4

Promoting Increased Energy Efficiency in Smart Grids by Empowerment of Customers

Rune Gustavsson
KTH School of Electrical Engineering
Sweden

1. Introduction

The *EU Climate and Energy package* is setting the 20-20-20 targets of future energy systems by 2020 and will change the landscape of future energy system in Europe and worldwide. The package sets the following objectives;

- reduce greenhouse gas emissions by 20%,
- increase the share of renewable energy to 20, and
- to make a 20% improvement in Energy Efficiency.

The European Parliament has continuously supported these goals. It is a common understanding that this change will require a transition from *monopolised hierarchically controlled* Power networks to *customer oriented Smart Grids* operating in *deregulated energy markets.* However, this poses several regulatory, organizational and technical challenges to be identified and addressed. To that end several international Smart Grid projects have been launched worldwide in EU, the US, and in China.

In a follow-up Proposal by EC is the *Energy Efficiency Plan 2011*. That is a Directive of the European Parliament and for the Council on Energy Efficiency[1] based on assessing results and findings so far versus the stated 20-20-20 targets. The assessments shows that the *major concerns* related to the expected fulfilment of the Energy packet target is related to meeting the Energy Efficiency (EE) goals, Figure 1.

Increased Energy Efficiency is expected be enabled by the following actions and their combinations:

- *Active intelligent* Distribution grids incorporating vast amounts of RES
- *Active and empowered* customers
- *Active operations* of markets

The term “active” in this setting refers to “smart” or “intelligent”. We suggest that careful selection and implementation of Multi-Agent technologies is crucial for Services supporting active customers, intelligent distribution grids and the two other recommended actions [2] (Section 2).

[1] Home page: http://ec.europa.eu/energy/efficiency/index_en.htm

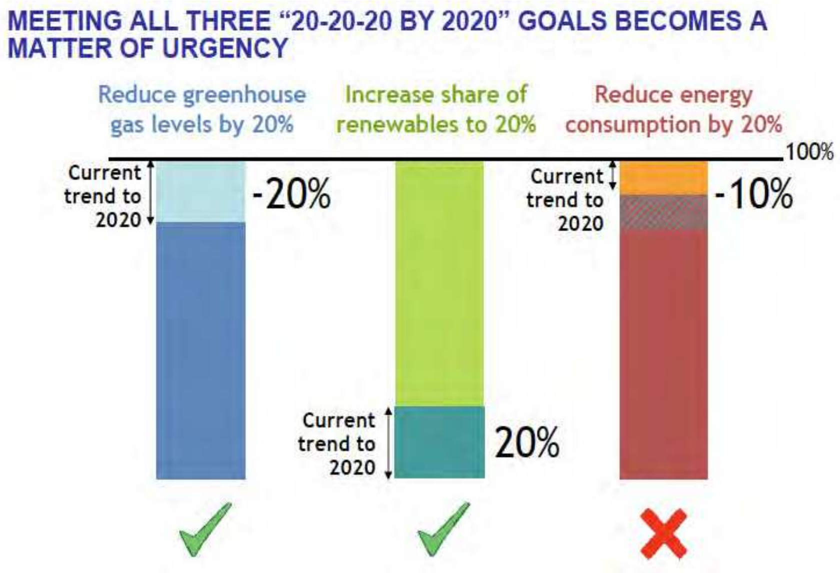


Fig. 1. Assessments of progress towards 20-20-20 objectives.

The Energy Efficiency Plan document makes the following explicit observations and recommendations concerning *Energy Service Companies* (ESCOs), *Customer empowerment*, *Smart grids and Smart meters* as a backbone for *smart appliances* thus enabling increased EE.

"Smart grids and smart meters will serve as a backbone for smart appliances, adding to the energy savings obtained by buying more energy efficient appliances. New services will emerge around the development of smart grids, permitting ESCOs and ICT providers to offer services to consumers for tracking their energy consumption at frequent intervals (through channels like the internet or mobile phones) and making it possible for energy bills to indicate consumption for individual appliances. Beyond the benefits for household consumers, the availability of exact consumption data through smart meters will stimulate the demand for energy services by companies and public authorities, allowing ESCOs to offer credible energy performance contracts to deliver reduced energy consumption. Smart grids, meters and appliances will allow consumers to choose to permit their appliances to be activated at moments when off peak cheaper energy supply or abundant wind and solar power are available – in exchange for financial incentives. Finally, they will offer consumers the convenience and energy saving potential of turning appliances on and off remotely.

Delivering on this potential requires appropriate standards for meters and appliances, and obligations for suppliers to provide consumers with appropriate information (e.g. clear billing) about their energy consumption including access to advice on how to make their consumption less energy intensive and thus reduce their costs. To this end, the Commission will propose adequate measures to ensure that technological innovation, including the roll-out of smart grids and smart meters fulfils this function. These measures will include minimum requirements on the content and format of information provision and services.

Further, the Commission needs to ensure that energy labels (energy performance certificates) and standards for buildings and appliances reflect, where appropriate, the incorporation of technology that makes appliances and buildings "smart grid ready" and capable of being seamlessly integrated into the smart grid and smart meter infrastructure. Appliances such as fridges, freezers and heat pumps could be the first to be tackled.

Improvements to the energy performance of devices used by consumers – such as appliance and smart meters – should play a greater role in monitoring or optimizing their energy consumption, allowing for possible cost savings. To this end the Commission will ensure that consumer interests are properly taken into account in technical work on labelling, energy saving information, metering and the use of ICT.

The Commission will therefore research consumer behaviour and purchasing attitudes and pre-test alternative policy solutions on consumers to identify those which are likely to bring about desired behavioural change. It will also consult consumer organisations at the early stage of the process. Consumers need clear, precise and up to date information on their energy consumption – something that is rarely available today. For example, only 47% of consumers are currently aware of how much energy they consume. They also need trustworthy advice on the costs and benefits of energy efficiency investments. The Commission will address all of this in revising the legislative framework for energy efficiency policy."

A summary of benefits for consumers through provision of proposed tailored Energy Services and Information is given in Figure 2,

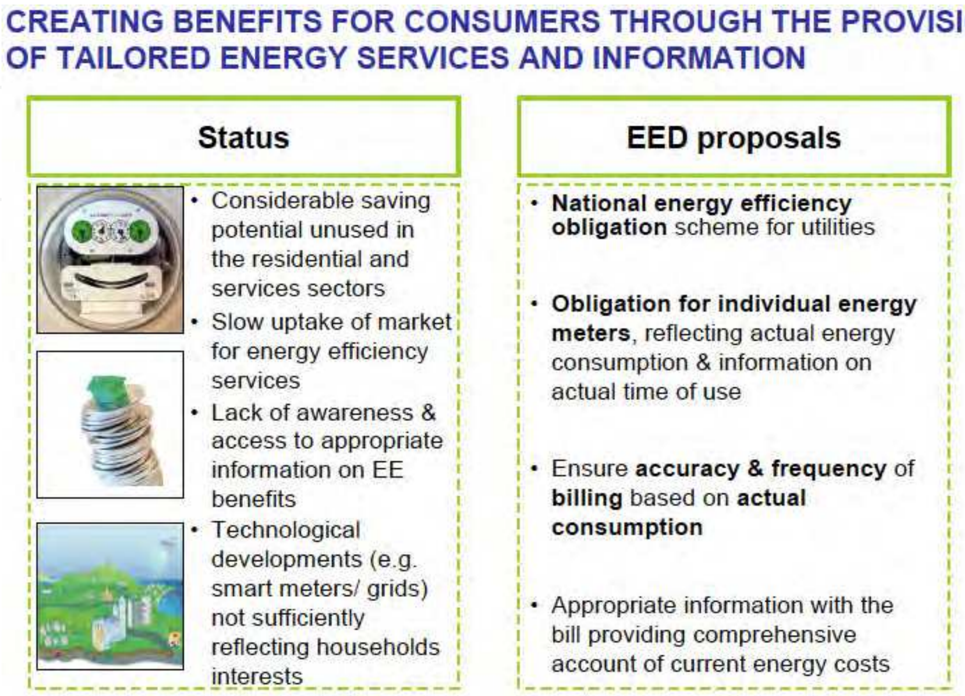
The remaining part of the chapter is organized as follows.

- Section 2 Smart grids – Architecture, Stakeholders, Challenges, Barriers and Solutions. We follow up some of the issues addressed in previous Section 1 Background.
- Section 3 Requirements engineering and Validation. In this section we are addressing some aspects of system Interoperability and customer acceptance based on found requirements. We also outline some engineering principles of trustworthy Smart grids.
- Section 4 Customer empowerment. In this section we give a high-level architectural view of customers in a Smart grid. In particular we differentiate between different types of customers (consumers), that is, consumers of home - centric energy-based services and consumers of business-based energy services. This section also outlines challenges related to implementations of the Energy Efficiency Plan 2011 refereed to above.
- Section 5 Information processing systems and sharing and protection of information. We address issues related to information sharing (interoperability) and information protection (security and integrity).
- Section 6 Cyber security and privacy. Assuring information security and privacy in Smart grids are major concerns for acceptance by all stakeholders, mot the least, customers.
- Section 7 Use cases, This section illustrate our approach and findings by two use cases related to empowerment of customers. That is, use cases related to Smart homes and Green energy. Use cases are the drivers of successful business cases of Smart grids. The use cases are basis for requirement engineering and validations of interoperability. Based on the use cases we identify corresponding Service Level Agreements (SLAs) supporting coordination of stakeholders providing the intended services respecting agreed upon Quality of Service (QoS). To enable reconfiguration of use cases supporting different types of Self healing and/or new business opportunities we also discuss the role of meta modeling in Smart grids.
- Section 8 Tools and Environments, We briefly describe some tools and environments supporting structured requirement engineering, design, development, monitoring,

maintenance and assessments of Smart grid pilots. Proper tools and environments are crucial for successful approaches of Smart grid solutions.

- Section 9 Conclusions and future work.

The chapter ends with a list of *References*.



