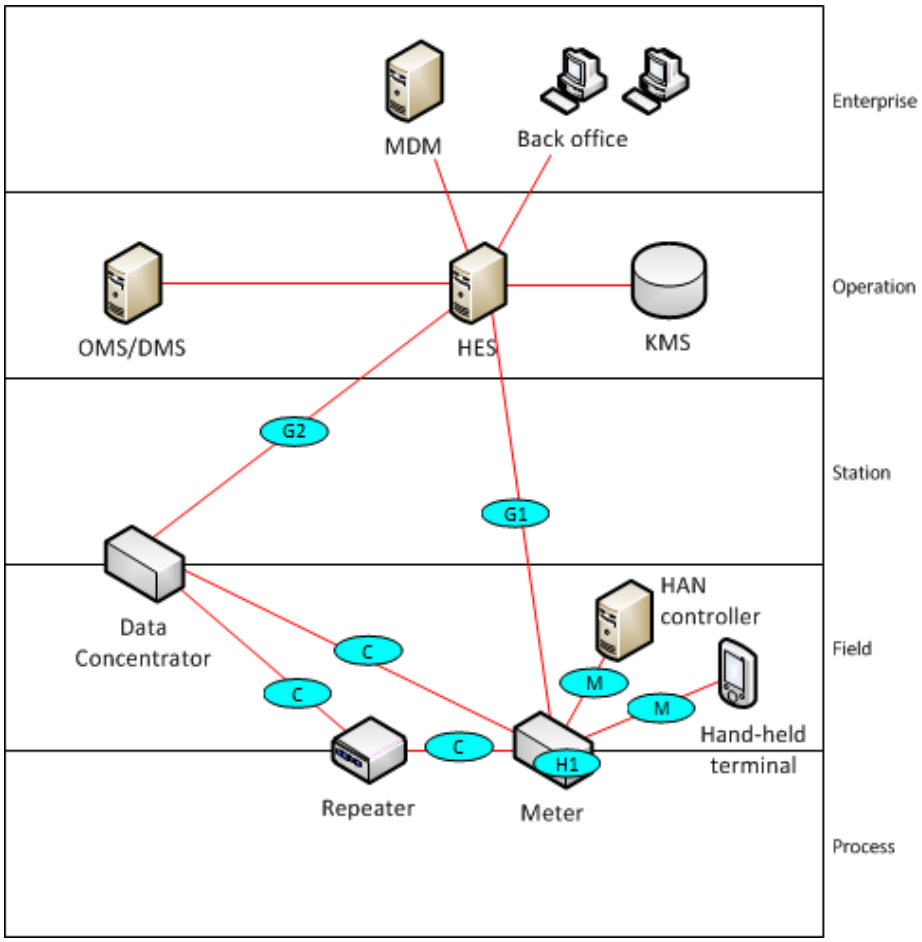


**Figure 9: Component Architecture Smart Metering. The interfaces are denoted using the M/441 notation.**

Table 6 below describes the communication interfaces of the Smart metering architecture and relates them to the M/441 reference architecture. It should be noted that the M/441 gives various options to connect end devices such as hand-held terminals, multi-utility meters, but also a local controller for the home area network (HAN) to the meter.



**Classification level: Public**

**Table 6: Mapping of M/441 interfaces to components in the SEGRID component architecture.**

| Interfaces in M/441 Reference Architecture | Smart metering interfaces in SEGRID architecture | Comment |
|---|---|---|
| **G1** | Meter WAN | GPRS, UMTS, mesh radio, optical fiber |
| **G2** | DC/Gateway WAN | GPRS, UMTS, mesh radio, optical fiber |
| **C** | LAN | Local network connecting meter to DC/gateway or to repeaters |
| **M** | Local Controller (HAN)/Customer Interface | The Metering end device interface (M interface) can be defined with different profiles according to CEN-CENELEC-ETSI.<br>To connect a hand-held terminal, the M interface is realized as optical port (infrared). |
| | Interface on the meter to connect end devices | |
| | Multi-Utility Interface | |
| **H1** | Display | User interface displaying current and historical information on consumption. |

There are many different communication standards for Smart metering. The communication stacks are typically modular, using generic standards. Giving a complete list of possible communication stacks is out of scope. Overviews and comparisons of various Smart metering communication standards can be found in [9] and [10]. Figure 10 gives an indication of how communication standards are connected. This is by no means the only option, as there are many ways to build a communication stack for Smart metering.

Similarly, there exist different data models for Smart metering. Widely used is the IEC 62056 COSEM model. Other standards such as the Open Smart Grid Protocol (OSGP) and Meters & More (SMITP data model) define their own data models.

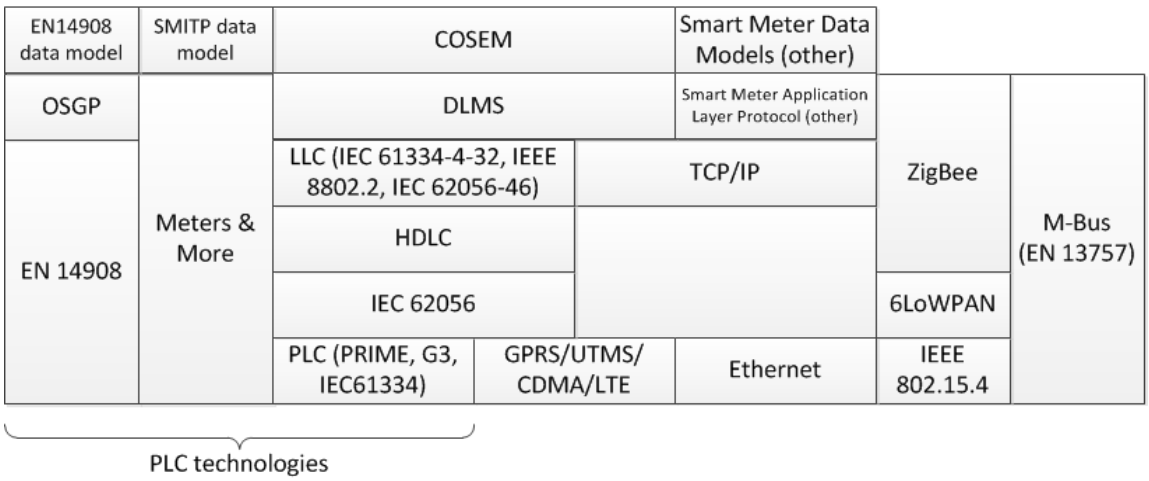


**Figure 10: Connections between selected smart metering communication standards.**



**Classification level: Public**

# 4 Stakeholders

There are several stakeholders interested in the implementation of a smarter grid. Many of them see the Smart Grid initiative as a move towards a sustainable and cleaner global economy, but naturally the actors comprised are also seeking other benefits with it, i.e., financial interest, managing and addressing the challenges of their business, etc. However, there is the case where government entities or organizations have no economic interest in the concept, but the challenge and mandate to ensure that the existing policies and legislation are guaranteed.

In the table below we will identify and describe the different actors involved in the development and implementation of a Smart Grid, according to the reference architecture described in Section 3.

**Table 7: Use Case Actors**

| Actor Name | Actor Role Description |
|---|---|
| **Distribution System Operator** | Organisation responsible for managing the distribution network that delivers electricity to the premises. |
| **Transmission System Operator** | Organisation responsible for managing the transmission network that delivers electricity to the distribution network. This stakeholder will not be considered as part of the SEGRID use case description despite the relevance of its role. |
| **Network Operator** | Organisation responsible for carrying out actions to manage load on the network<br>**Note:** This role is used for convenience and these actions may actually be carried out by NETSO, a Distribution Network Operator, a Supplier, an Aggregator, or any other party providing a Demand Response to Networks Businesses |
| **Energy supplier (retailer)** | Organisation responsible for establishing a contract with the customer for delivering and purchasing energy as a service and delivering value added energy services. |
| **Data hub** | A data hub is an organizational entity that acts as a collector of information of available customer loads and distributed production, facilitating this resource to the actors in power who need it. |
| **Micro-generation** | Sources of power from domestic properties or small-to-medium enterprises that are attached to the Smart metering System, such as PV, micro-wind turbines or micro-CHP. |
| **Customer** | Organisation, or person, consuming (consumer) or generating (producer) electricity at the premises. The Customer may also be the organisation or person con- |



Classification level: Public

| | |
|---|---|
| | tracted with the Supplier for the provisioning of energy.<br>When a customer is both consuming and generating electricity it might be named a prosumer. |
| **Data subject** | The natural person to whom the personal data relates. Personal data in this case can be usage data, financial information, consumption profiles, personal identifiable information (name, address, etc). The data subject can be the same entity as the Customer, but not necessarily, as the Customer may be just one person, a family, or the landlord. |

# 5 Use Cases

The SEGRID use cases are mainly focused on energy services and functionalities and we believe they represent the most important and most relevant stepping stones in the development of the electricity grid to the Smart Grid. The diversity of aspects that are to be supported provide a great flexibility for all the possible threat scenarios to be addressed while building innovative security technology. Each use case considers a number of different scenarios that were considered relevant for the SEGRID coming work. The described scenarios in the use cases below are country specific; other (European) countries can make use of different approaches.

## 5.1 Smart meter used for on-line reading of consumption and technical data

This use case refers to the smart meter capability of reading both the energy consumption and the energy generation of a customer. It is one of the most relevant Smart Grid capabilities since it replaces the costly manual readings. However, the smart meter has several other capabilities and services it can provide.

The functional architecture of use case 1, according to SGAM interoperability layers, is depicted below for future reference:



Classification level: Public

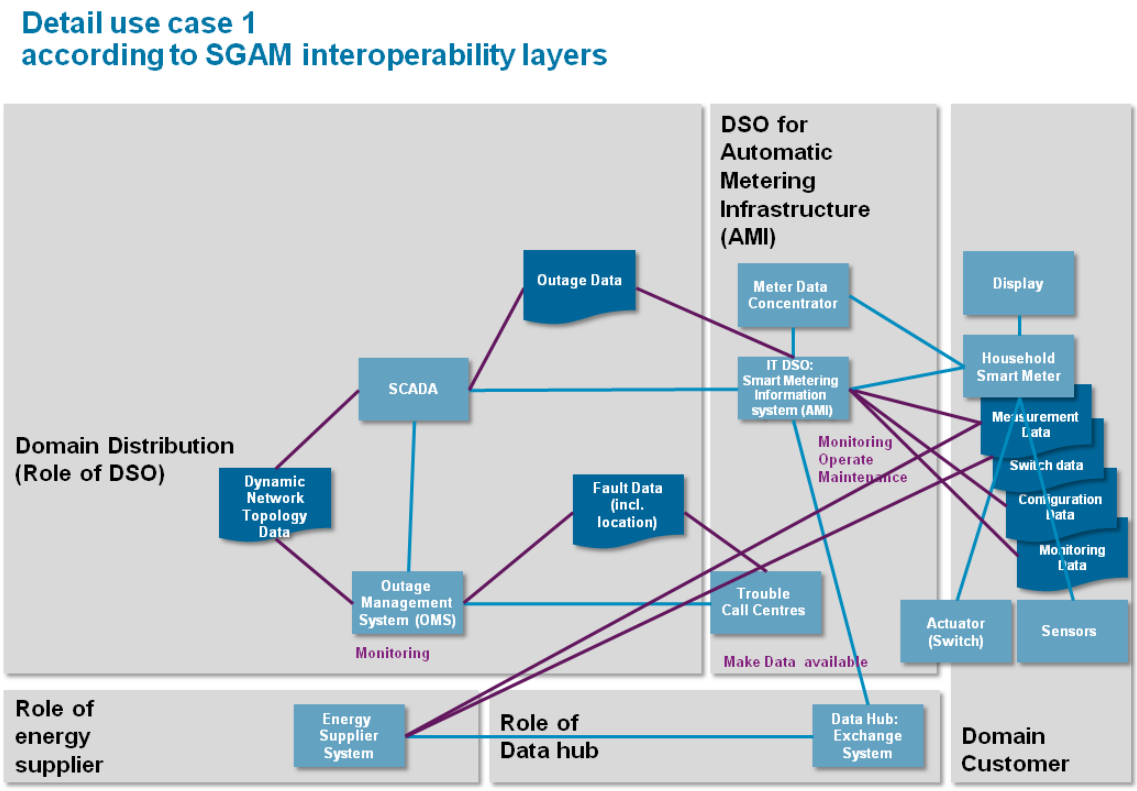


**Figure 11 - Functional architecture of use case 1**

The functional architecture of the different scenarios presented in use case 1, according to the SGAM zones, is depicted below for future reference:



