D3.2 – Overall System Requirements and Functional Specifications

Document ID:	SEMIAH-WP3-D3.2-v1.02
Document version:	Rev. 1.02
Document status:	Final
Dissemination level:	PU
Deliverable number:	D3.2
Deliverable title:	Overall System Requirements and Functional Specifications
WP number:	WP3
Lead beneficiary:	AU
Main author(s): (Listed alphabetically after first name.)	Dominique Gabioud (HES-SO), Erdődi László (UiA), Gillian Basso (HES-SO), Harald Unander (DEVO), Karl Werlen (MIS), Nils Ullveit-Moe (UiA), Rune H. Jacobsen (AU, editor), Stefan Funk (MIS), Stefan Siegel (FRAUNHOFER), Terje Gjøsæter (UiA).
Nature of deliverable:	R
Delivery date from Annex 1:	M6
Actual delivery date:	01.04.2015
Funding scheme / call:	STREP-FP7-ICT-2013-11
Project / GA number:	619560
Project full title:	Scalable Energy Management Infrastructure for Aggregation of Households
Project start date:	01/03/2014
Project duration:	36 months

Funded by the European Union

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 619560.

Executive Summary

This deliverable is the result of Task 3.1: Requirement analysis and Task 3.2: Definition of the overall architecture and system design of the SEMIAH project. The deliverables provides the set of requirements for the SEMIAH system as well as a high level system architecture, system model, and system design.

The report introduces the methodology chosen in the SEMIAH project for the high-level system design. The project uses the key concept of user stories to capture the functional requirements. User stories are key building blocks of agile and iterative development methods. Non-functional requirements are described in two areas of particular importance to SEMIAH. These are scalability requirements and requirements for security & privacy. The latter set of requirements is accompanied by a number of abuser stories in accordance with the chosen methodology.

Furthermore, the deliverable introduces as set of models to describe the SEMIAH system. The domain model puts SEMIAH into the concept of aggregated demand response and its relationship with the electricity wholesale markets. It introduces the *aggregator* role and links it to flexible consumption provided by prosumers who become SEMIAH members. Furthermore, actors and stakeholders of SEMIAH are introduced.

The SEMIAH system model provides an abstract description of the SEMIAH system. The system model introduces three distinct layers to provide means for generalizations of device, information objects, communications etc. The *IoT (Internet of Things) layer* has to role of providing an abstraction for field devices deployed in households. The *SEMIAH Objects layer* manages SEMIAH specific objects such as e.g., information objects. The *SEMIAH Control layer* has the role to control SEMIAH objects according to actors' requirements. As an example this could be the actuation of an appliance that is operated to provide flexibility for a household. In addition, the threat and the trust model used in security assessment effort are used to conceptualize security and privacy needs.

A first interaction of the SEMIAH system architecture is presented in the deliverable. The architecture is put into the context of smart grid standardization and smart grid architecture. A mapping between SEMIAH and the SGAM is provided. Other relevant architectures such as the IEEE 2030 standard for smart grid interoperability as well as the IoT reference architecture are discussed.

The technical architecture of SEMIAH provides a logical framework for the integration of components to form the SEMIAH infrastructure developed in work package 4 (WP4). It established the interfaces of interacting entities in the SEMIAH system. The hearth of the architecture is the Generalize Virtual Power Plants that can control the Home Energy Management System (HEMS) of the households of SEMIAH members. Decision support is provided through a provider interface to a set of algorithms that provides forecasting, aggregation and scheduling support developed in the project. These algorithms are key contributions of WP5. This interface is also used by existing components i.e., the EnergyOn platform from Misurio to provide an adaptation to the electricity wholesale market. The discussion ends with an introduction of two key components of the possible instantiations of the SEMIAH technical architecture. These are the virtual power plant component from Fraunhofer IWES – the IWES.vpp – and the EnergyOn platform from Misurio.

Abbreviations

AMI	Advanced Metering Infrastructure
API	Application Programming Interface
ARPU	Average Revenue Per User
AWS	Amazon Web Services
CEM	Customer Energy Manager
CEMS	Customer Energy Management System
CERT	Computer Security Incident Response
CHP	Combined Heat and Power
CIM	Common Information Model
CoAP	Constrained Application Protocol
CSIRT	Computer Security Incident Response Team
D	Deliverable
DER	Distributed Energy Resource
DoS	Denial of Service
DoW	Description of Work
DR	Demand Response
DSM	Demand Side Management
DSO	Distribution System Operator
EC	European Commission
EMG	Energy Manager Gateway
EMS	Energy Management System
ENISA	European Network and Information Security Agency
ESCO	Energy Service Company
FO	Flexibility Operator
FTP	File Transfer Protocol
GSI	Global Standards Initiative
GSM	Global System for Mobile Communications
GVPP	Generic Virtual Power Plant
HAN	Home Area Network
HEMS	Home Energy Management System
HES	Head End System
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
IaaS	Infrastructure as a Service
ICT	Information Communication Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institutes of Electrical and Electronics Engineers

IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSO	Internet Protocol for Smart Objects Alliance
IoT	Internet of Things
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
KNX	Konnex (KNX). Formerly known as European Installation Bus (EIB)
LNAP	Local Network Access Point
LTE	Long-Term Evolution (4G)
M2H	Machine to Human
M2M	Machine to machine
MDM	Meter Data Management
MDS	Model Driven Security
MLS	Multiple Levels of Security
MPC	Model Predictive Control
NASA	National Aeronautics & Space Administration
NIST	National Institute of Standards
NNAP	Neighbourhood Network Access Point
OASIS	Organization for the Advancement of Structured Information Standards
OGEMA	Open Gateway Energy MAnagement
PaaS	Platform as a Service
PBI	Product Backlog Items
PEV	Plug-in Electric Vehicle
PII	Personally Identifiable Information
RES	Renewable Energy Sources
REST	Representation State Transfer
RFID	Radio Frequency Identification
SCADA	Supervisory Control And Data Acquisition
SEMIAH	Scalable Energy Management Infrastructure for Aggregation of Households
SGAM	Smart Grid Architectural Model
SGCP	Smart Grid Connection Point
SOA	Service-oriented Architecture
SQL	Structured Query Language
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TOU	Time-of-Use Tariffs
TSO	Transmission System Operator
UCMR	Use Case Management Repository
UML	Unified Modelling Language

UMTS	Universal Mobile Telecommunications System
URI	Universal Resource Identifier
VMM	Virtual Machine Monitors
VPP	Virtual Power Plant
W3C	World Wide Web Consortium
WGFSS	Working Group First Sets of Standards
WP	Work Package
WT	Work Task
XACML	eXtensible Access Control Markup Language
XML	eXtendible Markup Language

Contents

List of Figures

List of Tables

1 Introduction

1.1 Scope

This deliverable is the result of Task 3.1: Requirement analysis and Task 3.2: Definition of the overall architecture and system design of the SEMIAH project. The deliverables provides the set of requirements for the SEMIAH system as well as a high level system architecture, system model, and system design. The deliverable puts requirements and system design into the context of European smart energy grid development and standardisation.

1.2 Methodology

This section describes the methodology used in work package 3 (WP3) to derive systems requirement and system architecture.

The overall process for WP3 work is depicted in Figure 1. The tasks are described below the figure. The figure presents a simplified process with focus on what kind of artefacts or description types that should be produced. Although the figure describes a sequential process, it should be interpreted as being iterative and with an increasing level of detail and precision as we get closer to the delivery date. The main input artefact to the process is mainly the SEMIAH Description of Work (DOW).

The result of the process will be collected and described in this document. The process has been depicted with free to use Bizagi BPMN modelling tool [2]. This tool has a low entry barrier for new users, and it can export and publish documentation and logical models in various formats.

It is proposed that the domain model, conceptual system model and use cases can be based on the Smart Grid Architecture Model (SGAM) framework and use cases as described in [1], chapter 7 (p.18): Main guidelines.

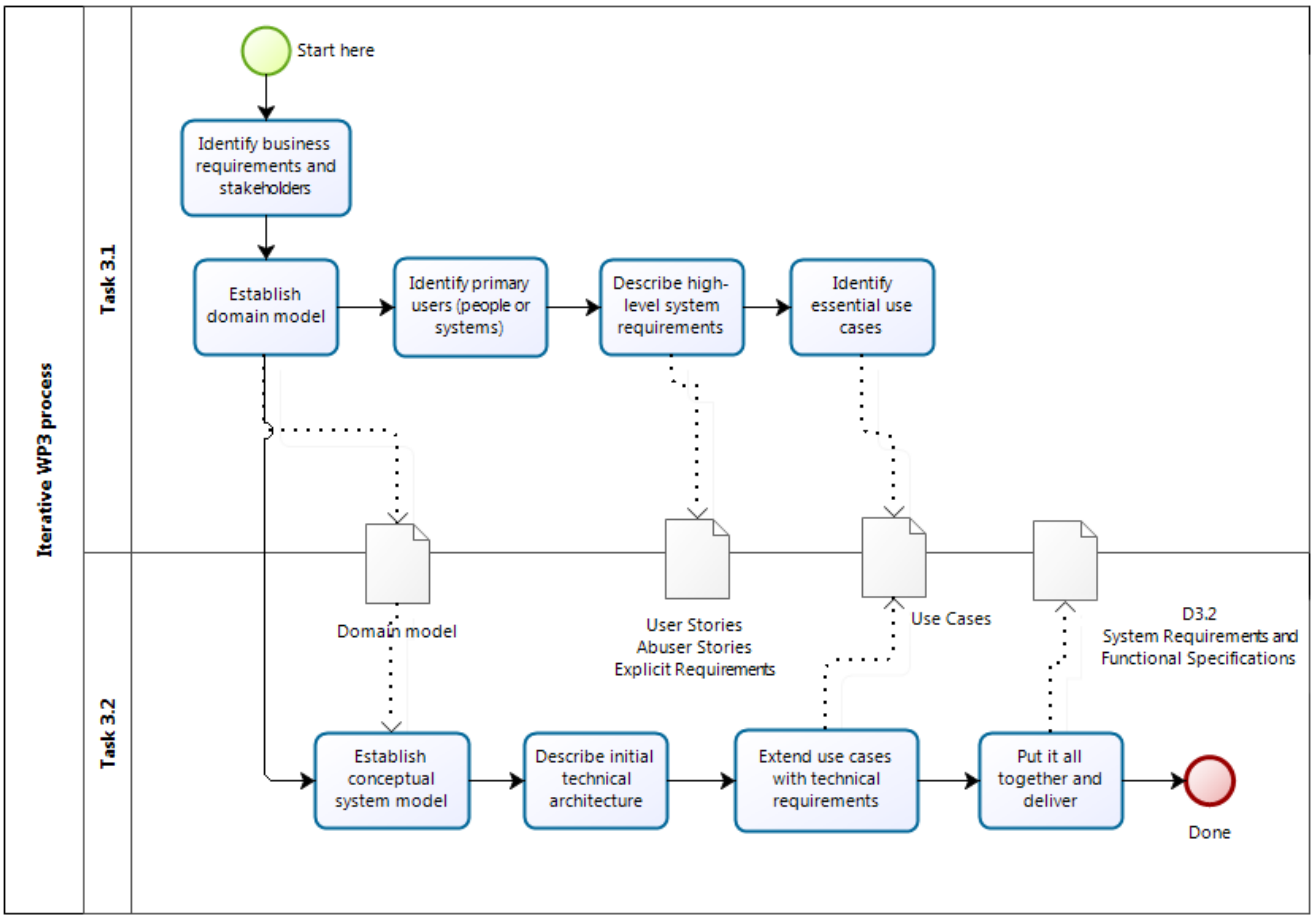

Figure 1: Iterative process for requirement and systems architecture development for WP3

The following list describes the identified process elements in more details:

Identify business requirements and stakeholders

The business requirements represent the set of requirements on the highest level. The result of the identification of business requirements can be found in Sections 2.

Establish domain model

The domain model is used to understand the context in which the system should operation. The SEMIAH domain model is given in Section 5.2.

Identify primary users/actors

The system users/actors need to be defined to understand how the system operated. A user/actor is something with behaviour, such as a person (identified by role), computer system, or organization. The result of the identification of system users can be found in Section 5.1.

Describe high level system requirements

The user stories in Section 4.2 express the requirements for the SEMIAH system. To support iterative development detailed requirements will evolve through the product backlog used during the development phase. The work with the product backlog is an ongoing activity. The approach taken is inspired by Scrum development.

Identify essential use cases

Work with use case design is part of the product backlog development.

Establish conceptual system model

The result of this activity can be found in Section 5.3.

Describe initial technical architecture

The technical architecture of SEMIAH is presented in Chapter 7. It is considered to be an initial architecture that may be elaborated and detailed alongside with the development and the build-up of new knowledge in the project.

Extend use cases with technical requirements

Use case designs derive from user stories. Use cases describe the detailed functional requirements of the system and these are part of the product backlog development and maintenance. The presentation of use cases are beyond the scope of this deliverable.

In addition, non-functional requirements are describes in the two most important areas of SEMIAH. Requirements on security and privacy are described in Section 6.2. The most important of this kind is the technical architecture as mentioned above, including interface specification. Non-functional requirements should also be included here; these are requirements to integrity, maintainability, availability, interoperability, performance, usability, etc. Where this is done in the context of use cases or not, is not essential.

Put it all together and deliver

This final step integrates the results of previous steps to provide a base for the systems requirements of the SEMIAH system. Further work on the refinement of requirements and solutions for development is deferred to the agile development process using the Product Backlog as a key tool for systems integration. Annex A provides initial instructions for work with the product backlog in SEMIAH.

1.3 Definitions

A number of artefacts to exchange knowledge between Task 3.1 and Task 3.2 have been used. These artefacts include domain model, use cases, user and ab-user stories. These concepts will be introduced in the following.

1.3.1 User Story

Kent Beck coined the term "user stories" in Extreme Programming in 1999 [15]. A user story is a short, simple description of a feature told from the perspective of the person who desires the new capability, usually a user or a customer of the system. The essence of user-centric and usage requirements elicitation is to focus on what the user wants to have, and not what the user wants the system to do.

A user story typically follows a simple template:

> *As a <type of user>,*
> *I want <to perform some task>*
> *so that I can <achieve some goal/benefit/value>.*

User stories need to be confirmed with the 3C guidelines below [17]:

Card: User stories are traditionally written on index cards or sticky notes, in short form. User narratives further explain these cards. Thus the main intention is to describe the user story in short form to allow common understanding of the user's need among all stakeholders.

Conversation: User stories shift the focus from writing about features to discussing them. In fact, these discussions are more important than whatever text is written.

Confirmation: Acceptance tests confirm that the story was delivered correctly.

1.3.2 Abuser story

An *abuser story* is a variant of a user story.

Abuser stories identify how attackers may abuse the system to damage the customer's assets be exploiting the system's functionality. Thus they state systems' security requirements.

1.3.3 Domain Model

A *domain model* in software engineering is a conceptual model of all the topics related to a specific problem. It describes the various entities, their attributes, roles, and relationships, plus the constraints that govern the problem domain. It does not describe solutions to the problem.

1.3.4 System Requirements Specification

A *system requirements specification* is detailed statement of the effects that a system is required to achieve. A good specification gives a complete statement of what the system is to do, without making any commitment as to how the system is to do it. It constrains only the externally observable behaviour and omits any design or implementation bias.

1.4 Reading guideline

Section 2 described the high-level requirements of SEMIAH. Readers who know the scope of the SEMIAH project may skip this part. Section 3 surveys the trend in smart grid standardization. This part gives a brief background of the standards' landscape that is important for the SEMIAH development. Again, readers with good knowledge in smart grid standardization may skip this part. A conceptual description of the SEMIAH system is given in Section 4. This includes a function description of the system from a number of user stories. Section 5 follows and introduces actor roles of the SEMIAH system. It provides a set of models to describe SEMIAH such as the domain model, the system model, and the security and privacy model. It furthermore includes a discussion on possible configurations of the SEMIAH system. Non-functional requirements in the area of scalability and security & privacy are given in Section 6. Finally, the SEMIAH system architecture is presented in Section 7. The architecture is introduced in the context of reference architectures taken from the smart grid standardization. Possible instantiations of the SEMIAH infrastructure are outlined in this section. Further work on the infrastructure lies within the scope of WP4.

2 Business requirements

The Description of Work (DOW) abstract is considered to describe the fundamental business requirements for the SEMIAH project.

Hence, the elicitation of business requirements have been based on the analysis of the approved and published abstract from the SEMIAH project. The business requirements are giving in Table 1.

The requirements are collected in a requirements list that will be extended with derived requirements (functional, non-functional and technical) for later mapping to test cases.

The key words: "*shall", "must",* or *"required"* mean that the definition is an absolute requirement for the system. Phrases containing key words: "*shall not"* or "*must not"* mean that the definition is an absolute prohibition. For optional requirements the key words: "*should*" or "*recommended*" are typically used. This means that there may exist valid reasons in particular circumstances to relax the requirement for a particular item.

ID	From DOW Abstract	Req. ID	Formalized Requirement
AB1	The consortium behind the SEMIAH project aims to pursue a major technological, scientific and commercial breakthrough by developing a novel Information and Communication Technology (ICT) infrastructure for the implementation of Demand Response (DR) in households.	AB1.1	The project *shall* develop a novel Information and Communication Technology (ICT) infrastructure for the implementation of Demand Response (DR) in households.
AB2	This infrastructure enables the shifting of energy consumption from high energy-consuming loads to off-peak periods with high generation of electricity from Renewable Energy Sources (RES).	AB2.1	The DR infrastructure *shall* enable shifting of energy consumption to off-peak periods.
		AB2.2	The DR infrastructure *shall* enable shifting of energy consumption to periods with high generation of electricity from Renewable Energy Sources (RES).
AB3	The project's innovative approach is based on the development of an open ICT framework that will promote an environment for the deployment and innovation of smart grid services in households.	AB3.1	The ICT framework *shall* be open.
		AB3.2	The ICT framework *shall* promote an environment for the development and innovation of smart grid services in households.
AB4	A centralised system for DR service provisioning based on aggregation, forecasting and scheduling of electricity consumption will be developed.	AB4.1	The project *shall* develop a centralised system for DR service provisioning.
		AB4.2	The DR system *shall* be based on electricity consumption
		AB4.3	The DR system *shall* support aggregation.
		AB4.4	The DR system *shall* support forecasting.
			The DR system *shall* support scheduling.
AB5	Furthermore, the project delivers a hardware solution for control of electrical loads at a competitive price.	AB5.1	The project *shall* deliver a hardware solution for households.
		AB5.2	The hardware solution *shall* enable control of electricity loads.
		AB5.3	The hardware solution *shall* have a

			competitive price.
AB6	The consortium will integrate security and privacy functions to prevent that the system is compromised.	AB6.1	The project *shall* integrate security functions to prevent that the system is compromised.
		AB6.2	The project *shall* integrate privacy functions to ensure that the privacy and integrity of the system users is not compromised.
AB7	Finally, the consortium will develop new business models for electricity players and residential customers to quantify costs and benefits for players in the value chain.	AB7.1	The project *shall* develop new business models for electricity players to quantify costs and benefits for players in the value chain.
		AB7.2	The project *shall* develop new business models for residential customers to quantify costs and benefits for players in the value chain.
AB8	SEMIAH will provide benefits to residential customers, energy utilities and the society in general, through lower electricity bills, peak demand reduction, improved integration of RES and higher stability of the electricity grid.	AB8.1	The project *shall* contribute to the reduction of the residential user's electricity bills.
		AB8.2	The project *shall* improve integration of RES.
		AB8.3	The project *shall* contribute to peak demand reduction and higher stability of the electricity grid.
AB9	Hereby, the project will enable savings in CO_2 emissions and fuel costs and reduce investments in electricity network expansions and electricity peak generation plants.	AB9.1	The project *shall* enable savings in CO_2 emissions.
		AB9.2	The project *shall* enable savings in fuel costs.
		AB9.3	The project *shall* contribute to reduced investments in electricity network expansions.
		AB9.4	The project *shall* contribute to reduced investments in electricity peak generation plants.

Table 1: SEMIAH Business Requirements (authoritative)

2.1 Requirement management and refinements

SEMIAH uses an agile development approach for implementation of system functions. A product backlog is used for development and maintenance of development artefacts. Artefacts are defined by user stories. The more detailed specification of implementation are handled by development teams responsible for the respective backlog items.

The process with refinement and management is further described in SEMIAH deliverable D3.1.

3 Trends in smart grid specifications

In this section, the SEMIAH system is put into the context of energy markets and the ongoing standardization effort related to smart energy grids. The purpose is to define the boundaries of the SEMIAH system and to identify the relevant standardization base.

3.1 Energy market development

The energy market liberalization is in a revival stage in many countries. Although most European countries are heading in the same direction with respect to energy market liberalization there are different starting positions and paces seen in this process when comparing country by country.

Figure 2 puts the SEMIAH project into the context of the Framework version 2 of the National Institute of Standards and Technology (NIST) [7].

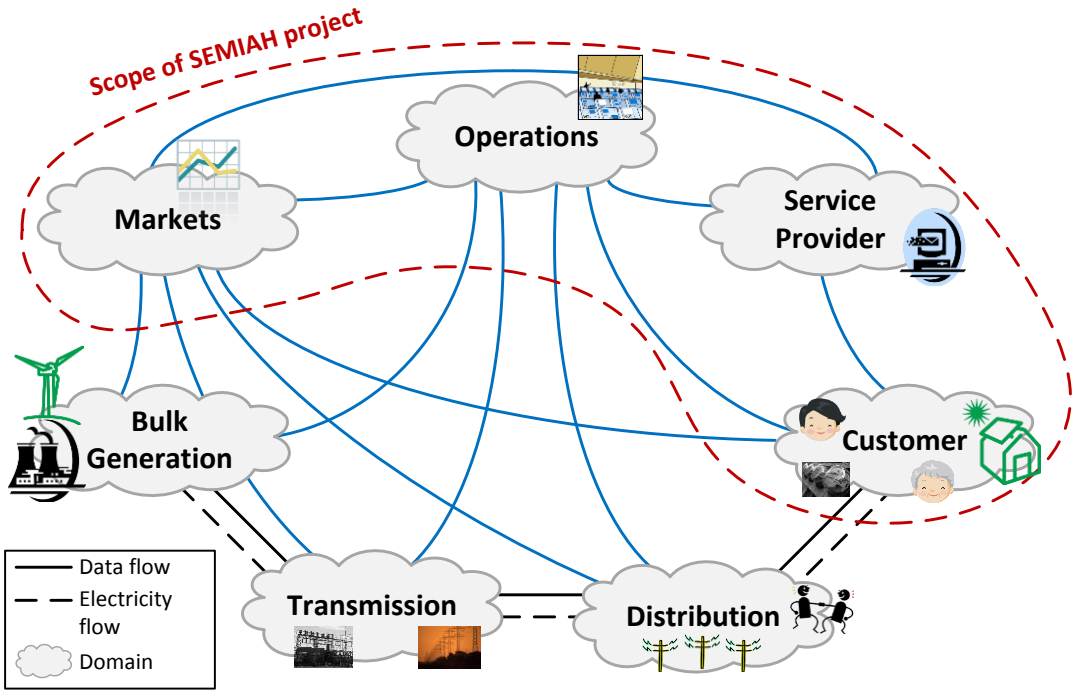

Figure 2: Positioning of SEMIAH development in the NIST Framework 2 context [7].

The NIST framework defines a conceptual model that comprises seven different domains:

- *Customer*: The end users of electricity, which might also generate, store, and manage the use of energy.
- *Markets*: The operators and participants in electricity markets.
- *Service Provider*: The organizations that provides services to customers and to utilities.
- *Operations*: The managers of the transport of electricity.
- *Bulk Generation*: The generators of electricity in bulk quantities and storage of energy for later distribution.
- *Transmission*: The carriers of bulk electricity over long distances. May also store and generate electricity.

More specifically related to SEMIAH is the development of the view of demand response as a market resource [9]. In the past, flexibility services would be provided by a top-down approach vertical integrated utilities (supply, transmission, distribution, service provider), whereas the future will more likely follow a bottom-up approach where flexibility is provided by energy consuming customers or energy producing & consuming customers (prosumers). In this scenario, new

business will develop and new market players will emerge to take on a key role as an *aggregator* of flexibility and access provider to markets.

In Figure 3, three different levels of flexibility can be illustrated. At the top-level, the trading of flexibility provided by virtual power plants (VPPs) takes place with the aim of maximizing profit for the market players. This imposes a set of *commercial constraints* on the service providers operating the Virtual Power Plants (VPP) because the offer for flexibility to the market must match the demand and hence determine the price for flexibility in the equilibrium between supply and demand.

At the service provider level (e.g., aggregator level) aggregation of flexibility from customers take place. This flexibility is pooled by VPPs operated by aggregation service providers. This flexibility is used for a two-fold purpose. First, it is used to balance the supply and demand of power in the grid locally in a cost-efficient way while ensuring power quality at all times. This balance is the responsibility of the Distributed System Operators (DSOs) i.e., Operations. Second, the remaining flexibility can be exploited for commercial purposes by, e.g., increasing the degrees of freedom for the energy supplier who is trading energy in the market. At this level *technical constraints* governs the operation as the power quality must meet strict requirements at all times.

On the bottom-level, i.e., the Customer level, the prosumers can deploy energy management systems to exploit flexibility in their energy consumption. An important trade-off between energy-efficient operation and operation with a high degree of flexibility exist. It is therefore likely that the prosumer must be presented with some kind of incentives to provide flexibility to the service provider since the energy-efficient operation of the residential homes inherently will attempt to lower the overall electricity cost and more indirectly also lower the CO_2 footprint. However, the customer will in all cases impose a set of *comfort constraint* because of the boundaries determined by the individual standards of living. For instance, a consumer would likely not allow the temperature of a residential home get too cold during winter time.