CREATING BENEFITS FOR CONSUMERS THROUGH THE PROVISION OF TAILORED ENERGY SERVICES AND INFORMATION

Status	EED proposals
• Considerable saving potential unused in the residential and services sectors • Slow uptake of market for energy efficiency services • Lack of awareness & access to appropriate information on EE benefits • Technological developments (e.g. smart meters/ grids) not sufficiently reflecting households interests	• **National energy efficiency obligation** scheme for utilities • **Obligation for individual energy meters**, reflecting actual energy consumption & information on actual time of use • Ensure **accuracy & frequency** of **billing** based on **actual consumption** • Appropriate information with the bill providing comprehensive account of current energy costs

Fig. 2. Promoting Active Consumers participating in EE efforts.

2. Smart grids – architectures, stakeholders, challenges, barriers and solutions

Modeling and Optimization of Sustainable Energy Systems poses several challenges. A starting point for our investigation is the *NIST Framework and Roadmap for future Smart Grids* [30]. The document identifies *seven domains* within the Smart Grid—*Transmission*, *Distribution*, *Operations*, *Bulk Generation*, *Markets*, *Customer*, and *Service Provider*. A Smart Grid domain is a high-level grouping of organizations, buildings, individuals, systems, devices, or other *actors* with similar objectives and relying on—or participating in—similar types of applications. Across the seven domains, numerous actors will capture, transmit, store, edit, and process the information necessary for Smart Grid applications.

The NIST Framework shows that future Smart grids support the following two flows:

- *Power (electrical) flows* (generation, transmission and distribution)
- *Information processing flows* (collecting, processing and distribution). The information flow has the following *two* objectives:
  - Monitoring and control of the energy flows (c.f., classical SCADA)
  - Monitoring and control of future and new energy based services in Smart grids

Both flows require protection and ancillary systems to support interoperability and Quality of Service.

The NIST Framework has also been adopted by IEEE in IEEE Guide for Smart Grid Interoperability for Energy Technology and Information Technology Operation with Information with the Electric Power System (EPS), End-Use Applications, and Loads (2011)[2]. The guide gives architectures for the different Domains as well as identified interfaces between them related to the information flows. Based on the ANSI/ISA-99 (now IEC 62443.02.01) protocols we can introduce levels of segmentation and traffic control inside control systems creating multiple separated Zones and conduits supporting "defense in the depth strategies" providing Cyber security (Section 6).

In general, actors in the same domain have similar objectives. To enable Smart Grid functionality, the actors in a particular domain often interact with actors in other domains, as shown in Figure 3. However, communications within the same domain may not necessarily have similar characteristics and requirements. For example, for communications or information within the Customer domain, simple meter readings have simple characteristics and requirements such as a meter communicates with a specific utility head-end system, while a customer portals need to have multiple users accessing it at the same time and to different accounts (*role based access*).

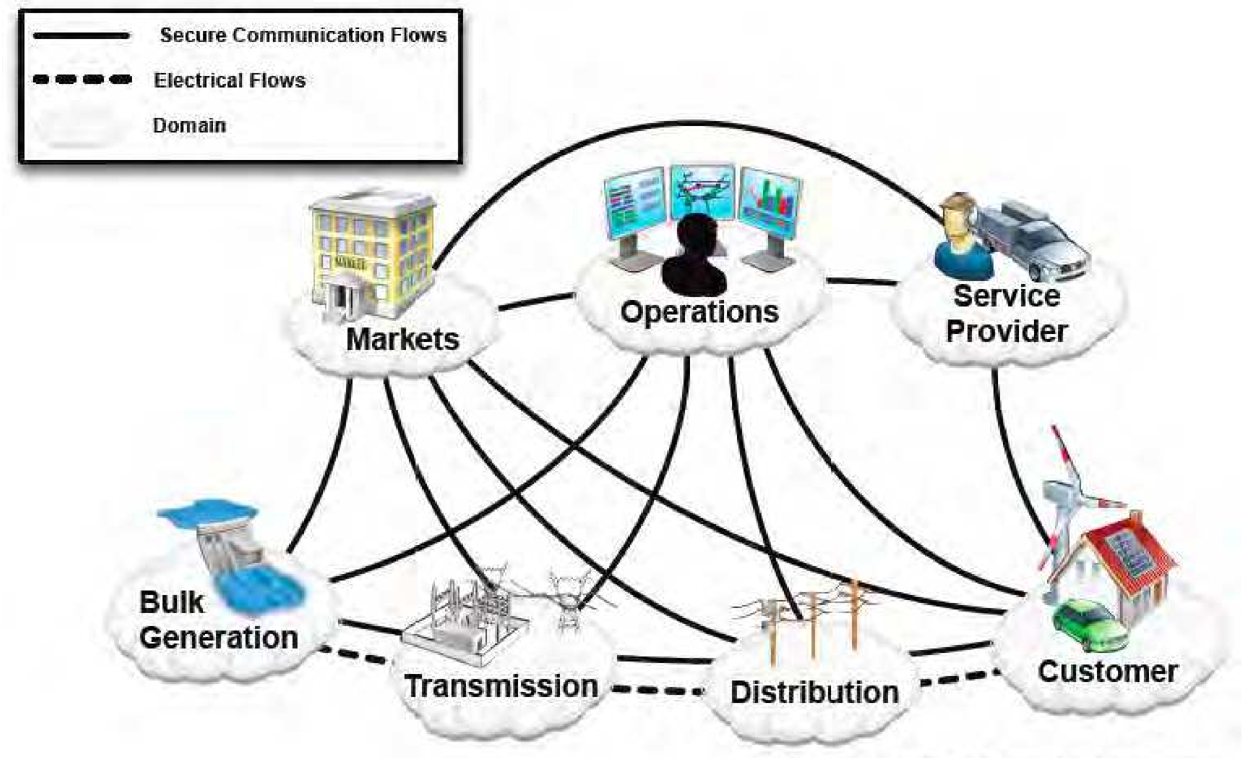


Fig. 3. NIST Framework of Smart grids as composed of seven domains.

Moreover, particular domains may contain components of other domains. For instance, the ten Independent System Operators and Regional Transmission Organizations (ISOs/RTOs) in North America have actors in both the Markets and Operations domains. Similarly, a distribution utility is not entirely contained within the Distribution domain—it is likely to

[2] Home page: http://standards.ieee.org/findstds/standard/2030-2011.html

contain actors in the Operations domain, such as a distribution management system, and in the Customer domain, such as meters.

The core of present day power systems is the *EMS – Energy Management System* monitoring and controlling the performance of production, transport and distribution of power. The EMS is supported by *SCADA systems* for monitoring and control as well as *support systems* for protection, optimization and billing. The stakeholders are *TSOs (Transmission System Operator)* responsible for the generation and transport grid, *DSOs (Distribution System Operators)* responsible for the distribution grid and service to *customers*.

We note the following inherent increased complexities of Smart grids compared to present day grids:

- *Increased number of Stakeholders* with new capabilities, roles and responsibilities
- *Increased complexity* of the electric grid that now has to incorporate vast amounts of *Renewable Energy Resources (RES)* and *Distributed Generation (DER)*
- A need of a *complementary ICT* information management system to support information exchange and sharing between stakeholders providing energy-based services in a secure and trusted way

More efforts are required by all stakeholders to enable improved future energy production, distribution and usage [1]. Furthermore, novel business models are required to support the transition from today’s situation to Smart grid based on markets of energy-based services [7, 12, 13, 14]. Providing novel services based on setting of customer comfort is one identified area by the EU projects FENIX[3] and SEESGEN-ICT[4]. Of particular interest to us is the *Customer Domain* given in Figure 4. From this figure it follows that we can have two kinds of Customers, *Home-based Consumers* and *Business-based Consumers* that can interact with actors of other domains in their business processes.

Proper Empowerment of those two kinds of customers can largely contribute to increased Energy Efficiency. However, we will in this chapter concentrate on the Home-based Consumer (Customer).

Given the central role of Customers and supporting infrastructures in the Energy Efficiency Plan 2011 (above) it is also clear that Customers could be important partners with other Stakeholders and ESCOs in providing substantial increases in EE in the future. However, clearly this take-up will to a large degree depend on the *trustworthiness of the supporting infrastructures*.

To support further investigations in this chapter along those lines we introduce different coordination views of the Smart grid Socio-technical system, Figure 5. One of the identified barriers of Smart grids is the inherent inflexibility to add more and flexible business cases in today’s power systems, due to tight coupling of the Grid hardware and SCADA systems [25, 26].

Future energy systems will become robust and efficient with a careful *supplement* of the SCADA systems with specifically designed and implemented ICT systems *ensuring Smart*

[3] http://www.fenix-project.org/

[4] http://seesgen-ict.erse-web.it/

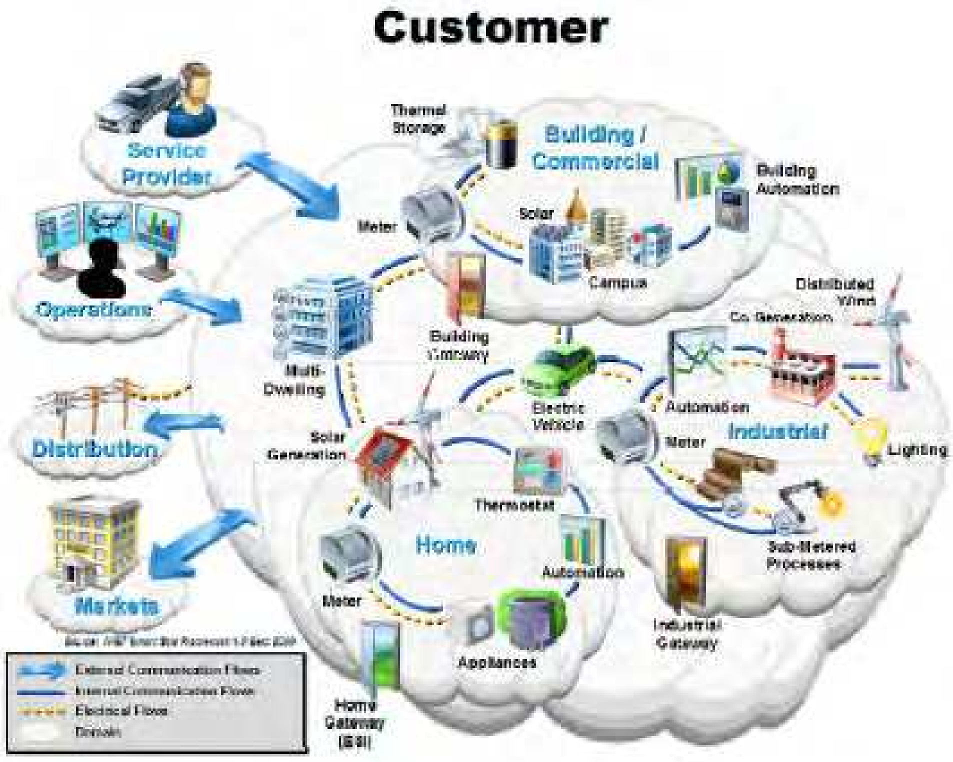


Fig. 4. The Customer Domain including different types of Consumers.

grid Interoperability (Figure 6). In this Chapter, we expand some novel ideas introduced in SEESGEN-ICT [1], deliverables D3-2, D3-3 and to assess identified barriers and implement relevant ICT solutions for future pilots of Smart Grids.