**Classification level: Public**

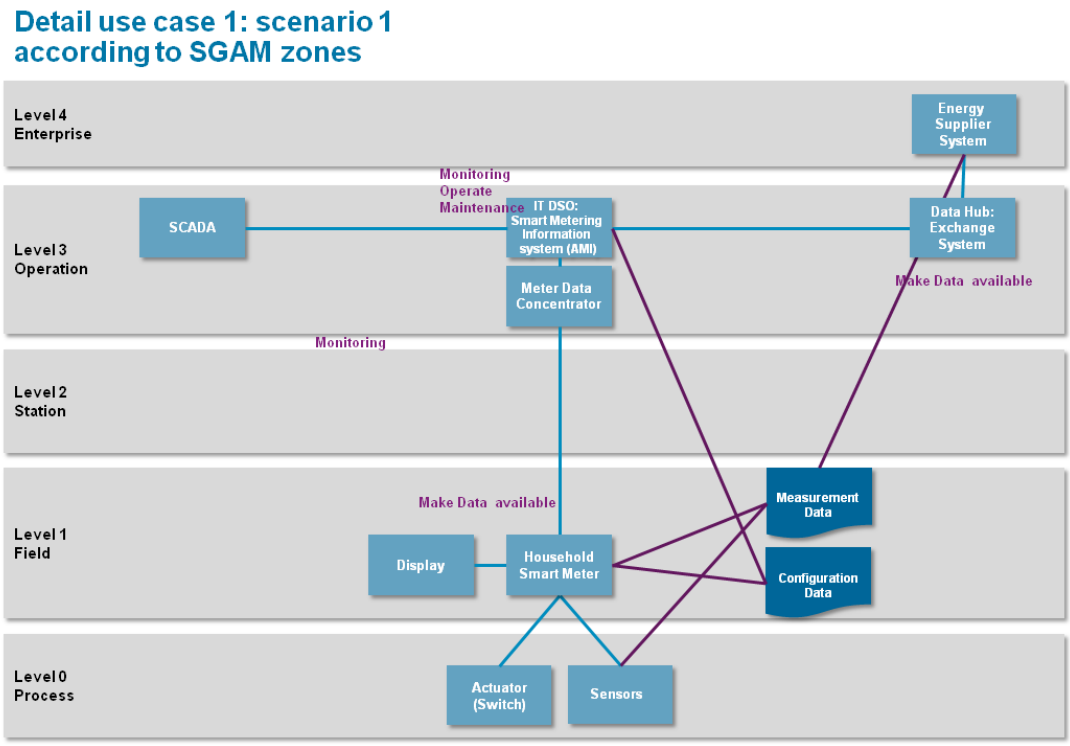


**Figure 12 - Functional architecture of use case 1, scenario 1: Metering**

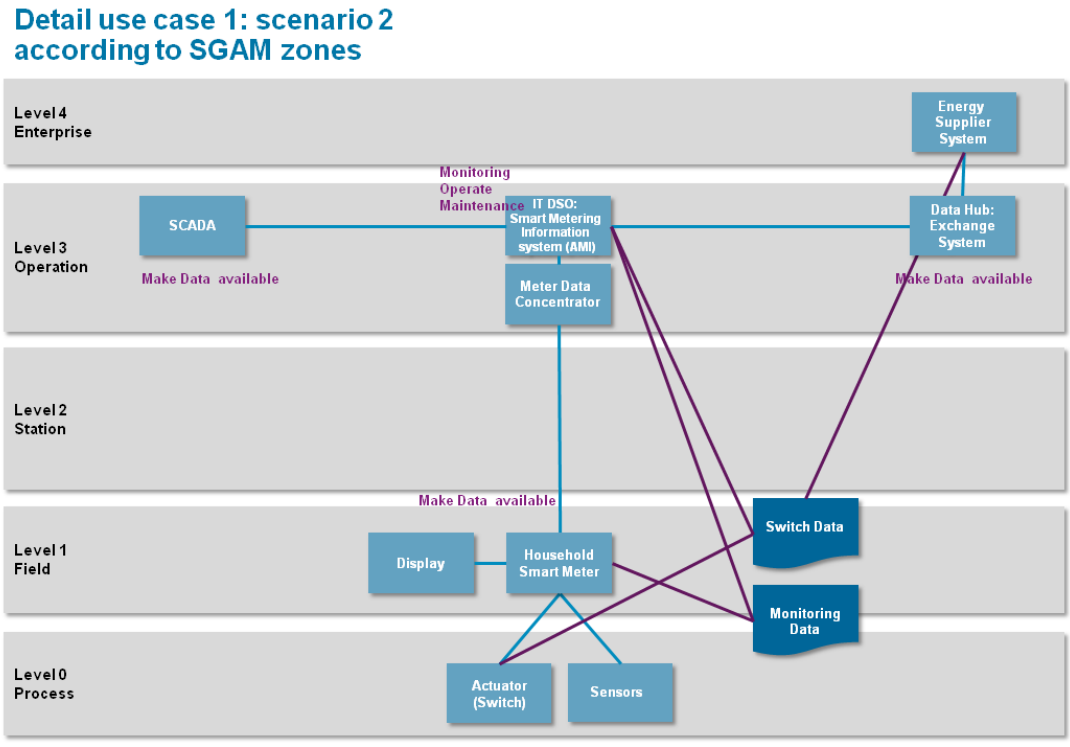


**Figure 13 - Functional architecture of use case 1, scenario 2: remote power switching**



**Classification level: Public**

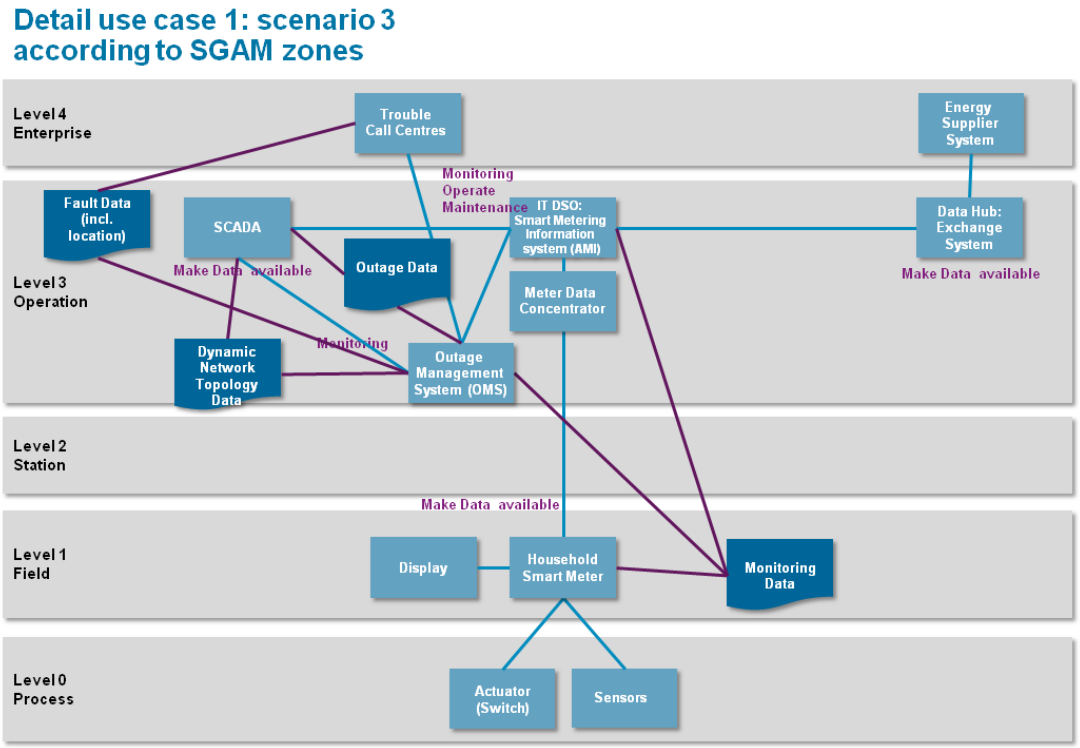


**Figure 14 - Functional architecture of use case 1, scenario 3: Outage management with last gasp**

In the table below, a description is given of the use case and each of its scenarios. This description shall be considered as a baseline for the SEGRID perspective work, over the different work packages.

**Table 8: Use case 1 and the use case 1 scenarios**

| Use Case #1 | Smart meter used for on-line reading of consumption and technical data |
|---|---|
| Description | The Smart meter at the customer's household sends the meter reading data to the IT DSO: Smart Metering Information system (AMI). This reading data may be routinely sent as centrally defined (e.g., periodic readings, interval values or load profiles) or per request, through the associated Meter Data Concentrator.<br><br>The DSO should facilitate the information to the energy suppliers, for billing and provision of commercial services. However, it might use it itself to support the management and operation of the power grid.<br><br>The reading data shall also be available in the Smart meter display and on the energy supplier internet website.<br><br>The Smart meter also allow the remote switching (‘Switch Data’) of a customer, due to the installation of a voltage switch on the meter. Its main purpose is to ensure that customers who fail to make their payments can be switched remotely to a prepay tariff and |



Classification level: Public

| | |
|---|---|
| | implementing, for example, rolling power cuts at times of supply shortage [11].<br><br>The Smart meter can also help a DSO understand the extent of a fault, and its location, since it is able to provide its status (even without power, due to last gasp capabilities). By sending AMI data ('Monitoring Data'), an outage management system (OMS) is able to trace the fault, facilitating the work force response and a more effective restore. For single outages, the meter can also be used to better understand if the outage is related to the utility service or is related to a problem within the customer's premises. |
| Flow | **Scenario 1: Metering**<br><br>a) For automatically scheduled readings:<br><br>1. Smart meter registers meter reading along with time/date stamp ('Measurement Data');<br>2. Smart meter records meter reading data in its memory ('Measurement Data');<br>3. Smart meter displays the metering data in its meter display ('Measurement Data');<br>4. Smart meter sends meter reading data ('Measurement Data') to the Smart metering information system managed by the DSO ('IT DSO: Smart Metering Information system (AMI)');<br>5. The DSO facilitates the metering data to the data hub ('Data Hub: Exchange System');<br>6. The data hub facilitates the metering data to the energy supplier ('Energy Supplier System');<br>7. The DSO may redefine the reading data profile at any time ('Configuration Data').<br><br>b) For requested meter readings:<br><br>1. The DSO requests meter read data from the Smart meter ('Measurement Data');<br>2. Smart meter registers meter reading along with time/date stamp ('Measurement Data');<br>3. Smart meter records meter reading data in its memory ('Measurement Data');<br>4. Smart meter displays the metering data in its meter display ('Measurement Data');<br>5. Smart meter sends meter reading data ('Measurement Data') to the Smart metering information system managed by the DSO ('IT DSO: Smart Metering Information system (AMI)'); |



**Classification level: Public**

| | |
|---|---|
| | 6. The DSO facilitates the metering data to the data hub ('Data Hub: Exchange System');<br>7. The data hub facilitates the metering data to the energy supplier ('Energy Supplier System');<br><br>**Scenario 2: Remote power switching**<br>a) Remote switch off<br>1) The energy supplier sends a remote switch off request (Switch Data') to the Data Hub, due to some regulated reason;<br>2) After authenticating and validating the control, the Data Hub sends the request to the correspondent DSO;<br>3) The DSO sends a remote switch off control ('Switch Data') to the Smart meter. The Smart meter can switch off the whole or part of the electrical supply to a household;<br>4) Whenever a request is not properly addressed by one of the actors, the sender should repeat it until it receives a successful acknowledge ('Monitoring Data') or a timeout, after a number of attempts;<br>5) The customer should be able to read at the Smart meter display ('Display') that it was subject to a remote switch off control;<br>6) The IT systems of the energy supplier, Data Hub and DSO should be updated accordingly.<br>b) Remote switch on<br>7) The energy supplier sends a remote switch on control to the Data Hub, due to some regulated motive;<br>8) After authenticating and validating the control ('Monitoring Data'), the Data Hub sends it to the correspondent DSO;<br>9) The DSO sends a remote switch on control to the Smart meter (from the 'IT DSO: Smart Metering Information system (AMI)');<br>10) Whenever a request is not properly addressed by one of the actors, the sender should repeat it until it receives a successful acknowledge ('Monitoring Data');<br>11) The customer should be able to read at the Smart meter display that it was subject to a remote switch on control;<br>12) The IT systems of the energy supplier, Data Hub and DSO should be updated accordingly. |