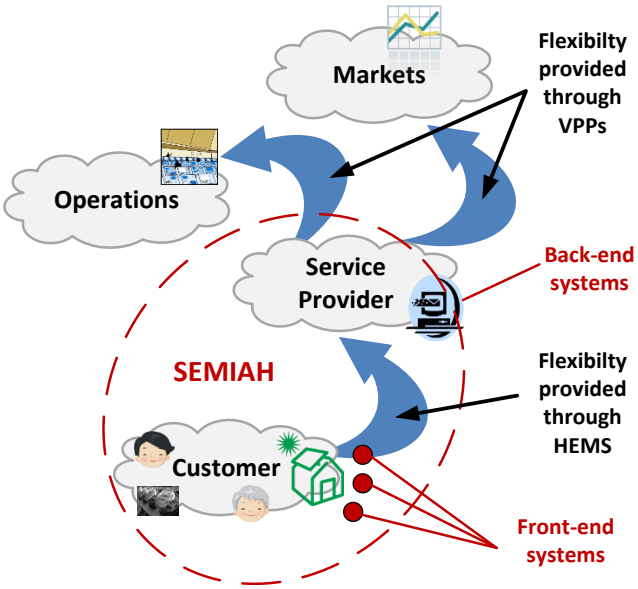

Figure 3: Flexibility service from a bottom-up approach.

Figure 3 positions SEMIAH in this context. The different levels of aggregation of the SEMIAH system are illustrated. As can be seen from the figure, SEMIAH extends the Service Provide level and the Customer level (dashed red line). This leads to a fundamental split of the functional

architecture of SEMIAH into a *back-end system* and a *front-end system* with an inherent one-to-many relationship. These two logical entities of SEMIAH assume quite distinct roles in providing an aggregated flexibility service from residential households. To illustrate this separation of concerns, the following functional distribution between the back-end system and the front-end system can be made:

SEMIAH aggregator back-end infrastructure

- aggregation of flexibility from SEMIAH front-end appliances
- optimal bidding strategy
- weather, load and price forecasting
- operator of a virtual power plant (VPP)
- model predictive control/optimization (single or multi-objective)

SEMIAH front-end / Smart Energy Gateways

- micro aggregation
- control of home appliances
- provide flexibility to service provider (schedule, probability, prediction)

The list above is not considered to be exhaustive and it may be elaborated further in the system design.

3.2 Standardization

A number of standardisation bodies have assumed responsibility for standardizing various aspects of the smart energy grid. This includes the standardization of physical properties, architectures, communication protocols, data models among others. The investigations into smart grid standardization and trends show that effort tends to segment around standards emerging from the field of power engineering, Internet Society including the World Wide Web standardization as well as a number of industrial alliances promoting key technology. In the following, we will introduce the relevant standardization in accordance with this segmentation.

3.2.1 Smart grid standards

Energy strategy in Europe is governed by three overarching objectives that concerns secure energy supply, a competitive environment for energy providers, and sustainability through the lowering of greenhouse gas emission, pollution and fossil fuel dependence [25].

Of particular importance to SEMIAH is the topic concerning markets and consumers since SEMIAH aligns with its aims at the integration of energy markets and European households and businesses. In this light, smart grids and smart meters are seen as enablers of better management of energy networks and of more efficient consumption.

In 2009 the EC established the Smart Grids Task Force to advise the Commission on the development and deployment of smart grids. The task force is divided into five Expert Groups of which the following parts are more relevant for SEMIAH:

- **Expert Group 1 "Smart Grid Standards".**
  A key contribution of this group is the publication of Mandate M/490 for smart grids in March 2011. “The objective of this mandate is to develop or update a set of consistent

standards within a common European framework that integrates a variety of digital computing and communication technologies and electrical architectures, and associated processes and services, that will achieve interoperability and will enable or facilitate the implementation in Europe of the different high level smart grid services and functionalities as defined by the Smart Grid Task Force."

- **Expert Group 3 "Regulatory Recommendations for Smart Grids Deployment".** Work in the expert group is ongoing. Two of the publications from this expert group are of particular importance for the SEMIAH system development:
  - **Concept of EnergyGrid sevices** [27] describes the need for providing a service oriented view of the future energy system. It introduces the concept of energy grid services and illustrates how customers can be engaged to support grid operation through e.g., DR programs.
  - **Methodology & New Applications** [4] contains the essence of mandate M/490 phase one. Among others it refines the smart grid conceptual model including a flexibility concept, smart grid use cases, and the smart grid architectural model (SGAM). Furthermore, it addresses standardization, cyber security & privacy as well as interoperability. A selection guide to the "Set of standards" is provided. The set of standards consists of system related standards and cross cutting standards. For the latter category the smart grid system has been broken down in several subsystems with each subsystem described by relevant use cases. Moreover, for each of these subsystems, reference architecture (components and interfaces) has been defined in SGAM from which a list of standards for each such system and its interfaces can be defined and evaluated. Of particular interest to SEMIAH is the subsystem: Demand/Response – Load management system. This will be discussed further in Section 7.1.

3.2.2 Internet of Things Standards

The Internet of Things infrastructure allows combinations of smart objects (i.e., wireless sensors mobile robots etc.), sensor network technologies, and human beings, using different but interoperable communication protocols and realises a dynamic multimodal/heterogeneous network that can be deployed also in inaccessible or remote spaces [12]. In this infrastructure, these different entities or "things" discover and explore each other and learn to take advantage of each other's data by pooling of resources and dramatically enhancing the scope and reliability of the resulting service.

Open standards are key enablers for the success of wireless communication technologies like RFID or GSM, and, in general, for any kind of Machine-to-Machine communication (M2M). Without global recognized standards such as the TCP/IP protocol suite or GSM/UMTS/LTE, the expansion of RFID and M2M solutions to the IoT cannot reach global scale.

Several organizations are today active in the standardization of the IoT. Figure 4 gives picture of the key standardization bodies with relevance to the SEMIAH project. Examples of these standardization bodies counts:

- **ITU-T**. The Global Standards Initiative on Internet of Things (IoT-GSI) under ITU-T promotes a unified approach for development of technical standards enabling the Internet of Things on a global scale.
- **ETSI M2M** technical committee is developing standards for machine to machine (M2M) communications.
- The **Internet Engineering Task Force (IETF)** is a key standardization body for protocol standards for the IoT [13]. Recently, IETF has strengthens its effort to provide recommendation of the use of Internet protocols for smart grid communications [21].

- **World Wide Web Consortium (W3C)** is providing web technology standards for the IoT. Its recent *Web of Things* initiative aims to develop Web standards for enabling open markets of applications and services based upon connected sensors and actuators and the Web of data.
- The **Organization for the Advancement of Structured Information Standards (OASIS)** works on the convergence between web standards. OASIS promotes and produces worldwide standards for security, IoT, cloud computing, energy, and other areas. It is driven by industry consensus.
- The **ZigBee Alliance** promotes and produces standards for ZigBee wireless communication devices. Besides the basic ZigBee communication standards the alliance produces a set of applications standards profiles targeting different domains. Most important for SEMIAH is the ZigBee Home Automation and the ZigBee Smart Energy [19].

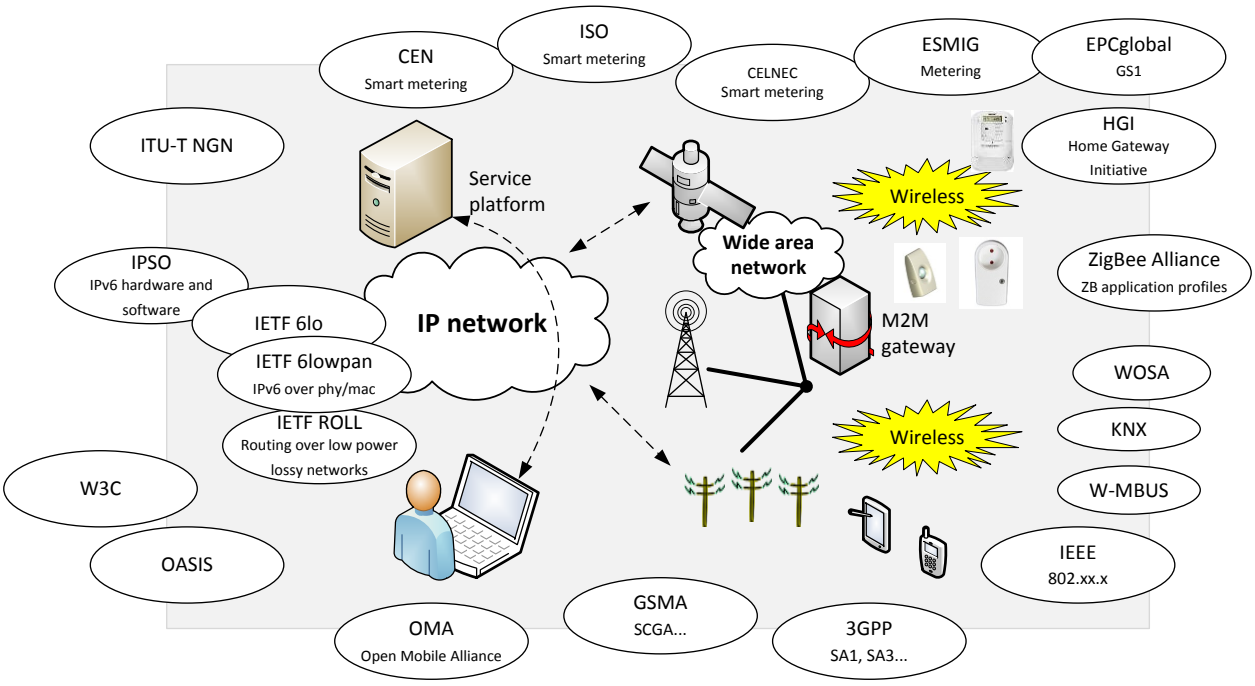

Figure 4: Standardization organizations for the IoT. Adapted from [13].

The different standardization bodies and industrial organizations are working on different segments of IoT communication network and IoT applications. This has resulted in a diverse landscape of standards. For the different applications domains such as e.g., smart grids the trend is to provide “super specifications” that points to a relevant subset of standards from one or more of the above mentioned standardization organization. As an example, the ZigBee smart energy application profiles points at a set of protocol standards from IETF and specifies data objects to be exchanged by using web services based on technology from W3C.

3.2.3 Assessment of standards in a SEMIAH context

Looking at the SEMIAH project in a standardization context reveals a number of immediate conclusions and comments.

For the SEMIAH front-end Home Area Network (HAN) technology from IETF and ZigBee alliances needs to be considered. ZigBee devices are today commercially available among other devices from DEVELCO. These devices are often fully or partly compliant to the ZigBee protocol standard

version 2 [20]. It is worth noticing that the ZigBee is approaching the Internet Society protocol suite in its recent effort to specify the third version of the ZigBee protocols (ZigBee 3.0). In 2013, the ZigBee and the Homeplug alliance jointly published an application profile for smart energy applications. The standard was adopted by IEEE in 2014 and is now an active standard (IEEE P2030.5-2013) [19]. The SEMAH project will focus on the ZigBee protocols suite and its evolution to establish a reliable HAN at the customer premises.

On the communication protocol side the Internet Society has made an effort to promote former protocol specification work as technology enabler for smart energy grid networks. RFC 6272 identifies a full suite of key infrastructure protocols of the Internet protocol suite for use in the Smart Grid [21]. The SEMIAH infrastructure will base on a selected subset of these protocols to establish secure and reliable communication on all levels in the system architecture.

The SEMIAH back-end relies on resent standardization related to web services and cloud computing evolution. Key technology standards relevant to SEMIAH can be gathered from the standards area of web design and applications and web architecture including specification for meta formats such as XML, JSON and protocols such as HTTP and identifier specifications such as URI format.

Data modelling is a key aspect of SEMIAH to ensure interoperability between stakeholder's systems. In accordance with the recommendation for European smart grids, the SEMIAH project will be based on the Common Information Model (CIM). CIM is an open standard that defines how managed elements in an information technology environment are represented as a common set of objects and relationships between them. This is intended to allow consistent management of these managed elements, independent of their manufacturer or provider. Within the energy domain CIM can be used for representing power system components and networks which has been primarily developed by the Electric Power Research Institute (EPRI) IEC61970/IEC61968. The standard is officially adapted by the International Electrotechnical Commission (IEC) to represent common components within power systems which can be used by energy management system (EMS) and application programming interface (API). This standard mainly specifies the interfaces between components, therefore allowing different software modules, from different vendors, to communicate with each other.

The CIM architecture is described by the Unified Modeling Language (UML) standardized by the Object Management Group (www.omg.org). It defines the components of a power system as UML classes and the relationships between them. This gives the base for a common model to describe communication and units of a power system, independent of any specific proprietary data standard or format, and hence facilitates the interoperability among software applications.

The exchange information within the electricity grid system is significant. The standards: IEC 61970 and IEC 61968 specify a CIM for utility data exchange. Together with IEC 62325, these standards constitute the core for the smart grid. Each of these standards has its own characteristics and supports different tasks within the grid.

IEC 61970 is a series of standards that describe information of energy management systems. They provide a set of instructions to simplify the integration of multi-vendor applications, as well as simplifying exchange of information to systems outside the control centre including transmission, distribution and generation systems that need to exchange real-time data with the control centre. Moreover, the standard series provides adequate interfaces for data exchange across legacy and new systems.

The standard series include the generation and transmission parts of the CIM. It represents a power system model exchange and other information exchanged, as well as specifications of an XML file format is for the information exchange. The CIM base model is given in IEC 61970-301 Specht-2013. The model describes the components of a power system, API and the relationship between each component. This standard consists of various packages that provide a logical view of the physical aspects of an EMS such as the Core, Wires and Topology packages to describe the

physical characteristics of a power network. The CIM base data model specified in IEC 61970-301 IEC61970-301 is expanded with additional objects within IEC 61968-11.

IEC 61968 is a series of standards that have been derived from IEC 61970 and aimed at simplifying inter-application integration and at supporting distribution management system. It is intended to support the integration of a utility enterprise that requires connecting different applications that are either legacy or new. IEC 61968 supports applications that require exchanging data on an event-driven basis. It is intended to be built with middleware services that broker messages between applications. The addressed interfaces include message exchange for network operations, operational planning and optimization, records and asset management, network extension planning, customer support, maintenance and construction, and meter reading and control. The standard series is limited to the definition of the interfaces. Therefore, technologies and methods used to implement these interfaces are out of scope of these standards.

IEC 61968-11 standard is a part of IEC 61968 that extends the CIM to support distribution management systems including customers, metering, load control, and others. The information model is defined by using UML that create a message payload in different formats. In this way, the standard will not be affected by either proprietary means or by the development of a next generation infrastructure.

IEC 62325 is a series of standards that defines energy market models and communications using CIM. The objective is to evolve standards for electricity market communications. It describes the communication formations of e-business in energy markets and system operations as well as communication between market operators. Business operation encompasses system applications with interfaces between different market participants in trading, consumption, market services and billing.

The analysis for security & privacy standards relevant for SEMIAH is given and described in more details in deliverable D8.1. The essential standards enumerates: ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC 15408:2009, and ISA/IEC-62443 from the ISO/IEC organization. To secure communication standards from the IETF are relevant such as the RFC 2196: Site Security Handbook, the RFC 2818: HTTP over TLS, and other related standards. Furthermore, there is the NIST that has relevant standards such as NIST 800-12; An Introduction to Computer Security; NIST 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems; and NIST 800-26: Security Self-Assessment Guide for Information Technology Systems. Since they are not European standards they may be considered only as an extension in SEMIAH.

4 System Requirements

This section introduces the stakeholders of the SEMIAH system. The main user stories are specified. These user stories constitute the main system requirements in accordance with the agile development model defined in the SEMIAH project.

4.1 Stakeholders

Table 2 identifies the most significant stakeholders of the SEMIAH system.

Stakeholder name	Description
Distribution System Operators (DSO)	The DSO is today the distribution network owner. In the future, the DSO may be a local system operator supporting the role of the TSO through the exploitation of the local flexibility. In order to support the system operation, the DSO will have to purchase necessary flexibility for the operation from large customers, aggregators, and microgrid operators through flexibility markets.
Transmission System Operators (TSO)	The TSO is the transmission system operator on a regional or national level. The TSO is responsible for the overall system operation maintaining the frequency and the real time balance between electricity generation and consumption. Balancing reserves and capacity are purchased in different markets from the other stakeholders.
Prosumers/Customers	Prosumers are consumers that also incorporate any form of DER and flexibility including demand response (DR). Prosumer households will have some sort of production e.g., photovoltaics and/or buffer capacity.
Bulk Producers	Bulk producers are the main energy suppliers in the power grid. Bulk producers can be subdivided into categories renewable energy sources (RES) and non-RES, and further grouped according to production stability, buffer capacity etc.
3rd Party Service Providers	There are different types of Service Providers identified: - energy traders - balance responsible operators - aggregators The **energy traders** are actors in the energy wholesale markets. These markets are slightly different from country to country mainly due to the different levels of regulation (or deregulation). The different marketplaces are divided based on time to delivery e.g. day-ahead market, intraday market etc. The physical balancing and operation of reserve markets are usually linked to the TSO. The **balance responsible operator** is an important role in the wholesale energy market. Obligations made by for instance an electricity provider/retailer to a set of customers must be traded and allocated in the day-ahead market. Price settlement for imbalances between obligations and physical volume is done in the balancing market and involves risk of higher costs. A commercial **aggregator** will operate in the markets as one entity on behalf of several actors. Usually, this is to establish bids above minimum bid-size and to reduce transaction costs. This role may be performed in stand-alone

	or in partnership with **energy traders**.
Product Developers	Vendors or developers of technology for smart energy control such as home gateways for automation.
Appliance Vendors	Appliance vendors interested in adapting their products to energy control
Telecom Operators	Telecom operators provide telecom services to the residential households. Many telecom operators are looking for ways to bring added value service to their existing customer based. The bundling with energy services is seen as a strong business opportunity for the telecom operators.
Smart Grid Service Developers	Developers of Demand Response (DR) services.
Computer Security Incident Response Team (CSIRT)	This is a team of trusted people (usually formed by Security analysts and coordinated by the Security manager) investigating suspicious security incidents identified by the Security Analysts (see below).
Privacy Ombudsman or Data Controller	This is a person or role in Information Security Management that is responsible for protecting the Personally Identifiable Information (PII).
Risk Analyst	This is a person, role or organisation in Information Security Management that manages and implements the overall risk assessment and management process. This can either be an actor that is external to the organisation, e.g., a third-party security analysis organisation, or within the organisation. The OCTAVE method[1] advocates the use of internal knowhow, as much as possible, to fulfil this role, as they have a significant amount of domain knowledge that should be leveraged in this process.
Security Analyst	This is a person or role in security operations that monitors security incidents for signs of intrusions, and proposes mitigation strategies to identified threats
Security Manager	This is a person or role in Information Security Management responsible for security. Furthermore, the Security Manager is responsible for identifying which security clearance that is required by the other persons or roles

Table 2: SEMIAH stakeholders

4.2 Main user stories

The tables in the sections below present a set of user stories for SEMIAH. User stories have been used in the requirement analysis phase and have made the foundation of use cases to specify the functional requirements of the SEMIAH system. The main user stories are divided according to the main actors of the SEMIAH system.

In the SEMIAH project user stories are maintained on a virtual board by using a tool called Trello [24]. This allows user stories to develop in an agile way during the project.

4.2.1 Distribution System operator (DSO)

Essential parts from the DSO user stories concern grid stability. A key desire of the DSO is to shift electricity demand away from the daily peak power demand. First, this ease the effort required to maintain grid stability. Second, it helps to postpone necessary arge investments in grid reinforcements resulting from the general increase of electricity usage in the society.

[1] OCTAVE method http://www.cert.org/resilience/products-services/octave

As a…	I want to…	so that…
Distribution System Operator (DSO)	schedule a global power profile move in the consumption / generation / storage pattern on a particular feeder	congestion on that feeder is suppressed / avoided, power quality will stay within the permitted range, no disconnection of intermittent renewables will be required, and grid reinforcement is delayed / made unnecessary.
	manage the capacity reserve for power profile moves on a feeder	I know the achievable margin on that feeder in case of congestion or power quality, and I can adapt the margin on that feeder to my needs.
	be informed on the success / failure of my global power profile moves	I have a feedback on my power profile move requests.
	integrate the flexibility service into the control center operation	the flexibility service is part of my distribution system operation procedures.
	have some control on the power profile moves requested by energy suppliers	I avoid that power profile moves requested by energy suppliers put my grid at risk.
	implement the flexibility service on a service independent framework	I can later on implement on the framework a service to collect load curves and transmit them to the market clearing entity (activity as metering system operator), and I can later on implement on the framework a service allowing me to use local devices as sensors (e.g. meters) or as actuators (e.g. in-feed inverters).
	have the service to be trustworthy, secure and reliable	I can trust the estimated capacity reserve and so that external hackers cannot take over and control the service, or use it as a bridgehead towards attacking other internal services.
	have strong access control for controlling services and deploying updates	I avoid malicious intrusion. This includes the possibility to change digital certificates and encryption algorithms if these have been compromised. Note that simple password protection is not considered strong access control on its own.
	protect the data of the company (both in transit and at rest) by using encryption.	I can keep data confidential. This includes protecting technical information about the services which may be used to attack the system.
	system configuration changes to be tested and to be safe before deployment and I want.	I avoid loss of availability due to misconfigurations, unsafe states, and errors etc.
	a secure log of which system deployment operations that is being performed by whom,	to ensure auditability and nonrepudiation

Table 3: User stories of the DSO

4.2.2 Electricity energy supplier provider

Most of the electricity is today traded in the energy markets and the price for electricity is determined by supply and demand (ideally). The electricity energy supplies are active players in these markets. The SEMIAH aggregator system needs to be informed about current and future electricity market development such as “ahead” price information. Likewise, the electricity energy suppliers are interested in getting information about planned operation of the SEMIAH operation because this will influence on the demand side.

A direct interface for control between the electricity energy supplier and the SEMIAH aggregation service provider is not anticipated. Information can be exchanged through – possible commercial – information services. E.g. the day-ahead prices in the market can be subscribed to by SEMIAH and downloads via FTP such as in the case of NordPoolSpot for the North European spot market. SEMIAH can provide an information service to publish planned schedule for the aggregated demands of its users.

As a…	I want to…	so that…
Electricity energy supplier	schedule a global power profile move in the consumption / generation / storage pattern of my customers	I can minimize the acquisition cost of energy, I can adapt my global power profile to my intermittent generation, I can minimize the balance energy for my balance group, and I can successfully respond to call control reserve activation.
	manage the capacity reserve for power profile moves on my customers' premises	I can increase / decrease the margin for energy purchase / sales operations, I can be sure to dispose of a big enough margin to clear the balance energy within a calculation period, and I can reliably offer bids for control reserve.
	be informed on the success / failure of my global power profile moves	I have a feedback on my power profile move requests.
	be informed on power profile move operations requested by DSOs on my customers' premises	I can take actions to mitigate the effect of these operations.
	integrate the flexibility service into my market operation	the flexibility service can be used in a way similar to other market instruments.
	implement the flexibility service on a service independent framework	it can be later on reused for other services to my customers (information on own consumption / production, sustainability of consumed energy, context based advices for energy efficiency…).
	package a flexibility product for my clients (communication, rewarding scheme, contract...)	I can increase the loyalty of my current clients and acquire new ones.
	the service to be reliable and also be resistant to market manipulations and fraud.	I can provide a sustainable business and deliver reliable services to my customers and users.
	market sensitive information to be kept confidential and ensure strong access control and ensure non-repudiation on use of the energy trading interface	the risk of fraud is reduced and I can provide transparency and auditability service to my customers and users.

Table 4: User stories of the electricity energy provider

4.2.3 Prosumer/Customer

SEMIAH will likely not be in a situation to have the full control of all appliances in the residential homes for a number of reasons. The most striking reason is the “human in the loop”; meaning that end user may change their energy usage patterns at will such as rescheduling and even interrupting appliances. This challenge illustrates the need for establishing service guarantees to the provided flexibility services of SEMIAH. To counter this SEMIAH has made a selection of appliances that are less exposed to user interventions (see Section 0) and also integrated probabilistic methods in the planning and scheduling of electricity demand cf. Task 5.2 from the DoW.

As a…	I want to…	so that…
Prosumer	synchronise my consumption / local production with the intermittent generation of renewables	I can bring a concrete contribution to the energy turnaround.
	be informed in a simple, concise and unbiased way on my electrical energy consumption, including its flexible use	I can understand my local energy consumption / generation / storage profile.
	allow external entities to automatically exploit the flexibility of my processes	my electricity bill is reduced.
	to be able to take precedence over the automated flexibility control system	I can take the reins of the system if I find the behavior of the flexibility control system inappropriate.
	avoid that my local generation is disconnected from the grid	the locally generated energy is not lost.
	have control over the distribution of my personal data	I can manage my privacy as I want.
	be sure that my appliances are operated in an appropriate way	the flexibility system would not damage them nor reduce their efficiency.
	to be able to manage addition / removal of appliances to / from the flexibility control system	I have the (full) control over my premises.
	to be able to configure the flexibility control system	my comfort level is not lowered below my expectations.
	have a simple and fair contract with the entity(ies) managing my flexibility	I can trust that benefits are shared.
	have a trustworthy and secure energy management solution	malicious actors cannot use the service as a bridgehead to monitor or attack elements in my home or computer network, malicious actors cannot exploit information about my behavior to do damage or break into my house.

Table 5: User stories of the prosumer

4.2.4 Telecommunication provider

The emergence of energy management service for the residential household is an opportunity for the telecommunication operators to provide value added services to the prosumer/consumer. These services may be bundled with already existing telecommunication services such as broad band internet access.

As a…	I want to…	so that…
Telecom operator	on the basis of my telecom gateway, deploy and manage a distributed infrastructure for the operation of value added home services	I can increase my ARPU (Average Revenue Per User), and I can increase the loyalty of my clients.
	gather as many data as possible (data related to my customers)	valorize them (through services, which are mostly unknown yet).

Table 6: User stories of the telecommunication operator

4.2.5 The Abuser

The abuser story is a way to capture potential vulnerabilities in software systems, using the standard user story format. While user stories are written from a user perspective, abuser stories are written from an attacker's perspective. It describes the enemy's mal-intent and motivation and ease the formulation of system requirements related to security and privacy.

As an…	I want to…	so that…
Abuser	perform a denial of service attack by blocking access to the server from the HEMS	I can interrupt energy services.
	block the user's access to electricity	I can, blackmail, or disrepute the service provider.
	destabilise the grid by turning on (and/or off) lots of electrical appliances in the neighbourhood	I can interrupt energy services.
	turn on a user's hot plate from outside, to create a fire and burn down the house.	I can disrepute the service provider.
	turn off a user's TV during the Football Cup Finals or Eurovision Song Contest	can be entertained.
	attack or disrupt the aggregator services or core services in the electricity grid using the HEMS as a bridgehead.	I can interrupt energy services.
	attack vulnerable cloud-based services (e.g., aggregator services).	I can interrupt energy services and steal personal information.