Figure 5 captures some of the challenges identified in [1] To cope with coordination of different sets of stakeholders we propose introduction of *Service Level Agreements* (SLAs). SLAs are identified and set up supporting business cases with identified stakeholders. *Key Performance Indicators* (KPIs) are identified and monitored during deliverance of the agreed upon energy based services. In Figure 5 some challenges are identified in transforming Business models, related Stakeholders and relevant Infrastructures into SLAs. Challenges related to supporting ICT infrastructures are also indicated, e.g., *real time dependencies and data management*. In particular the *cross-point* between high-level and low-level system views is indicated. That is, high-level business oriented infrastructures such as web-services and low-level infrastructures supporting distributed systems such as OPC have to be suitable *interoperable* (Section 7 Use cases), It should be noted that for classical SCADA systems, we have a *bottom up integration* of signals from the EMS system to the top operator level for management of monitoring and control with no need to address this cross-point.

We will come back to Figure 4 and Figure 5 in Section 3 Requirements engineering and Validation as well as in Section 4 Customer empowerment and Section 5 Information processing systems and sharing and protection of information. Issues related to the cross-point will be addressed in Section 7 Uses Cases. Basically, we will introduce Service Level Agreements (SLAs) to coordinate stakeholders providing energy-based services by selected clusters. Furthermore monitoring of Key Performance Indicators (KPIs) of SLAs will enable validating selected Interoperability criteria and Quality of Service (QoS).

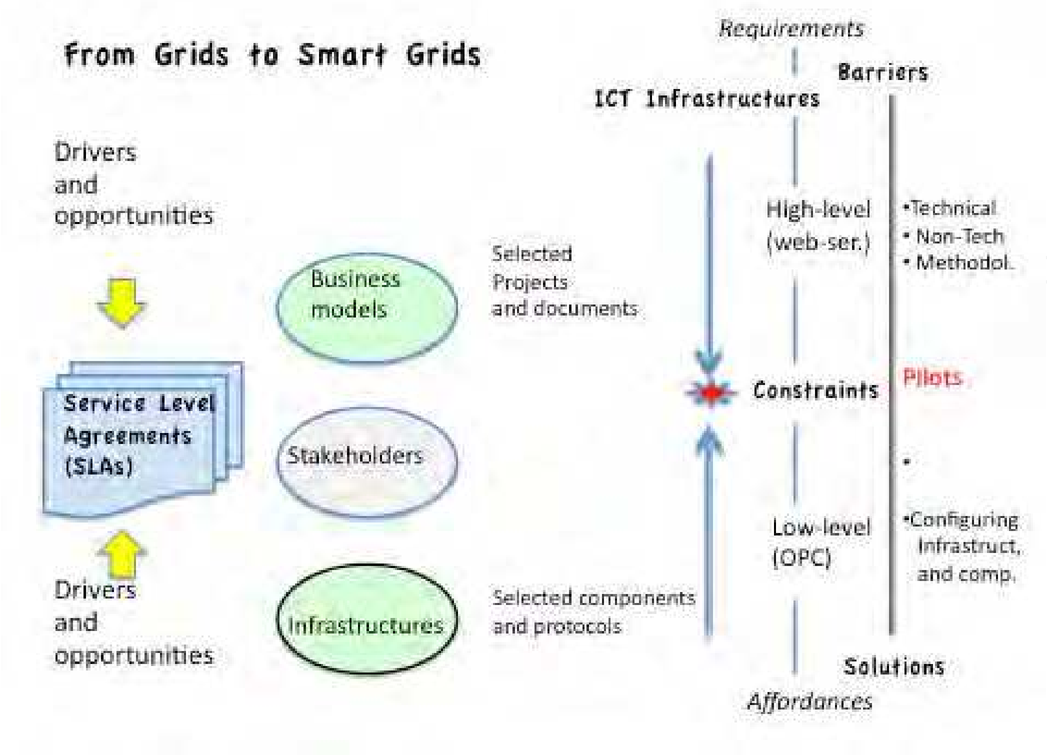

from Grids to Smart Grids
Drivers and opportunities
Service Level Agreements (SLAs)
Drivers and opportunities
Business models
Stakeholders
Infrastructures
Selected Projects and documents
Selected components and protocols
Requirements
ICT Infrastructures
Barriers
High-level (web-ser.)
•Technical
• Non-Tech
• Methodol.
Constraints
Pilots
•
Low-level (OPC)
•Configuring Infrastruct. and comp.
Solutions
Affordances

Fig. 5. Coordination aspects of future Smart grids.

One of the identified *barriers* in this transition of systems into Smart grids, is the inflexibility to add more and flexible business processes into today's power systems, due to the tight vertical (in voltage levels) coupling of the Grid hardware and operator stations by SCADA (Sensory control and Data Acquisition) presented in [4, 5]. Future energy systems will hopefully become robust and efficient with careful integration of ICT (Information Communication and Technology). However, due to the difficult to predict nature of changes in the infrastructures and business models as well as regulatory uncertainties, the pace of uptake and implementation of Smart Grid is hard to predict.

The scope and purpose of monitoring has lately, however, changed towards *ensuring interoperability* of systems due to *increased complexity* of the systems at hand. As a matter of fact, analysis of larger blackouts, such as the August 14, 2003 blackout in northeast United Stated and Ontario, has shown that this kind of event can be attributed to sequences of *interoperability failures*[5] of related systems. The systemic property of *Interoperability* has been proposed by organisations such as NIST[6] and GridWise[7] in the US and is also adopted by EU.

NIST has the following definition of Interoperability:

"The capability of two or more networks, systems, devices, applications or components to exchange and readily use information, securely, effectively and with little or no

[5] GridWise Architecture Council Report: *Reliability Benefits of Interoperability*, 2009, pp. 7 – 9.

[6] Home page: http://www.nist.gov/smartgrid/

[7] Home page: http://www.gridwiseac.org/

inconvenience to the user. The system will share a common meaning of the exchanged information and this information will elicit agreed-upon types of response." [NIST[8]]

The following additional requirements are put forward by GridWise Architecture Council (GWAC[9]):

- "an agreed expectation for the response of the information exchange"
- "requisite quality of service in information exchange: reliability, fidelity, security"
- "the results of such interactions enables a larger system capability that transcends the local perspective of each participating subsystem"

GWAC has proposed the following *Interoperability Framework* consisting of three *Interoperability Categories* (Technical, Informational and Organizational) and *Crosscutting Issues* related to *non-functional* requirements, such as *Energy Efficiency* (EE). The Technical interoperability is enabled by *proper open protocols and network technologies*. In order to *verify or validate* interoperability of Smart grid systems we have to identify *suitable views* of those systems. We argue that such views can be provided and monitored by suitable *Service Level Agreements* (SLAs) [3, 14, 27, 28, 29, 30]. The SLAs will take into accounts business cases and involved stakeholders to assure relevant Quality of Service (QoS). That is, *also* take into account the *Informational and Organizational* categories of the GWAC Framework (Section 3).

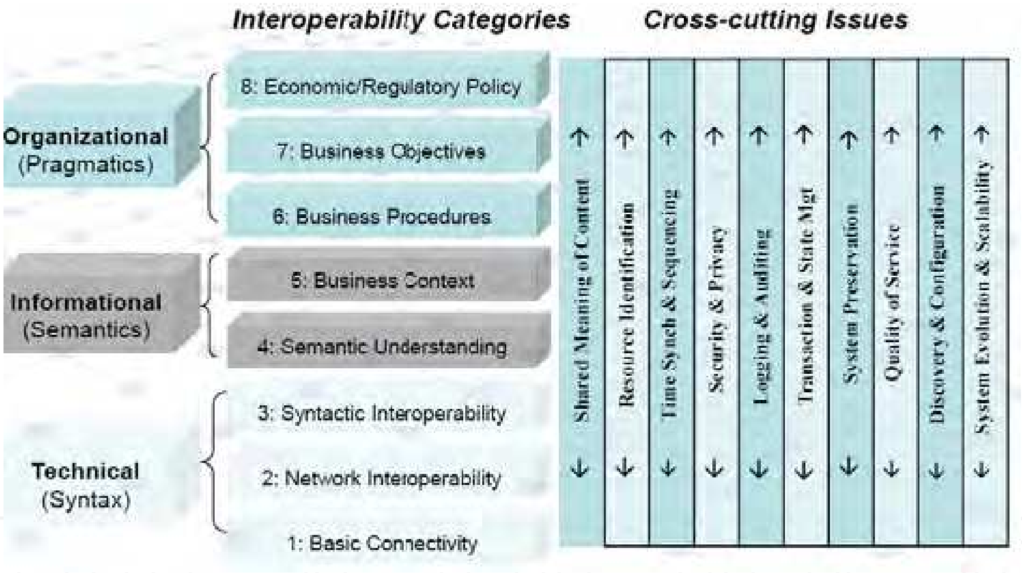


Fig. 6. GWAC Interoperability Framework with a layered set of Categories and non-functional Cross-cutting Issues.