**Classification level: Public**

| | |
|---|---|
| | **Scenario 3: Outage management with Last Gasp**<br>1) Smart meters send a last gasp message ('Monitoring Data') to the DSO OMS, just before losing its power;<br>2) The OMS receives and adequate number of last gasp messages to be able to make an outage analysis;<br>3) The OMS automatically processes and analyses the information received, based on a real-time distribution network model ('Dynamic Network Topology Data'), to determine where the most probable fault location is ('Outage Data').<br>4) The DSO can send a repair crew to the probable location of the fault to enable a quick repair. The DSO is able to reduce costs, increases customer satisfaction, and reduce outage duration;<br>5) Connection between the DSO and a Trouble Call Centres enables Call Centre operators to give accurate information ('Fault Data') to other customer calling about the same fault.<br>6) Restoration is confirmed based on meter information ('Monitoring Data') sent to the DSO |
| Stakeholders/Actors | • Customer<br>• Distribution system operator that operates and maintains the Smart meter, collects the reading data and facilitates the data to the energy suppliers.<br>• Energy supplier the customer has contract with or an aggregator. |
| System and Information Assets | **Information assets:**<br>• Measurement Data<br>• Switch Data<br>• Configuration Data<br>• Monitoring Data<br>• Fault Data (incl. location)<br>• Outage Data<br>• Distribution network model<br>**System Assets**<br>• Smart Meter<br>• Display<br>• Actuator (Switch)<br>• Sensors<br>• Meter Data Concentrator<br>• IT DSO: Smart Metering Information system (AMI)<br>• SCADA<br>• Data Hub: Exchange System |



**Classification level: Public**

| | |
|---|---|
| | • Energy Supplier System<br>• Call Centres<br>• Outage Management System (OMS) |
| Assumptions and Constraints | • The Smart meter is capable of collecting and registering the metering data, and has the means to communicate with the Smart metering information system of the DSO.<br>• The customer has access to its metering data both from the Smart meter display and the energy supplier internet website.<br>• The DSO has means to communicate and control the metering functionalities of the Smart meter.<br>• The DSO, the energy supplier, Data Hub is aware when a failure has occurred. |

## 5.2 Load balancing renewable energy centrally

By central load balancing of renewable energy the DSO is able to balance the renewable energy supply to the demand, in a way such that regional congestion is avoided. The decision making is all done centrally, by the DSO SCADA system. The system is constantly acquiring data from the loads and generation units, and, if required, issues controls to the MV RTUs at the DER.

The functional architecture of use case 2, according to SGAM interoperability layers, is depicted below for future reference:



Classification level: Public

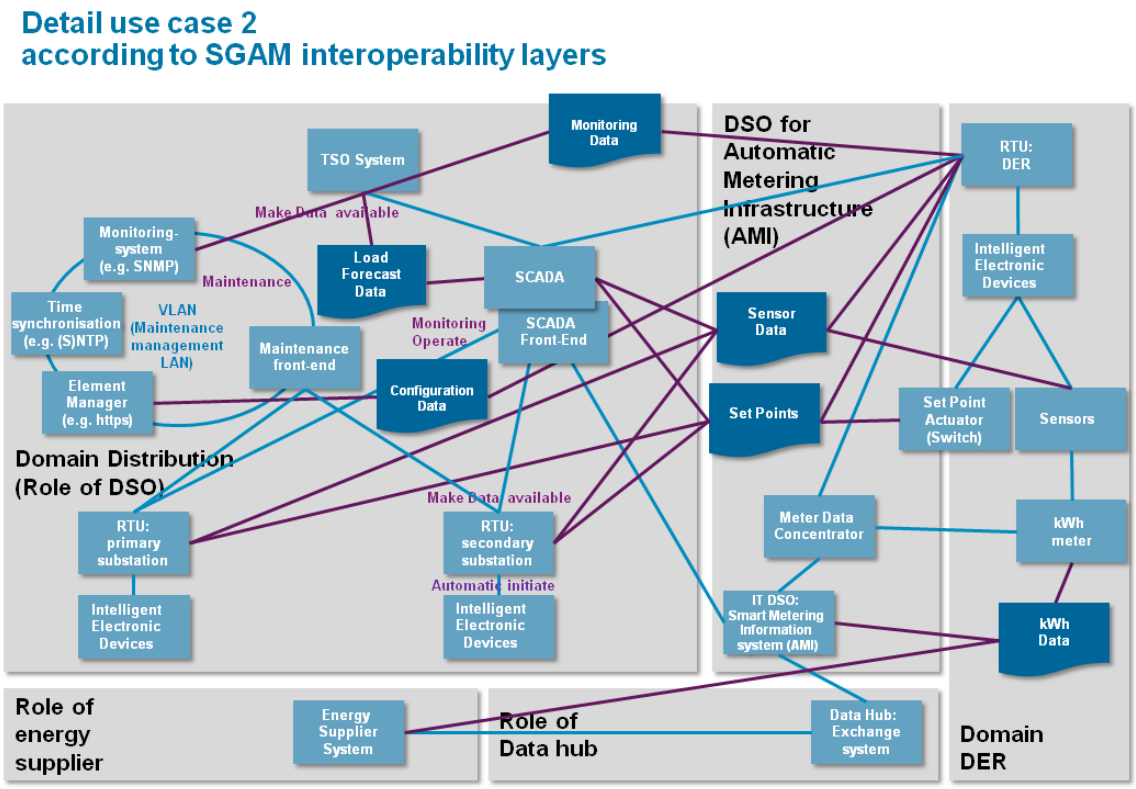


**Figure 15 - Functional architecture of use case 2: Load balancing renewable energy centrally**

The functional architecture of the different scenarios presented in use case 2, according to the SGAM zones, is depicted below for future reference:



**Classification level: Public**

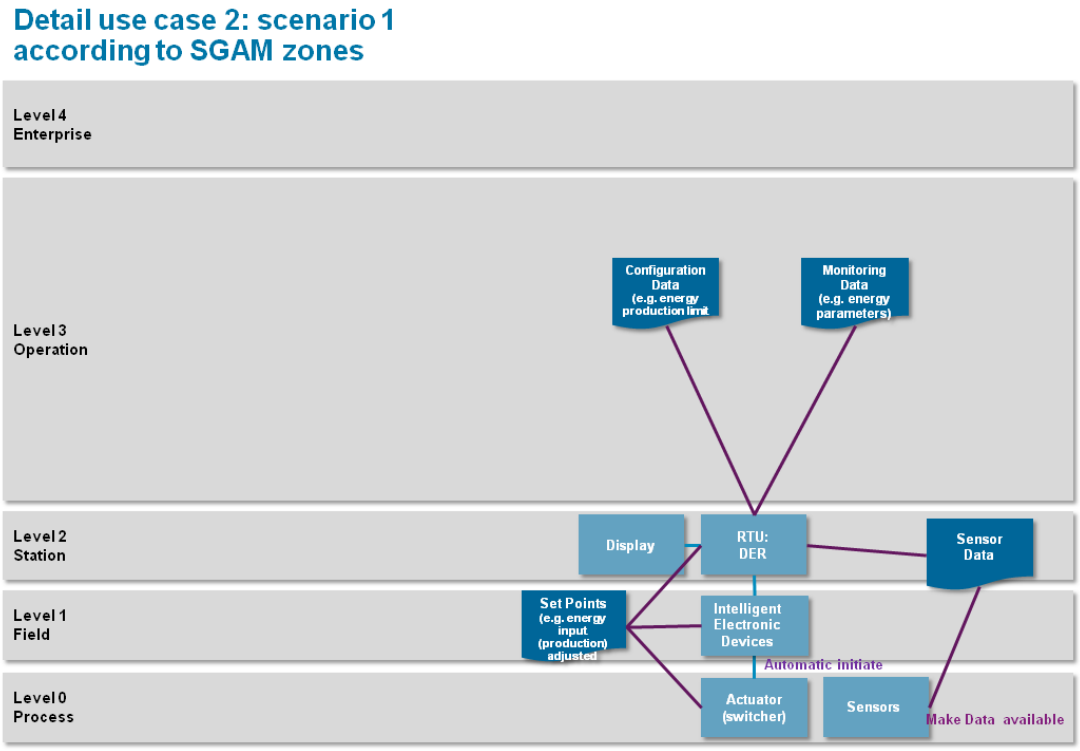


**Figure 16 - Functional architecture of scenario 1 of use case 2: Managing Power Quality (Voltage Control)**

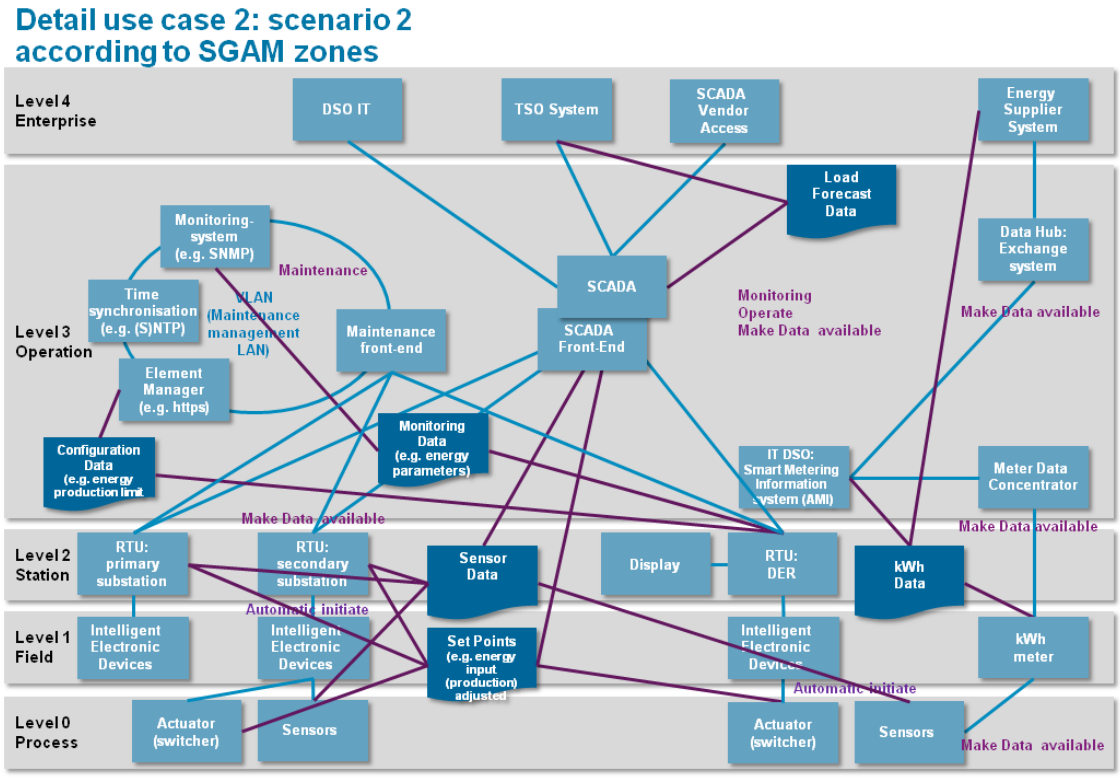


**Figure 17 - Functional architecture of scenario 2 of use case 2: Balancing MV renewable generation centrally**



Classification level: Public

In the table below, a description is given of the use case and each of its scenarios.