Abuser	reduce my electricity bill by manipulating the meter readings.	I can have economic benefit.
	steal a neighbour user's electricity	I can have economic benefit.
	manipulate the electricity market to my advantage using the virtual power plant infrastructure.	I can have economic benefit.
	gather prerequisites for use in complex attacks.	I can launch attacks by exploiting the user's computer infrastructure.
	learn a user's HEMS login details through phishing (email/web-page/phone call) for use in later attacks	I can impersonate the user and get economic benefits.
	detect a user's TV habits and behaviour patterns	I can target advertisement.
	detect absence patterns	I can plan a burglary.
	collect as much Personally Identifiable Information as possible	benefit from identity theft
	collect information about famous people's behavior	exploit it for "journalism" purposes
	collect information to know when the user is likely to arrive to or leave the household	I can take candid pictures of them without their consent.
	sniff the traffic between HEMS and the devices	I can gain and exploit information about the users habits.
	decrease my energy bill by modifying the data sent by the HEMS to the VPP	I can get an economic benefit
	get access to the Energy Management Gateway	I can launch further attacks
	gain information from the VPP to get the data of the customers	I can impersonate the user and get economic benefits.
	gain access to the VPP to modify my data	I can get an economic benefit or be entertained.
	stop the functioning of the VPP by sending crafted packets	I can interrupt energy services
	escalate my privileges to get admin rights to the system (when acting as normal user)	I can access privileged functions of my HEMS for economic benefits or for entertainment.

Table 7: Abuser stories

5 Conceptual models for SEMIAH

The SEMIAH system should rely on established conceptual models from the Smart Grid domain. Figure 5 is the starting point for the model of SEMIAH and it illustrates the conceptual model of smart grids on a high level.

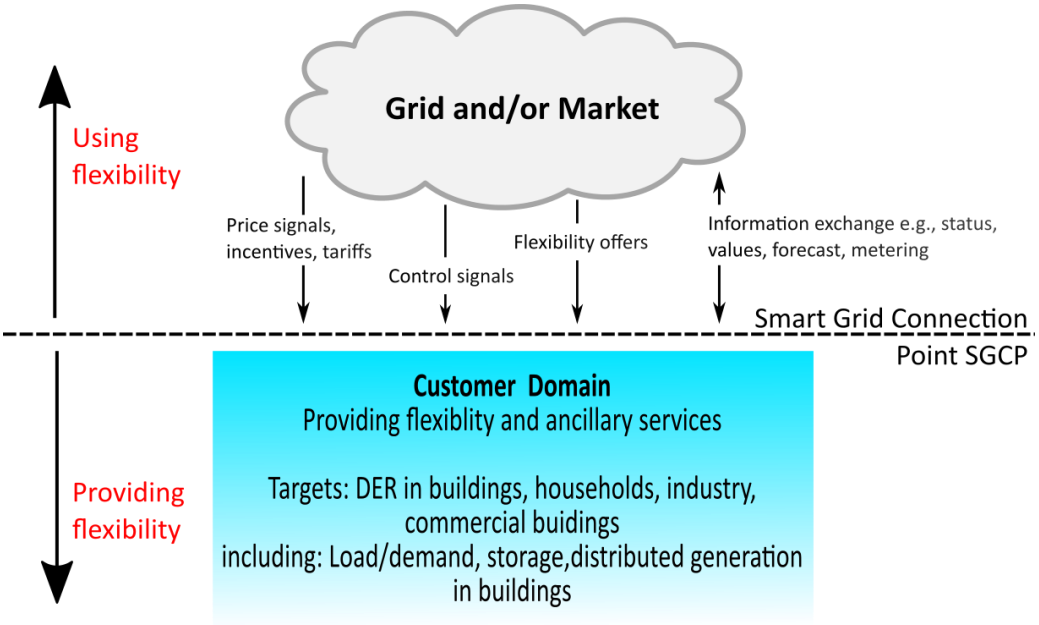

Figure 5: Conceptual Model (from [1], chapter 8.2)

The flexibility concept is described in great detail in [1] and further refined in [2].

In the SEMIAH project we will adapt the flexibility offering concept of the MIRABEL project [2].

"The flexibility [offering] concept assumes that parties connected to the grid produce offerings of flexibility in load and (distributed) generation. Thereby, so-called flex-offers are issued indicating these power profile flexibilities, e.g. shifting in time or changing the energy amount.
In the flex-offer approach, consumers and producers directly specify their demand and supply power profile flexibility in a fine-grained manner (household and SME10 level). Flex-offers are dynamically scheduled in near real-time, e.g. in case when the energy production from renewable energy sources, such as wind turbines, deviates from the forecasted production of the energy system."

In the flexibility concept, the management (control) of flexible demand and supply is fully interchangeable at the Smart Grid Connection Point (SGCP) [2]. This interface allows, in principle, any connected party with flexible generation, consumption and/or storage to participate in a DR operation.

The following subsection introduced the actors from SGAM that are relevant for SEMIAH. Hereafter follows a presentation of a domain model. Moreover, the SEMIAH system model presents an abstract model to describe the key concepts of SEMIAH. Finally, the security and privacy models used in SEMIAH are presented.

5.1 Actors

Table 8 shows a list of selected actors relevant for the SEMIAH system adapted from [1]. The complete actor list with descriptions can be found in [1], Annex A.

Name	Actor Type	Actor Description
Actor A	External Actor	External actor (Smart Grid Market Role) interacting with the system functions and components in the home or home automation network through the energy management communication channel. Examples of such market roles are the Energy Provider, the Energy Services Provider, the aggregator, etc.
Actor B	External Actor	External actor (Smart Grid Market Role) interacting with the system functions and components in the home or home automation network through the metering communication channel. This actor is responsible for collecting metering data. Examples of such market roles are the DSO, metering company, etc.
Aggregator	Role	The aggregator offers services to aggregate energy production from different sources (generators) and acts towards the grid as one entity, including local aggregation of demand (Demand Response management) and supply (generation management). In cases where the aggregator is not a supplier, it maintains a contract with the supplier.
Consumer	Role	End user of electricity, gas, water or heat. As the consumer can also generate energy using a Distributed Energy Resource. The user is sometimes called the “Prosumer”.
Customer Energy Manager (CEM)		The CEM is a logical function optimizing energy consumption and or production based on signals received from the grid, consumer’s settings and contracts, and devices minimum performance standards. The CEM collects messages sent to and received from connected devices; especially the in-home/building sector has to be mentioned. It can handle general or dedicated load and generation management commands and then forwards these to the connected devices. It provides vice versa information towards the “grid / market”. Note that multiple loads/generation resources can be combined in the CEM to be mutually controlled. When the CEM is integrated with communication functionalities it is called a Customer Energy Management System or CEMS.
Energy Management Gateway (EMG)	System	An access point (functional entity) sending and receiving smart grid related information and commands between actor A and the CEM, letting the CEM decide how to process the events. The communication is often achieved through an internet connection of through a wireless connection.
Flexibility Operator (FO)	Role	The FO is a generic role which links the role customer and its possibility to provide flexibilities to the roles market and grid; generic role that could be taken by many stakeholders, such as a DSO company, an Energy Service Company (ESCO) or an energy supplier
Smart Device	External Actor	A smart device may be an appliance, generator or storage device (Local storage devices include direct and functional electricity storages such as electrochemical batteries, heat pumps and micro CHP such as fuel cells with heat buffers, air conditioning and cooling devices with thermal inertia, etc.).

	The smart device can receive data directly from the grid, though an interface with the CEM and can react to commands and signals from the grid in an intelligent way. Since the smart device is outside the scope of the SGCG, it must be seen as an external actor

Table 8: Selected actors from M/490.

The section in the SEMIAH technical architecture will revisit some of these actors. For instance, Actor A and Actor B appear in Figure 17 while other actors will appear in the following subsections. A mapping between M/490 actors and the SEMIAH stakeholders presented in Table 2 is beyond the scope of this deliverable.

5.2 Domain model

The domain model method of software engineering is applied to SEMIAH in order to capture the basic conceptual description of the domain and its actors. For simplicity only the most essential actors for the basic operations of SEMIAH is demonstrated. A domain model is also referred to as a conceptual model of a domain.

Figure 6 shows the domain model for SEMIAH. The key actors are the consumer (depicted as a Prosumer), the DSO, and the Electricity Trader.

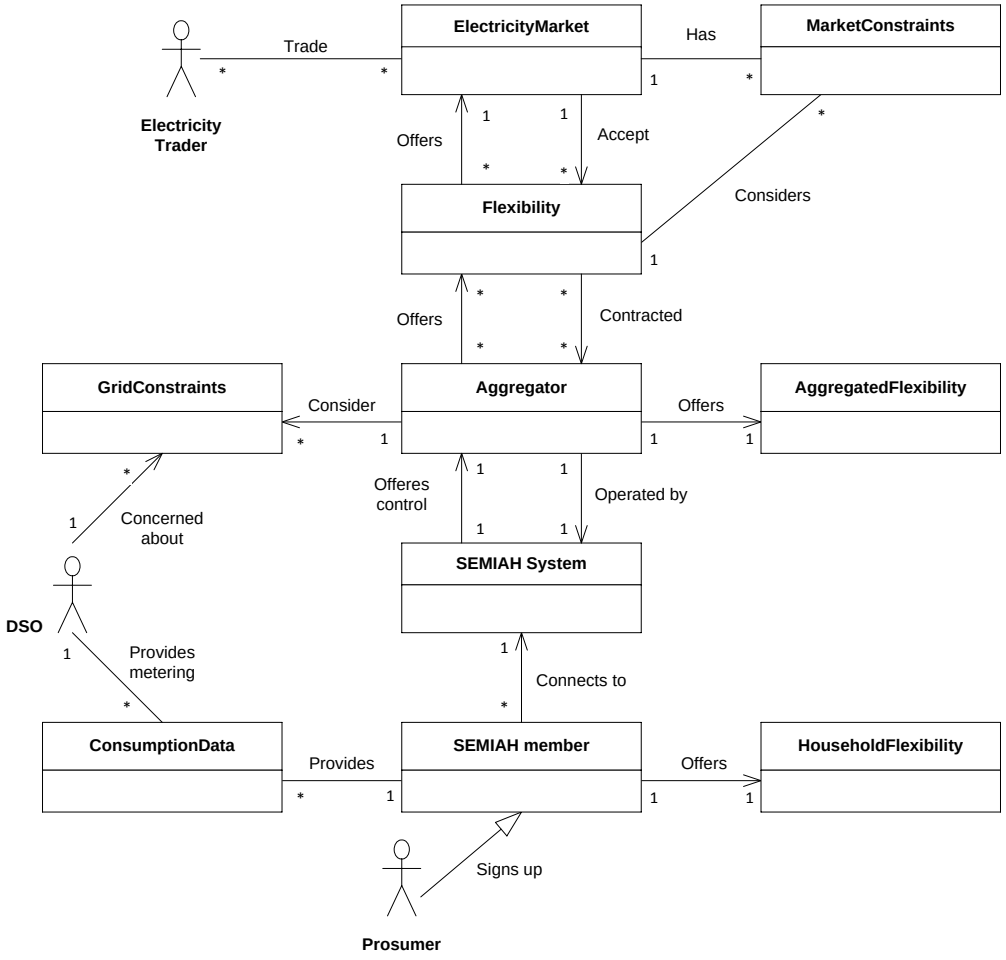

Figure 6: SEMIAH domain model depicted as a UML class diagram.

The Prosumer decides to become a SEMIAH member and to prove flexibility for his/her household (HouseholdFlexibility). Data from household consumption (ConsumptionData) is collected by the DSO. Local production can be regarded as negative consumption. For simplicity, it is assumed that the DSO also operates the advanced metering infrastructure that collects the consumption data.

In order to provide flexibility to the grid the SEMIAH member connects to the SEMIAH System. The SEMIAH System is operated by an Aggregator service provider. This service provider aggregates the flexibility of a large number of households (AggregatedFlexibility). In order to contribute to the overall balancing of the power grid, the Aggregator needs to consider the constraints (GridConstratins) which is the concern of the DSO.

Electricity Traders in the market (ElectricityMarket) are interested in trading flexibility (Flexibility) offered by Aggregator service provides competing in the market. The market has constraints that need to be taken into account when providing offers of flexibility. For simplicity only one electricity market is modelled. The Electricity Trades make decisions on whether to buy or sell flexibility from/to the market. In the model, it is assumed that all flexibility is traded through an electricity market.

5.3 System model

The conceptual model provides input to the definition of the SEMIAH system model described in this section.

5.3.1 Overview

The SEMIAH system model is designed as a layered model, with a philosophy similar to the OSI model well known in the telecommunication world.

The three defined layers are:

- the *IoT* (Internet of Things) layer, whose role is to provide an abstraction for field devices deployed in households;
- the *SEMIAH Objects layer*, which manages SEMIAH specific objects; and
- the *SEMIAH Control layer*, whose role is to control SEMIAH objects according to actors' requirements.

The layered model is illustrated in Figure 7.

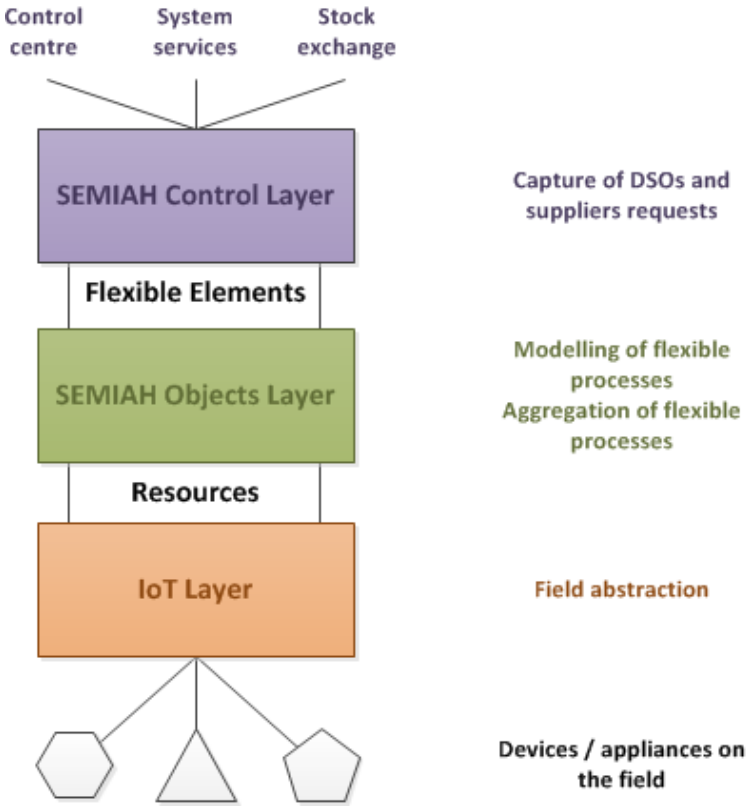

Figure 7: SEMIAH layered model

5.3.2 The IoT layer

SEMIAH has to collect measurement values and to control output values on appliances. Appliances may belong to different categories (heat pumps, washing machines, electrical meters etc.). Within a single category, appliances may be of different models e.g., heat pump model X1 of manufacturer X etc. Different appliance models of the same category feature different ways to access the same input and output parameters and often also a different set of parameters. The fundamental role of the IoT layer is to provide an abstract view of that diverse world to the SEMIAH objects layer.

The IoT layer provides the following services to the SEMIAH Objects layer:

1. The SEMIAH Objects layer disposes of a uniform method to access input and output parameters. This method must be independent of appliance models, but also independent of appliance categories. Hence data acquisition method, local communication protocols etc. are abstracted by the SEMIAH IoT layer. The abstract representation of an appliance is called a resource in SEMIAH.
2. The SEMIAH Objects layer can address appliances through a coherent semantics. Ideally semantics is defined at the appliance category level, i.e., there is a *resource type* per appliance category.

The problem to provide a uniform access to heterogeneous devices and appliances is not specific to SEMIAH. In fact, it is a key issue in any IoT framework, hence the name of the layer. In contrast, most resource types are specific to SEMIAH.

5.3.3 The SEMIAH Objects layer

The most relevant object in the SEMIAH Objects layer is the “Flexible element”. Such an element:

- knows at each instant the flexibility it can provide in the close future, and
- enables to reserve and to activate that flexibility.

Individual processes (space heating with heat pump, electrical car, dishwasher etc.) are basic flexible elements.

Collections, which are sets of *processes* and/or sub-collections, are also flexible elements. Hence, a collection must express its flexibility and provide some controllability. The collection's flexibility is an aggregation of the flexibility of its members. When requested to activate its flexibility, a collection must dispatch the request between its members.

Collections have two roles:

- they allow strongly reducing the number of elements presented to the SEMIAH Control layer, and
- they allow enforcement of constraints for flexibility aggregation and dispatching of flexibility requests.

A flexible element (i.e., a process or a collection) can be linked to one or several IoT layer's resources.

Collection types are not defined in the system model since they can be dynamically defined to match specific environments. A list of possibly meaningful collections is given below:

- "Household" or "Building" collection: set of all processes in the household / building;
- "Feeder" collection: all collections / processes connected on a given feeder;
- "Market group" collection: set of all collections / processes belonging to owners having a contract with a given market actor (typically an electricity supplier);
- "Electrical cars" collection: set of all electrical cars.

Constraints can be specified at the process level and at the collection level. An example of a constraint for a thermal process is the constraint that a temperature must remain in a given band to provide comfort to the customer.

For a building collection, a constraint could be for example the limitation of the consumed power.

Key issues for the SEMIAH Objects model are:

- **Semantics**: Data models for flexible elements (processes and collections) expressing the effective flexibility through a limited number of parameters. A data model for a "flexibility activation request" must also be elaborated.
- **Aggregation algorithm**: Flexibility for a collection is calculated through aggregation of the members' flexibility. Appropriate aggregation algorithms have to be determined.
- **Scheduling algorithm**: Assume a collection receives a flexibility activation request from a parent collection or from the SEMIAH Control layer. The role of the scheduling algorithm for a collection is to dispatch a request among the collection members. The role of the scheduling algorithm for a process, is to define time intervals where the device can be started.

The system model should put as few constraints as possible on semantics as well as on aggregation and scheduling algorithm. Thenceforth, new semantics or new algorithms can be supported without changes in the system model.

5.3.4 The SEMIAH Control Layer

SEMIAH allow DSOs' and electrical energy suppliers' actors to activate flexibility to fulfil their specific objectives. The goal of the SEMIAH Control Layer is to capture user specific requests. Typically relates to grid control, ancillary services or stock exchange. The SEMIAH Control Layer processes requests so that they can be forwarded to the SEMIAH Objects Layer.

The SEMIAH Control Layer addresses SEMIAH Objects' flexible elements. Hence, the SEMIAH Control Layer can control collections and/or individual processes.

5.4 UML model

The system model is defined as a UML class diagram. A package corresponds to each of the three layers sketched above. The package bears the same name as its corresponding layer.

The full system model is presented in Figure 8.

In addition, the SEMIAH grid package organizes classes that actuate electricity consumption in accordance with request form the SEMIAH Control Layer.

In the following, the UM model is explained in details.

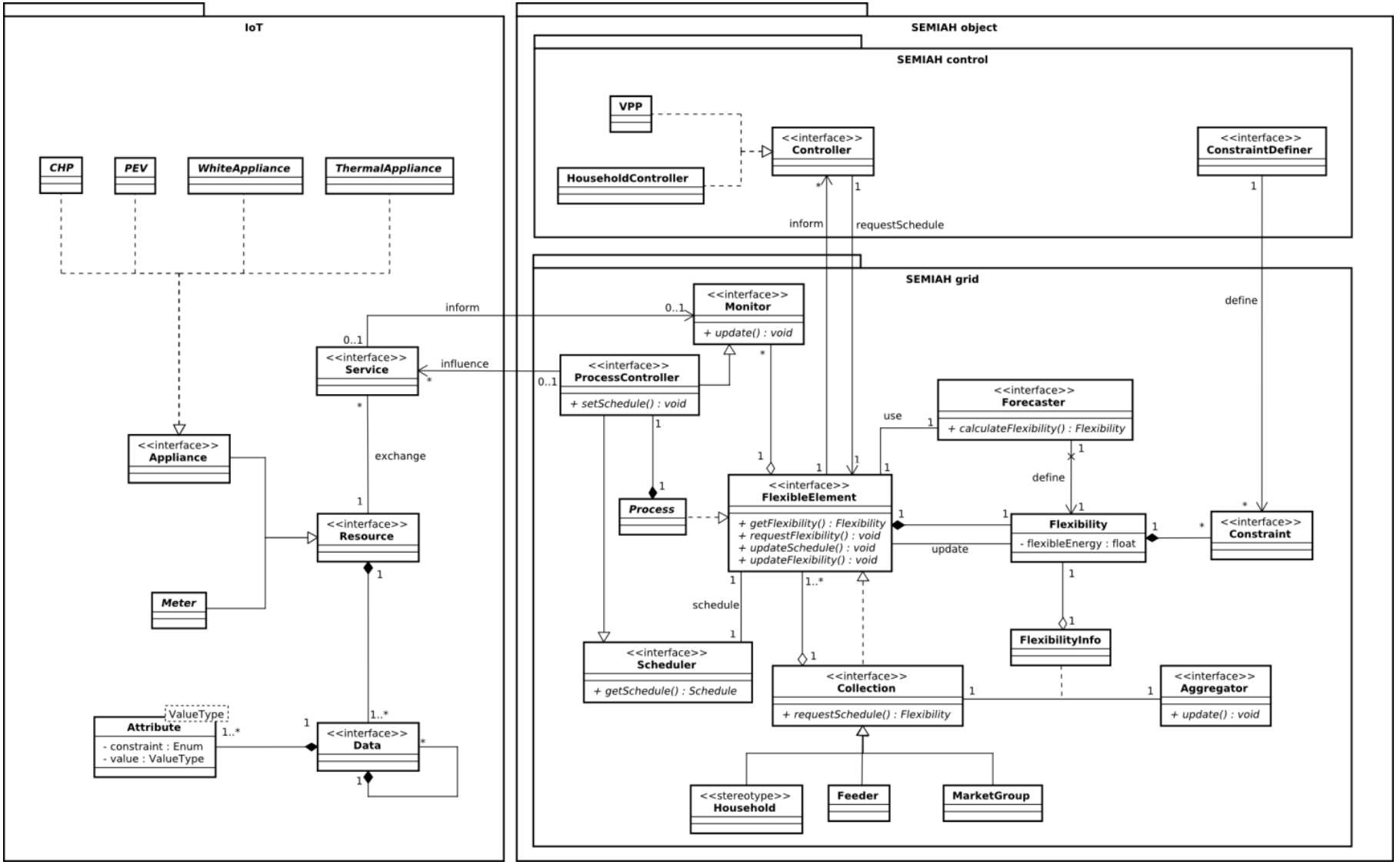

Figure 8: Class diagram for the SEMIAH model

5.4.1 The IoT package

The IoT package manages the Resources (resource interfaces) and provides access to their Data (data interface). A Resource represents a device, for example an Appliance (appliance interface) consuming or producing electrical energy or a Meter of any type.

A Data provides a way to organize the Attributes inside a Resource. It represents a set of Attributes grouped together for a common use.

The Service (service interface) provides an access from external tools to Attributes of a Resource. This is the only visible part of the package for an external tool. The external tool can access a Resource from a Service depending on the right defined by a Resource.

The Resource concept has been taken over from OGEMA [22].

The organisation of the Data is inspired by the IEC 61850 standard widely used for grid control [23].

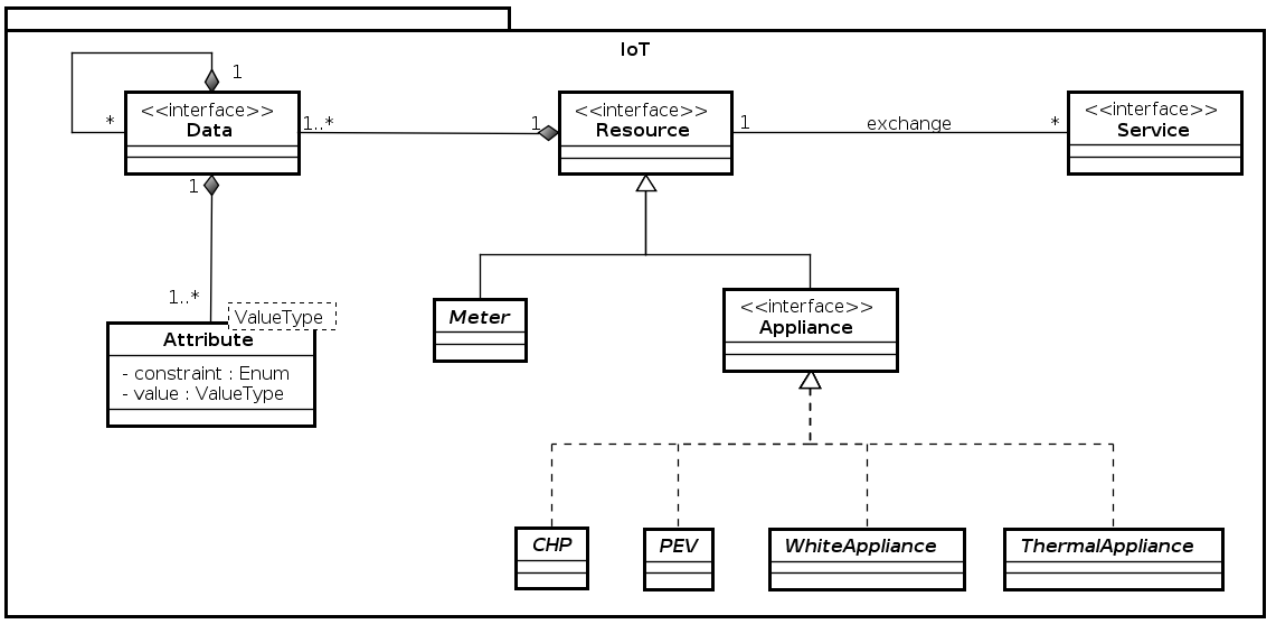

Figure 9: Class diagram: The IoT package of the SEMIAH architecture

The Resource types are given as example and are not part of the system model.