The concept of "smart" in Smart Grids refers mostly to "Smart distribution grids" utilizing smart energy system components, empowered and active customers and flexible and resilient systems. This is enabled by a transition of today's hierarchical and mostly proprietary systems to open, loosely coupled and flexible service oriented systems. Obviously, flexible pattern oriented interaction models are here key enabler. In short, a transition to sustainable Smart Grids will benefit from utilization and use of agent

[8] Home page: http://www.nist.gov/smartgrid/
[9] Home page: http://www.gridwiseac.org/

technologies. We have during the last decade addressed different views on technologies underpinning design and implementation of Interoperability according to Figure 6. That is, *agent systems* [3, 5, 7] , *service oriented systems* [4, 6] , *critical infrastructures* [8, 9, 11, 16, 24], *experimental environments* [8, 9, 15, 24, 25, e, g], and SLAs [12, 26, 27, i]. In short, in order to design and validate interoperability of views of smart grids, we configure and monitor SLAs based on agent-oriented services. Design, implementation and validation are utilizing aggregation tools and experimental environments.

Introducing agent-based services or implementing *Service Oriented Multi-agent Systems (MAS)* facilitates taking into account intelligence or smartness of future Smart Grids. Agent technologies allow modelling systems as configurations of smart flexible components, e.g., *Active Network Management* (ANM) of Distribution Grids [18]. *The IEEE Power and Energy Society Multiagent Systems Working Group*[10] aims to promote the openness of agent architectures within the power domain. In this paper we argue that *Service Level Agreements (SLAs)* provides a *control and monitoring structure of MAS* assuring inter-operability and QoS.

3. Requirements engineering and validation

Proper Requirements Engineering is the underpinning of design, implementation, validation and maintenance of systems. This is especially important for future Smart grids due to the inherent complexities of *coordinating different sets of stakeholders* in *changing market environments* with *internal and external threats*. In short, among desired system requirements complementing selected functional and non-functional requirements, we also have to address different aspects of *self-healing in cases of breakdowns* of SLAs and methods to support *adjustments and reconfigurations of business cases*. In short we need to address *meta-models* of SLAs to allow *resilience and flexibility*.

In Section 5 Information processing systems and sharing and protection of information is addressed as enabling technologies of Interoperability. The important issues of security, privacy and vulnerabilities of Information processing systems (ICT and SCADA) will be further addressed in Section 6 *Cyber security and privacy*.

Figure 7 expands upon Figure 3 and depicts a composite high-level view of the actors within each of the Smart Grid domains. This high-level diagram is provided as a reference diagram. Actors are devices, systems, or programs that make decisions and exchange information necessary for executing applications within the Smart Grid. The analysis and discussions later in this chapter expand upon this high-level diagram and include logical interfaces between actors and domains.

From Figure 3 and Figure 7 we have a high-level conceptual architecture of Smart grids domains and the power and information flows between domains and actors. Furthermore, in Figure 7 some high level components and their interfaces are depicted.

Requirements engineering concerns meeting *functional requirements and constraints* of the flows as well as means of *instrumentation, monitoring and controlling* sensors and actuators regarding *Key Performance Indicators* (KPIs).

[10] Home page: http://ewh.ieee.org/mu/pes-mas/

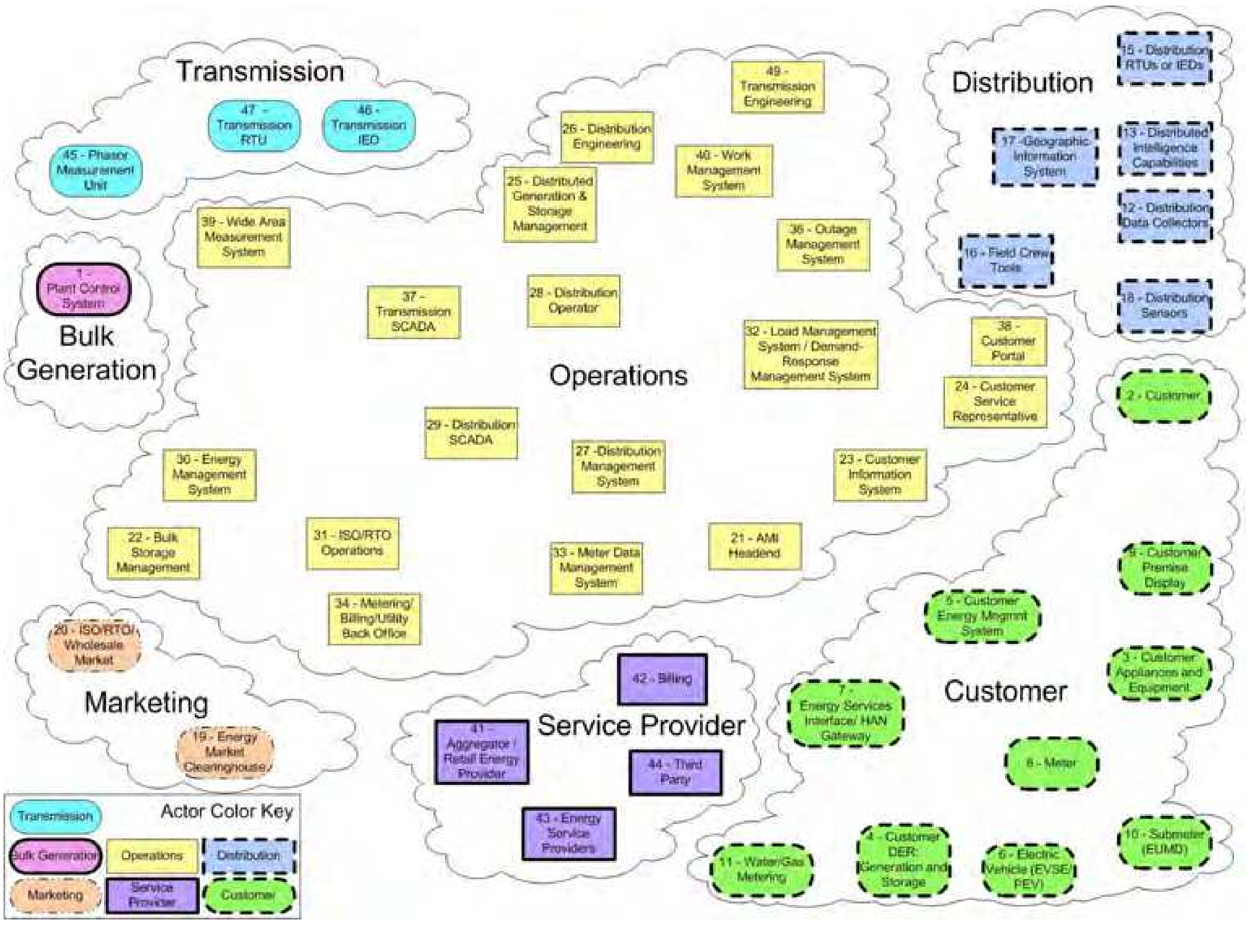

Transmission
47 - Transmission RTU
46 - Transmission IED
45 - Phasor Measurement Unit
1 - Plant Control System
Bulk Generation
49 - Transmission Engineering
26 - Distribution Engineering
25 - Distributed Generation & Storage Management
40 - Work Management System
39 - Wide Area Measurement System
36 - Outage Management System
37 - Transmission SCADA
28 - Distribution Operator
32 - Load Management System / Demand-Response Management System
Operations
38 - Customer Portal
24 - Customer Service Representative
29 - Distribution SCADA
27 -Distribution Management System
23 - Customer Information System
30 - Energy Management System
22 - Bulk Storage Management
31 - ISO/RTO Operations
21 - AMI Headend
33 - Meter Data Management System
34 - Metering/ Billing/Utility Back Office
Distribution
15 - Distribution RTUs or IEDs
17 -Geographic Information System
13 - Distributed Intelligence Capabilities
12 - Distribution Data Collectors
16 - Field Crew Tools
18 - Distribution Sensors
2 - Customer
9 - Customer Premise Display
5 - Customer Energy Mngmnt System
3 - Customer Appliances and Equipment
7 - Energy Services Interface/ HAN Gateway
Customer
8 - Meter
10 - Submeter (EUMD)
11 - Water/Gas Metering
4 - Customer DER: Generation and Storage
6 - Electric Vehicle (EVSE/ PEV)
20 - ISO/RTO/ Wholesale Market
Marketing
19 - Energy Market Clearinghouse
42 - Billing
41 - Aggregator / Retail Energy Provider
Service Provider
44 - Third Party
43 - Energy Service Providers
Actor Color Key
Transmission
Bulk Generation
Operations
Distribution
Marketing
Service Provider
Customer

Fig. 7. Composite High-level View of the Actors within Each of the Smart Grid Domains.

In Figure 5 of Section 2 we illustrate some views and challenges to be addressed in requirements engineering for Smart grids. It captures the *constraints that Interoperability criteria* (Figure 6) have to *comply with concerns* from the different Interoperability Categories *with affordance*s from the supporting infrastructures, for instance at Customers premises (Section 4 and Section 7). The high-level demands have to meet the low-level affordances and constraints. Compare with Figure 6, where the Organizational and Information Categories have to meet the Technical Category as well as relevant Cross cutting Issues while meeting interoperability goals. The Service Level Agreements involves concerned stakeholders as well as Key Performance Indicators (KPI) to be monitored to ensure interoperability and Quality of Service. In [1] a set of *Barriers* and *Solutions* related to Smart Grids have been identified as well as suitable ICT systems.