**Table 9: Use case 2 and the use case 2 scenarios**

| Use Case #2 | Load balancing renewable energy centrally |
|---|---|
| Description | Load balancing renewable energy is a way of automatically controlling distributed generation, to balance the renewable energy supply to the demand, in a way that regional congestion is avoided.<br>This capability allows:<br>a) Taking the most advantage of distributed generation to meet consumption needs;<br>b) Avoiding failures in the grid and thus, increasing the quality of service.<br>This specific use case refers to load balancing renewable energy centrally, where a head-end SCADA system is responsible for receiving and processing all the metering information, and decide whether to increase or decrease the MV Distribution Energy Resources (DER) generation, based on the demand. The decision making is made by the DSO.<br>Additionally, the SCADA system is also responsible for managing the quality of the energy supplied by the DER, ensuring it complies with regulation. |
| Flow | **Scenario 1: Managing Power Quality (Voltage Control)**<br>1. The DSO responsible for defining ('Load Forecast Data' and possibly 'Configuration Data') and controlling (actual 'Sensor Data', current 'Set Points' and other 'Monitoring Data') the generation power and the Power Quality parameters for the producer. The generated power ('Set Points') may be dynamic to limit the feed-in power.<br>2. The producer should be able to access the information of its facility by means of the HMI of its DER RTU, to know the current status of its operation (actual 'Sensor Data', current 'Set Points' and 'Monitoring Data') and the defined Power Quality parameters as well as the energy production limits (Set Points').<br>3. The parameters of the energy and power generated by the producers are monitored (actual 'Sensor Data', current 'Set Points' and other 'Monitoring Data') by the DSO. In case the quality parameters do not fit into the defined frame ('Load Forecast Data' and possibly 'Configuration Data') the reactions according to the strategy are applied ('Set Points');<br>In case the generated power limit ('Load Forecast Data' and possibly 'Configuration Data') is exceeded (by 'Sensor Data'), or |



Classification level: Public

| | |
|---|---|
| | the Power Quality parameters are not within the limits, the DSO reacts by adjusting the generation power ('Set Points') to bring the feed-in power or the Power Quality parameters according to the limit ('Load Forecast Data' and possibly 'Configuration Data') or by disconnecting the generation unit from the grid.<br><br>**Scenario 2: Balancing MV renewable generation centrally**<br>1. The DSO monitors (actual 'Sensor Data', current 'Set Points' and other 'Monitoring Data') the power generation and consumption of all the customers. This information is aggregated in the DSO SCADA system.<br>2. The SCADA system has information ('Load Forecast Data') about the forecast of the energy consumption and production for a specific period of time.<br>3. The SCADA system is constantly gathering information from the field (actual 'Sensor Data', current 'Set Points' and other 'Monitoring Data') and comparing it with the forecast ('Load Forecast Data'). The objective is to guarantee an as much as possible balanced system, by controlling both the demand and generation, to prevent destabilization of the grid.<br>a) Consumption lower than generation<br>4. According to the result of the analysis, almost in real time, if there is a technical constraint (difference between actual 'Sensor Data' and 'Load Forecast Data'), the DSO will send a new set point ('Set Points') to a set of RTUs through its SCADA system at the producers' premises, to reduce their power generation.<br>5. The RTUs will then interact with the generation facilities (Set Points'), to reduce their power generation.<br>b) Consumption higher than estimated<br>4. According to the result of the analysis, almost in real time, if the energy consumption is higher than what is expected (difference between actual 'Sensor Data' and 'Load Forecast Data'), the DSO will send a new set point ('Set Points') to a set of RTUs through its SCADA system at the producers' premises, to enable the increase of their power generation.<br>5. The RTUs will then interact with the generation facilities ('Set Points'), to increase their power generation.<br>6. All the information ('kWh data' that measure the production) related with the number of producers that were involved in any specific energy balancing activity (resulting in the 'Set Points') will be shared with the Data Hub. |



**Classification level: Public**

| | |
|---|---|
| | 7. The Data Hub is responsible for sharing this information ('kWh data' because of the 'Set Points') with the energy suppliers that will then act accordingly to the contractual terms they have with the producers. |
| Stakeholders/Actors | • Customer that produces and optionally consumes energy;<br>• Producer that owns a generation facility<br>• DSO responsible for operating the power grid and guarantee quality of service;<br>• Data Hub aggregates all the information relevant to the several energy supply chain stakeholders, and facilitates it accordingly.<br>• Energy supplier the customer has contract with. |
| System and Information Assets | **Information assets:**<br>• Sensor Data<br>• Load Forecast Data<br>• kWh Data<br>• Set Points<br>• Configuration Data<br>• Monitoring Data<br>**System Assets:**<br>• Intelligent Electronic Devices<br>• RTU: secondary substation<br>• RTU: primary substation<br>• SCADA front-end<br>• SCADA<br>• TSO System<br>• Access to TSO Data (ICCP)<br>• SCADA Vendor Access<br>• DSO IT<br>• Data Historian<br>• Maintenance front-end<br>• Element Manager (e.g. https, SSL/TLS)<br>• Time synchronization e.g. (SNTP)<br>• Monitoring system (e.g. SNMP)<br>• RTU: DER Meter<br>• Display<br>• Set Point Actuator (Switch)<br>• Meter Data Concentrator<br>• IT DSO: Smart Metering Information system (AMI)<br>• Data Hub: Exchange system<br>• Energy Supplier System |
| Assumptions and | • The customer is notified about Power Quality parameters |



**Classification level: Public**

| | |
|---|---|
| Constraints | and the energy production limits by its corresponding energy supplier or distribution system operator.<br>• The customer has means to monitor the Power Quality and to control the energy producing appliances.<br>• The DSO is actively monitoring the energy being generated by the MV distributed generation.<br>• The energy supplier has a contract with the producers, defining individual strategies related with the supply of energy to the grid.<br>• The DSO has the legal consent to actively manage the energy generation of the MV producers, according to a contractual agreement. |

## 5.3 Dynamic power management for smart homes, smart offices, electric vehicles

Dynamic Power Management is based on the use of flexibility in demand and supply. The device agent, controlling the customer loads, offers services such as “increase demand” or “decrease demand” to the central management system, which monitors the state of the grid at the supply side and might decide to use those services automatically or it might propose the usage of those services to the Grid Operators. This use case defines when and how these services can be used.

The functional architecture of use case 3, according to SGAM interoperability layers, is depicted below for future reference:



Classification level: Public

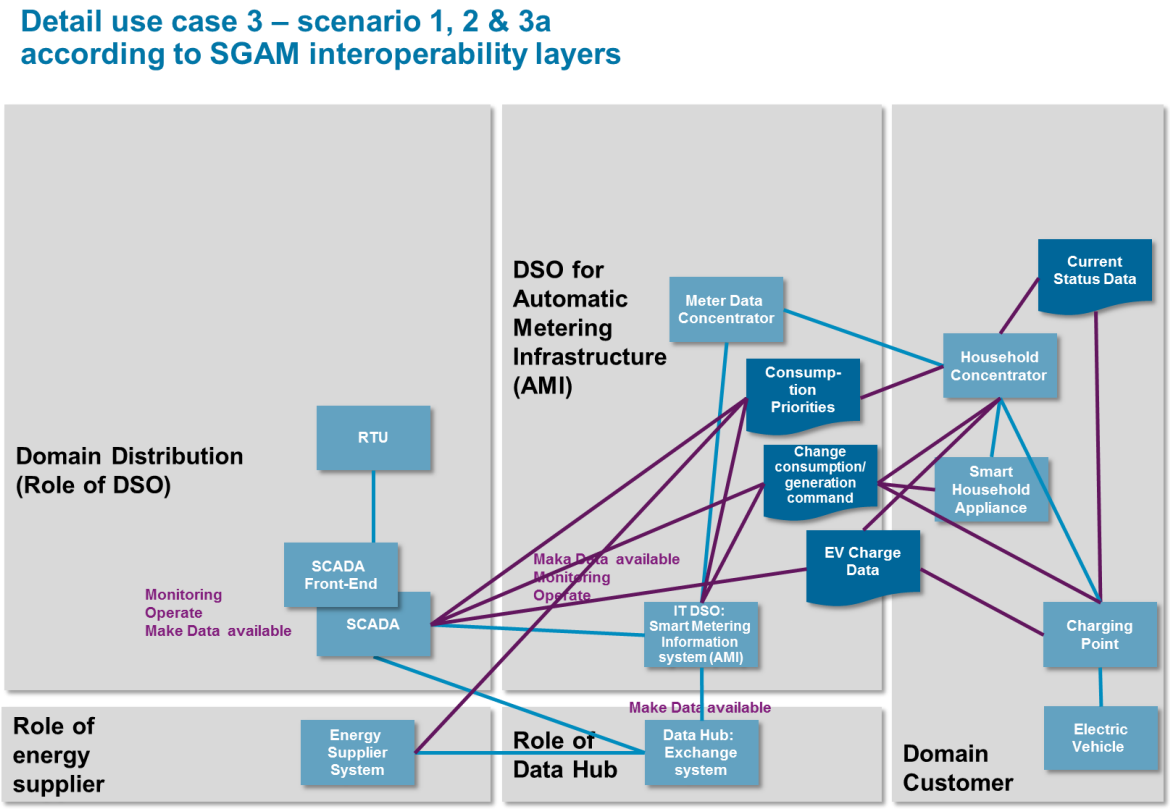


**Figure 18 - Functional architecture of use case 3: Dynamic power management for smart homes, smart offices, electric vehicles**

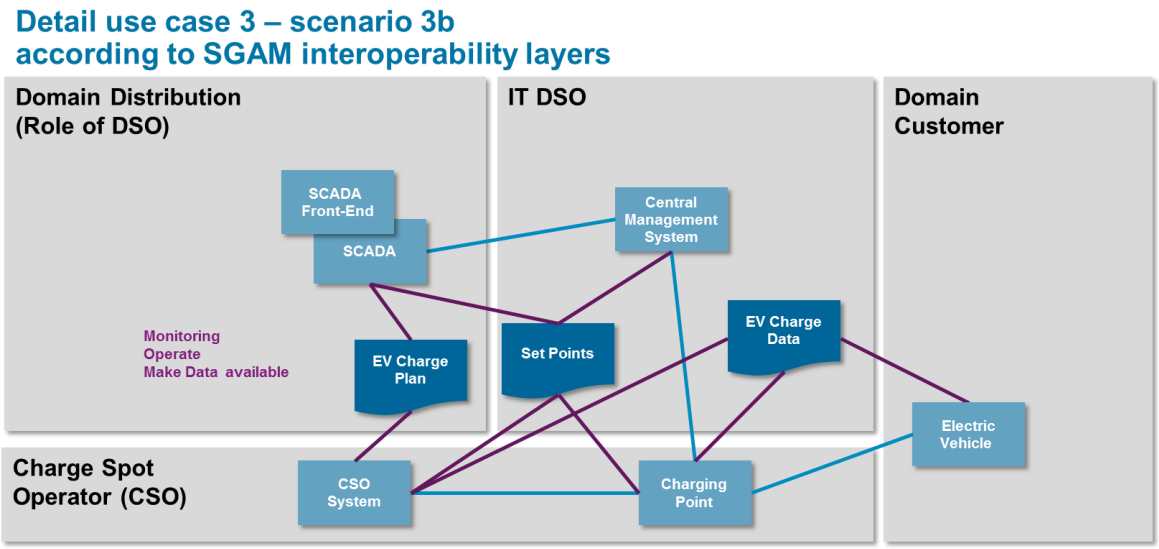


**Figure 19 - Functional architecture of use case 3: Dynamic power management for smart homes, smart offices, electric vehicles; Scenario 3: Optimized charging of EV b) At a public location**

The functional architecture of the different scenarios presented in use case 3, according to the SGAM zones, is depicted below on a single figure, for future reference:



**Classification level: Public**

In the table below, a description is given of the use case and each of its scenarios.