5.4.2 The SEMIAH Objects package

The UML class diagram for SEMIAH Objects package is presented in the Figure 10.

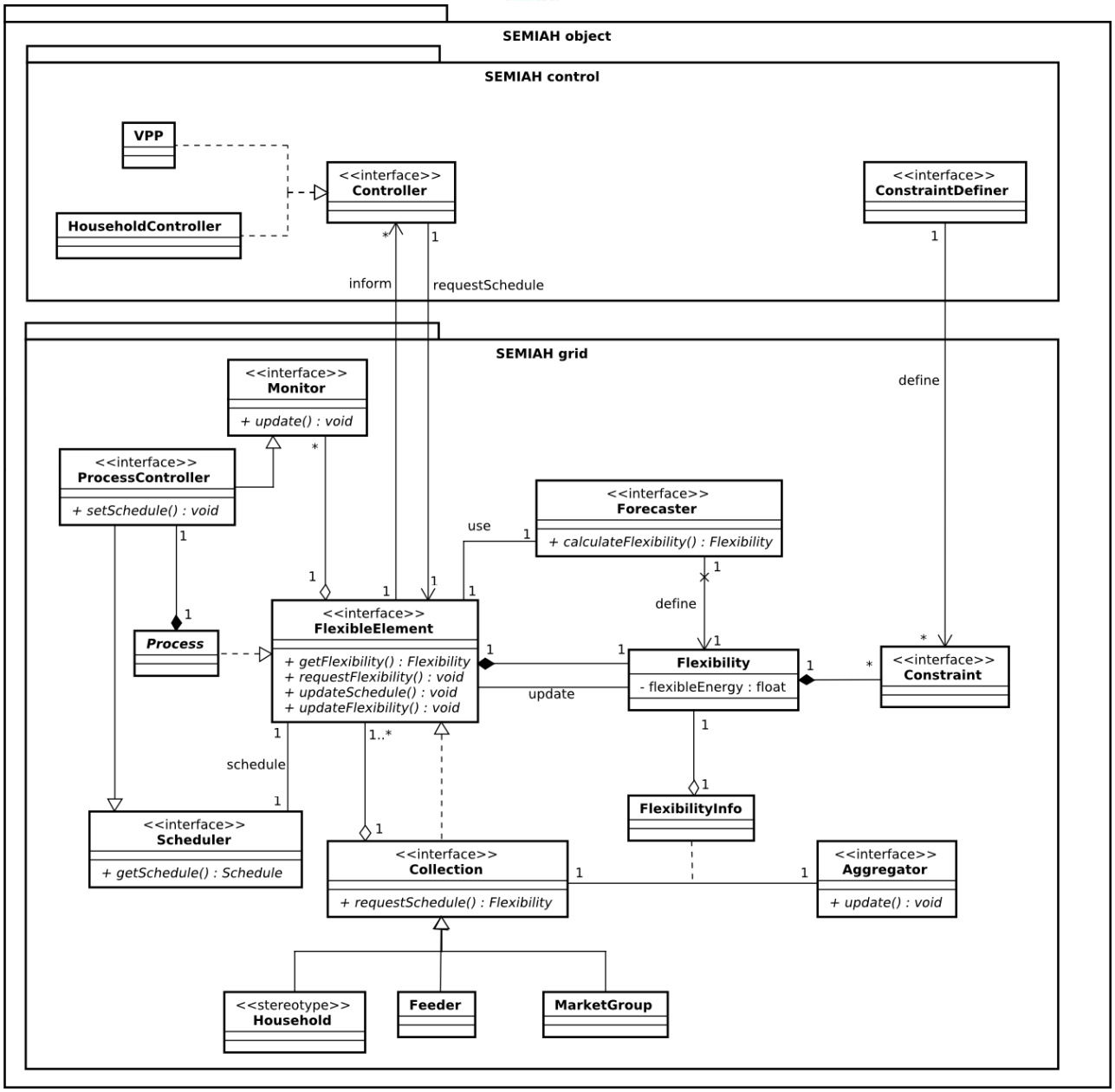

Figure 10: UML class diagram for the SEMIAH Objects package

In the SEMIAH Objects package, the main class is FlexibleElement belonging to the SEMIAH Grid package. It provides a bidirectional communication with Controllers (part of the SEMIAH Control package) representing the SEMIAH actors. A Controller can:

- be informed on the current Flexibility (i.e., the current estimation of the flexibility for the near future) provided by a FlexibleElement, and
- request the activation of available flexibility.

A FlexibleElement can be either a Process or a Collection. A Process abstract an atomic flexible process like for example “space heating”. A Process is linked to one or more IoT Resources.

The Process state is essentially stored in its Flexibility object. Each time a Resource linked to the Process is updated the Forecaster upgrades the Process Flexibility. When the Process is requested to activate flexibility, it asks its ProcessController to set (in real-time) appropriate Resource parameters and to check that the request is really performed as expected.

A Collection features also a Flexibility. When the Flexibility of one of its member (either a Process or a Collection) is modified significantly, the Collection's Aggregator updates the proper Flexibility of the Collection.

Flexibility calculation for a Process or a Collection has to consider constraints (formalised using the Constraint interface).

When a Collection is requested to activate Flexibility, its Scheduler dispatches the request among all member elements.

The Collections listed in In Figure 10 (Household, Feeder, MarketGroup) are given as examples and are not part of the system model.

5.4.3 The SEMIAH Control package

FlexibleElements of the SEMIAH Objects package requires that an external entity interact with them to concretely activate available flexibility in whole or in part. This is precisely the role of a Controller instance.

A VPP (Virtual Power Plant) is a class, typically instantiated by a larger software component that orchestrates FlexibleElement instances to address market objectives and / or grid control objectives.

The definition of constraints for FlexibleElement instances is also a part of the SEMIAH Control package.

5.4.4 Example of objects for a simple SEMIAH system

Figure 11 presents a simple possible UML object diagram for a SEMIAH system. The HouseholdController "householder" manages flexibility of the Household "household1", which contains two Processes, each of them being linked to an object implementing the Resource interface. "household1"'s "consumptionMonitor" object typically holds the consumption of the household as measured by the electrical meter. The ProcessController "heatingManager1" is responsible for the real-time control of the heating system. The current temperature is passed to the SEMIAH Objects package through the "temperatureSensor1" Monitor interface.

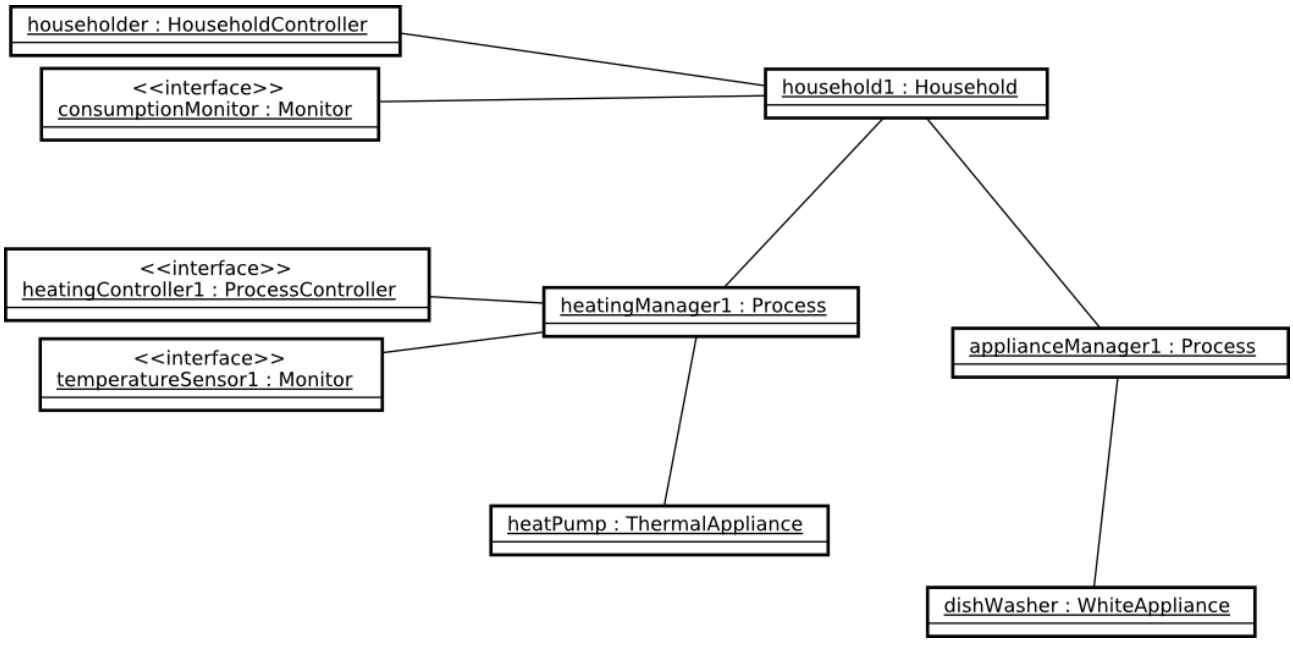

Figure 11: Example of a simple UML object diagram for a SEMIAH system.

5.4.5 Sequence diagram for flexible element status update

When the status of a Resource object is updated, the flexibility of a Process is updated through its Monitor interface. The flexibility of the Collections including that Process is also calculated anew.

A sample sequence diagram is presented on Figure 12.

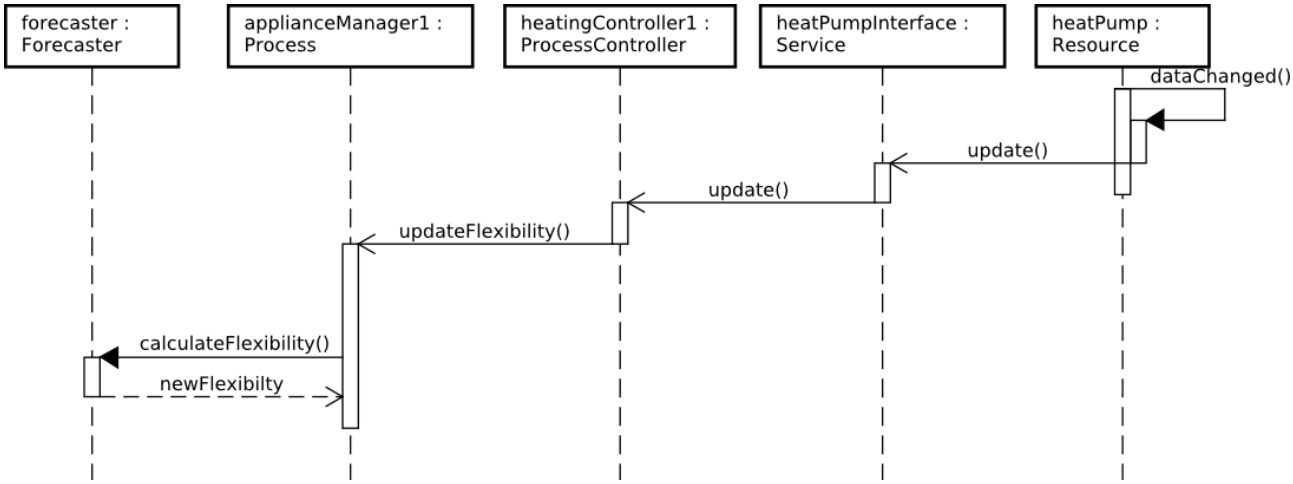

Figure 12: Sequence diagram for an updated Flexibility trigger example.

The figure shows a sequence diagram for a change in a Resource triggers Flexibility update of a Process and of a Collection.

5.4.6 Sequence diagram for a flexibility activation

A controller can ask FlexibleElement instances (for example a Household Collection instance as in Figure 13) to activate the flexibility by calling the setSchedule() method. The Scheduler dispatches the activation request among the Collection members. The Forecaster is responsible for updating the flexibility of Collections (basically, the requested flexibility is subtracted from the current flexibility). Finally, Process instances mandates their ProcessController to control Resources in real-time.

For simplicity, the sequence diagram of Figure 13 considers only one member per Collection. Obviously collections have several members and the setSchedule() method of each member is called.

Figure 13 shows only the transfer of a flexibility request from the Controller that originates from a ProcessController, which is in charge of implementing part of it. Each FlexibleElement must report to its parent Collection (or to the Controller) the status of the requested Schedule. This step is not shown in the sequence diagram.

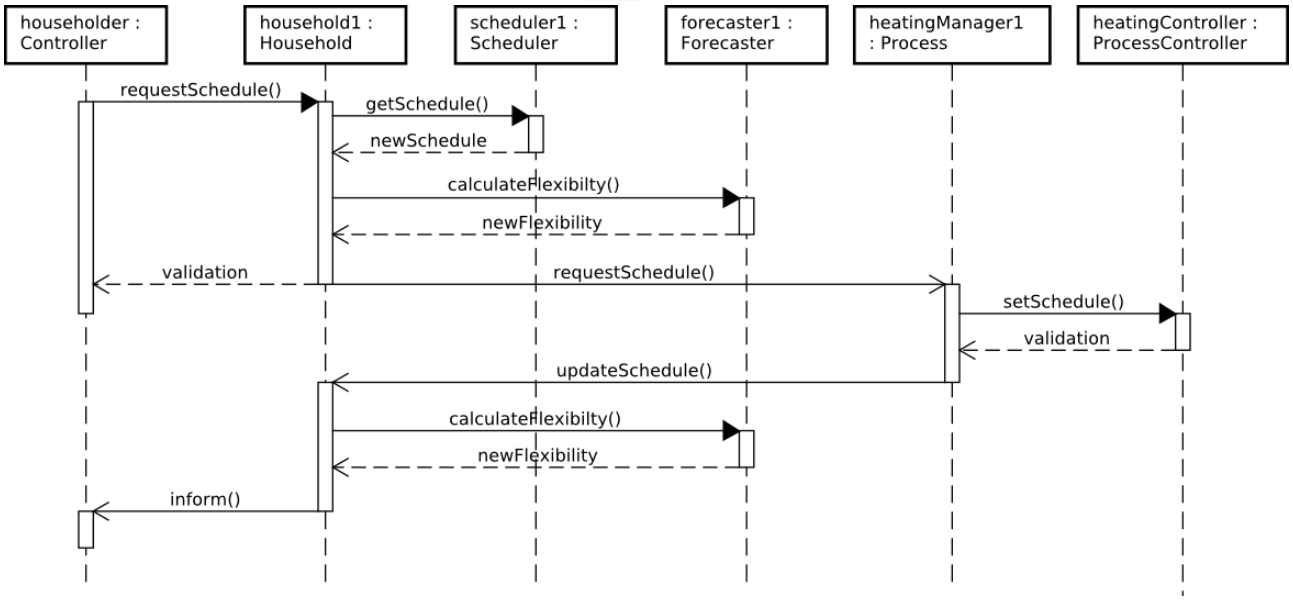

Figure 13: Sequence diagram: A Controller object requests schedule of flexibility

Whilst the previous section dealt with the system model of the key functions of the SEMIAH aggregation service provider, the project scope also depends on a two important areas of non-functional requirements: 1) Security and Privacy and 2) Scalability. These areas of non-functional requirements will be analysed and presented in the following sections.

5.5 Security and Privacy Models

This section describes the modelling of security and privacy in a SEMIAH context. It starts with an introduction to principles and best practices in cyber security. It introduces a threat model for SEMIAH and put this into the context of ENISA security. Finally, it discusses a trust model for SEMIAH and established a chain of trust.

5.5.1 Principles and Best Practices in Security

The different aspect of the best practices in security and privacy are presented from the 5-faceted model shown in Figure 14.

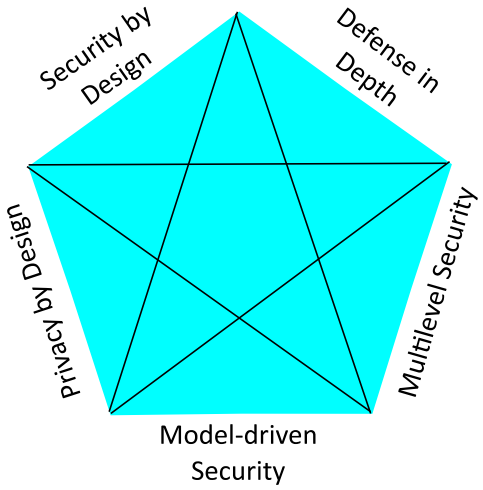

Figure 14: Model for best practices in security and privacy for system analysis.

A brief description of each facet in the model follows in the list below:

- **Security by Design.** Security by design, in software engineering, means that the software has been designed from the ground up to be secure. Malicious practices are taken for granted and care is taken to minimize impact when a security vulnerability is discovered or on invalid user input.
- **Privacy by Design.** Privacy by Design is an approach to systems engineering which takes privacy into account throughout the whole engineering process. The concept is an example of value sensitive design, i.e., to take human values into account in a well-defined matter throughout the whole process and may have been originally derived from this. The concept originates in a joint report on “Privacy-enhancing technologies” by a joint team of the Information and Privacy Commissioner of Ontario, Canada, the Dutch Data Protection Authority and the Netherlands Organisation for Applied Scientific Research in 1995.
- **Defense in Depth.** Defense in depth is a concept in which multiple layers of security controls are placed throughout an information technology (IT) system. Its intent is to provide redundancy in the event a security control fails or a vulnerability is exploited that can cover aspects of personnel, procedural, technical and physical for the duration of the system's life cycle.
- **Multilevel Security.** Multilevel security or multiple levels of security (MLS) is the application of a computer system to process information with incompatible classifications (i.e., at different security levels), permit access by users with different security clearances and needs-to-know, and prevent users from obtaining access to information for which they lack authorization.
- **Model-driven security.** Model driven security (MDS) is the tool supported process of modelling security requirements at a high level of abstraction, and using other information sources available about the system (produced by other stakeholders). These inputs, which are expressed in Domain Specific Languages (DSL), are then transformed into enforceable security rules with as little human intervention as possible. MDS explicitly also includes the run-time security management (e.g., entitlements/authorisations), i.e., run-time enforcement of the policy on the protected IT systems, dynamic policy updates and the monitoring of policy violations.

5.5.2 Coverage

Security should cover all aspects of the system:

- Information security
- Software security
- Physical security
- Hardware security
- Network and communication security
- Cloud services security

Important aspects of information security to cover:

- Confidentiality
- Access control
- Risk management
- Trust
- Resilience
- Integrity
- Availability
- Authenticity
- Non-repudiation

5.5.3 Threat model

The following are some common approaches to threat modelling:

- Attacker-centric (attackers' goals and how to achieve them)
- System-centric (possible attacks for each element of the system)
- Asset-centric (which assets are threatened)

The SEMIAH project will take a multi-faceted approach to threat modelling and start by enumerating important factors including system elements, valuables, attacker types and motivations, possible attacks, and potential attack points.

The important factors of the threat models are:

- System elements / assets
    - HEMG (OGEMA-based Home Energy Management Gateway)
    - HEM User interface for Configuration (web/smart phone)
    - Communication channel in home (ZigBee)
    - Controlled Home Devices
    - Communication channel HEMG to Back-end server (TCP/IP over broadband)
    - Back-end Server (Restful web services HTTP/HTTPS)
    - VPP
    - Market interface module
- Valuables to protect
    - Company confidential info (credentials, configurations, etc.), personaly identifiable information for users

  - Deep grid / ICT systems
  - Grid Stability
  - Access to Electricity for customers
  - Electricity Company revenue
  - Marketplace
- Attacker types
  - Hacker-as-hobby
  - Hacker-for-hire
  - Bad Neighbour
  - Bad Advertiser
  - Bad competing electricity company
  - Fraud
  - Insider
- Attacker motivations
  - Money (more business for competing company or hacker-for-hire)
  - Free (stolen) electricity
  - “Fun” (hobby-hackers or “script kiddies”)
  - Political reasons (sabotage against opposition, or terrorism)
  - Grudges (bad neighbours)
- Possible attacks
  - See abuser stories
- Potential attack points in the system to be protected
  - User (need to be warned about possible social engineering/phishing attacks)
  - HEMG
  - HEMG user interface
  - Local ZigBee communications
  - Local devices
  - Communication channel HEMG – back-end server
  - Communication channel DSO - back-end server
  - Communication channel energy supplier - back-end server
  - Communication channel forecast provider – back-end server
  - Communication channel third parties – back-end server
  - Back-end Server

5.5.4 ENISA-based Taxonomy of Threats

The proposed ENISA security measures for smart grids contain a taxonomy of threats for smart grid services:

- Natural disaster (fire, flood, thunder, environmental disaster, etc.).
- Damage, loss of IT assets (damage by 3rd party, test corruption, loss of information integrity, loss or destruction of devices, media, documents, media, information leakage)
- Outages (loss of Internet, network, support services, energy, lack of resources, personnel, strike).
- Nefarious activity, abuse/cyber-attacks (ID theft, spam, DoS, malicious code/activity, social engineering, abuse information leakage, rogue certificates, HW/SW manipulation, manipulate information, misuse of audit tools, falsification of records, misuse of information, information systems, unauthorised: access, administration, software installation, software use, compromising confidential information, abuse authorisations hoax, badware, remote activity, targeted attacks).
- Deliberate physical attacks (bomb attack/threat, sabotage, vandalism, theft, information leakage, sharing, and unauthorised physical access).
- Unintentional damage (Erroneous: information sharing/leakage, use or administration of systems/devices, use of unreliable information, unintentional alteration of data, inadequate design, planning/adaptation).
- Failures/malfunction (Device/system failures, disruption of communication links, power supply failure, service provider failure, malfunction).
- Eavesdropping, interception, hijacking (wardriving, intercepting information, man in the middle session hijacking, repudiation of actions, reconnaissance/information gathering, replaying messages).
- Legal (Unauthorised use of copyrighted material, failure to meet contractual obligations, violations of laws).

5.5.5 Trust Model

A fundamental concept in information security is the *chain of trust*. A chain of trust is a hierarchical trust model where each element gains/derives trust from being trusted by an element higher up in the chain. At the top of the chain is the *trust anchor*, for which trust is assumed and not derived. This may be trusted hardware in the case of a chain of trust in a software platform, or a root certificate authority (CA) in the case of a chain of trust for digital signatures and certificates. A variant of the chain of trust is the *web of trust*, forming a decentralised trust model as used by PGP[2] and GPG[3] for connecting a public key and its owner, as an alternative to the CA-anchored public key infrastructure.

5.5.5.1 Important factors for a trustworthy system

Software systems consisting of more than one component rely on the composition and cooperation of these components to successfully accomplish their purpose. These designs often depend on the correct functioning of the existing parts. They will be inherently insecure if any of these parts are run in a potentially hostile environment, for example in a mobile device or in cloud-based services in SEMIAH's case.

Offloading security functions from server to client exposes those functions to a much less trustworthy environment, which is one of the most common causes of security failures predicated on misplaced trust.

[2] Pretty Good Privacy (http://www.pgp.com)

[3] Gnu Privacy Guard (https://www.gnupg.org)

Designs that place authorisation, access control enforcement of security policy or embedded sensitive data in client software, thinking that it will not be discovered, modified or exposed by adversaries are inherently weak. Such design will often lead to compromises. For SEMIAH, this means that we should not trust pure client side access control decisions, for example using hard-coded user name and password in the home energy management gateway. The system should rather rely on a centrally managed federative access control system, using existing established and tested standards. The mobile devices should also use a centrally managed access control solution for accessing the web server. Also calls into the SEMIAH APIs from business partners (e.g. from the market side, DSO or TSO) should be considered client software which requires proper access control enforcement.

When untrusted clients send data to the SEMIAH system or perform a computation on its behalf, the data sent must be assumed to be compromised until otherwise proven. Such systems are therefore unsuitable for performing security sensitive tasks. In the case of SEMIAH, there will be limits for how much we can trust the underlying cloud-based platform. We should therefore be very cautious on how computations and data that may be sensitive are being treated in this case. We should also aim at building the home gateway secure by design, so that it by default can be trusted by the rest of the system.

5.5.5.2 The SEMIAH Chain of Trust

Trust boundaries

SEMIAH needs to identify trust boundaries for data in transit and protect these boundaries with appropriate data protection policies. There will for example be trust enclaves in SEMIAH for major functional blocks like the front-end, back-end and web server.

- Secure network communications
  - Encrypted links (e.g. HTTPS/TLS/IPsec).
  - Trust between services can be achieved by using digital certificates and requiring authentication by these certificates during link setup.

Front-end hardware

The HEMG (home energy management gateway) hardware should be reasonably tamper-proof and trusted as the root in the HEMG system chain of trust. The hardware should if possible only allow booting from signed software[4].

SEMIAH software platform (OGEMA)

Only signed applications from trusted sources can run on the platform. The software platform itself should only boot on trusted hardware. Only authenticated and authorised users are allowed to interact with the system. The system will communicate with the back-end using authenticated secure end-to-end connections to avoid data being intercepted by a man-in-the-middle attacker.

Software

Only signed software is allowed to run on the SEMIAH HEMG software platform. Only authenticated and authorised users are allowed to interact with the software.

[4] Note that this may not be possible to enforce completely, since the Develco hardware lacks a trusted platform module, which means that trusted boot will not be available.

Users

Users are required to perform secure authentication (preferably two-factor, at least for users with authority to perform changes to the system) to log onto the system. Authentication and authorisation should be back-end-based, not local to the HEMG.

In the case of a temporary internet connection failure, the HEMG will fall back to a basic energy management algorithm, and credentials caching can be used to allow access to the management interface in the case of shorter network outages

Back-end system

The back-end system should communicate business critical information with the HEMGs over authenticated secure connections. Internal communication between components of the back-end system; data handling and storage including proper management (preferably reversible anonymisation) of sensitive Personally Identifiable Information (PII); management of HEMGs and users should be not only efficient and scalable, but also secure.

External components and untrusted data in a potentially hostile environment

Can the HEMG trust the connected smart appliances? That the smart meter is sending correct data? That the heater is off when it says that it is off? On the other hand, can the smart appliances trust the HEMG? That the orders they receive are authorised by the user, and that the information they send will be handled with a sufficient level of confidentiality and integrity? Sanity checking and validation of all data is essential in a system where it is difficult to guarantee the trustworthiness of external components.

Data received from an untrusted source should always be properly validated before processing [30].