It should be noted that in the classical grid the information processing system is by and large proprietary SCADA systems. The SCADA system *integrates* information *bottom-up* from the grid to the system operators and allows sending control signals *top-down* to the grid components: In short, a *stove-pipe* system! In Smart Grids we also need ICT systems providing horizontal as well as vertical interoperable information exchange between stakeholders (Section 5). In Figure 5 the *interactio*n between low-level and high-level SLAs is indicated. We will address this challenge later in the case study *Customer empowerment* (Section 4 and Section 7).

Identified challenges include coordination of sets of stakeholders and monitoring of processes related to new energy-based business processes. To that end we have advocated introduction and use of mechanisms based on Service Level Agreements (SLAs). Introduction of SLAs also enables a principled structuring of Smart Grid systems and related data flows [26, 27, i]. We will also address some of those topics in this Chapter.

Our approach towards modelling and implementing Smart Grid is utilizing carefully chosen infrastructures in flexible couplings and integrations (configurations) of system components [4, 6, a]. The configurations should support monitoring of processes by *clusters of SLAs implementing selected scenarios* of Smart Grids.

The *power flows* of power systems must fulfil the *electric constraints* balancing *active* and *reactive* power in real time. This balance in terms of KPIs includes voltage, current and frequency. Introduction of DERs will potentially affect voltage and frequency and has to be controlled. This issue will further be discussed in *Section 7 Use cases*.

Furthermore power could be of *two types*: *DC* or *AC*. *Transformation* between *power types* and *voltage levels* (low, medium, high) will assure proper functioning of the grid infrastructures.

The trustworthy information processing and information sharing system of Figure 3 has also to take into account *similar constraints* as the power system. Firstly the information can be modelled in the following three different *types* [9]:

- I_1, *Information payload*. This is the information type shared among stakeholders.
- I_2, *Communication related information*. This type of information that manages the networking tasks, e.g., by middleware.
- I_3, *Processing information*. Running code of executable tasks for stakeholders. Cyber attacks are targeting at manipulating I_3 by exploiting vulnerabilities (Section 6).

Usually, information security focuses on protection of type Information payload since it primary concerns *Confidentiality, Integrity, and Availability* (CIA) of stakeholder centric information. However, external cyber attacks usually try to take control of the processes by *manipulatin*g the run-time stack containing code (I_3) (e.g., Buffer overflow). We can also have directed attacks on the SCADA system itself (e.g., the worm Stuxnet[11]) (Section 6).

Obviously, the different information types I_2 and I_3 can be *compared with Reactive and Active power of AC grids.* They divide the processing and electric power into two parts that must interact to enable working systems. In the case of Information systems, given a fixed amount of computational power, there is a *trade-off* between communication processing and task solving processing allowing a trade-off between communication costs and local task solving capacity in distributed systems. We also only have only one chargeable part in each case (active power and task processing). The reactive power is used to maintain energy balance during changing loads, but is not directly chargeable to customers. However, the customers have to pay transmission and distribution cost beside the energy consumption costs, For information systems there is in the same way separate costs for *communication (networking)* and *customer services*.

[11] http://en.wikipedia.org/wiki/Stuxnet

Finally, as with power systems, information can be transformed into *levels.* The GWAC *Interoperability Framework* (Figure 6) identifies the following eight *Interoperability Categories (levels)* that fall into the following categories (bottom up).

- *Technical*: Basic Connectivity, Network Interoperability, Syntactic Interoperability
- *Informational*: Semantic Understanding, Business Context
- *Organizational*: Business Procedures, Business Objectives, Economic/Regulatory Policy

The organizational categories emphasize the *pragmatic* aspects of interoperation. They represent the policy and *business drivers* of interoperation. The information categories emphasize the *semantic* aspects of interoperation. They focus on what information is being exchanged and its *meaning*. The technical categories emphasize the *syntax* or format of the information. They focus on how the information is *represented* within a *message exchange* and on the *communication medium*.

Information types consequently have *data formats* and *exchange protocols* for the technical categories. Interoperability on higher semantic categories has to be supported by *dialogue-based* protocols and *semantic annotations* (Section 4, Section 5, and Section 6).

Figure 5 complements Figure 3 and Figure 6 in providing a *structured approach* towards tool-based Design and Implementation and Validation of Smart grid *Pilots* (Section 8).

We can now *rephrase* the proposal Energy Efficiency Plan 2011 and recommendations of Section 1 (Figure 2) as follows. Future Smart grids should support:

- Empowerment of Customer to *automatically manage and control clusters* of customer-centric *smart appliances* and to dynamically change user profiles to *meet user preferences* and market models.
- *Trustworthy* and transparent business and use-case *information management* and *information exchange* with customers and other stakeholders.

Requirements engineering will *match* the relevant business case with stakeholders' capabilities and concerns with affordances from the infrastructures (Figure 5). A selection of relevant components of the Interoperability Categories together with a selection of relevant Cross- cutting Issues give the input to negotiating and setting up a suitable SLA. To support this activity we have developed a suitable tool (Section 8). I should be noted that adding the constraints (e.g., crosscutting issues) might result in that we do not have *any* initial solution. Addressing interoperability can add or delete constraints towards an acceptable solution. *Pilots and validations*, based on requirements, can now be addressed (Section 8).

The following Sections will address challenges related to the recommendations above in more detail.

4. Customer empowerment

The concepts and ideas of *Customer empowerment* are arguably the most revolutionary in the transition towards Smart grids (Section 1). The traditional roles of customers have been as *passive loads* of the grid. Sometimes even refereed to as "two holes in the wall". The billings by the DSOs have been based on *fixed tariffs* and *measured consumption at customer sites* done *at pre-defined* intervals using *Automatic Meters Reading* systems (AMR). During the 90ties, some efforts where made to allow DSOs to *control* the consumption of customers by introducing different schemas of *Demand Side Management (DSM).* By different time-based fixed tariffs the DSOs could to some extent *alter t*he amount of energy delivered to customers during agreed upon conditions and intervals. During the beginning of this century a new generation of meters allowing *remote reading* were introduced and deployed in several countries. However, most of these meters only allowed *unidirectional* information flows from meter to DSOs. *Bidirectional* enabled metering systems allowing true communication between customers and DSOs is the focus of future *Smart Metering Systems* (SMS). In fact those mew kinds of Smart Meters could be seen as *Intelligent access tools* between *prosumers* (a mixture of producer and consumer) and other stakeholders in a local energy market (Figure 7).

The changing views of customers from passive "two holes in the wall" to active empowered stakeholders of future Smart grids requires changes of mindsets and implementation of supporting technologies and legal frameworks. These changes of mindsets are pre-conditions for acceptance and uptake of Smart grids. The underpinnings here are *trustworthiness, usefulness* and *added value*.

NIST provides the following definition of the Customer.

"Customer is an entity that pays for electrical goods or services. A customer of the utility, including customers who provide more power then they consume (prosumers)".

Customer empowerment aim at:

1. Identifying and eliminate or circumvent identified shortcomings by customers in pursuing selected tasks.
2. Enable trustworthy information exchange with other stakeholders and with smart appliances

The solutions are development of context sensitive tools and environments (item 1) and validation of appropriate views of Interoperability (item 2). We will address some of those aspects in Section 5 Information processing systems, Section 7 Use cases, and Section 8 Tools and Environments. As Use cases we address the following aspects of customer empowerment:

- Support for customer to *include/change* energy provided by *Renewable Energy Sources (RES/DER)* in the customer profile.
- Support for customer to take part in agreements in trustworthy curtailment of energy,

The first use case address increasing user involvement in selecting energy sources. The second use case illustrates trusted behaviour in service break-downs, Both are handled by setting up and monitoring suitable SLAs.

In both those use cases we have to take into the *dependency* between business cases and its impact by the physical status of the energy system (voltage control) (Figure 5).

From Figure 4 and Figure 7 we can identify some of the *Actors (tasks) related to the Customer Domain* of Smart grids. From the NISTIR 7628 document we have the following high- level listing of Actors, tasks, and infrastructure components based on Figure 7:

- *Customer Appliances and Equipment*. A device or instrument designed to perform a specific function, especially an electrical device, such as a toaster, for household use. An electric appliance or machinery that may have the ability to be monitored controlled and/or displayed.
- *Customer Distributed Energy Resources (DER) Generation and Storage*. Energy generation resources, such as solar or wind, used to generate and store energy (located on customer site) to interface to the controller (HAN – Home Area Network / BAN) to perform an energy related activity.
- *Customer Energy Management System (EMS)*. An application service or device that communicates with devices in the home, This application service or device mat have interfaces to the meter to read usage data or the operations domain to get pricing or other information to make automated or manual decisions to control energy consumption more efficiently. The EMS may be a utility subscription service, a third party, offered service, a consumer-specified policy, a consumer-oriented device. Or a manual control by the utility or consumer
- *Customer Premises Display*. This device will enable customers to view their usage and cost data within their home or business
- *Sub-Meter - Energy Usage Metering Device (EUMD).* A meter connected after the main billing meter. It may not be a billing meter and is typically used for information monitoring purposes.
- *Electric Vehicle Service Element/Plug in Electric Vehicle (EVSE/PEV)*. A vehicle primary driven by a rechargeable battery that may be recharged by plugging into the grid by recharging from a gasoline-driven generator.
- *Home Area Network Gateway (HAN Gateway)*. An interface between the distribution, operations, service provider, and customer domain and the services within the customer domain.
- *Meter*. Point of sale device used for transfer of product and measuring usage from one domain/system to another.
- *Customer Premise Display*. This device will enable customers to view their usage and cost data within their home or business.
- *Sub-Meter – Energy Usage Metering Device (EUMD)*. A meter connected to the main billing meter. It may or may not be a billing meter and is typically used for information-monitoring purposes.
- *Water/Gas Metering.* Point of sale device used for the transfer of product (water and gas) and measuring usage from one domain to another.