**Table 10: Use case 3 and the use case 3 scenarios**

| Use Case #3 | Dynamic power management for smart homes, smart offices, electric vehicles |
|---|---|
| Description | This use case refers to the capability of dynamically managing 1) controllable power storage devices, such as batteries in charging cars, and 2) controllable (smart) home appliances, such fridges or air conditioners, with the purpose of reshaping, to a small extension, the consumption profile of a given area.<br>The objective is to improve grid efficiency, hosting capabilities for DER and maintainability, by performing small changes in the configuration of the mentioned types of devices, when required and up/down to a given limit that must have been agreed with the customer at some point in time. |
| Flow | There is a signed contract between the energy supplier and the customer. The customer subscribes to a service which defines a set of devices at the customer's home that can be controlled by the distribution system operator to a certain extent, inside well-defined limits and in well-defined conditions. The customer also agrees to let the distribution system operator monitor and control these values for this specific purpose.<br>In the scenarios below the DSO has the role of an aggregator.<br><br>**Scenario 1: Centralized control of available loads**<br>1. The DSO continuously monitors the power grid and compares the collected data with predefined optimal and security values;<br>2. The DSO detects a deviation from the optimal and security values;<br>3. The DSO verifies that the grid presents the required capacity to compensate a part or all of it through Dynamic Power Management;<br>4. The DSO controls a group of customers' devices (i.e., air conditioners, refrigerator consumption levels, swimming pool heating system) in order to adjust its configurations to decrease demand ('Change consumption/generation command');<br>5. The Customer is informed (through individual notification and/ or monthly service usage report) that its services are being used (when, how, how much);<br>6. The Customer should not change the devices' configuration |



Classification level: Public

| | |
|---|---|
| | unless it is necessary to turn off the device or there is an urgent event;<br>7. The grid state returns to the optimal and secure values;<br>8. The DSO returns the customer's devices to their original configuration (before point 4) ('Change consumption /generation command');<br>9. The Customer is informed (through individual notification and/ or monthly service usage report) that its services are not being used anymore;<br>10. The DSO updates the customer's service usage data in the central systems.<br><br>**Scenario 2: Load shifting - Centralized control and automation of home appliances**<br>1. The customer configures a Smart Household Appliance to execute a given program: for instance, loading and trying to start a smart washing machine (changes the 'Current Status Data' towards the Household Concentrator);<br>2. The customer Household Concentrator is aware of peak and off-peak hours and schedules the program's execution to off-peak hours;<br>3. The customer Household Concentrator informs the DSO of the planned load ('Consumption Priorities', includes details on among others the load, estimated duration, planned start time, latest possible start time) and offers the execution of the program as a service to the DSO;<br>4. The DSO continuously monitors the power grid and compares the collected data with predefined optimal values. When the DSO sees consumption growing on its way to peak hours, the DSO verifies that the grid presents the required capacity to perform load shifting through Dynamic Power Management;<br>5. The central management system of the DSO uses the service offered by the customer's Smart Household Appliance. The Household Concentrator is asked to execute the program immediately or at a given schedule ('Change consumption/generation command');<br>6. The Customer is informed (through individual notification and/ or monthly service usage report) that its services will be used (when, how, how much);<br>7. The Customer should not change the devices' configuration unless it is necessary to turn off the device or there is an |



**Classification level: Public**

| | |
|---|---|
| | urgent event;<br>8. The DSO updates the customer's service usage data in the central systems.<br><br>**Scenario 3: Optimized charging of EV**<br>a) At a customer's household<br>1. A customer connects an electric vehicle to the charging point at his home;<br>2. The charging point has a number of possible charging configurations which differ in charging time and costs;<br>3. The charging point is configured when the vehicle must be ready for use and, therefore, it also knows when a charging program must be executed; it is also aware of the current time and peak and off-peak hours; with this information, it schedules the charging program execution to an optimized time (Charge Point informs the Household Concentrator of the preferred program using 'Current Status Data' and 'EV Charge Data');<br>4. The customer Household Concentrator/Charge Point offers the execution of the program as a service to the central management system ('Consumption Priorities' and 'EV Charge Data' includes details for example on the require EV energy demand, charge plan, duration, planned start time, latest possible start time);<br>5. The DSO continuously monitors the power grid and compares the collected data with predefined optimal values. The DSO estimates the future demand of EV charging based on received customer schedules and charging configurations (step 4); it also creates/ makes adjustments to a global EV scheduling model, which is used in the estimate calculations. The DSO creates a new and optimized global model and calculates the required configurations that must be applied to customer charging devices through Dynamic Power Management to optimize EV charging;<br>6. The DSO management system uses the service offered by the customer EV, i.e., the Charging Point is asked to execute the program immediately or at a given schedule and with a given configuration ('Change consumption/generation command');<br>7. The Customer is informed (through individual notification and/ or monthly service usage report) that its services will be |



**Classification level: Public**

| | |
|---|---|
| | used (when, how, how much);<br>8. The Customer should not change the devices' configuration unless it is necessary to turn off the device or there is an urgent event;<br>9. The DSO updates the customer's service usage data in the central systems.<br><br>b) At a public location<br>1. An electric vehicle (EV) arrives at a Charging Point at a public charge spot.<br>2. The driver identifies the EV at a Charge Spot Operator (CSO), which also collects EV-dependent information ('EV Charge Data').<br>3. Based on this data the CSO creates a charge plan for this EV ('EV Charge Plan') and submits the charge plan to the DSO for approval.<br>4. The DSO continuously monitors the power grid and compares the collected data with predefined optimal values. The DSO estimates the future demand of EV charging based on received EV Charge Plans. The DSO determines whether or not this charge plan (step 3) can be executed within local grid-capacity.<br>5. If the calculated charge plan can be executed, the DSO sends the command ('Set Point') to the CSO and the EV is charged according to the plan.<br>6. If the plan does not fit within all constraints, the DSO responds with a request for a new plan and provides information on the available capacity in the network segment and the EV identifiers of EVs of the CSO in the network segment.<br>The CSO determines new charge parameters and create a new charge plan ('EV Charge Plan'). It can do this based on negotiations with the requesting EV user or other EV's of even other CSO's. The new charge plan ('EV Charge Plan') is again submitted to the DSO for approval <go to step 4>.<br>7. The DSO updates the charging station's usage data in the central systems. |
| Stakeholders/Actors | • Consumer customer that agreed to let his devices be controlled by the DSO to a certain extent, inside well-defined limits and in well-defined conditions |



**Classification level: Public**

| | |
|---|---|
| | • DSO responsible for operating the power grid and guarantee quality of service<br>• Energy supplier the customer has contract with<br>• The Charge Spot Operator (CSO) operates and maintains a set of Charging Points for charging EVs. The CSO negotiates with the DSO on charging plans, according to customer demand and available capacity. |
| System and Information Assets | **System Assets:**<br>• Household Concentrator<br>• Smart Household Appliance<br>• Charging Point<br>• Smart Meter<br>• Display<br>• Sensors<br>• Actuator (switcher)<br>• Meter Data Concentrator<br>• IT DSO: Smart Metering Information system (AMI)<br>• RTU at substation<br>• SCADA<br>• SCADA Front-End<br>• TSO System<br>• Data Hub: Exchange system<br>• Energy Supplier System<br>• Electric Vehicle (EV)<br>**Information Assets:**<br>• Measurement Data<br>• Sensor Data<br>• Switch Data<br>• Change consumption/generation command<br>• Consumption Priorities<br>• Current Status Data<br>• Set points<br>• Monitoring Data<br>• Load Forecast Data<br>• Dynamic Network Topology Data<br>• EV Charge Data<br>• EV Charge Plan |
| Assumptions | • The customer agrees with the limits and conditions presented by the energy supplier or distribution system operator, which were adjusted to the customer's specific situation.<br>• The customer has a set of controllable devices. |



**Classification level: Public**

| | |
|---|---|
| | • The customer and energy supplier have a signed contract.<br>• The energy supplier has means to control the customer's devices.<br>• The customer has means to monitor the actions taken by the DSO.<br>• The customer has means to interrupt the service, given the occurrence of a predefined set of events. |

## 5.4 Load balancing renewable energy regionally (substation automation)

Load balancing renewable energy regionally is a way of control imposed by DSOs, to locally balance the renewable energy supply to the demand, to avoid congestion and/or local power quality problems like unacceptable voltage rise. The difference with Load balancing renewable energy centrally is that the control is shifted to automated subsystems. These automated systems could be on the scale of a primary MV substation or even on an underlying secondary MV/LV substation.

The functional architecture of use case 4, according to SGAM interoperability layers, is depicted below for future reference:

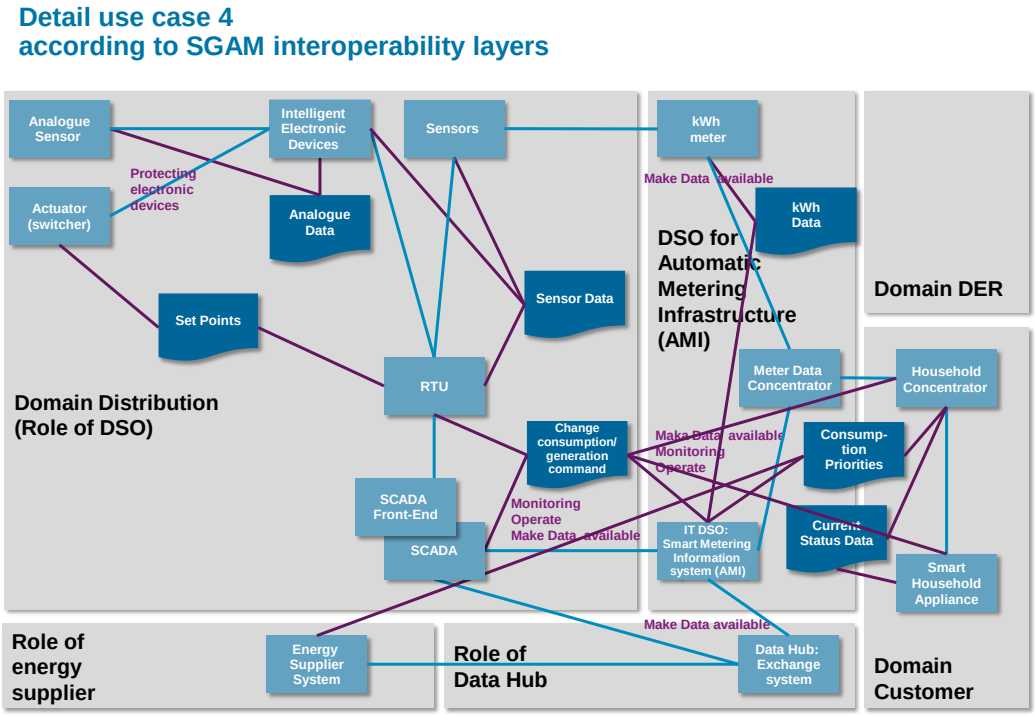


**Figure 20 - Functional architecture of use case 4: Load balancing renewable energy regionally (substation automation)**



Classification level: Public

The functional architecture of the different scenarios presented in use case 4, according to the SGAM zones, is depicted below for future reference:

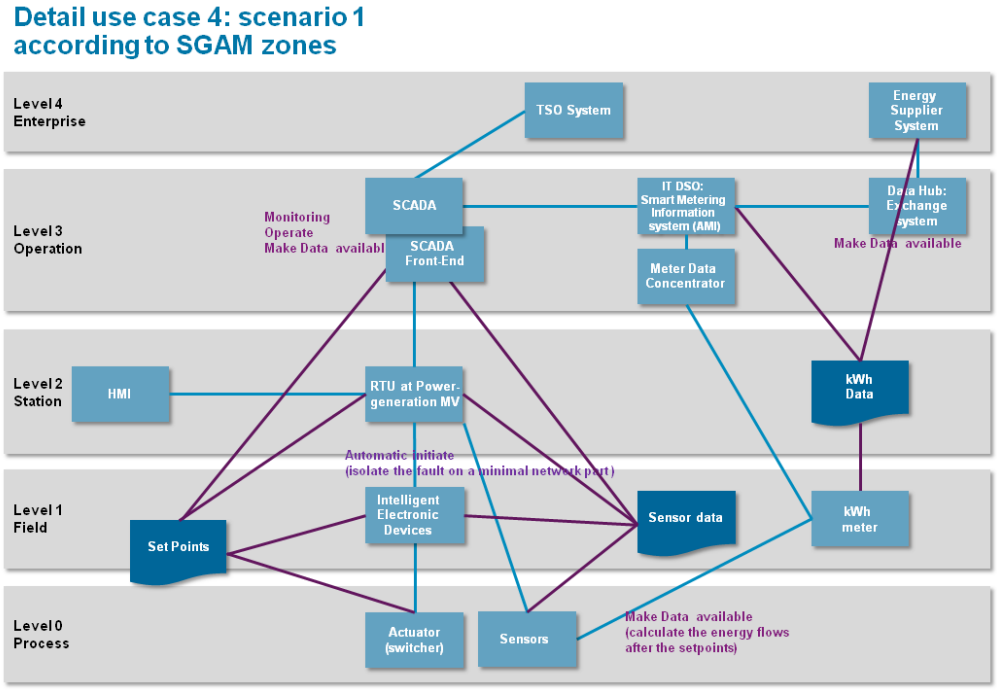


**Figure 21 - Functional architecture of scenario 1 of use case 4: Balancing MV renewable generation**

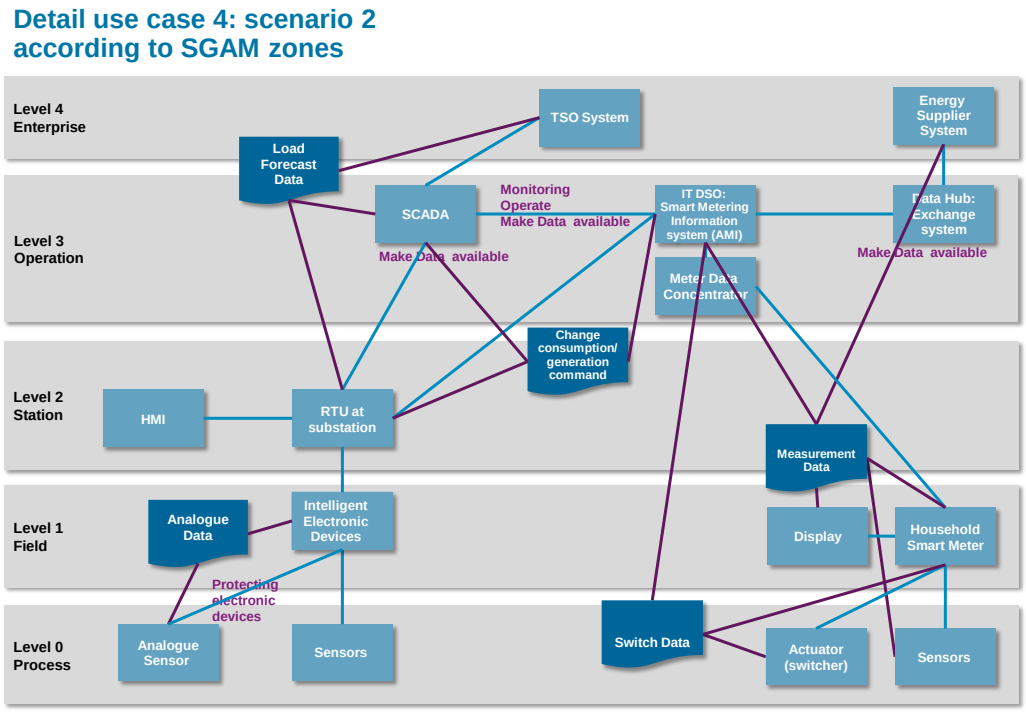


**Figure 22 - Functional architecture of scenario 2 of use case 4: Balancing LV renewable generation**



**Classification level: Public**

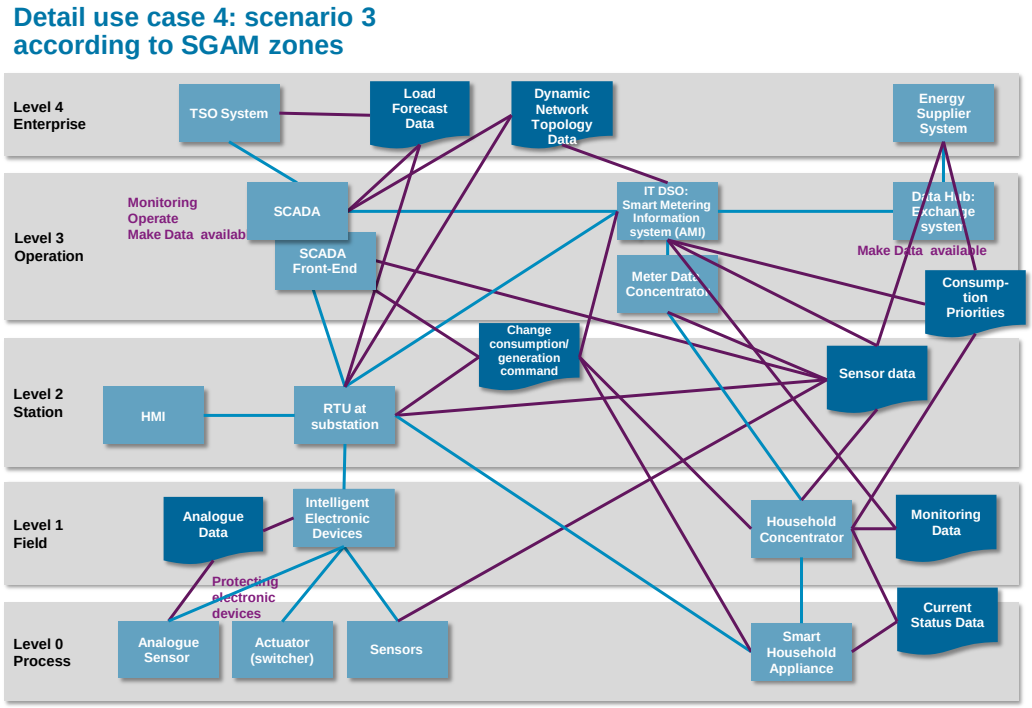


**Figure 23 - Functional architecture of scenario 3 of use case 4: Balancing LV energy consumption locally**

In the table below, a description is given of the use case and each of its scenarios.

**Table 11: Use case 4 and the use case 4 scenarios**

| Use Case #4 | Load balancing renewable energy locally |
|---|---|
| Description | Load balancing renewable energy is a way of automatically controlling and monitoring both the distributed generation and consumption, to balance the renewable energy supply to the demand, in a way regional congestion is avoided.<br>This capability allows:<br>a) Taking the most advantage of distributed generation to meet consumption needs;<br>b) Avoiding failures in the grid and thus, increases the quality of service.<br>This specific use case refers to load balancing renewable energy locally, to balance the renewable energy supply to the demand, to avoid congestion and/or local power quality problems like unacceptable voltage rise. The control is done by automated subsystems in the RTUs which, under the SEGRID reference architecture, are present on the scale of MV primary and secondary substations. |
| Flow | 1. The DSO monitors the power generation and consumption of all the customers. This information is aggregated at (primary and |



Classification level: Public

| | |
|---|---|
| | secondary substation level, at the DSO primary RTUs (most of all by 'Sensor Data').<br>2. The RTUs are constantly aware of the network topology ('Dynamic Network Topology Data') by supervision of circuit breaker status ('Fault Data: Breaker State Data') and gather information from all the loads that are connected to the substation and the generation facilities ('Feeder Data', 'Sensor Data' and 'Analogue Data').<br>3. Based on an energy forecast performed on a day-head basis ('Load Forecast Data'), with the estimated consumption for that substation, the centralized generation that will be injected by the HV/MV substation and the MV and LV distributed generation, the RTU is aware of the measuring values that should be gathering from all the distributed sensors (LV and MV generation and consumption meters, transformer sensing, measured active and reactive power, etc).<br>4. Considering that the transmission network will guarantee the supply on their side, if there is any deviation from the estimation both to demand or generation, the RTU will trigger one or more than one of the following energy balancing mechanisms:<br><br>**Scenario 1: Balancing MV renewable generation**<br>1. According to the result of the analysis, almost in real time, if the energy consumption is higher or lower than what is expected (based on data, but in this case related to 'Sensor Data'), the DSO will send a new set point ('Set Points') to a set of RTUs at the producers' premises, to either increase or decrease their power generation.<br>2. The RTUs will then interact with the generation facilities, to react accordingly to the DSO request (by means of 'Set Points').<br>3. Based on the contractual agreement with the energy supplier, the producers will be compensated ('kWh Data' because of the 'Set Points') for the service they are providing to the grid.<br>4. All the information ('kWh Data' because of the 'Set Points') related with the number of producers that were involved in any specific energy balancing activity will be shared with the Data Hub.<br>5. The Data Hub is responsible to share this information ('kWh Data' because of the 'Set Points') with the energy suppliers that will then act accordingly to the contractual terms they have with the producers. |



**Classification level: Public**

| | |
|---|---|
| | **Scenario 2: Balancing LV renewable generation**<br>1. According to the result of the analysis, almost in real time, if the energy consumption (based on many data, but in this case related to 'Measurement data') is lower than what is expected, the DSO will send a switch off order ('Switch Data') to the generation Smart meter at the producers' premises, to switch off its supply to the power grid.<br>2. Based on the contractual agreement with the energy supplier, the producers will be compensated for the service they are providing to the grid ('Measurement Data' because of the 'Switch Data').<br>3. All the information ('Measurement Data' because of the 'Switch Data') related with the number of producers that were involved in any specific energy balancing activity will be shared with the Data Hub.<br>4. The Data Hub is responsible to share this information ('Measurement Data' because of the 'Switch Data') with the energy suppliers that will then act accordingly to the contractual terms they have with the producers.<br><br>**Scenario 3: Balancing LV energy consumption locally**<br>1. The customer specifies the Consumption Priorities ('Consumption Priorities') for his Smart Household appliances.<br>2. The DSO sends a Change consumption/generation command ('Change consumption/generation command') to the customer and the Consumption Priorities are applied for his Smart Household appliances.<br>3. If the limitation does no longer exist the customer appliances operate in normal mode, i.e., the energy Consumption Priorities are not applied.<br>4. The customer may redefine the priorities at any time ('Consumption Priorities') and is informed about the current status ('Current Status Data').<br>5. All the information ('Sensor Data' because of 'Change consumption/generation command') related with the number of customers that were involved in any specific energy balancing activity will be shared with the Data Hub.<br>6. The Data Hub is responsible to share this information ('Sensor Data' because of 'Change consumption/generation command') with the energy suppliers that will then act accordingly to the |



**Classification level: Public**

| | |
|---|---|
| | contractual terms they have with the producers.<br>7. The RTUs at the primary and secondary substations will be responsible to manage all the different energy balancing mechanisms available (based on 'Sensor Data', but also on 'Breaker State Data', 'Feeder Data', 'Dynamic Network Topology Data' all resulting also in 'Load Forecast Data'), as well as the result of their implementation in the right balancing between supply and demand.<br>8. The compliance of the customers to the services required by the grid should be monitored ('Monitoring Data'), since they will carry contractual benefits to the customers. |
| Stakeholders/Actors | • Customer that consumes and optionally produces energy;<br>• DSO responsible for operating the distribution power grid and guarantee quality of service;<br>• Energy supplier the customer has contract with.<br>• Data Hub |
| System and Information Assets | **Information assets:**<br>• Analogue Data<br>• Sensor Data<br>• Measurement Data<br>• kWh Data<br>• Change consumption/generation command<br>• Consumption Priorities<br>• Current Status Data<br>• Set points<br>• Switch Data<br>• Monitoring Data<br>• Fault Data: Breaker State Data<br>• Sensor Data: Feeder Data<br>• Load Forecast Data<br>• Dynamic Network Topology Data<br>**System Assets:**<br>• Analogue Sensor<br>• Actuator (switcher)<br>• Sensors<br>• Intelligent Electronic Devices<br>• RTU at Power generation MV<br>• RTU at substation<br>• Short Circuit Indicators<br>• Feeder Protection<br>• HMI |



**Classification level: Public**

| | |
|---|---|
| | • kWh meter<br>• SCADA<br>• Access to TSO Data (ICCP)<br>• Smart Meter<br>• Display<br>• Household concentrator<br>• Smart Household Appliance<br>• Meter Data Concentrator<br>• IT DSO: Smart Metering Information system (AMI)<br>• Data Hub: Exchange system<br>• Energy Supplier System |
| Assumptions and Constraints | • The customer is notified about Power Quality parameters and the energy production limits by its corresponding energy supplier or distribution system operator.<br>• The customer has means to monitor the Power Quality and to control the energy producing appliances<br>• If the aggregator is involved, the customer's strategy can allow the aggregator to control the customer's energy production |

## 5.5 Automatic reconfiguration of the power grid

Automatic reconfiguration and self-healing in Smart Grids is a subject that is studied in European projects like Grid4EU [3] and fits in near future grids, however DSOs today are testing pilots of self-healing distribution grid, namely in MV grids with radial or ring typologies. The goal is to locate and isolate the fault through a network (re)configuration minimizing the number of affected customers and power parameters. This kind of systems uses an ICT layer with peer-to-peer communication between the involved substations. An interesting example is given in [4].