- Do not make assumption on ordering of API calls (e.g., in our case make REST calls idempotent where possible, to make the code independent of server side state.)
- Do not assume that the user interface is able to restrict what the user can send to the server (i.e., performs boundary control checks, use typed SQL clauses instead of strings etc.).
- Avoid building business logic solely on the client side, or attempting to store secrets in the client.

If private or confidential information must be stored or sent to the client, the system should be designed to be able to cope with potential compromise, i.e. the sensitive information should not be revealed. In particular aim at avoiding the following pitfalls:

- The same shared secret should not be used on all the clients, use different shared secrets.
- If necessary, make the validity of what is stored on the client limited in time.
- Design the system to degrade gracefully if one or a set of clients have been compromised.
- Consider the context where code will be executed, where data will go and where data comes from, in order to avoid vulnerabilities due to trusting components that are not trustworthy.
- Identify and block malicious actors.

6 Non-functional Requirements of SEMIAH

Non-functional requirement is a requirement that specifies criteria that can be used to judge the operation of a system, rather than specific behaviours. Non-functional requirements complement the functional requirements of a system and are often a result of the analysis of the availability, stability, scalability, etc. but also other aspects such as e.g., safety, security & privacy, and performance.

In SEMIAH there are two categories of non-functional requirements that need special attentions since these constitute main research challenges of the project. First, the SEMIAH system has to be able to scale to a large number of households (>200.000) to provide an aggregated demand response. Second, the system must be secure and must provide a proper level of privacy protection. These sets of non-functional requirements will be discussed in the following sections.

6.1 Scalability

6.1.1 Non-functional requirements for Scalability, Availability, and Interoperability

The following Table summarises the non-functional requirements concerning the scalability of the SEMIAH system. The requirements on scalability have been derived from the SEMIAH DOW section B1):

Req. id.	Key element	Description
6.1.1.1	Scalability	Development of aggregation, forecasting and scheduling algorithms capable of managing at least 200 000 households.
6.1.1.2	Availability	Integration and verification of back-end system to ensure 24/7 operation.
6.1.1.3	Scalability	Deployment of demonstrator in 200 households.
6.1.1.4	Scalability	Development of a large-scale simulator to emulate the behaviour of 200 000 households.
6.1.1.5	Scalability	The deployment of SEMIAH in 200.000 households would allow the shifting of 90 GWh/year of electrical consumption from fossil fuels to RES, thereby reducing the gap between RES produced and consumed.
6.1.1.6	Scalability	Peak peak reduction can help in saving energy by 120 GWh/year.
6.1.1.7	Interoperability	Solution will be compliant with the IEEE 2030-2011 standard for Smart Grid interoperability.
6.1.1.8	Scalability	SEMIAH should be able to manage entire systems and millions of appliances and TWhs of energy by designing an architecture that is inherently parallelisable, scalable, reliable and robust.
6.1.1.9	Performance	The system will have real-time Demand-Response within less than 5 minutes response time.

Table 9: Scalability requirements

6.1.2 Scalable Security Management

The security management process also needs to handle the security erosion which occurs because threats change over time and system changes and new features may introduce new threats and vulnerabilities. Efficient system and configuration management is very important for SEMIAH, since it will need to be able to scale to potentially millions of home energy management gateways. This means that secure design must keep flexibility in mind. The system must support an efficient and secure update mechanism for handling patching of vulnerabilities.

6.1.3 Cloud Computing Environment

To satisfy the scalability requirements, SEMIAH should be able to run the virtual power plant as a cloud-based service. This has several implications both from a security and privacy perspective which will be investigated in this section.

Essential characteristics of cloud-based services, is that it is an on-demand self-service with broad network access, so that different thin or thick clients, phones, laptops, workstations, servers, etc. can connect to these services. Cloud-based services provide resource pooling, so that hardware resources can be shared using virtual machines and dynamically assigned on-demand. Such services also provide rapid elasticity, so that the service can scale rapidly up or down on demand. It is also a measured service, so that you typically can have a “pay-as-you-go” subscription, where you only pay for the computing resources that are being utilised.

6.1.4 Cloud Service Models

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The two former service models will be discussed below. The latter service model is not considered relevant for the SEMIAH project.

6.1.4.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service is the most basic cloud-based service model. This essentially means that you can manage processing, storage, networks as well as run arbitrary software (operating systems or applications) on top of the cloud-based infrastructure.

It is possible to define and control your own virtual infrastructure using IaaS, but you do not control the underlying cloud infrastructure (i.e., the Virtual Machine Monitors - VMM).

OpenStack (http://www.openstack.org) is a free and open source cloud computing platform initially made to be API compatible with Amazon Web Services. It is being managed by the OpenStack foundation, and was started by Rackspace hosting and NASA. Several large companies has since joined the foundation, including Ericsson, Oracle, several Linux vendors, VMWare and IBM. The objective is to create a standardised IaaS execution environment.

One challenge a Norwegian or Swiss VPP providers might experience with cloud services, is that cloud providers within EU might not send harddisks containing copies of sensitive data to non-EU countries for legal reasons. This happened when the Norwegian company Geodata sent harddisks to Amazon Web Services (AWS) in Ireland in order to copy large amounts of data into the servers. AWS subsequently denied sending the disks back, because Norway was outside EU [28]. Similar scenarios could happen if virtual power plant companies need to back up large amount of cloud stored data in order to have local copies of them. This shows that one must remember that there may be legal issues with cloud-based services, as well as remembering that there actually is some real hardware running in the cloud. It may matter where this hardware is running, especially for critical infrastructures like the Smart grid, and it may not be trivial to copy or back up large amounts of data via cloud-based services. This is not an issue for the SEMIAH demonstrators, but it could be a risk to consider when the deployed service grows large.

A limitation with using IaaS, is that SEMIAH will need to manage the cloud infrastructure itself. There is no easy way to scale the virtual services up beyond the capacity of a single underlying hardware server. It is possible to add a software layer on top of these virtual services that handle redundancy and adds scalability by adding virtual servers, however if this is necessary, then it might be better to consider the next service model: Platform as a Service (PaaS), which inherently supports such scalability.

6.1.4.2 Platform as a Service (PaaS)

Platform as a Service (PaaS) means that you deploy your own or purchased applications using the cloud provider's application programming interface (API). Examples of such interfaces are Amazon Web Services or Google App Engine.

An advantage with PaaS is that the platform does all the heavy lifting of abstracting the cloud programming interface from the underlying hardware. The cloud service provider also typically provides some guarantees for the basic security of the underlying platform in the form of a service level agreement (for example detecting and patching software vulnerabilities, detecting attacks on the infrastructure etc.). This means programming towards virtual cloud resources that are elastic and can dynamically scale up or down according to need. This solves much of the technical problems on how to deploy systems and how to handle scalability that otherwise must be explicitly considered if Infrastructure as a Service is being used. For SEMIAH, PaaS would allow the virtual power plant to scale up or down according to need, without having to consider limitations in the underlying hardware. Designing the VPP scheduling as a PaaS service could for example be one way to ensure that the scheduling scales sufficiently well.

A potential downside is however the pay-as-you-go model, which may be expensive, depending on the business scenario, especially for data-heavy applications sending many messages.

A drawback with PaaS, is that the platforms are not yet standardised, which being locked in to the API of the cloud service provider [29]. This may make it a challenge to move the service to another and possibly cheaper cloud provider, which is not desirable for SEMIAH. A risk could be that the PaaS provider went out of business. What do you do then? Another challenge with PaaS, is that you then depend on the security model of the cloud provider, which may not be sufficient to the needs of SEMIAH. This means that security controls, for example encryption needs to be added on top of the virtual power plant application. This means that the application is responsible for its own security, and must take necessary precautions since it runs in an environment that may not be sufficiently trustworthy. It may then be better to use existing solutions or software on Infrastructure level which has a proven security track record, provided that one is willing to take the additional cost of properly managing the security of the different virtual machines.

One advantage with PaaS is that it usually ensures some level of data integrity and data persistency, ensuring that data is being backed up several places. Transaction support ensures the possibility to roll back to a previous state. This means that SEMIAH may not need to explicitly manage backups with a PaaS solution, given that the PaaS provider is considered sufficiently trustworthy. It is still possible to back up the entire data store, if a local backup is desirable. Objects in the data store (an object-oriented nosql database) will however need to be explicitly encrypted when confidentiality protection is required.

6.1.5 SEMIAH and the cloud

SEMIAH will consist of a mix of SEMIAH specific components, proprietary software modules from Misurio and Fraunhofer as well as hardware units running OGEMA. This means that SEMIAH will not be able to run a pure cloud-based service model. The service model will need to be a hybrid between cloud and own managed devices, as well as potentially a hybrid between own cloud infrastructure and platform-as-a-service, if we decide to use this.

6.2 Security and Privacy Requirements

This section refines the non-functional requirements related to security. Requirements are organized in accordance with the model for security and privacy described in Section 5.5.

6.2.1 Security by Design

The system shall adhere to the principles of security by design as far as possible. This results in the following set of non-functional requirements:

Req. id.	Key element	Description
6.2.1.1	Trust	Earn or give, but never assume trust.
6.2.1.2	Authentication mechanism	Use an authentication mechanism that cannot be bypassed or tampered with.
6.2.1.3	Authorisation	Authorize after you authenticate.
6.2.1.4	Separate data and control instructions	Strictly separate data and control instructions, and never process control instructions received from untrusted sources.
6.2.1.5	Validate all data	Define an approach that ensures all data are explicitly validated
6.2.1.6	Use of cryptography	Use cryptography correctly. Here the term “correctly” covers many aspects. Several standards on cryptographic provides code examples for cryptographic routines to ease a correct implementation. Also certified software and hardware components are available in the market.
6.2.1.7	Sensitive data	Identify sensitive data and how they should be handled.
6.2.1.8	Consider users	Always consider the users.
6.2.1.9	External components	Understand how integrating external components changes your attack surface.
6.2.1.10	Change handling	Be flexible when considering future changes to objects and actors.To control change of a system a well-defined change management procedure should be implemented.

Table 10: Security by design requirements

6.2.2 Privacy by Design

The system shall adhere to the principles of privacy by design as far as possible. This results in the following set of non-functional requirements:

Req. id.	Key element	Description
6.2.2.1	Proactive, not reactive; Preventative not	SEMIAH should aim at utilising proactive measures for protecting private or confidential information, where the design anticipates and prevents privacy-invasive events before they happen.

	remedial.	
6.2.2.2	Privacy as the default setting.	SEMIAH should aim at protecting users' personal data by default. This means that if the user does nothing, then their privacy remains intact.
6.2.2.3	Privacy embedded into design.	SEMIAH aims at embedding privacy into the design and architecture of the Demand Response system. It will not be bolted on as an add-on after the fact. This means that privacy becomes an essential component of the core functionality being delivered. Privacy will be integral to SEMIAH, without diminishing functionality.
6.2.2.4	Full functionality – positive sum, not zero sum.	Privacy by design aims at accommodating all legitimate interests and objectives using a "win-win" approach. Privacy and security functionalities complement and enhance each other. This is not only a theoretical statement. We expect that there for example will be direct synergy between functionality required to protect confidentiality and privacy, for example in the case of secure logging systems providing forensics capabilities of who did what for sensitive system operations. The same base technologies can be used for protecting the users private data [5].
6.2.2.5	End-to-end security – full lifecycle protection.	Privacy by design should apply from private or confidential data is being created and until it can be securely destroyed in a timely fashion. SEMIAH may need to utilise several cryptographic techniques in order to achieve this, including end-to-end link encryption, encryption of sensitive data at rest as well as methods for secure destroying of such sensitive data, for example by invalidating keys. This ensures that also all backup copies of such data are being invalidated. It furthermore means that strong, centrally managed access control mechanisms should be used, in order to ensure that sensitive data can be destroyed at end of subscription.
6.2.2.6	Visibility and transparency – keep It open.	This ensures that all stakeholders can be assured that SEMIAH is operating according to the stated promises and objectives, subject to independent verification. Its components and operations remain visible and transparent to users and providers.
6.2.2.7	Respect for user privacy – keep it user-centric.	This means that SEMIAH should keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice and empowering user-friendly options.

Table 11: Privacy by design requirements

6.2.3 Methods and Tools for Security and Privacy Management

Following are optimal requirements related to methods and tools for security and privacy management. This results in the following set of non-functional requirements:

Req. id.	Key element	Description
6.2.3.1	Risk assessment/gap analysis, safeguards, vulnerability management	Methods and tools for risk assessment/gap analysis, safeguards, and vulnerability management will be defined.
6.2.3.2	Anonymisation, pseudonymisation, encryption to reduce identified privacy leakages	Methods and tools for anonymisation, pseudonymisation and encryption to reduce identified privacy leakages will be adapted from the Reversible anonymiser and the PRECYSE toolkit.

Table 12: Requirements for tools and methods in security and privacy

A set of tools to support security and privacy is available in SEMIAH. The relevant tools are briefly introduced here and further elaborated in SEMIAH Deliverable D8.1:

- **Reversible anonymiser.** The Reversible anonymiser for XML documents is a tool that supports anonymisation of XML documents and messages using an eXtensible Access Control Markup Language (XACML) anonymisation and authorisation policy [6].
- **XACML policy editor.** The XACML policy editor is a related project which has defined an easy to use policy editor for XACML authorisation and anonymisation policies. The policy editor provides graphical policy language that is easy to use for policymakers, and removes much of the complexity in managing the complex XML-based XACML policies.

7 Reference Architecture

Among the most prominent architectural solutions for the smart grid, SGAM [9], IEEE 2030 [10] and the IoT architecture are the ones most representative of the work that is being done in the project. As they have already been described in referenced documents, only the parts most implied in the SEMIAH project have been included here.

The following sections introduce the relevant reference architectures and then describe the SEMIAH high-level functional architectures.

7.1 SGAM Architecture

Today, the Smart Grid Architecture Model (SGAM) is one of the most compelling and holistic views of the Smart Grid [9]. The architecture aims to provide a description of it from two perspectives. The first perspective deals with the five different interoperability layers. This layer can be separated in from a functional point of view: Component, Communication, Information, Function, Businesses and a smart grid plane with a high level of granularity that further separates the Smart Grid into Domains: Generation, Transmission, Distribution, DER and Customer Premises and Zones: Process, Field, Station, Operation, Enterprise, Market. This description of the smart grid has been depicted in Figure 15.

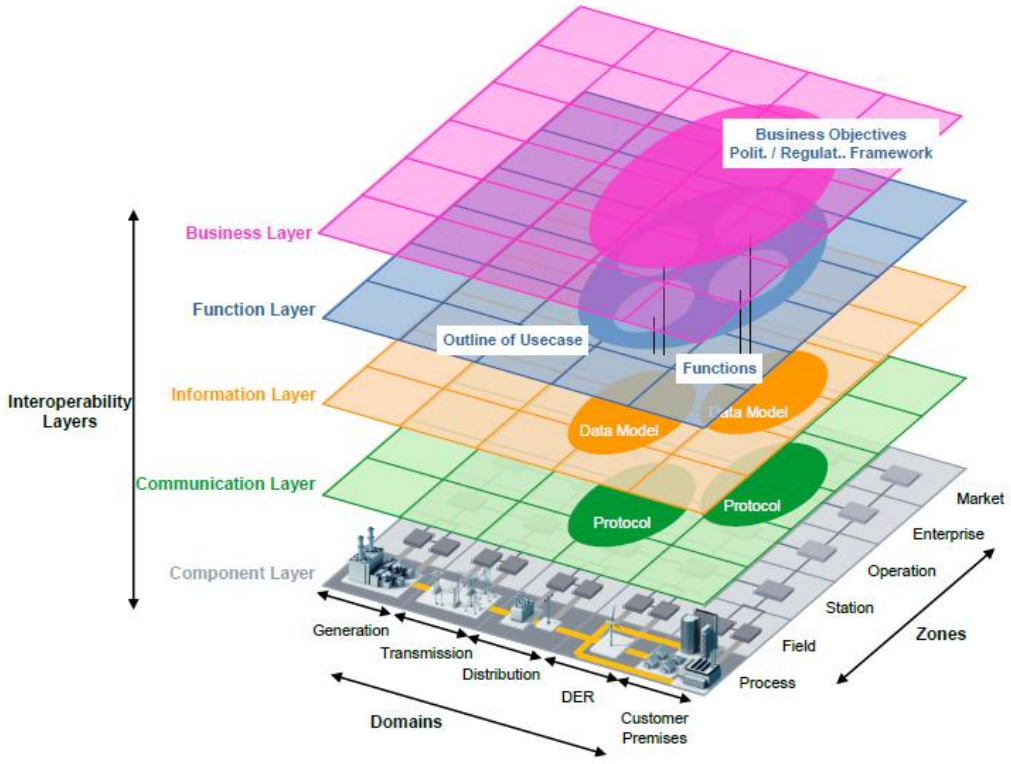

Figure 15: SGAM framework interoperability layers. Reproduced from [9]

The Smart Grid Plane covers the complete electrical energy conversion chain. This includes the domains listed in Section 3.1 with the additions of a DER domain Representing distributed electrical resources directly connected to the public distribution grid. These distributed electrical resources may be directly controlled by DSO responsible for the distribution of electricity.

The SGAM zones represent the hierarchical levels of power system management which considers the concept of aggregation and functional separation [9]. By the concept of aggregation in power system management the following aspects are considered:

- Data aggregation: data from the field zone is usually aggregated or concentrated in the station zone in order to reduce the amount of data to be communicated and processed in the operation zone.

- Spatial aggregation – from distinct location to wider area (e.g. HV/MV power system equipment is usually arranged in bays, several bays form a substation; multiple DER form a plant station, DER meters in customer premises are aggregated by concentrators for a neighborhood)

The concept of SGAM Zones is further elaborated in Section 7.2.5 of [9].

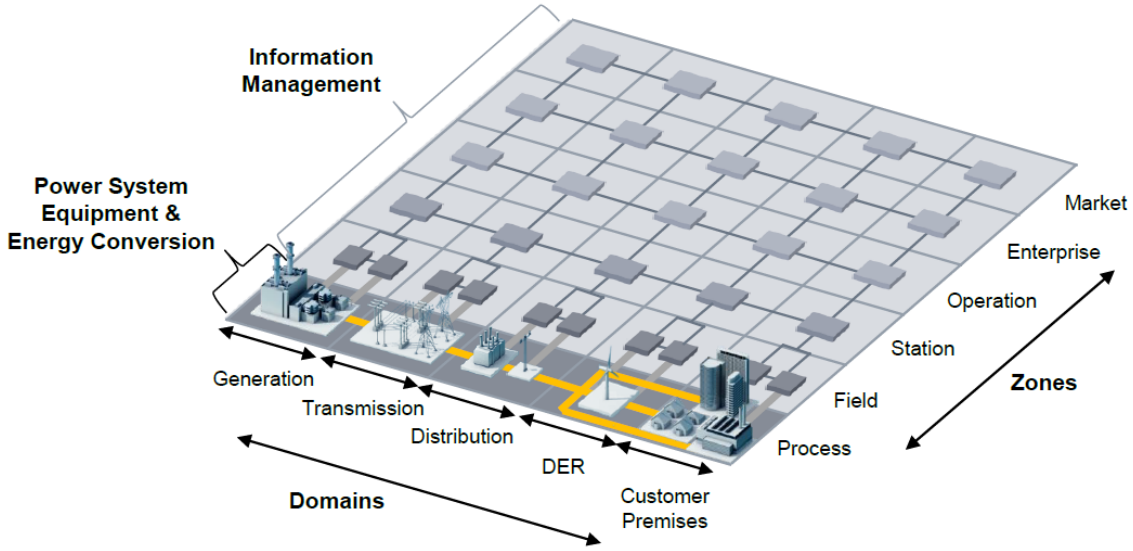

Figure 16: Smart grid plan with domains and zones mapping. Reproduced from [9].

This separation put forward by the SGAM model is very useful to divide tasks according to the requirements. As far as this document is concerned, the SEMIAH architecture would be placed at the information layer.

Furthermore, it is also somewhat linked to the Communication layer, for in the SGAM model it is charged with protocols and mechanisms that aim to guarantee the interoperable exchange of information between entities, among other duties.

The system architecture can be based the architectural model as defined by IEC. An interactive version of this model is available in [4]. This model is aligned with the Smart Grid Architectural Model which is described under the M/490 mandate in [1].

7.1.1 Flexibility functional architecture

In [2] a flexibility functional architecture is described. The architecture supports the DR/DSM together with automation functions on the customer side, here called the Customer Energy Manager or CEM. The CEM provides the flexibility of connected smart devices, through the energy management gateway, while the smart metering and the simple external consumer display provide a number of functionalities. The energy management gateway communicates with the metering channel and the smart metering through the Smart Metering Gateway.

Note that the actors in the architecture are functional entities from Table 8. The communication path between the smart metering gateway and energy management gateway is optional. The information exchange between the metering channel and energy management channel will take place between Actor A and Actor B by using communication related to grid operation through the electricity markets.

The external actors A and B, identified in this functional architecture represent (systems of) market roles that communicate through the Smart Grid Connection Point (SGCP). The actual role of actor A or B depends on the local market organization in a member state and competition. In the scope of this report, actor A is defined as the external actor communicating with the energy management gateway while actor B is defined as the external actor communicating with the smart metering gateway.

Functionalities of HES, NNAP, MDM, smart metering and the simple external consumer display are described in more detail in [2].

The communication in the metering channel (going via MDM, HES and NNAP) is not described in detail in the use cases of the demand and production (generation) flexibility cluster since, in these use cases, their function is to pass through the information sent between smart metering gateway and actor B. Although the NNAP and LNAP can include intelligence to locally and independently implement Smart Grid services and applications, their service in the current flexibility use cases is to pass through the information.

This functional architecture can be mapped to the SGAM as shown in Figure 17.

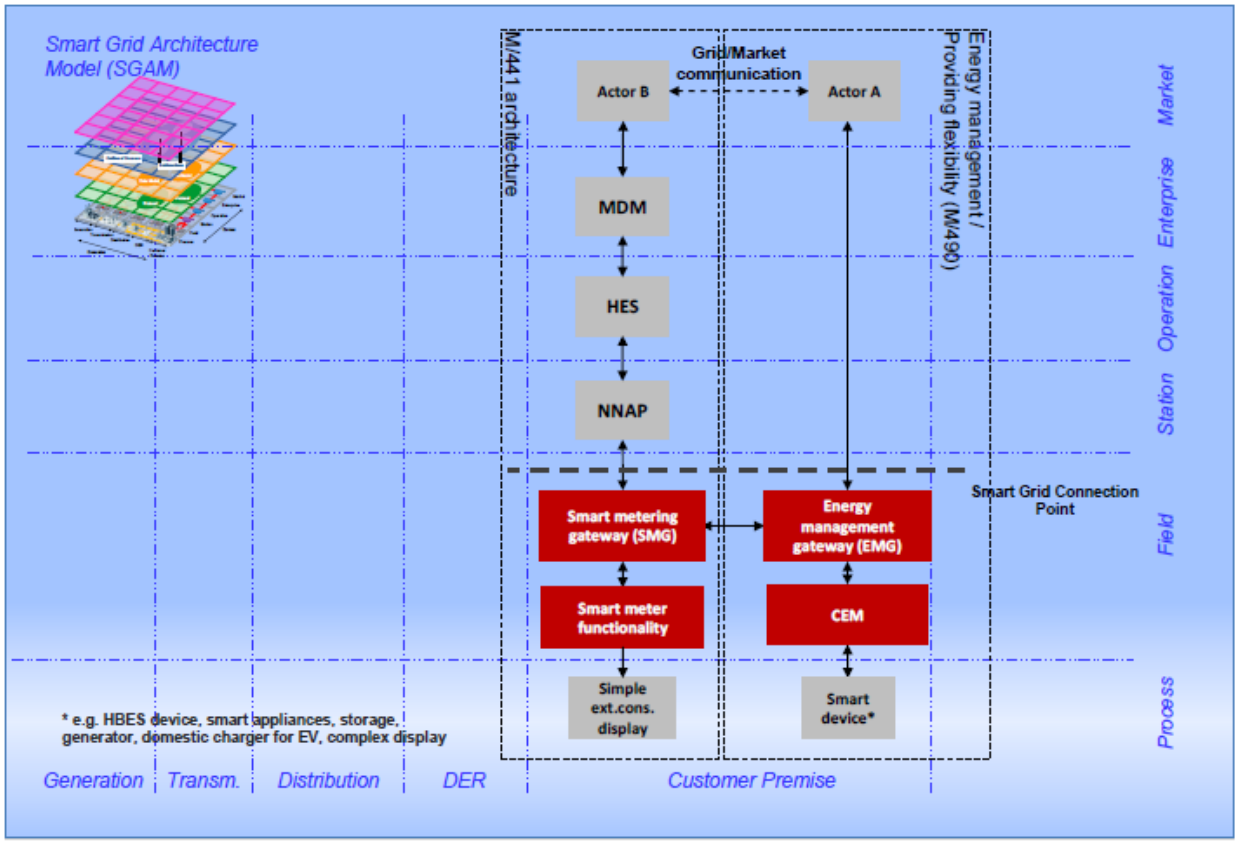

Figure 17: Flexibility functional architecture from [2]

Two logical systems are present under the SGCP: a smart metering and a CEM. Together, they define the logical and physical borderline and interface from the customer to the grid/market or from the grid/market to the customer. Although tariff may change without automatic response like time-of-use tariffs (TOU) these are possible and considered as a simple DR application. An

automatic reaction on tariff changes, like e.g., a combined real-time price / volume tariff or other signals from outside shall make use of flexibility offers from the consumers. This automatic reaction will be managed by the CEM.

The CEM is a logical function optimizing energy consumption and or production based on signals received from the grid, consumer's settings and contracts, and devices minimum performance standards. The CEM collects messages sent to and received from connected devices; in particular in the in-home/building sector. It can handle general or dedicated load and generation management commands and then forwards these to the connected devices. It provides vice versa information towards the "grid / market". Note that multiple loads/generation resources can be combined in the CEM to be mutually controlled.

7.1.2 Mapping of SEMIAH to SGAM

The overall view of all main systems of a smart grid onto the SGAM plane allows positioning each system in the domains and zones, as shown in Figure 18 [1]. The introduction to these main systems is given in Table 3 of [1].