The most important Customer related infrastructures potentially supporting increased EE are selections of:

- Customer EMS
- HAN Gateway
- Customer DER Generation and Storage
- Smart devices and appliances

Configurations of those components of Figure 7 correspond to *Slices* of Figure 6 that can be recast in terms of Cloud Computing [28]. Cloud Computing comes basically in three types:

- Software as a Service (SaaS)

- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

A Current example of PaaS is *Windows Azure Platform*[12] a supplementary SaaS is Microsoft Online Services[13]. An other example is *Amazon Elastic Compute Cloud* EC2[14]. Cloud computing allows *resource sharing and outsourcing*. Well-known examples include sharing of large data centres that implies large IT-based increases in EE.

So far, it has been very few investigations of the impact on Cloud computing technologies on future Smart grids. Obviously Customer based infrastructures and services could benefit from *different types* of SaaS, PaaS or IaaS solutions with *selected combinations of stakeholders*. The selected customer actors could then play different roles in the corresponding Service Level Agreements.

The different Cloud Computing types correspond to *different slices* of the GWAC Interoperability Framework Figure 6. A SaaS offers an environment (device) with a *fixed* integration of Interoperability categories, allowing easy plug in of software services. An interesting trend is here Smart phones (e.g., iPhone) with Apps[15]. Paas and IaaS allows not only plug in of Apps but also customized configuration of higher-level Informational and/or Organizational Categories. Devices accessing a PaaS or IaaS thus support the user with a richer environment than a device accessing a PaaS (single service support).

It should be noted from Figure 5 that a *fixed physical infrastructure* could support *several separated virtual overlay infrastructures* allowing structures reuse of physical resources in virtual settings. Of course, there is a *price to pay* (*performance and security*) for this flexibility.

For a Customer accessing a set of Smart home actors he/she can choose to access each of them individually as smart services (Apps). However, due to complexities of management or lack of overview, this solution can create cognitive overloads and become contra-productive. We should aim at flexible grouping of actors with common interfaces to customers including support tools.

In Section 6 we take a selection of selected actors in addressing these challenges. But as a preparation, we need to take a deeper view on challenges and solutions related to customized information processing systems supporting information sharing and learning. The material in those sections takes into account referenced produced thesis work and papers related to several international and national R&D project from the R&D Group Societies of Computation (SoC) at Blekinge Institute of Technology (BTH) [22, 32, a, b, c, d, f, h].

5. Information processing systems and sharing and protection of information

The following basic relation, Figure 8, between *Information*, *Representation* and *Interpretation* is captured from [19, 20] on *meaning* of *Situations and attitudes*. It captures the relation between Information (data) and its Representation (text, video, graphics) that has to be

[12] Home page: http://www.microsoft.com/windowsazure/

[13] Home page: http://www.microsoft.com/online/

[14] Home page: http://aws.amazon.com/ec2/

[15] Home page: http://www.apple.com/iphone/apps-for-iphone/

Interpreted by an agent with certain *capabilities*. The meaning by the receiving agent of the Representation should reflect the intended meaning by the sending agent. To assist the receiving agent some times *empowering* tools are provided to support interpretation.

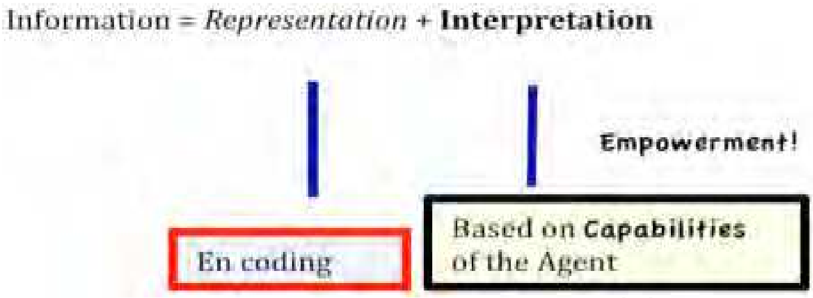

Information = Representation + Interpretation
Empowerment!
En coding
Based on Capabilities of the Agent

Fig. 8. Relations between Information (data), its representation and Interpreted meaning by an agent.

Basic challenges to be addressed in *designing and validating Interoperability* (Figure 6) are:

- Information sharing in teams requires *common understanding* (Interoperability)
- Information *hiding* is based on cryptographic representation
- Information *management needs tools* (*role and credential based access control* and data flow assurance). Enabling technologies are here *information models and structures*.

Addressing and validating Interoperability based on the frameworks by NIST, GWAC and IEEE requires standards related to connectivity (protocols), Information sharing and contextual issues (Figure 6). Protocols establish *horizontal connectivity* between stakeholders at different Interoperability Categories.

Standards supporting different aspects of Interoperability include *IEC protocols* IEC 61850[16] (connectivity) and IEC 61970-302 & 61968-11 (Common Information Model[17]), *MultiSpeak protocols* [18]and *OPC UA*[19] *protocols*.

The most important feature of those standards is the introduction of structured Information Models. In the IEC case the modeling techniques from UML (including XML Schema and RDF Resource Description Framework) are used with implementation techniques such as web services. MultiSpeak and OPC UA also use similar approaches. Common abstract data modeling supports translations between the different implementations. However, the different implementations have different performance profiles.

The following Figure 9 shows a CIM model of a Transformer consisting of four objects with attributes and attribute values, The UML models uses Class Hierarchies and UML Class diagrams together with *Inheritance, Associations*, *Aggregations* and *Compositions*.

From Figure 9 we can search for and find, or set, attributes belonging to a given object. This allows us to compose attributes belonging to a given object (stakeholder) from other objects.

[16] User Group: http://iec61850.ucaiug.org/default.aspx
[17] CIM User Group: http://cimug.ucaiug.org/default.aspx
[18] Home Page: http://www.multispeak.org/Pages/default.aspx
[19] OPC UA Home Page:
http://www.opcfoundation.org/Default.aspx/01_about/UA.asp?MID=AboutOPC

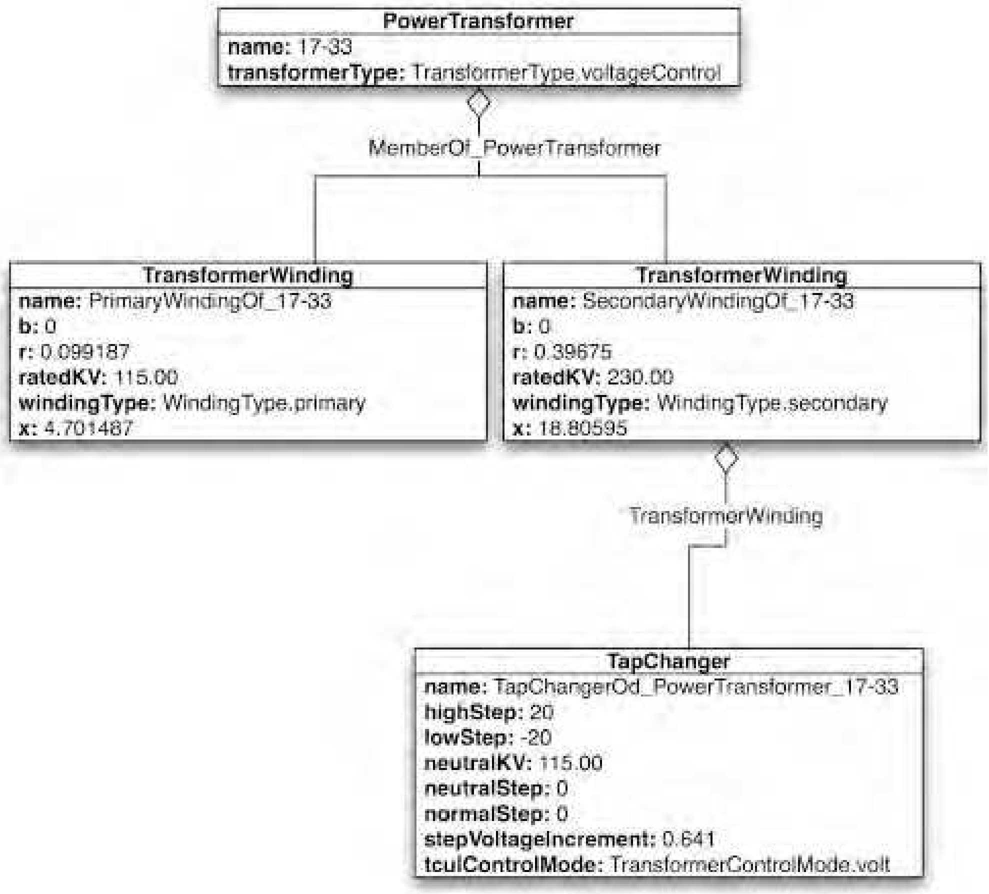

PowerTransformer
name: 17-33
transformerType: TransformerType.voltageControl
MemberOf_PowerTransformer
TransformerWinding
name: PrimaryWindingOf_17-33
b: 0
r: 0.099187
ratedKV: 115.00
windingType: WindingType.primary
x: 4.701467
TransformerWinding
name: SecondaryWindingOf_17-33
b: 0
r: 0.39675
ratedKV: 230.00
windingType: WindingType.secondary
x: 18.80595
TransformerWinding
TapChanger
name: TapChangerOd_PowerTransformer_17-33
highStep: 20
lowStep: -20
neutralKV: 115.00
neutralStep: 0
normalStep: 0
stepVoltageIncrement: 0.641
tculControlMode: TransformerControlMode.volt

Fig. 9. CIM model of the object Transformer with four sub objects and attributes.

In fact we can give a semantic mapping of object attributes onto other attribute. Hence a *semantic mapping of attributes both horizontally and vertically* across the Interoperability Framework of Figure 6.

Modeling the relevant CIM components (Figure 9) gives us basic *Representations* of Information to be *interpreted and validated* by the different stakeholders to ensure Interoperability according to Figure 6 and Figure 8. The CIM models have to be *interpreted* with the correct semantics, given by the *competencies* and supporting *tools* of the stakeholders in case.

To address these challenge we have developed a methodology supporting *trustworthy engineering* of complex systems. The main components of our model for *engineering trustworthy systems* are as follows (Figure 10).