The functional architecture of use case 5, according to SGAM interoperability layers, is depicted below for future reference:



Classification level: Public

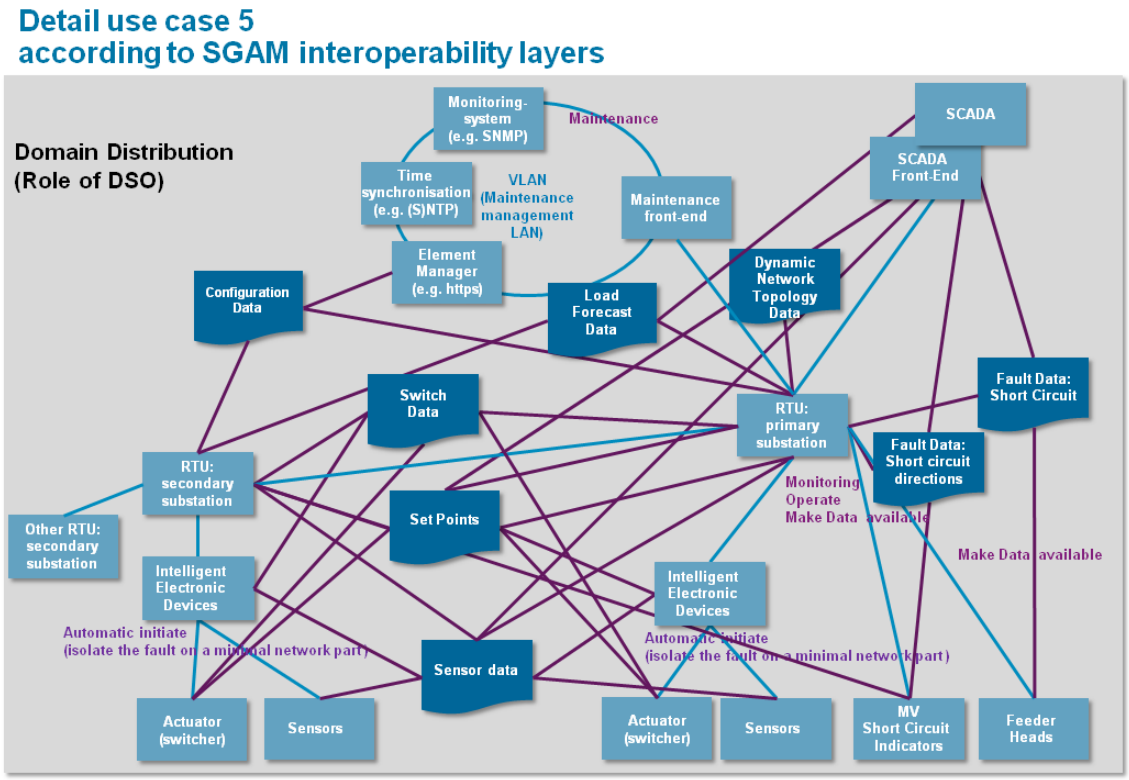


**Figure 24 - Functional architecture of use case 5: Automatic reconfiguration of the power grid**

The functional architecture of the different scenarios presented in use case 5, according to the SGAM zones, is depicted below for future reference:



**Classification level: Public**

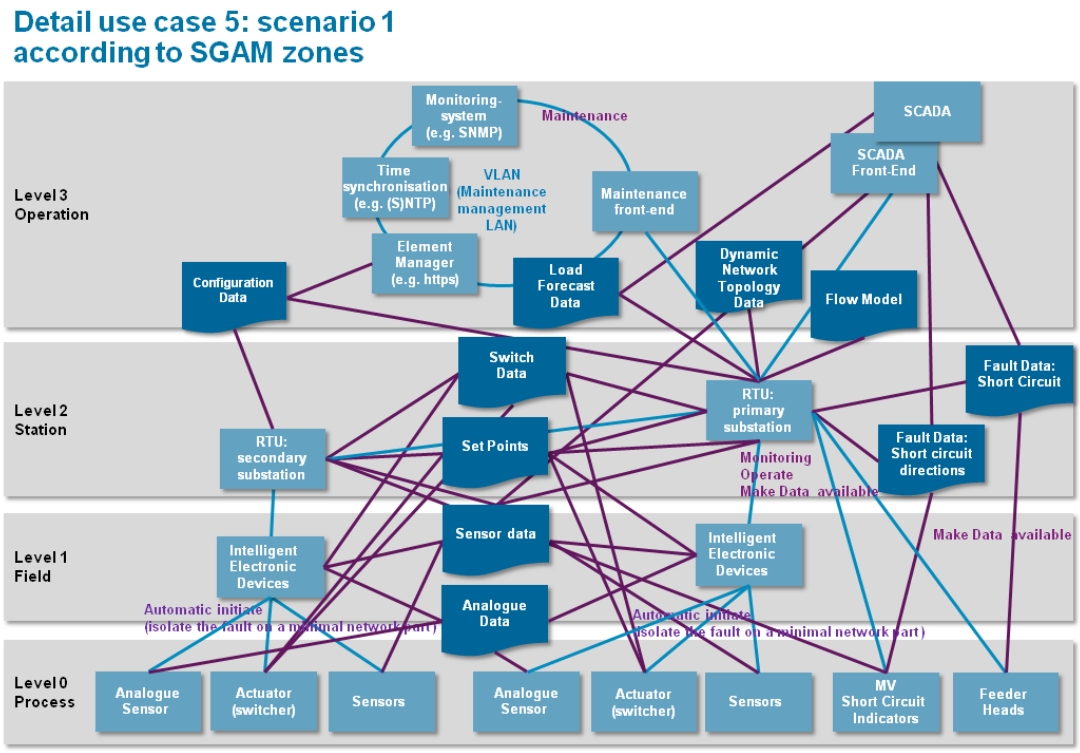


**Figure 25 - Functional architecture of scenario 1 of use case 5: Centrally decided isolation and restoration at faults in MV network**

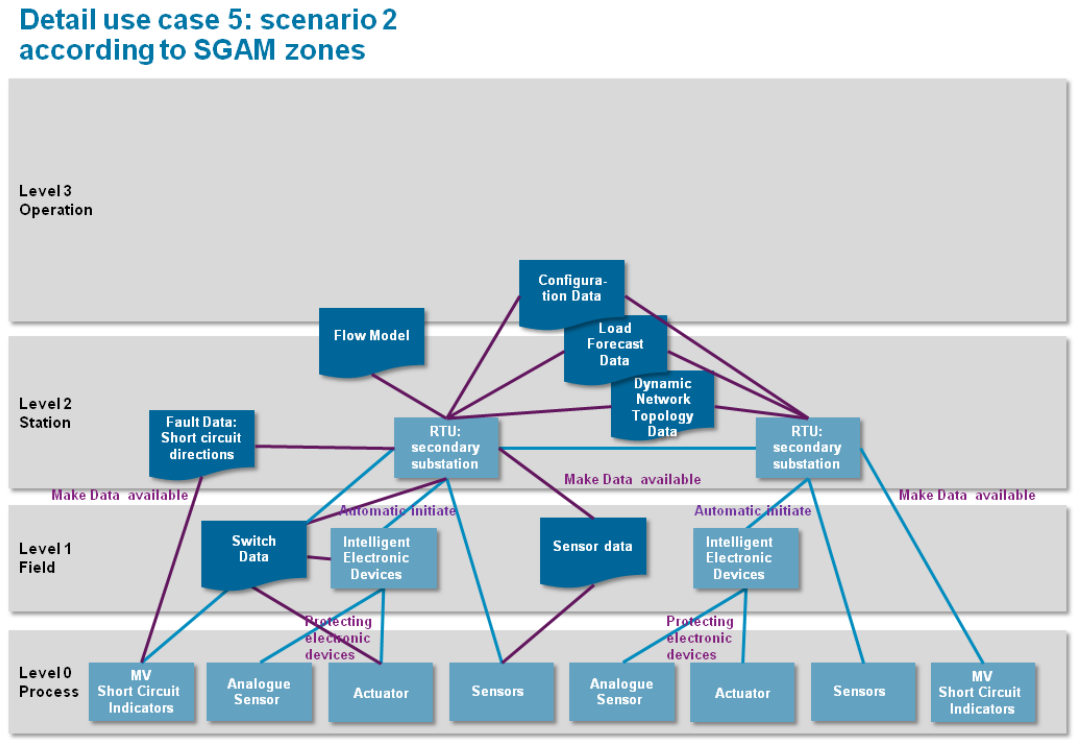


**Figure 26 - Functional architecture of scenario 2 of use case 5: Distributed isolation and restoration at faults in the MV network**



**Classification level: Public**

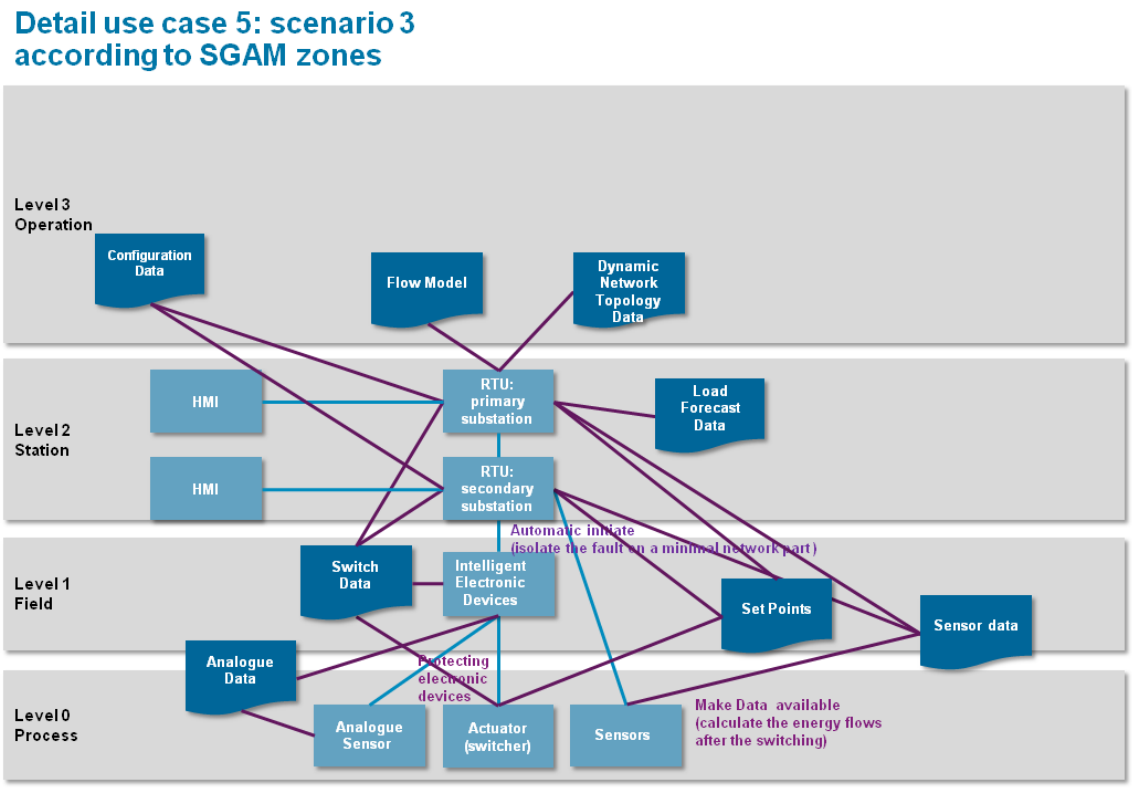


**Figure 27 - Functional architecture of scenario 3 of use case 5: Minimization of losses in the MV network using switching**

In the table below, a description is given of the use case and each of its scenarios.