In SGAM, the SEMIAH system belongs to the *Aggregated Prosumers Management System* and belongs to the *Demand and Production (generation) Flexibility* Systems. The Aggregated prosumers management system comprises the Advanced Metering Infrastructure (AMI) itself, the Home Area Network (HAN) gateway, customer energy management systems (CEM), building management systems and smart devices. These are elements in a demand response management system, which offers alternative channels to the home/building, the AMI being one of them.

The function or domain of this system is described as *Demand and Production (generation) Flexibility Systems*, and these are its defined use cases (Reference [1], chapter 7.5.1):

- Generation forecast
- Load forecast
- Load forecast of a bunch of prosumers in a demand response program (from remote)
- Managing energy consumption or generation of DERs via local DER energy management system bundled in a DR program
- Managing energy consumption or generation of DERs and EVSE via local DER energy management system to increase local self-consumption
- Participating to the electricity market
- Receiving meteorological or price information for further action by consumer or CEM
- Registration/deregistration of customers in DR program
- Registration/deregistration of DER in DR program

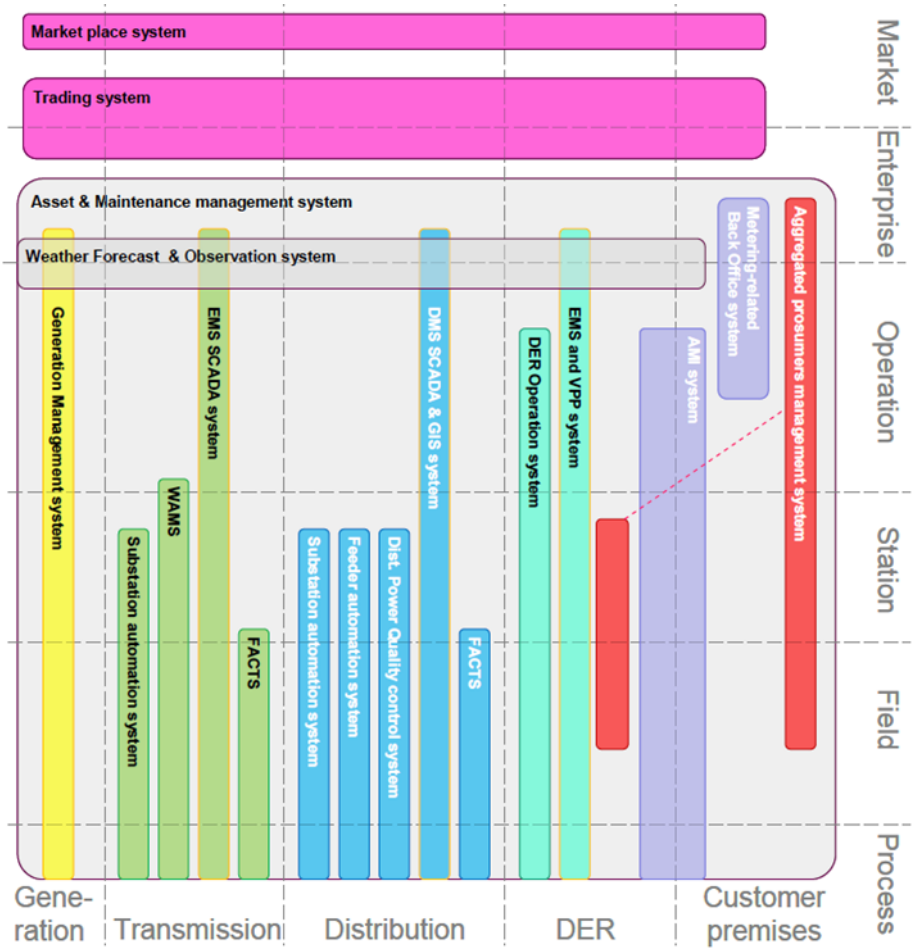

Figure 18: The smart grid systems mapped on SGAM (from [1]).

From [1] we derive a relevant set of use cases for SEMIAH by looking at the Aggregated prosumer management subsystem. The relevant high level use cases are (only titles provided for simplicity):

- Receiving meteorological or price information for further action by consumer or CEM
- Direct load/generation control signals
- Managing energy consumption or generation of DERs via local DER energy management system bundled in a DR program
- Registration/de-registration of smart devices
- Enabling remote control of smart devices

Use cases for smart grid development under the mandate M/490 are stored in the Use Case Management Repository (UCMR). The use cases are available from https://usecases.dke.de/sandbox/. To inspect use cases a “dummy user” with read-only rights can be used (user name: LookatMe; password: LookatMe). An example of a display of a smart grid use case entitled “Retrieve status of smart device” is shown in Figure 19.

Annex C lists the generic use cases from the repository that are considered relevant for the SEMIAH project.

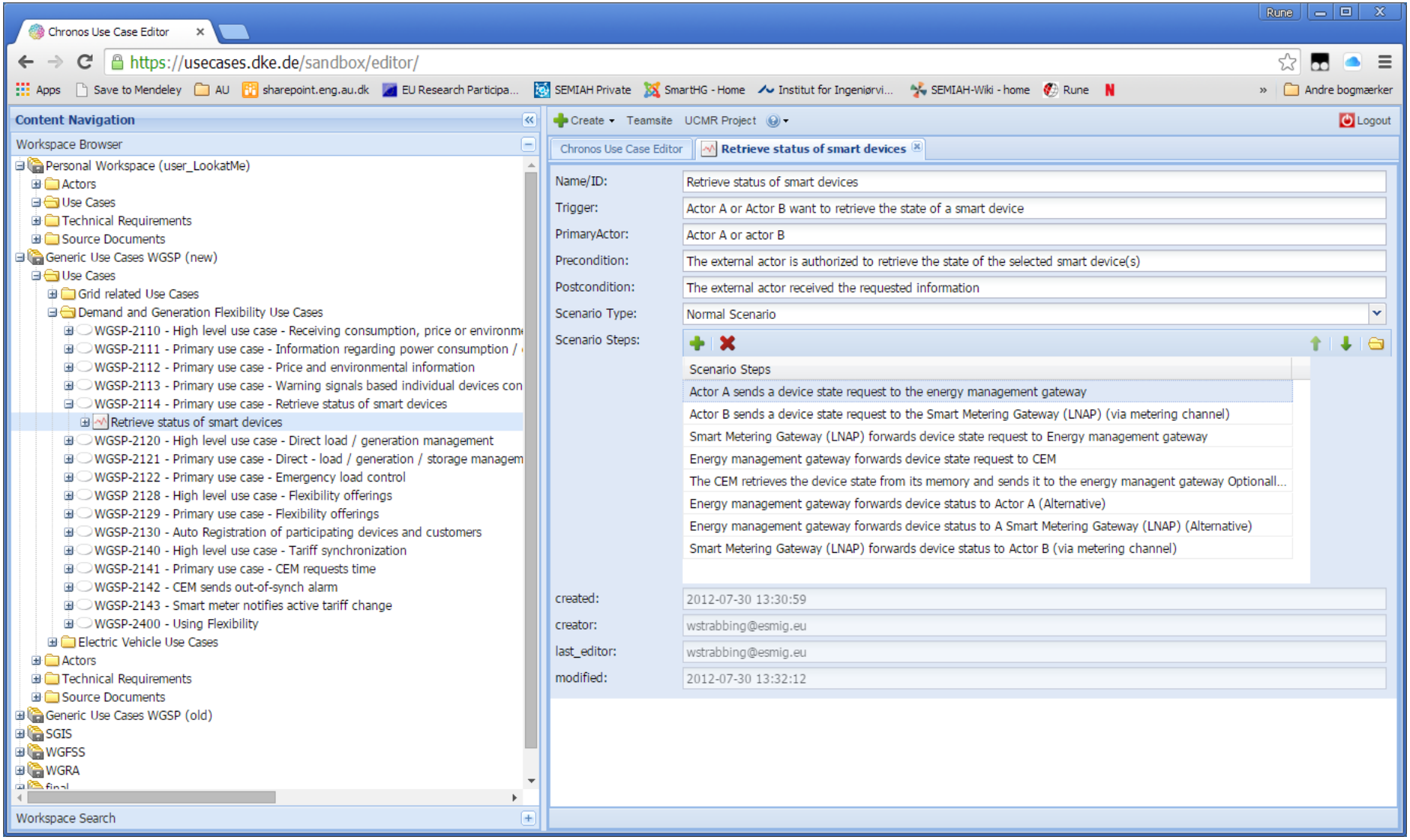

Figure 19: Example of use case from UCMR

A mapping of our actual SEMIAH components to SGAM has been done in Figure 20. Colour coding is used for different SGAM layers. The gray boxes are components; the blue boxes belong to the function layer, while the green boxes are on the communication layer.

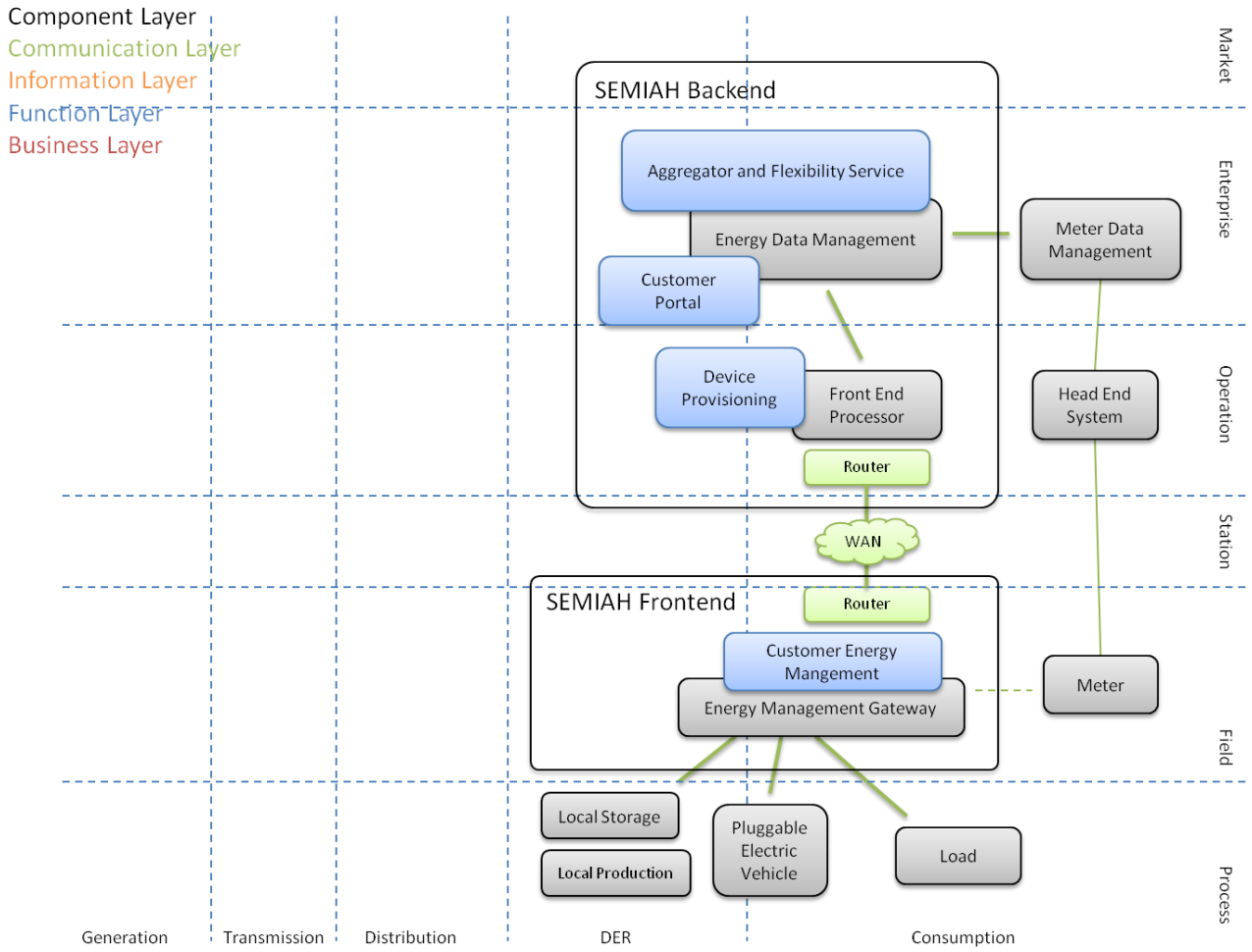

Figure 20: Mapping of SEMIAH functional components/subsystems onto SGAM.

There is a split between functions that are close to zones: Market, Enterprise, Operation and functions that are close to the Field and Process zones. Hence, it becomes natural to provide a clustering of functions that belong to the SEMIAH back-end and SEMIAH front-end respectively.

Table 13: Short descriptions of SEMIAH high level functions.

Function name	Short description
Aggregator and Flexibility services	The function provides aggregation and scheduling of appliance loads for a large number of prosumer households that offers their flexibilities to the SEMIAH system. Aggregation takes into account constraints of the grid such as e.g., feeder capacity. The function needs accurate load and generation forecasting for efficient scheduling. The scheduling takes into account the constraint of the households. The aggregated DR from the function is provided is input for the electricity wholesale market as

	aggregated flexibility offers. Such flexibility offer needs to take into account the constraints of the electricity markets such as the “size” of a demand response e.g., tradeable units of 5 MWh.
Customer Portal	The function provides an interface between the SEMIAH system and the SEMIAH members (customers). These customers can configure the flexibility offers by providing information about home appliances and flexibility.
Device Provisioning	The function prepares an installation of a SEMIAH system in a household. It allows the customer to run through an initial configuration procedure and connects the household with the DR services of the aggregator. Cyber security and privacy protection settings are also put into operation.
Customer Energy Management	The function is responsible to run households based on information and controls provided by the Aggregator and Flexibility services function. The function provides sensing and actuation in the household and is responsible for connecting smart appliances to the SEMIAH system.

7.2 IEEE 2030 Standard

Unlike SGAM, that attempts to establish a more holistic point of view regarding the smart grid, IEEE 2030 is targeted towards system interoperability [10]. One of its main ideas is the ability to have a collection of devices with different features scattered among several subsystems, not necessarily related one to the other, and interacting with each other by means of device interfaces.

The standard attempts to shift from a very specific deployment (Advanced Metering Infrastructure, etc.) to a more general one that will allow the application of high level overviews (NIST, IEC, etc.) as depicted in Figure 21.

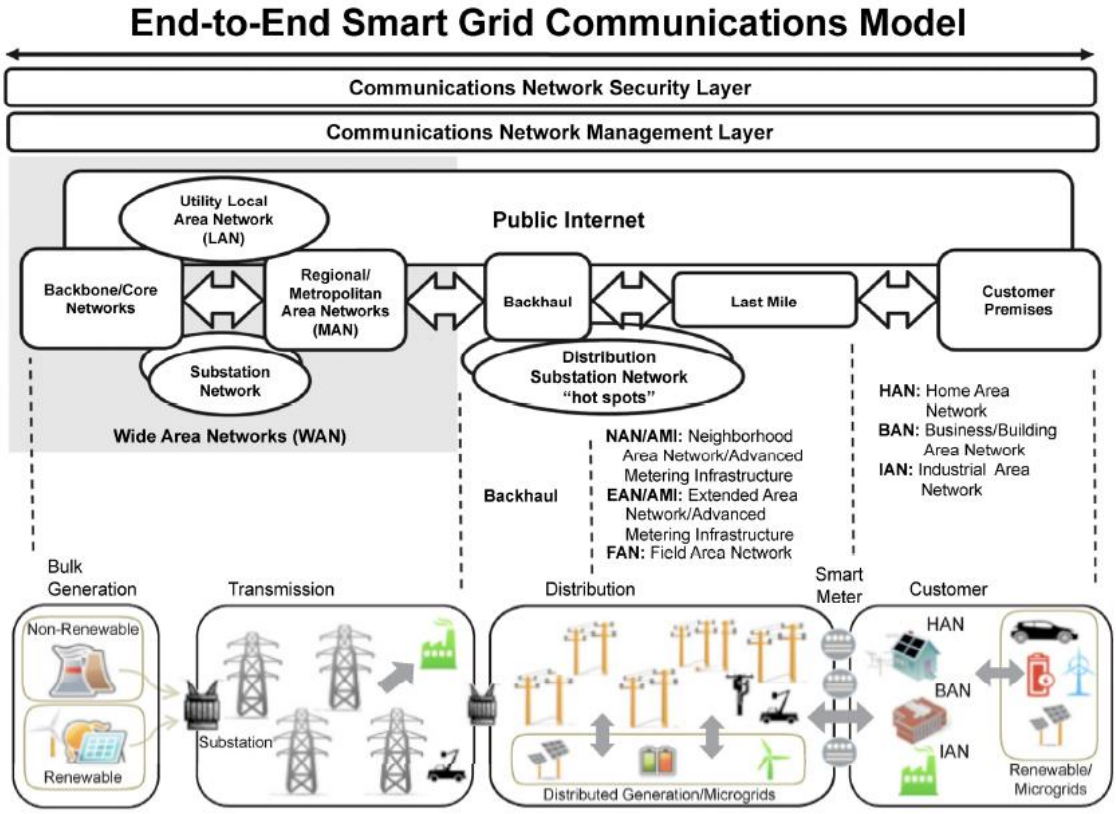

Figure 21: Smart grid model of IEEE 2030. From Ref. [10]

The methodology used in the standard focuses on three interoperability architectural perspectives (IAP) to describe the smart grid: Power Systems (PS-IAP) view, Communication Technology (CT-IAP) and Information Technology (IT-IAP). This segmentation allows the different types of interoperability to be sorted.

Although the focus of the IEEE 2030 approach primarily copes with integration and interoperability between the power grid and Information and Communication Technologies, it has been useful as inspiration for a middleware architecture that will offer interoperability both for hardware devices effectively, Advanced Metering Infrastructure- and applications that are expected to be utilized by end users in a comfortable manner.

The SEMIAH project aims to adapt to the interfaces specified in the IEEE 2030 standard for smart grid interoperability.

7.3 Internet of Things Reference Architecture

Internet of things (IoT) is a technology which allows physical objects to form an interconnected information network. The physical objects ("things") that are in use in everyday life have the possibility to gain new capabilities as they become part of the IoT technology.

The main driving reason behind the IoT technology is to provide the capability for any physical object to be connected at any time, to anything or anyone and anywhere IoT group cluster book (www.internet-of-things-research.eu/cluster_book.htm). This ubiquitous connectivity provides opportunities for improved control and management of real world objects from perspectives ranging from automation to business processes.

Smart grid: is an intelligent energy distribution network. Smart grid uses sensors monitoring different aspects of the energy distribution network in order to ensure stability and reliability of energy distribution. Unlike the present electrical grid, the electrical smart grid does not only transfer electricity but also data. These data are then used to adjust the grid parameters. This directly relates to IoT technology, as in smart grids there will be sensors embedded in different parts of the power grid such as e.g., in the substations. The data then have to be transmitted wirelessly or by wire to the monitoring center where decisions regarding the grid performance are taken. Data from the grid will also be accessible to consumers and producers in order to balance the electricity production and consumption. This will lead to easier management of renewable sources of energy connected to the distribution network.

Smart house: is a concept of technology where household appliances communicate with one another (M2M) and to the inhabitants of the house (M2H) in order to automate specific household tasks as well as improve the comfort for inhabitants. Also the building itself is embedded with sensors, detecting the location of the inhabitants and setting house parameters accordingly. This concept again closely relates to IoT technology. Appliances will have communication capabilities and possibilities of remote control, which means they will be able to identify themselves to the network, communicate data to the owner or receive remote commands from the owner. Data from the smart house could be also used for cooperation with smart grid technology that would provide the grid with capabilities of demand response.

Smart appliances: Smart appliance is a concept where household appliances are embedded with identification and communication capabilities. This will enable the ability to the appliances to be controlled remotely or by centralized control system in a household and receive data from appliances. The service center of the manufacturer of the appliance can also utilize the data for remote diagnostics. Smart appliances are a subset of the smart house concept and by enabling demand response also extends to the smart grid technology.

The IoT technology consists of different building blocks (technologies and devices) and their interoperability. The integration of these building blocks to work together for a unified purpose forms the IoT architecture. The architecture of an IoT system can be broken down into three different high level architectural layers as endpoint devices, middleware and cloud services as illustrated in Figure

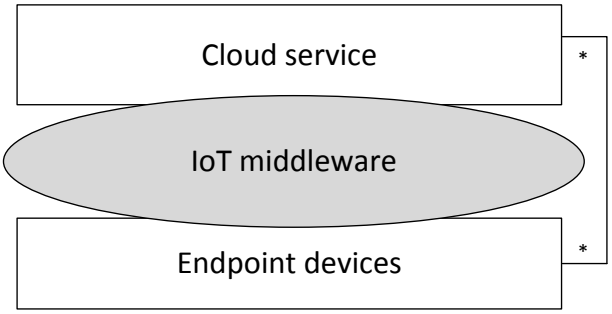

Figure 22: Internet of things architecture.

Figure 22 shows how the different architectural layers overlap and affect each other. Endpoint devices have many to many relationships with cloud services, and middleware is used as an abstraction layer for application developers and technology.

7.3.1 Endpoint devices:

Endpoint devices are electronic devices embedded into the everyday objects that provide these objects with the capabilities of sensing, communication, identification and actuation. The devices should be IP capable or able to cooperate with an IP gateway. These two capabilities must be present in the physical object in order for it to become an IoT object. The sensing is handled by object specific sensors that work together by using communication (IP) subsystems. The same is applied to the actuation capabilities, physical objects can be equipped with different types of actuators, which cooperate with the communication and identification subsystem. It is these endpoint devices that create the backbone of the IoT technology and generate data and events associated with different physical objects. The creation of a viable IoT ecosystem requires these devices to be present ubiquitously in everyday objects.

7.3.2 Middleware:

Middleware in IoT environment will act as a layer that abstracts the heterogeneity of the networks that IoT environment will consist of. Middleware is necessary as it is expected that some level of heterogeneity will remain despite further work in standardization in IoT environment. Middleware allows different technologies and functional blocks to work together and provides the abstraction layer for developers, which simplifies development of IoT products and solutions. It shall be capable of addressing different sensor nodes without the developer knowing if they are connected directly using IP or a gateway is present. Also the hardware specific structures must be abstracted from the developer. The functional blocks that must work together to create a viable IoT environment are context detection, device discovery, communication, data management and security. The current state of middleware is such that it can support specific domains (for example sensor networks or cloud services) but is not capable of supporting all of the domains necessary for IoT environment. As the capabilities of endpoint devices and services provided by cloud providers continue to evolve and improve, it is important for the middleware to act as a bridge between the two and provide an abstraction layer enabling the development of solutions from the endpoint device to the cloud. It is also important that middleware is capable of accommodation of

increasing number of IoT devices and scale towards the increasing volume of data generated by the endpoint devices as well as increasing volume of communication between the endpoint devices and cloud services. IoT middleware is currently an area of active research.

Examples of middleware for the IoT that has gained great popularity recently is message-oriented middleware system which implements queuing systems to handle the distribution of a large amount of sensor data and signalling traffic over the Internet.

7.3.3 Cloud services:

Cloud computing is a computing paradigm that is based on usage of many networked computers. These computers can be on a public network such as internet and as such can provide services and solutions for end users anywhere where there is internet access. Different cloud services are provided today that range from data storage and archival services to information sharing and cloud based operating systems. Cloud computing provides benefits as it allows for users to interact with different content online without the need to run specific software locally or allows to manage and share big amounts of data transparently. Cloud computing is an essential part of IoT environment. The services provided by cloud computing in the IoT environment enable the users to manage the large amounts of data generated by the end devices as well as present these data in a meaningful matter. The ubiquity of embedded sensors in the IoT environment represents a challenge as the amount of raw data and events generated by these sensors can reach an amount that cannot be comprehended by humans without aggregation and selection services. Cloud services today are service provider specific and do not inter-operate with one another. This situation does not provide sufficient building blocks for creation of viable IoT environment as the basic promise of IoT is access to any data anywhere and anytime. For cloud services to play a viable role in IoT is either necessary to define a common access interface for different cloud services or cloud service must be able to advertise which access method it uses for communication with end devices. One such access method can be achieved the usage of RESTful communication. RESTful communication uses HTTP protocol for service requests and responses that are well established in cloud services and many cloud service providers provide a RESTful interface for communication with their service. The endpoint devices can be also adapted to use REST by either using HTTP or, in case of constrained devices CoAP protocol.

8 SEMIAH technical architecture

In many ways, the key functionality of the SEMIAH system can be considered as a middleware layer in the IoT architecture.

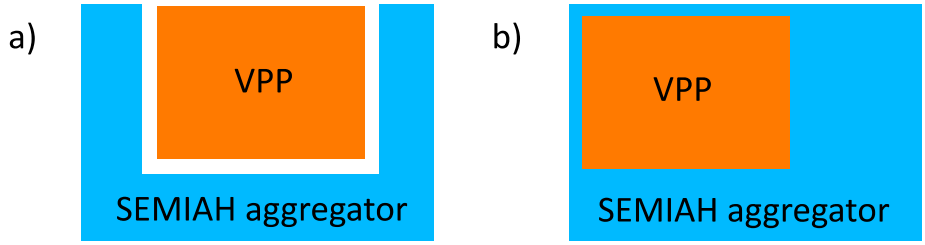

Figure 23: Different configurations of the SEMIAH aggregator with respect to the Virtual Power Plant (VPP) component.

Figure 23 should two distinct architectural configuration of the SEMIAH system. In configuration a), the SEMIAH aggregator subsystem “wraps” the Virtual Power Plant (VPP) component and becomes the integration layer between a centrally controlled VPP and the distributed set of residential households (a.k.a. “the horse shoe model”). This configuration allows or IoT protocols and middleware to be used in the communication between the VPP component and the aggregation layer. In configuration b), The VPP is an integral part of the SEMIAH aggregator function. The interface between the VPP and the aggregation layer is private to the SEMIAH system.

8.1 Technical architecture - Overview

Figure 24 shows an abstract view of the SEMIAH technical architecture. The heart of the architecture is the Generic Virtual Power Plant (GVPP). The GVPP has a number of consumer and provider interfaces to be listed below.