In setting up a Service Level Agreement (SLA) among stakeholders in delivering a energy based service we will use a negotiation tool for that purpose (Section 8 Tools and Environments). To allow for Interoperability we use the GWAC Framework of Figure 6. The different stakeholders bring upfront their *concerns* regarding selected Interoperability Categories and restricting Cross-cutting Issues.

During the negotiating phase agreements are found among stakeholders on *Trust aspects* to be monitored during deliverable of services. An important finding here is to agree upon the

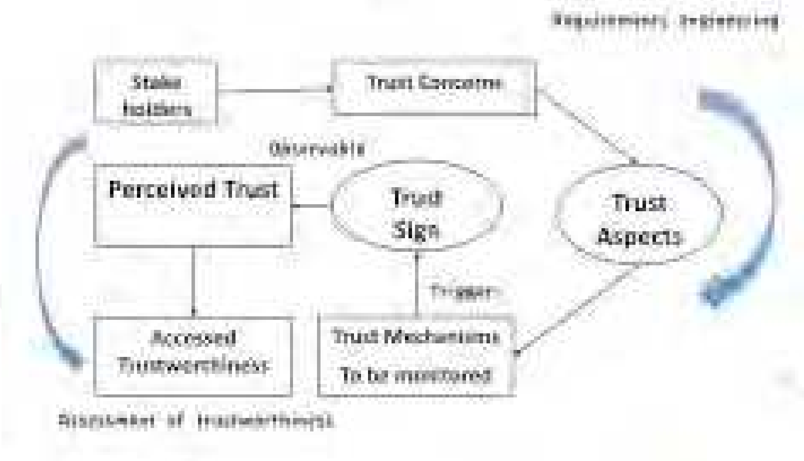


Fig. 10. Main components of Engineering trustworthiness.

shared meaning of related Key Performance Indicators (Figure 8!), Selected *Trust aspects* are translated into *Trust Mechanisms* to be implemented and monitored, The status of the trust mechanisms are implemented as *Trust signs* to be observed by related stakeholders. The trust signs are implemented using the *CIM modeling tools*. *Observing and interpreting* those signs can enable a shared awareness of the state of the system by the stakeholders. The design can then be *validated* against the chosen business case. The common understanding of the signs ensures that we have *interoperability and trustworthiness*. The following Figure 11 summarizes the achieved solution to *interoperability and shared semantics* illustrated by the red vertical line between two signs.

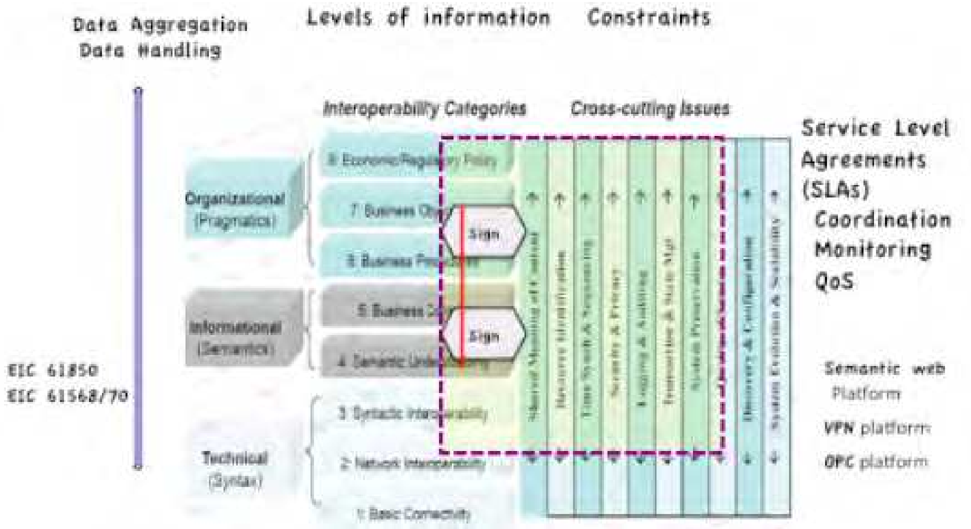


Fig. 11. The Interoperability Framework revisited. The vertical red line between signs illustrate verified interoperability.

In the process we have *identified a common semantics* for stakeholders in a *selected context*. Furthermore we can design and implement *empowerment tools* and *validation procedures* based on those findings (Figure 8).

To summarize: The output of the SLA negotiation process is a specification of a business process with *identified effect* (mission statement) delivered by identified stakeholders (roles, capabilities, concerns) and with indentified KPIs assuring trustworthiness and QoS to be monitored. The requirements also constitute a *meta-model* of the business process. This allows for identification and implementation of *self-healing mechanisms* maintaining a selected set of KPIs as invariants. Meta models also allows adjustments of SLAs, again maintaining some invariant properties, reflecting *controlled flexibility* of business cases.

6. Cyber security and privacy

Assuring Cyber security and privacy are arguably the most challenging and demanding tasks underpinning trustworthiness and thus acceptance and uptake of Smart grids. Both concepts are examples of cross-cutting issues of the GWAC Framework (Figure 10). Of particular importance are those issues in cases of Customer empowerment. Addressing aspects of cyber security and identifying countermeasures we can use the model supporting engineering of trustworthiness given i Figure 10.

The following Figure 12 sets the scene for Cyber attacks and other vulnerability related threats to Smart grids and its stakeholders.

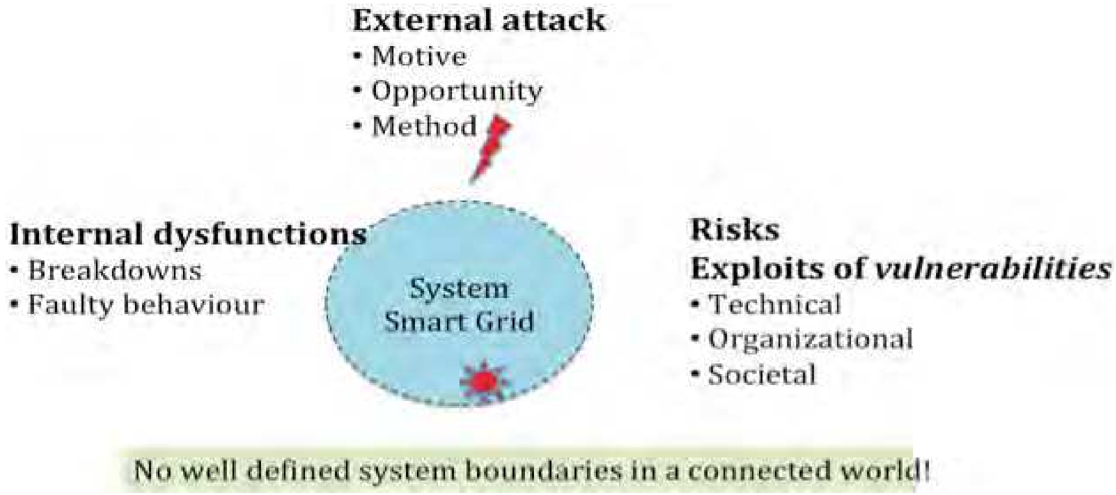


Fig. 12. Threats and exploitable weaknesses of Smart grids.

Threats could be realized given the Motive, Opportunity and Methods to exploit system vulnerabilities or by system dysfunctional behaviors. To cope with those threats we can do high-level attack three analysis or bottom up system hardening or a combination. In either case the core problem appears when a component, software, agent get improper access to data storage or exchange (Section 5). To remedy this several access control policies have been proposed.

To cope with these and related cyber threats The White House has issued a *National Strategy for Trusted Identities in Cyberspace (INSTIC)* in April 2011.The Strategy vision is:

Individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choices, and innovation.

The US Federal Government is initiating two short term actions to implement the Strategy. These are to:

- Develop an implementation Roadmap
- Establish a National Program Office (NPO)

The main purpose is to provide means and policies supporting trusted *Role based Access Control* with mechanisms supporting *revocation of identities and credentials*.

Issues related to security threats involve new kinds of recent attacks (since 2010). That is *Advanced Persistent Attacks* (APT), or advanced and targeted cyber attacks on infrastructures (*sabotage, business intelligence, thefts)*.

Examples include:

- *Stuxnet* – industrial sabotage of Siemens (Distributed Control Systems) DCS in Iran
- *Ghostnet* – theft of diplomatic information
- *Aurora* – theft of source code and IPR at Google
- *Night Dragon* – industrial and commercial intelligence of large oil companies
- *PS3/PSN attack* – business sabotage on Sony Play Station Networks

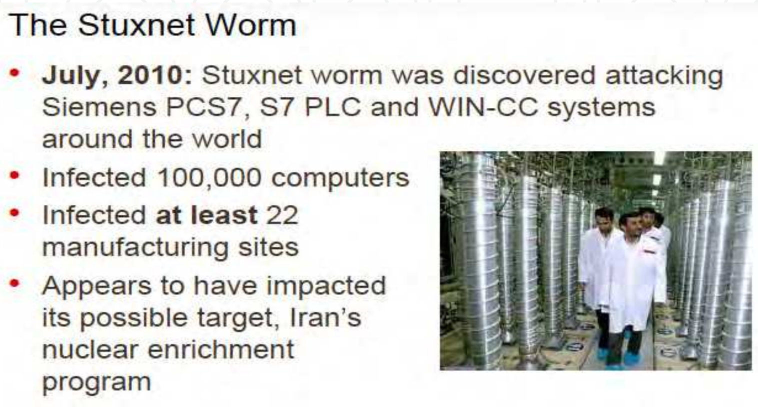
Also under attack:

- RSA
- Intellicorp

These kinds of targeted attacks, of course, also pose cyber threats via systems aiming at empowering the customer, such as AMI systems.

With thousands of workstations and servers under management, most enterprises have little to no way to effectively make sure they are free of malware and Advanced Persistent Threats (APTs). APTs are broadly defined as sophisticated, targeted attacks (as opposed to botnets, banking Trojans and other broad-based threats) that rely heavily on unknown (zero-day) vulnerabilities and delivery via social engineering.