**Table 12: Use case 5 and the use case 5 scenarios**

| Use Case #5 | Automatic reconfiguration of the power grid |
|---|---|
| Description | By increasing the monitoring level at MV grids, the DSO is able to identify and locate MV faults.<br>Furthermore, the accuracy of the fault identification and localization is higher and quicker, leading to faster repair or self-healing actions which will increase power quality and improve grid resilience.<br>Automatic reconfiguration might be done locally, when the local systems and automatisms have all the required information, or it might also require central systems' involvement, when more information is needed or when a higher level of coordination is required. Similarly, the need for reconfiguration might be identified locally, with locally originated information, or centrally, with information from the entire grid systems.<br>Self-healing mechanisms provide control procedures to reconfigure the MV grid so that any permanent grid fault would be automatically isolated and parts of the grid restored, enabling repair teams to step forward in line with all DSO safety procedures |



Classification level: Public

| | |
|---|---|
| | The objective is to improve the quality of service by decreasing power supply interruptions in terms of frequency and duration, at the same time minimizing the affected area. |
| Flow | **Scenario 1: Centrally decided isolation and restoration at faults in MV network**<br><br>If a fault occur in the MV network, e.g. a cable failure.<br><br>1. The distribution system operator (DSO) continuously monitors and controls the power grid, both centrally in the grid dispatch centres, and remotely through the use of automatisms.<br><br>2. The primary substation RTU monitors the MV grid parts under its responsibility and identifies parts of the network where a fault has occurred. The central RTU uses information from protection at Feeder Protection ('Fault Data: Feeder Data') and from short circuit indicators ('Fault Data: Fault Directions) placed in strategic positions, both bi-directional and uni-directional, to identify and locate faults.<br><br>3. The primary RTU knows the static topology of the MV grid ('Configuration Data') through import from an engineering system. Also line parameters, e.g. complex impedances ('Line Parameters (e.g. impedances) Data'), are imported from the engineering system which normally placed at the grid dispatch centre.<br><br>4. The primary RTU creates a dynamic topology model of the MV network based on the imported static topology and from circuit breaker states. At breaker state change a new dynamic topology model is calculated ('Dynamic Network Topology Data').<br><br>5. The primary RTU uses data from protection and short circuit indicators together with the dynamic topology of the network ('Dynamic Network Topology Data') to identify faulty equipment. The primary RTU will then try to isolate the fault on a smallest possible network part by opening load breakers at secondary substations and closing protection at primary substations ('Switch data'). Isolation can be done as recommendations to the operators at the central dispatch or by automatic commands by the primary substation RTU.<br><br>6. When the fault is isolated the primary RTU will try to re-energize as many customers as possible using back-feed, i.e. by closing normal opened breakers (NOP) in ring configurations ('Switch Data'). However, such an operation might lead to overloads on the back-feeding feeder so a Load Flow calculation ('Flow Model') must be performed to calculate the energy flows after the switching. In order to avoid unnecessary switching a |



**Classification level: Public**

| | |
|---|---|
| | short term load forecast is included is used by the Load Flow calculation to also calculate the load flows in the short term future (a few hours) (all 'Load Forecast Data').<br>7. During all these steps information is sent to central dispatch that can activate or de-activate the automatic reconfiguration function ('Configuration Data').<br><br>**Scenario 2: Distributed isolation and restoration at faults in the MV network**<br>1. In the locally and distributed decided scenario the smaller RTUs of each secondary substation will decide the dynamic topology of the MV network by questioning its neighbouring substations. To do this a peer-to-peer communication between secondary substations is used. By combining the information received in each substation and sending it to all other substations that are included in the supervised network a dynamic topology model can be created that is known to all secondary substation RTUs ('Dynamic Network Topology Data').<br>2. If the configuration is changed by switching ('Switch Data'), i.e. new neighbours occur, or disappear, for one or more substations, the topology model is updated for all substations ('Dynamic Network Topology Data').<br>3. With this information available in in all substations, each of the substations can decide by itself to open or close load breakers ('Switch Data') under its control in order to isolate faults in network parts and/or restore energized sections. This is done without using any central system. It is a self-healing network.<br>4. Line impedances ('Line Para-meters (e.g. impedances) Data') are imported to each secondary RTU in advance. In this way each of the secondary RTUs can calculate the real-time Load Flow before and after restoration switching ('Load Forecast Data').<br><br>**Scenario 3: Minimization of losses in the MV network using switching**<br>1. The RTU in the primary substation receives information about the static topology ('Configuration Data') and line parameters, e.g. impedances, ('Line Parameters (e.g. impedances) Data') from a central engineering system where all data of the MV grid is defined.<br>2. All RTUs in the secondary substations communicates with the RTU in the primary substation and send real-time information |



**Classification level: Public**

| | |
|---|---|
| | about currents, active and reactive power, phase angels and voltages ('Sensor Data') plus digital information about load breaker states ('Digital Data').<br>3. Based on this information the RTU in the primary substation calculates a dynamic topology state ('Dynamic Network Topology Data') plus an optimal power flow ('Flow Model') with minimal losses and optimal voltage profiles.<br>4. The primary substation RTU also includes a forecast function that can predict loads in the short term future ('Load Forecast Data'). Based on the forecasted loads the primary substation RTU calculates load flows for the short term future with and without switching.<br>5. The primary RTU decides if a switching ('Switch Data') shall be performed in order to reach a more optimal load flow state, also considering short term forecasted load changes ('Load Forecast Data').<br>6. The switching ('Switch Data') can either be recommended to the operators in the central dispatch centre or executed automatically. |
| Stakeholders/Actors | DSO |
| System Assets and Information Assets | **Information assets:**<br>• Sensor Data<br>• Set points<br>• Switch Data<br>• Fault Data: Breaker State Data<br>• Fault Data: Feeder Data<br>• Configuration Data: Line Parameters (e.g. impedances)<br>• Dynamic Network Topology Data<br>• Flow Model<br>• Load Forecast Data<br>• Configuration Data<br>**System Assets:**<br>• Actuator (switcher)<br>• Sensors<br>• Intelligent Electronic Devices<br>• RTU: secondary substation<br>• RTU: primary substation<br>• HMI<br>• Short Circuit Indicators<br>• Feeder Protection<br>• SCADA front-end<br>• SCADA |



**Classification level: Public**

| | |
|---|---|
| | • View on TSO Systems<br>• Maintenance front-end<br>• Element Manager (e.g. https)<br>• Time synchronization e.g. (S)NTP<br>• Monitoring system (e.g. SNMP) |
| Assumptions and Constraints | Technical constraints:<br>• An engineering system from where static topology and line parameters are imported<br>• Isolation and restoration logic in primary and secondary RTUs<br>• Circuit breakers that can be controlled<br>• Measuring sensors<br>• Short term load forecasting functionality<br>• Dynamic topology calculations and Load Flow capabilities<br>Other assumptions:<br>• It is possible to remotely control the grid.<br>• The grid already presents a level of automation. |



**Classification level: Public**

# 6 Glossary

This glossary serves as inventory of technical terms and abbreviations used in the document. For detailed background information on cryptographic primitives or testing procedures we refer to the referenced literature.

| | |
|---|---|
| **CEN** | European Committee for Standardization. |
| **CENELEC** | European Committee for Electrotechnical Standardization. |
| **CSO** | Charge Spot Operator. |
| **DC** | Data Concentrator. |
| **DER** | Distributed Energy Resources |
| **DMS** | Distribution Management System. |
| **DSO** | Distribution System Operator. |
| **Dx.y** | Deliverable x.y |
| **EMS** | Energy Management System. |
| **EMSP** | E-Mobility Service Provider. |
| **ETSI** | European Telecommunications Standards Institute. |
| **EV** | Electric Vehicle. |
| **G3** | Alliance for PLC technology. |
| **GIS** | Geographical Information System. |
| **GPRS** | General Packet Radio Service. |
| **GUI** | Graphical User Interface. |
| **HAN** | Home Area Network. |
| **HES** | Head-End System. |
| **HMI** | Human Machine Interface. |
| **HV** | High Voltage. |
| **IEC** | International Electrotechnical Commission (ISO). |
| **IED** | Intelligent Field Device. |
| **ISO** | International Organization for Standardization. |
| **LAN** | Local Area Network. |
| **LN** | Local Network. |
| **LV** | Low Voltage. |
| **MDMS** | Meter Data Management System. |
| **Meter** | The term “meter” refers unless stated otherwise to the electricity meter. When necessary the document distinguishes between electricity meter and utility meter. |
| **MV** | Medium (level) Voltage. |
| **micro-CHP** | Micro combined heat and power. |
| **NN** | Neighbouring Network. |
| **OMS** | Outage Management System |
| **OSCP** | Open Smart Charging Protocol |
| **OSGP** | Open Smart Grid Protocol |
| **OSI model** | The ISO Basic Reference Model for Open Systems Interconnection. |



**Classification level: Public**

| | |
|---|---|
| **PLC** | Power Line Communication. |
| **PQ** | Power Quality |
| **PV** | Photovoltaic |
| **RTU** | Remote Terminal Unit. |
| **SCADA** | Supervisory Control and Data Acquisition. |
| **SE** | Secure Element. |
| **SEGRID** | *S*ecurity for smart *E*lectricity *GRID*s. |
| **SGAM** | Smart Grid Architecture Model. |
| **SG-CG** | Smart Grids Coordination Group (ETSI). |
| **SMITP** | Smart metering Information and Telecommunication Protocol. |
| **TSO** | Transmission System Operator. |
| **Tx.y** | Task w.y |
| **UMTS** | Universal Mobile Telecommunications System |
| **Utility meter** | Meter for, e.g., power, gas, water, and heat consumption. |
| **WAN** | Wide Area Network. |
| **WPx.y** | Work Package x.y |
| **3G / 4 G** | Third/ Forth generation mobile communication. |



**Classification level: Public**

# 7 References


[1] The German Feed-In Tariff: Recent Policy Changes, Deutsche Bank, September 2012

[2] VDE-AR-N4105 and DIN V VDE 0126-1-1/A1

[3] Grid4EU, A Large-scale demonstration project of advanced smart grids solutions with wide replication and scalability potential for Europe. A European Smart Grid project under EC FP7 Research Program. http://www.grid4eu.eu/

[4] E. Coster, W. Kerstens and T. Berry; Self Healing Distribution Networks Using Smart Controllers; CIRED; 22nd International Conference on Electricity Distribution; Stockholm, 10-13 June 2013.

[5] IEC 61850, a standard for the design of electrical substation automation and it is a part of the International Electrotechnical Commission's (IEC) Technical Committee 57 (TC57) reference architecture for electric power systems.

[6] IEC 60870-5 is one of the IEC 60870 set of standards which define systems used for telecontrol (supervisory control and data acquisition) in electrical engineering and power system automation applications. Part 5 provides a communication profile for sending basic telecontrol messages between two systems, which uses permanent directly connected data circuits between the systems.

[7] IEC 61970 series of standards deals with the application program interfaces for energy management systems (EMS). The series provides a set of guidelines and standards to facilitate:

- The integration of applications developed by different suppliers in the control center environment;
- The exchange of information to systems external to the control center environment, including transmission, distribution and generation systems external to the control center that need to exchange real-time data with the control center;
- The provision of suitable interfaces for data exchange across legacy and new systems.

[8] ISO/IEC 7498-2:1989, Information Processing Systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture, ISO, Switzerland.

[9] M/441 EN; "Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability"; European Commission Directorate-General For Energy; Brussels; 12th March 2009.

[10] M/490 EN; "*Smart Grid Mandate Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment*"; European Commission Directorate-General For Energy; Brussels; 1st March 2011.




**Classification level: Public**

[11] http://www.cl.cam.ac.uk/~rj4/Papers/meters-offswitch.pdf

[12] http://www.nema.org/Storm-Disaster-Recovery/Smart-Grid-Solutions/Pages/Smart-Meters-Can-Reduce-Power-Outages-and-Restoration-Time.aspx

[13] http://www.nema.org/Storm-Disaster-Recovery/Smart-Grid-Solutions/Pages/Smart-Meters-Can-Reduce-Power-Outages-and-Restoration-Time.aspx

[15] https://www.smartgrid.gov/

[14] http://wwwenergynetworks.org/modx/assets/files/electricity/futures/smart_meters/ENA_requirements_for_electricity_smart_meters_V2_220410/pdf

[16 ] CEN-CENELEC-ETSI. Functional reference architecture for communications in Smart metering systems. Technical Report 50572. December 2011.

[17] CEN-CENELEC-ETSI Smart Grid Coordination Group. First Set of Standards, November 2012.

[18] CEN-CENELEC-ETSI Smart Grid Coordination Group. Smart Grid Reference Architecture, November 2012.

[19] CEN-CENELEC-ETSI Smart Grid Coordination Group. Smart Grid Information Security, December 2014.

[20 ] ENISA Smart Grid Security – Report on recommendations for Europe and Member States, 2012.

[21] ENISA Smart Grid Security – Annex 2 to Report on recommendations for Europe and Member States: Security aspects of Smart Grids, 2012.

[22] ENISA Smart Grid Security – Annex 5 to Report on recommendations for Europe and Member States: Related initiatives, 2012.

[23] ENISA – Technical Guidance on security measures, version 2.0, October 2014.

[24] NIST – Framework for improving critical infrastructure cybersecurity, version 1.0, February 2014.

[25] NIST – NISTIR 7628: Guidelines for Smart Grid Cybersecurity – Volume 1: Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements, revision 1, September 2014.

[26] NIST – Special publication 1108r3: NIST Framework and Roadmap for Smart Grid Interoperability Standards, release 3.0, September 2014.

[27] CEN/CENELEC/ETSI SGCG – Smart Grid Information Security intermediate report, version 1, December 2014.



**Classification level: Public**

[28] CEN/CENELEC/ETSI SGCG – Smart Grid Information Security, November 2012.

[29] IEC 62351 is a standard developed by WG15 of IEC TC57. This is developed for handling the security of TC 57 series of protocols including IEC 60870-5 series, IEC 60870-6 series, IEC 61850 series, IEC 61970 series & IEC 61968 series. The different security objectives include authentication of data transfer through digital signatures, ensuring only authenticated access, prevention of eavesdropping, prevention of playback and spoofing, and intrusion detection



**Classification level: Public**