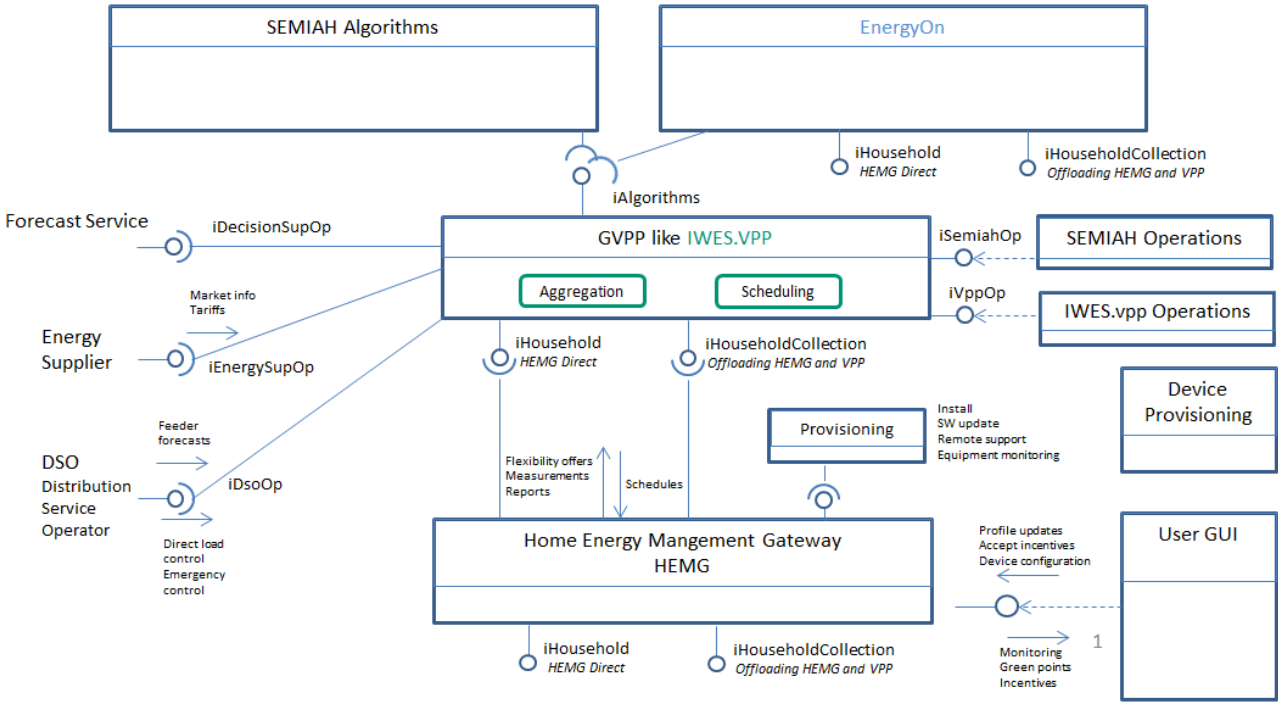

Figure 24: SEMIAH technical architecture. In the figure the letter "i" is used as a prefix for the naming of SEMIAH system interfaces

Consumer interfaces:

- *iDecisionSupOp:*
  Used to deliver forecast information e.g., RES production, CO_2 emission rate etc. to support decisions of the GVPP

- *iEnergySupOp:*
  Used to deliver information related to energy markets such as time varying price information.

- *iDsoOp:*
  Use by DSO to disseminate grid related constraints, provide direct control and for emergency control.

Provider interfaces:

- *iAlgorithms:*
  The GVPP has an open interface for 3rd party components to interface to virtual power plant (VPP) operations. For instance, this may be new algorithms for electricity load aggregation, load forecasting and load scheduling. The interface is also a pivot point for integration of components developed and used in SEMIAH e.g., a module for interfacing to modules that can adapt to energy trading markets in relevant countries.

- *iSemiahOp:*
  Used for operation and maintenance of the SEMIAH system.

- *iHousehold:*
  Used for connecting and controlling the household appliances through the HEMG.

- *iHouseholdCollection:*
  The interface is similar to iHousehold except that is operates of collections of e.g., households and/or appliances.

- *iVppOp:*
  Used for operation and maintenance of the IWES.vpp components planned for use in the SEMIAH pilot.

8.1.1 Possible instantiations of the SEMIAH technical architecture

The SEMIAH consortium brings two distinct VPP components into play from two: IWES.vpp from FRAUNHOFER and the EnergyOn platform from MIS. Both component can be integrated an adapted the SEMIAH architecture. The following section outlines the possible instantiations of a SEMIAH technical architecture being considered for the SEMIAH project.

8.1.1.1 Architecture based on IWES.vpp

The VPP is a key component in the aggregated control of household flexibility. Fortunately, a virtual power plant component (software) is available within the consortium. This component can be the basis for an instantiation of the SEMIAH system architecture.

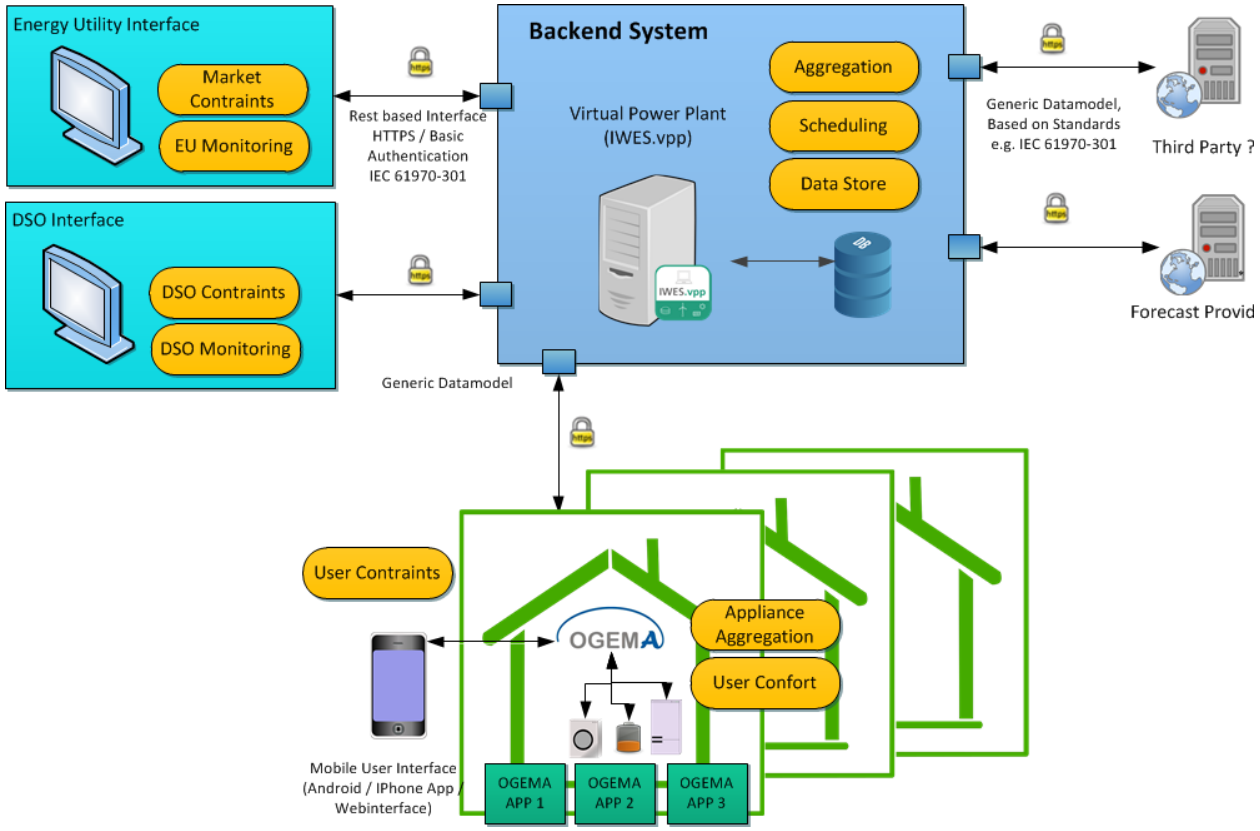

Figure 25: SEMIAH technical architecture with IWES.vpp

Figure 25 shows a way to connect the SEMIAH back-end system directly with the households. The presented architecture is in line with the client-server architecture, in which many clients request and receive service from a centralized server. The server provides a standardized transparent interface to clients so that a client is unaware of the specifics of the system (i.e., hardware and software). The advantages of this architecture are:

- *Central resources*: server manages resources that are common to all clients
- *Eases security*: reduced attack surface to the system assets (i.e., database)
- *Upgradeable architecture*: clients can be added or removed without affecting the SEMIAH system
- *Scalability*: The main focus for scalability if the SEMIAH system is the back-end system

The central back-end system is the single-point-of-failure. With redundant systems this can be easily counteracted.

The virtual power plant (VPP) IWES.vpp from FRAUNHOFER is based on the pattern of service-oriented architectures (SOA). Each service of the VPP has a specific task in the system and they are loosely coupled via a message-oriented middleware. New modules can easily be added to meet new requirements. For a good performance on the persistence layer the NoSQL database MongoDB is used. In this proposal the back-end system consists of the virtual power plant. The VPP aggregates the households and collects the necessary data to run the load, scheduling and aggregation algorithm. The novel algorithms can be easily integrated in the system, because of the previously-mentioned service-oriented architecture.

The system has multiple interfaces to external components, such as OPC-XML-DA, IEC 61400-25 MMS and MODBUS to receive values, e.g. forecast and measured values.

To connect the households with the VPP, one further interface should be provided. The interface is also based on RESTful web services and a generic data model. The appliances within one household are registered with the OGEMA framework. In terms of distributed computing, the OGEMA framework can aggregate the appliances within the household, in contrast to the VPP which aggregates the households. This approach may reduce server load and increase privacy, because no external component know which appliances are in the households. The web and/or mobile front-ends for the end-users connect directly with the OGEMA gateway and receive detailed information about all appliances.

8.1.1.2 Architecture based on EnergyOn Platform

Principle

The EnergyOn platform constitutes a VPP. The participating installations, power plants, storage facilities or loads provide flexibility. The platform aggregates these elements and exploits them on the balancing energy market, the day-ahead market and the intraday market. The optimization approach selects the best option bearing in mind various data and forecasts. In addition, the costs for balancing energy, operation and network are also included in the evaluation, so that these are kept as low as possible with maximum yield. The EnergyOn platform is constantly in data communication with the power plants via an online interface. This allows it to adjust schedules to suit circumstances that are continually changing.

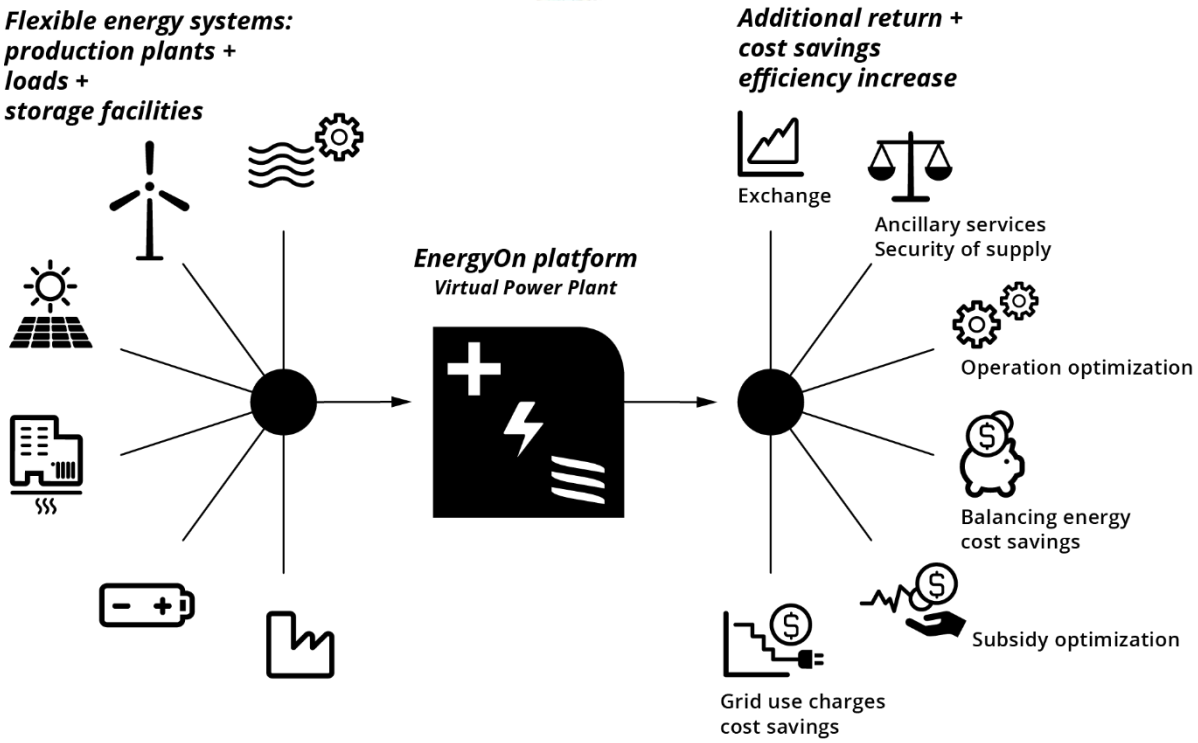

Figure 26: Schematic diagram of the EnergyOn platform

By means of participant pooling, a range of new options open up, particularly for smaller plants where production is volatile. On an individual basis, it would not be possible for many of them to participate in the ancillary services market or in the electricity exchange. Alongside opening up new markets, synergies are also exploited within the virtual power plant. If, for instance, the marginal costs of production are lower than the current market price, it makes sense to feed integrated consumer installations with their own production and optimize so-called on-site consumption.

Technology

The Optimizer:

Misurio has more than 20 years of experience in optimizing flexible energy systems. Misurio optimization is at the heart of products such as optimal scheduling (BestBid), and optimizing controls for power plants, energy storage devices and flexible loads (SmartControl). This optimization also forms the basis of economic and feasibility studies for evaluating investment projects and new business ideas).

With its optimizer Misurio offer the following applications:

EnergyMap

EnergyMap involves studies for the analysis of potential and the evaluation of business models. The customer receives quantitative data about the potential for earnings and cost reductions at his plants. Analyses can be carried out either with historical market and company data or with scenarios on the basis of long-term forecasts.

The evaluations are based on computer simulations over longer periods of time. Misurio differentiate between so-called “ex-post” and “ex-ante” analyses. “Ex-post” looks at the simulation time as a unit and assumes that all-time series (prices, load profiles, etc.) are known in advance. Since this is not the case in reality, “ex-post” optimization delivers results that are over optimistic. It is, however, less extensive

and is especially suited to making a rough estimate of the economic value and the comparison of variants. “Ex-ante” optimization looks at each 15 minutes time interval individually, i.e. a separate optimization calculation is carried out for each time step. It only uses information which is actually available at the given point in time. It works with forecasts and takes the costs of forecast errors into account. The year simulation is very extensive but delivers results that are closer to reality.

The Misurio evaluations of sensitivity analyses are a special feature. Sensitivity factors such as price levels, price volatility, sales, etc. are analyzed individually and portrayed in a 2D image. For the 2D image the sensitivity factors are spread across two axes (e.g. political factors and market factors) and presented graphically. This graphic presentation allows a very rapid assessment of how changes in the influential factors affect the assessment.

Similar to EnergyMap, **SimEnergy** provides an assessment of flexible energy systems. SimEnergy gives the customer a simulator that is tailored to his needs, enabling him to carry out his own calculations.

BestBid is a software tool for planning the implementation of flexible energy systems. It supports energy traders in structuring product lines in order to manage flexible plants in an optimal way. BestBid is suited not only to compiling offers for auctioning ancillary services, but also to buying and selling energy on the day-ahead and intraday spot markets. Costs for compensation energy and grid usage fees can also be included in the model. There is the option of aggregating smaller plants prior to a pool.

This is a multi-stage, phased and holistic process. BestBid uses the schedules and forecasts that are available at the time in question. Each optimization level takes into account the transactions that have already been completed and also incorporates future opportunity costs.

BestBid offers the user optimized and staged options incl. statements of probability of whether the offer will be accepted. The trader can either forward the proposed deals as they are or adapt them manually before putting them on the market.

SmartControl is a predictive control mechanism (MPC = Model Predictive Control). Once it is known which offers have been accepted, schedules for the plant-pool can be produced and these then need to be implemented. SmartControl is a tool for optimizing operations. Based on the overall timetable, short-term changes to the schedule, updates of forecasts and the status of the plants can be carried out by means of regular optimization and the schedules of the individual plants can be recalculated. The current schedules are handed over to the process control system and from there are transmitted to the individual plants.

The **VPP-Module** (Virtual Power Plant) implements a business model for the virtual power plant. All transactions are recorded in a trading book. Costs and revenues are shown in the accounting records. At the end of the month the pool revenues are distributed to the individual plants by means of a simulation. The pool operator has thus broken down the verification of success to the individual plant level. The pool members thus have verification of success for each individual plant. On this basis, for example, a participating energy provider can offer its customers a pricing model for flexible plants.

The EnergyOn platform:

Figure 27: The EnergyOn platform has arisen from the integration of the optimizer applications BestBid, SmartControl, and VPP

The EnergyOn platform has arisen from the optimizer applications BestBid, SmartControl and the VPP. The EnergyOn platform has all the function blocks required for operating a virtual power plant. The sequencing of applications for operating this power plant is illustrated here. All optimization activities refer to the product line structure, implementation, operation and costing analysis for the day “d”:

approx. d-10 to d-15	BestBid	In order to prepare weekly special offers (e.g. secondary control reserve, tertiary control reserve), targets for long term storage systems need to be optimized. Furthermore, opportunity costs are calculated where targets are not met. Using this method, expected prices in the long-term are shown on the short-term optimization. BestBid provides offers for the weekly auctions which are released by traders and brought onto the market as special offers. Bids that are accepted need to be borne in mind as secondary conditions in the course of the next optimization.
approx. d-2 to d-4	BestBid	Creating offers for day-ahead auctions (tertiary control reserve or short-term reserve) is carried out according to the same principle as for weekly auctions. Bids that are accepted need to be borne in mind as secondary conditions in the course of the next day-ahead optimization.
d-1	BestBid	Day-ahead optimization puts the overall timetable for the pool on the market. The limit prices are calculated on the basis of current forecasts. After the clearing process on the stock market, the definitive day-ahead schedules can be calculated.
d	BestBid	During the day, further offers for the intraday market are created and the schedules adapted in accordance with these. Intraday business serves either to take advantage of market opportunities, i.e. attractive prices for the additional purchase or sale of energy, to correct forecast errors and business results or cross-compensation after requesting balancing energy.
d	SmartControl	The plants are managed via the system for optimizing operations (SmartControl). Optimizing operations captures actual measured data via the process control system. It takes schedules and current forecasts (predictive control) into account and, from these, calculates nominal values and

schedules for the individual plants. These are transferred to the plants via the process control system. SmartControl is a dynamic control system, i.e. optimization is repeated on a continuous basis. Normally, optimization occurs every few minutes or when events take place which are of significance for the company that owns the plants.

End of the month

At the end of the month a statement is prepared with a performance review for the individual plants. On the basis of the entries in the trading book and the accounts, distribution keys are calculated with which the overall revenue can be attributed to the individual units.

IT architecture

Figure 28 shows the architecture of the EnergyOn platform. Each layer in the architecture is introduced below.

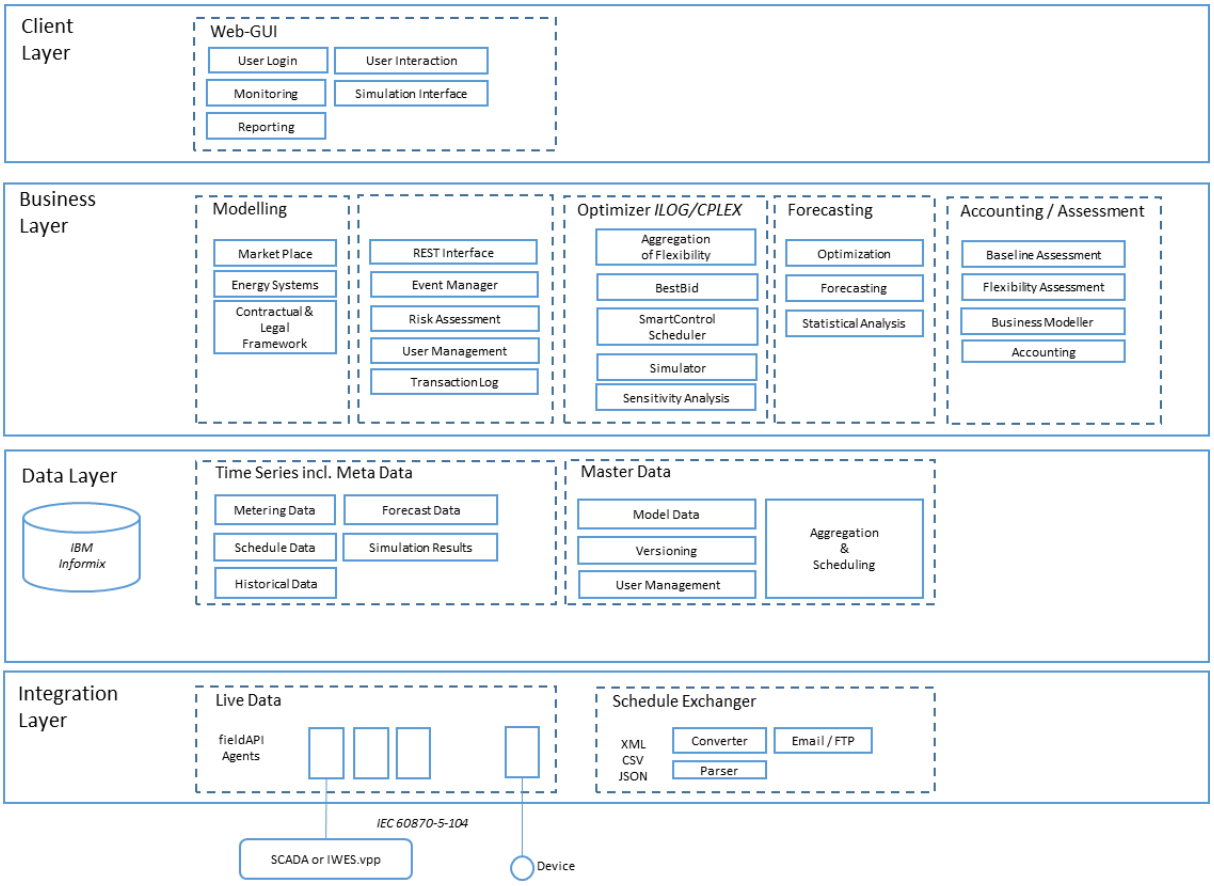

Figure 28: The architecture of the EnergyOn platform with its function blocks is divided into four main levels.

Integration layer

The integration layer of the EnergyOn platform is connected to a SCADA system or the IWES.vpp, which ensures the communication with all integrated plants/households in real time. At the same time, the connected system assumes the standardization of the times series that are delivered and thus allows the data to be registered in a structured way on a database. As well as the systems, the integration layer must also be capable of receiving and sending its schedules. This task is done by the so-called schedule exchanger. If connected to the IWES.vpp, the EnergyOn platform either receives data from each single household or data that is already aggregated to some part. The

flexibility which is provided by this set-up allows the SEMIAH project to run the back-end only by the EnergyOn platform or by both, IWES.vpp and EnergyOn platform, at the same time. Like this a maximum of freedom for SEMIAH is provided and the developed bounded to the EnergyOn platform.

Data layer

The time series that are received from the integration layer and other data, such as weather, production and consumer data, are collected in an Informix database and passed on to the super ordinate business layer. This data flow is by no means one-way. Time series are also sent from the business layer to the data layer to be registered on the database.

Business layer

The business layer represents the real core of the EnergyOn platform. It comprises the entire modulation, the optimization, the forecasting and the accounting system for the platform. In addition there are further functions such as risk and user management. The business layer thus creates the significant added value of the EnergyOn platform and presents the biggest distinction to competitors' products.

Client layer

The client layer describes the user interface of the EnergyOn platform. It allows the end user to steer and control the VPP. In addition, an integrated data center allows an informative and user-friendly means of reporting, which makes it possible to provide full ex-post analysis. Alongside these operative features, there is also the option for the user to carry out simulations of interesting scenarios. This is delivered through an interface designed specially to offer this feature.

8.2 Considerations for deployment

The system model as presented in Section 5.3 does not address the distribution of objects on concrete computing devices. The underlying assumption is that any object can be implemented on any device and that some distributed systems technology will implement the interactions between objects.

The following computing devices can be considered:

- Home energy management gateway in each household / building,
- Feeder management device typically located in the secondary substation,
- Full-featured server or (private or public) cloud service.

The distribution of objects on devices is influenced by:

- hardware costs and energy consumption of computing devices,
- telecommunication bandwidth,
- prosumer's expectation and legal requirements for privacy,
- prosumer's need for confidentiality protection
- management of complexity (to supervise the system and for software updates).

Figure 29 presents some possible deployment topologies. The VPP component is assumed to be hosted on its own server. The most appropriate balance could evolve over time in the project. For SEMIAH, the following generic rules apply:

- The VPP component is an existing software module integrated into SEMIAH through a SEMIAH defined API (Application Programming Interface).

- All SEMIAH models and all SEMIAH algorithms are independent of deployment topologies and of distributed systems technologies.

For the development of the SEMIAH system infrastructure, the integration test and the demonstration an appropriate topology will be selected and the SEMIAH framework will be developed accordingly.

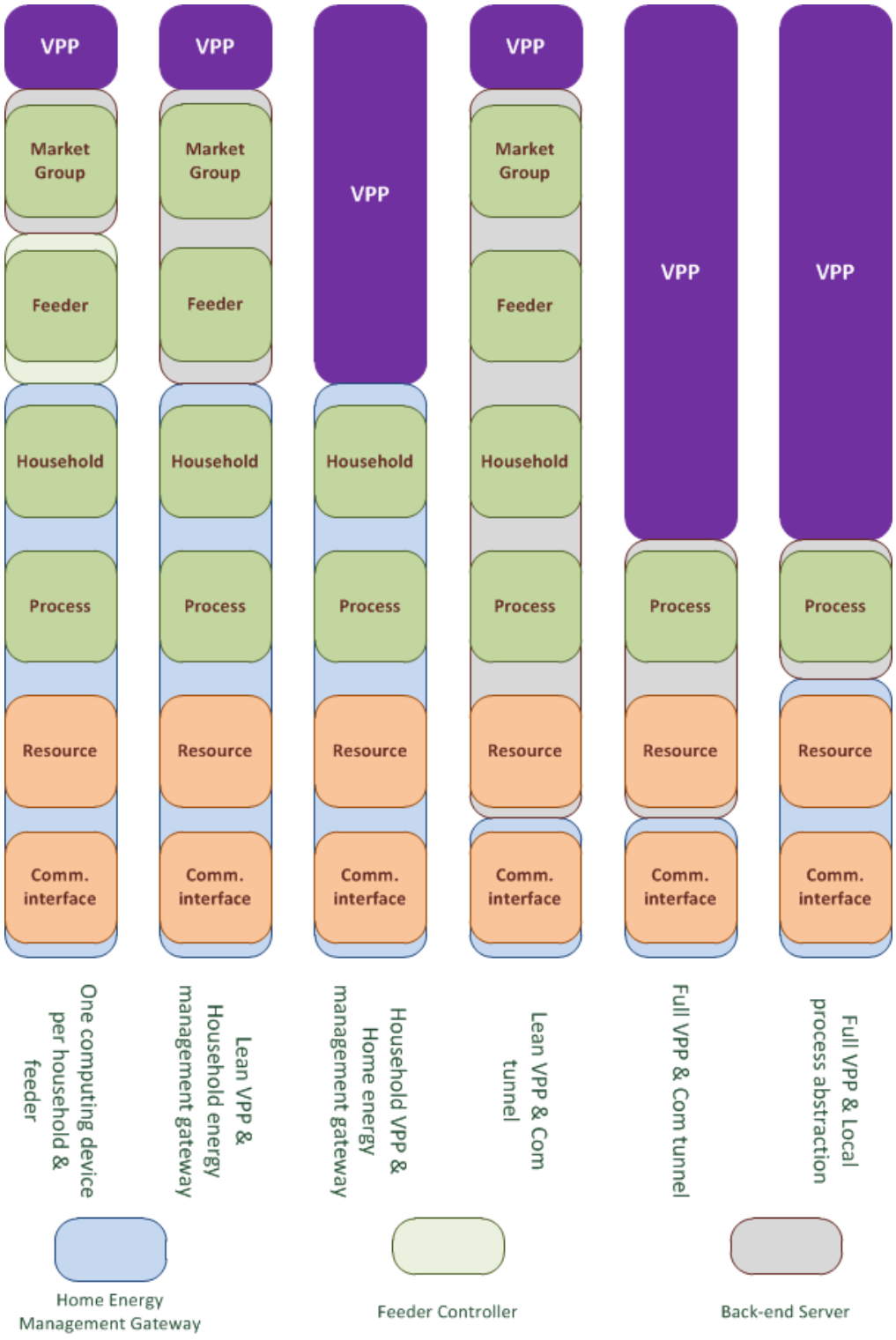

Figure 29: Several possible deployment architectures for SEMIAH.

The SEMIAH system is considered to be flexible with respect to the possible deployment architectures. These deployment scenarios may differ from DSO to DSO due to e.g., the different levels of liberalisation of the electricity grid and related energy service in each country.

The selection of specific deployment architectures for the SEMIAH pilot testing is for further study. Deliverable D7.2 will detail the chosen deployment scenario of the SEMIAH project.

9 References

[1] CEN-CENELEC-ETSI Smart Grid Coordination Group – First Set of Standards. Part of M/490. November 2012. Available from ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/First%20Set%20of%20Standards.pdf (Standard).

[2] Process modeller from bizagi company home page. Available from: http://www.bizagi.com/en/products/bizagi-process-modeler (Web page).

[3] CEN-CENELEC-ETSI Smart Grid Coordination Group – Sustainable Processes. Part of M/490. November 2012. Available from: ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Sustainable%20Processes.pdf (Standard).

[4] IEC Smart Grid Standards Map. Last accessed January 2015. Available from http://www.iec.ch/smartgrid/mappingtool/ (Web page).

[5] SG-CG/ M490/F_ Overview of SG-CG Methodologies Version 3.0. Part of M/490. November 2014. Available from: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_Methodology_Overview.pdf (Standard).

[6] Craig Larman, Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development (3rd Edition), Chapter 6. Prentice Hall. October 2004. (Book)

[7] Alistair Cockburn, Writing Effective Use Cases. Addison-Wesley Professional. October 2000. Pre-publication draft available from: http://alistair.cockburn.us/get/2465. (Book).

[8] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0. 2012. NIST Special Publication 1108R2. National Institute of Standards and Technology (NIST). (Standard).

[9] Rahimi, F.; Ipakchi, A, "Demand Response as a Market Resource Under the Smart Grid Paradigm,", IEEE Transactions on Smart Grid, vol.1, no.1, pp.82,88, June 2010. doi: 10.1109/TSG.2010.2045906 (Paper).

[10] CEN-CENELEC-ETSI Smart Grid Coordination Group – Smart Grid Reference Architecture. Part of M/490. November 2012. Available from: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Reference_Architecture_final.pdf (Standard).

[11] IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads, IEEE Std. 2030-2011 (2011). (Paper).

[12] Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., ... & Doody, P. (2011). Internet of things strategic research roadmap. Internet of Things-Global Technological and Societal Trends, 9-52. (Paper).

[13] Ishaq I, Carels D, Teklemariam GK, Hoebeke J, Abeele FV, Poorter ED, Moerman I, Demeester P. IETF Standardization in the Field of the Internet of Things (IoT): A Survey. Journal of Sensor and Actuator Networks. 2013; 2(2):235-287. (Paper).

[14] Soma Bandyopadhyay, P. Balamuralidhar and Arpan Pal. Interoperation among IoT Standards. Journal of ICT Standardization. Vol: 1 Issue: 2. November 2013. (Paper).

[15] SG-CG/M490/Methodology & New Applications, Annex B Concepts, Elements and Tools for the Smart Grid Methodology Version 1.0. Part of M/490. December 2013. Available from:

http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group3_methodology.pdf (Standard).

[16] Kent Beck, Extreme Programming Explained: Embrace Change, Addison-Wesley, 1999. (Book).

[17] Venkata Gayatri and Krishnamurty Pammi, Agile User Stories; The Building Blocks for Software Project Development Success, 20 September 2013. Available at https://www.scrumalliance.org/community/articles/2013/september/agile-user-stories (Web page).

[18] John Daintith. "System requirements specification." A Dictionary of Computing. 2004. Retrieved September 30, 2014. Available from Encyclopedia.com:http://www.encyclopedia.com/doc/1O11-systemrequirementsspcfctn.html

[19] Standard for Smart Energy Profile Application Protocol, P 2030.5-2013, IEEE Communications Society/Power Line Communications (COM/PLC).

[20] ZigBee Specification (version 2) 2008, ZigBee Alliance.

[21] F. Baker and D. Meyer, Internet Protocols for the Smart Grid, RFC 6272, Internet Society. (2011). Available from https://tools.ietf.org/html/rfc6272 (Standard).

[22] Christoph Nölle, “Resources”, OGEMA Wiki. Available at: https://www.ogema-source.net/wiki/display/OGEMA/Resources. Accessed December 2014. (Web page).

[23] Power Utility Automation, IEC 61850 standard family, IEC. Available from: http://www.iec.ch/smartgrid/standards/ (Standard).

[24] Trello collaborate board. Available from: https://trello.com/ (Web page).

[25] Energy Strategy, Secure, competitive, and sustainable energy. Available from: http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm (web page).

[26] European Smart Grid Task Force. Available at: http://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force (web page).

[27] Peter Hermans, The concept of Energy Grid1 Services; A new perspective. The Smart Grid Task Force Expert Group 3. Part of M/490. Available from: http://ec.europa.eu/energy/sites/ener/files/documents/xpert_group3_energy_grid_services.pdf

[28] M. Jørgensrud, ”Amazon web services - Geodata måtte ‘smugle’ harddisk gjennom Sverige”, 2014. Available from: http://www.digi.no/930720/geodata-maatte-smugle-harddisk-gjennom-sverige . Accessed: 29-oct-2014. (web page).

[29] E. Hossny, S. Khattab, F. Omara, og H. Hassan, “A Case Study for Deploying Applications on Heterogeneous PaaS Platforms”, in 2013 International Conference on Cloud Computing and Big Data (CloudCom-Asia), 2013, s. 246–253.

[30] I. Arce, Kathleen Clark-Fisher, N. Daswani, J. DelGrosso, D. Dhillon, C. Kern, T. Kohno, C. Landwehr, G. McGraw, B. Schoenfield, M. Seltzer, D. Spinellis, I. Tarandach, og J. West, “Avoiding the top 10 software security design flaws”. IEEE Computer Society, 2014.

Annex A Product backlog development

A.1 Idea

The idea is to move in the direction of agile (or Scrum). Take a look at the "Agile analysis process" for more details. Currently we are in the phase of "PBI Identification", where the idea is to collect items for the product backlog.

The product backlog items (PBIs) are ordered by the Product Owner based on considerations like risk, business value, dependencies, date needed, etc. Those items can be expressed as user stories, use cases, or any other requirements approach that the group finds useful. But whatever the approach, most items should focus on delivering value to customers.

When the initial product backlog is in place, the highest priority items are distributed to development teams, which will then start working on their features, after the kick-off or sprint planning meeting.

A.2 Trello instructions

We will collect the Product Backlog Items (PBIs) on Trello cards, in boards called "Product Backlog - something". When a team is given (or takes) a feature, its corresponding card is moved to the team's board, where the feature is followed up, typically in "To do", "Ongoing" and "Done" lists.

Trello is available from the web: https://trello.com

A.3 Creating the Trello board

Anyone in the organisation can create a board. Remember to change the visibility to "Org Visible" as soon as you want to share what you have created. Org members decide themselves if they will join the board or not.

A.4 Joining SEMIAH Trello boards

In order to join a SEMIAH board, click on the SEMIAH name on the top meny and choose View Organisation Page, and join the board (details to be defined).

Annex B ENISA-based Security and Privacy

B.1 Security governance & risk management (ENISA Domain 1)

Security governance and risk management consists of the following elements:

- Information security policy

This involves writing and maintaining a high-level written policy

- Organisation of information security

Information Security should be organised as stated in the following sub-requirements:

- Security roles and responsibilities

Technical enforcement can be authentication mechanisms (e.g. the Security Assertion Markup Language (SAML) and authorisation mechanisms (e.g. XACML).

- Information security procedures

These are procedures (manual or automated) that support the information security policy. For example: XACML privacy policies or authorisation policies, firewall rules, IDS rules, configuration management system configuration, written procedures etc.

- Risk management framework
- Manage assets, vulnerabilities, threats and threat frequency and risk, including integrating with vulnerability assessment systems and asset scanning systems.
- Aggregate risks, for example using an attack tree or attack graph based approach.
- Support existing security management standards, for example the ISO27000 set of security management standards, the German BSI Grundschütz or the open Spanish standard Magerit.

Verinice (http://www.verinice.org) is an open source risk assessment framework that supports most of these features. The PRECYSE project has created a MAGERIT catalogue of countermeasures that could be used as a baseline. This catalogue is free as opposed to the ISO27000 and BSI Grundschütz catalogues.

Verinice can be integrated with the open source vulnerability scanning tool OpenVAS (http://www.openvas.org), so that the results of vulnerability scans can be imported into the risk assessment tool.

OpenVAS can also be integrated with vulnerability tests written in the Open Vulnerability Assessment Language (OVAL), which allows for performing passive vulnerability tests on hosts instead of using active vulnerability tests, explicitly testing for vulnerabilities. The latter may be problematic to perform on a critical infrastructure in operation. However nonintrusive OVAL tests can also be performed on systems in operation.

- Risk assessment should be performed at regular intervals:

This includes:

- Performing vulnerability scanning;
- Reassessing other risks;
- Use a risk management framework to detect the gap in security.

Risk treatment plan:

- The risk treatment plan can either be written manually, or automatic for commonly occurring risks;
- Automatic management can for example be done using reports in the Common Remediation Enumeration (CRE) format;
- Each report explains good practices for managing a given risk.

B.2 Management of third parties (ENISA Domain 2)

- Third party agreements are needed;
- They should ensure that availability, integrity and confidentiality is preserved;
- The agreement should be incentive compatible, if possible, meaning that the third party does not benefit from cheating or doing its duties poorly;
- Monitor compliance of contractual obligations;
- Using key performance indicators;
- Acceptance criteria are needed.
- Auditing, for example using interactive tests in the Open Checklist Initiative Language (OCIL).
- Technical means should be implemented in order to make the third party operation auditable, for example using secure logging services which guarantee non-repudiation, so that the third party cannot deny having done a certain operation.
- The secure logging should also ensure transparency, so that SEMIAH systems can verify that the operation is being performed according to the contract;

In other words, trust, but verify.

The Reversible Anonymiser (http://launchpad.net/reversible) could be a useful building block for implementing secure logging services.

B.3 Secure lifecycle process (ENISA Domain 3)

- Perform security requirements analysis and specification;
    - Ends up in a requirements specification document (e.g. D3.1).
- Create an inventory of smart grid components/systems;

The risk assessment system Verinice supports managing an inventory of assets;

OpenVAS can be integrated with the passive realtime asset detection system (prads), in order to populate or perform consistency checks on the catalogue of IP assets in the risk assessment framework. OpenVAS can furthermore be integrated in Verinice.

- Secure configuration management;
- This involves ensuring secure deployment of system configurations, for example using digitally signed system configurations;
- The integrity of deployed system configurations should be verified using tools supporting file integrity checks (for example OSSEC, http://www.ossec.net);
- Key shares can be used to implement separation of duties constraints (multi-party authorisation), for example to ensure that more than one stakeholder must agree to deploy

a given configuration, or to enforce that a standard workflow has been followed where configurations have been verified in testing before they are being deployed.

- Secure configuration management also includes the possibility to roll back to the last known good configuration.
- Secure documentation of configurations;
- RFC 4741 NetConf could be a possible candidate standard for handling configuration management in SEMIAH.
- The Reversible Anonymiser could also be useful for enforcing multi-party authorisation policies and configuration deployments (in particular deployment of privacy/authorisation policies).
- The documentation of system configurations is sensitive information that can be abused if it falls in the wrong hands. Such information should therefore be handled as confidential information, for example by enforcing access control on who can read this information, secure logging of who have read the information as well as secure archiving when the information is at rest.
- Maintenance of smart-grid components;
- The configuration management system should enforce installation of only digitally signed software, firmware, patches and configurations.
- Disposal of smart-grid components/systems;
- Ensure that procedures exist for wiping or destroying components that may contain sensitive information, to avoid information leakage when equipment is being decommissioned.
- Change management;
- Ensure that only authorised and tested configuration changes can be deployed.
    - This can for example be done by using a cryptographically enforced workflow for deploying configuration changes.
- There must be a possibility to roll back to the last known good configuration.
- Security testing of smart grid components/systems;
- This can be used using vulnerability scanning tools like OpenVAS and OVAL tests, as described earlier.

B.4 Personnel security, awareness and training (ENISA Domain 4)

1. Personnel screening;

- The human resource department needs to perform background checks and security vetting of personnel that may have access to private or confidential information.
- This must be reflected in the security levels that a user can access.

2. Personnel changes;

- There must be routines and technical systems that can create, modify or revoke user accounts.
    - SEMIAH could make use of existing federative access control systems here, for example Shibboleth (http://shibboleth.net), which is a scalable federated identify solution that amongst others supports using SAML for authentication and XACML

for authorisation of users. Shibboleth can furthermore integrate with an organisation's existing directory services.

3. Security training and certification;

- It is important to establish and maintain security awareness in the organisation. This means that a training programme, exercises etc. is needed.

B.5 Incident response & information knowledge sharing (ENISA Domain 5)

1. It is important that the organisation has incident response capabilities;

- For example a 24x7 managed security service detecting attacks;
- Intrusion detection and prevention systems installed;
- Attack response procedures and digital forensics capabilities;
- Routines that quickly can fix a problem and restore services to normal operation.
    - SEMIAH can make use of several existing technologies for this, for example Snort (http://www.snort.org) or Suricata (http://www.suricata-ids.org) for network-based intrusion detection, Prelude-IDS (http://www.prelude-ids.org) or similar for implementing a Security Incident and Event Management System (SIEM).
    - There will probably need to be a separate intrusion detection system for OGEMA

in order to detect attacks and abuse of the home energy management gateway. This will probably be a new software module, unless it can be installed as an operating system service below OGEMA. This can also be used for detecting system faults.

- Private or confidential information can be protected by utilising the Reversible Anonymiser.
- Efficient backup routines and/or virtual machine snapshots can be used to restore core services quickly after an attack.
- There will probably also need to be a centralised alarm correlation system, in order to reason on and reduce the total number of alarms. Prelude-IDS is one tool that can be used as a building block for this.

2. Vulnerability assessments;

- Software vulnerabilities in existing software modules

can be detected using vulnerability scanning tools like OpenVAS together with OVAL tests.

- Vulnerabilities in own software

can be detected using software code inspections and fuzzing test tools (e.g. fuzzdb) that tries to impose random, but plausible input within given bounds to a given software module, in order to detect crashes or abnormalities due to poor input validation.

3. Vulnerability treatment;

This includes configuration management and patching routines, as has been discussed earlier.

- Information on how to detect and mitigate vulnerabilities should be shared with peer organisations and security organisations if possible.

For example by registering CVE vulnerabilities in the Mitre database, informing national Computer Emergency Response Teams about attacks, exchanging threat information with peer organisations using the Structured Threat Information eXchange (STIX) and Trusted Automated Exchange of Indicator Information protocols.

B.6 Audit and accountability (ENISA Domain 6)

SEMIAH should include the following mechanisms in order to ensure auditability and accountability:

1. Auditing capabilities
    - A central component for ensuring autidability and accountability is using a secure logging scheme. This means using techniques like remote logging as well as storing the logs in a tamper resistant manner, so that only authorised stakeholders can access log information on a needs basis.
    - The SEMIAH tools will need to implement logging operations at appropriate points in the source code, in order to log when sensitive operations are being performed. These points will need to be identified during system design.
2. Monitoring of smart grid information systems;
    - In addition to logging critical operations in own source code, several other tools and techniques can be used by SEMIAH. For example:
        - Intrusion detection systems for logging attacks and security policy violations;
        - Network monitoring (e.g. OpenNMS) for monitoring service operation;
        - Integrity checking tools for monitoring file access (e.g. OSSEC).
3. Protection of audit information;
    - The secure logging system should also support nonrepudiation, so that access to sensitive commands or information cannot be denied, in order to provide transparency.
    - The secure logging service may need to implement a time-based encryption scheme, where data automatically is invalidated after a given time period, for example to support data retention mechanisms, or to comply to data protection requirements. This ensures that sensitive material in backup copies cannot be accessed after the legal data retention period has expired.
    - Encryption is a key technology for keeping confidential audit log information secure.

B.7 Continuity of operations (ENISA Domain 7)

Continuity of operations entails the following:

1. Maintain essential functions after disruption;
    - Detect disruption using network management tools (e.g. OpenNMS), alternatively using intrusion detection systems.
    - Restore operation according to defined and tested procedures as fast as possible, for example using backup media or virtual machine snapshots for cloud-based services.
    - If operation is being disrupted due to a Denial of Service attack or lack of resources, then one way to mitigate the attack might be to scale up the service, assuming that critical parts are implemented using a cloud provider platform that allows for elastic scalability according to need (i.e. using Platform as a Service).
    - Compliance tests can be used to verify that the service continuity procedures work as expected. OCIL tests can be used to implement such procedures.
2. Emergency communication services;
    - Verify that emergency procedures and communication services work.
    - OCIL tests can be used to implement this.

B.8 Physical security (ENISA Domain 8)

Important factors of physical security are:

1. Maintain physical security;
    - OCIL compliance tests can be used for verifying procedures.
2. Log and monitor physical access;
    - Physical alarms could be configured to send alarms to the IDS, so that the 24x7 operations centre could detect and handle such alarms.
    - Privacy-enhanced operation should be preferred, for example based on the Reversible Anonymiser.
3. Physical protection of remote equipment;
    - For example trigger an IDS alarm if smart grid equipment is being opened or tampered with.

B.9 Information systems security (ENISA Domain 9)

Information systems security is a broad area that amongst others covers:

1. Policy for classification/disclosure of sensitive/secret information;
    - The XACML privacy policy for the Reversible Anonymiser can be used for this.
2. Data security;
    - Data at rest can be protected using disk encryption, database encryption or the Reversible Anonymiser.
    - Data in transit can be protected using HTTPS/TLS or a VPN solution.
    - Data integrity can be protected by using digital signatures, or checksums for less critical data. Tools like OSSEC can be used to verify file integrity.
    - Data availability can be ensured using backup or redundant storage media, database servers etc.
3. Account management;
    - Single sign-on and directory services/LDAP can be implemented using for example Shibboleth.
    - Logical access control supporting two factor authentication, SAML and XACML
4. Secure remote access;
    - Using virtual private networks (VPN) e.g. IPsec.
5. Information security;
    - SEMIAH back-end:
        - Cloud-based systems can run heavy information security tools, for example IDS tools (Suricata/Snort), SIEM tools (e.g. Prelude-IDS), host-based IDS (e.g. OSSEC), anti-virus (e.g. ClamAV), anti-spam (e.g. SpamAssassin).
    - SEMIAH front-end:
        - The OGEMA front-end also needs protection, but less heavy solutions are needed, due to limited resources.
        - For example a tailor-made host-based IDS solution based on log analysis.
        - Firewall functionality can if needed also be built in to the front-end, since the underlying Linux operating system supports this.
6. Media handling;
    - Secure procedures are needed for access, storage, distribution and destruction of storage media.
    - Sensitive data must be protected during the entire lifecycle.
    - This can be done using techniques like the Reversible Anonymiser, encryption or similar.

B.10 Network security (ENISA Domain 10)

Requirements for achieving network security:

1. Functional and secure network segregation
    - The Domain/Enclave model can be used for segregating the network, where the Domain protects the network and the Enclave is the network being protected. This is the model used for network segregation in the PRECYSE project (http://precyse.eu/).
    - Concerted firewall rules define the allowed traffic within an enclave, and denying everything else by default.
    - IDS whitelist monitors allowed traffic. Traffic that is not allowed will cause IDS alarms.
2. Secure network communications
    - Encrypted links (e.g. HTTPS/TLS/IPsec).
    - Trust between services can be achieved by using digital certificates and requiring authentication by these certificates during link setup.

B.11 Resilient and robust design of critical infrastructure (ENISA Domain 11)

1. Minimum threat exposure;
    - This can be achieved using IDS whitelisting, restrictive firewall rules only allowing traffic that is explicitly permitted, vulnerability scanning tools (OpenVAS and OVAL) to detect known vulnerabilities, patching and upgrading with subsequent testing to remove vulnerabilities.
2. Resiliency;
    - Resiliency can be achieved using tested crisis procedures, redundancy, graceful degradation during fault or attack and quick recovery after a crisis.
3. Safe continuity after interruption of services
    - Consider the geographical location of components, ensuring that “all eggs are not in the same basket”.
    - Ensure that the service is resumed in a sensible state after interruption, or if it needs to be restored from a virtual machine snapshot or backup.
    - Ensure graceful degradation, for example so that the service still can be managed and kept working if part of the grid or communication networks fall out.
    - Avoid that the critical parts of the infrastructure has hard dependencies to (i.e., cannot function without) less critical parts.

Annex C Use cases collection

In this Annex smart grid use cases that are relevant for SEMIAH have been selected from UCMR and listed here. The UCMR is a collaborative Use Case editing tool to create and Use Cases based on the SGCG Sustainable Processes work group's effort.

Use cases are structured into high level (HL) use cases and primary use cases. A high level use case may include one or more primary (P) use cases embedded.

C.1 Demand and Generation Flexibility Use Cases

The use cases relevant to SEMIAH belong to the Demand and Generation Flexibility category of the generic use cases.

UC tag	Type	Name
WGSP-2020	-	Controlling energy consumption or generation via CEMS or directly with smart appliances.
WGSP-2110	HL	Receiving consumption, price or environmental information for further action by consumer or a local energy management system. *Includes WGSP-2111, WGSP-2112 WGSP-2113, WGSP-2114.*
WGSP-2111	P	Information regarding power consumption / generation / storage of individual smart devices.
WGSP-2112	P	Price and environmental information.
WGSP-2113	P	Warning signals based individual devices consumption.
WGSP-2114	P	Retrieve status of smart devices
WGSP-2120	HL	Direct load / generation management. *Includes WGSP-2121 and WGSP-2122.*
WGSP-2121	P	Direct - load / generation / storage management.
WGSP-2122	P	Emergency load control.
WGSP-2128	HL	Flexibility offerings. *Includes WGSP-2129.*
WGSP-2129	P	Flexibility offerings.
WGSP-2130	-	Auto Registration of participating devices and customers
WGSP-2140	HL	Tariff synchronization. *Includes WGSP-2141, WGSP-2142, and WGSP-2143.*
WGSP-2141	P	CEM requests time
WGSP-2142	P	CEM sends out-of-synch alarm
WGSP-2143	P	Smart meter notifies active tariff change
WGSP-2400	-	Using Flexibility

C.2 Demand and production (generation) flexibilities

Use case in this section are selected from the demand and production (generation) flexibilities cluster (WGFSS-CL11) of UCMR.

UC tag	Type	Name
WGFSS-HL43	HL	Generation forecast
WGFSS-HL44	HL	Load forecast
WGFSS-HL45	HL	Load forecast of a bunch of prosumers in a DR program (from remote)
WGFSS-HL46	HL	Managing energy consumption or generation of DERs via local DER energy management system bundled in a DR program
WGFSS-HL47	HL	Managing energy consumption or generation of DERs and EVSE via local DER energy management system to increase local self-consumption

WGFSS-HL48	HL	Participating to the electricity market
WGFSS-HL49	HL	Receiving metrological or price information for further action by consumer or CEM
WGFSS-HL50	HL	Registration/deregistration of customers in DR program
WGFSS-HL51	HL	Registration/deregistration of DER in DR program

At the time of writing this deliverable, only the list with accompanying names of the use cases from the cluster have been defined in the UCMR.