The reminding part of the section will give a short summary and lessons learned from the Stuxnet attack followed by highlights from a report from McAffe (August 2011) on *Operation Shade RAT* (Remote Access Tools). We also give a short overview of challenges related to privacy and security. The Section ends with some recent technologies to successfully address APT and RAT threats.

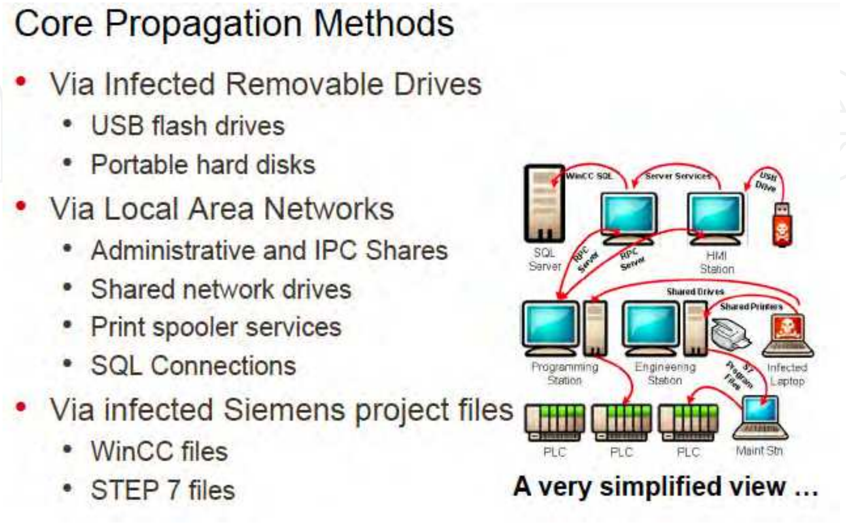


The Stuxnet Worm

- **July, 2010:** Stuxnet worm was discovered attacking Siemens PCS7, S7 PLC and WIN-CC systems around the world
- Infected 100,000 computers
- Infected **at least** 22 manufacturing sites
- Appears to have impacted its possible target, Iran's nuclear enrichment program

Fig. 13. The attacks by the Stuxnet worm.

The Stuxnet attack has been analyzed, for instance, by its detector Symantecs in the *W32. Stuxnet Dossier*[20]. The following Figure 14 gives the different propagation methods used by the worm. The starting point was an infected USB flash drive, followed by attacks on Local area Networks including SQL connections. The final steps of the attack were on Siemens WnCC and STWP 7 files.



Core Propagation Methods

- Via Infected Removable Drives
  - USB flash drives
  - Portable hard disks
- Via Local Area Networks
  - Administrative and IPC Shares
  - Shared network drives
  - Print spooler services
  - SQL Connections
- Via infected Siemens project files
  - WinCC files
  - STEP 7 files

A very simplified view ...

Fig. 14. Propagation methods of the Stuxnet worm.

Some lessons learned are:

- A modern Industry Control System (ICS) is highly complex and interconnected
- Multiple potential pwthways exists from the outside world to the process controllers
- Assuming an air-gap between ICS and corporate networks is unrealistic
- Focusing security efforts on a few obvious pathways (such as USB storage drives or the Enterprise/ICS firewall) is a flawed defense
- A perimeter defense is not enough (firewalls)
- We must harden the entire system
- We need Defense in Depth

Siemens gives an illustration of Defense in Depth in a recent (post Stuxnet) report, Figure 15. In the Figure are architectures for the functions Data Exchange, Real time data, Real time controlling, Maintenance, and Support given.

Threats to *privacy* are based on *misuse* of information related to individuals. This information can either be *generated* as footprints by individuals or *gathered* by tracing the behavior of the individual in cyber space using different kinds of *spyware*. Theft of identities or credentials is often a staring point in attacks on privacy.

A background to NSTIC Proposal is hat *identity theft* is costly, inconvenient and all-too common:

- In 2010, 8.1 million U.S. adults were the victims of identity theft or fraud, with total costs of $37 billion.

[20] Home page: http://www.symantec.com/connect/blogs/w32stuxnet-dossier

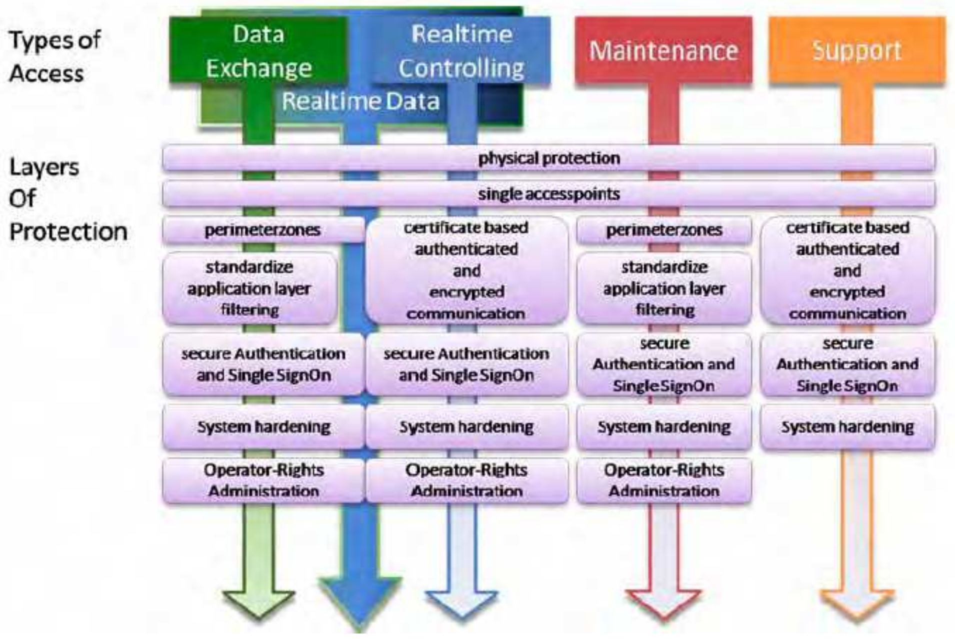

Types of Access
Data Exchange
Realtime Controlling
Realtime Data
Maintenance
Support
Layers Of Protection
physical protection
single accesspoints
perimeterzones
certificate based authenticated and encrypted communication
perimeterzones
certificate based authenticated and encrypted communication
standardize application layer filtering
standardize application layer filtering
secure Authentication and Single SignOn
secure Authentication and Single SignOn
secure Authentication and SingleSignOn
secure Authentication and Single SignOn
System hardening
System hardening
System hardening
System hardening
Operator-Rights Administration
Operator-Rights Administration
Operator-Rights Administration

Fig. 15. Defense in depth architectures for different functionalities of Smart grids.

- The average out-of-pocket loss of identity theft in 2008 was $631 per incident
- Consumers reported spending an average of 59 hours recovering from a "new account" instance of ID theft.

Threats on information (information security) is usually described by the CIA model as attacks on *protection* of:

- Confidentiality
- Integrity
- Availability

Privacy is then an aspect of confidentiality. Information integrity assures that information is not tampered. Availability assures access by stakeholders to information. Obviously the CIA highlights three potentially conflicting concerns. The inherent conflict between information sharing and information protection is also illustrated in Figure 8, In short, there is *no generic "best" solution to proper information sharing and information security*, We can only aim at trustworthy system interoperability (Figure 11).

Due to this *inherent conflicting complexity* there are a wealth of R&D efforts on these subjects. A good source is the IEEE journal *Security & Privacy*. From our perspective, trustworthiness of SLAs based on context of business cases (use cases), is a *promising strategy* to gain more context dependant views on cyber security and privacy (Figure 11).

Empowered stakeholders, for example customers, have access to tools that could *potentially* be used for remote access (*Remote Access Tools – RAT*). Stuxnet was exploiting vulnerabilities to configure a *remote access and attack* tool. The following facts are condensed from the recent McAffee[21] White paper (August 2011) *Revealed: Operation Shady RAT* based on collecting and analyzing logs from a Command & Control (CC) server *used by intruders* since

[21] Home page: http://www.mcaffe.com/

2006. Figure 16 gives an overview of attacked organizations, companies and agencies by RAT. The attacks had duration of months to years and were not detected.

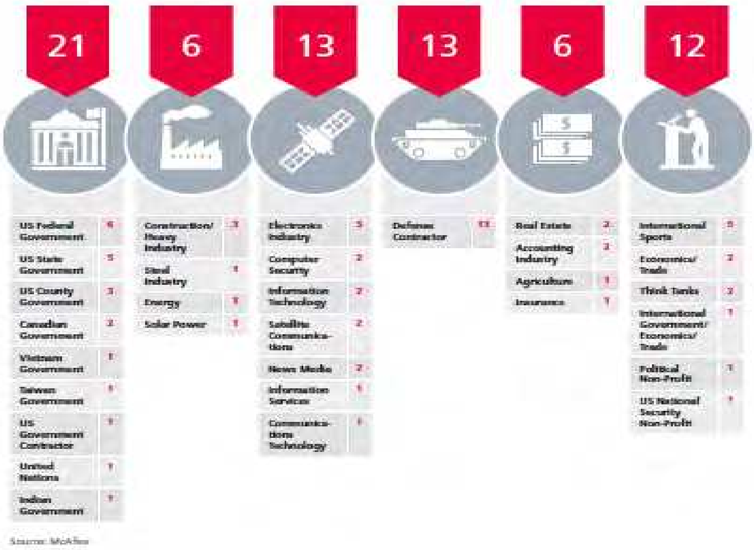


Fig. 16. Log based RAT attacks on selected organizations, companies or agencies.

- Vast amounts of data (petabytes) has been *lost* to (unknown) users
- The loss represent a *massive economic threat* to individual companies and industries and even countries that face the prospect of decreased economic growth in a suddenly more competitive landscape and the loss of jobs in industries that lose out to unscrupulous competitors in other part of the world

The McAffe report illustrates a large amount of undetected cyber attacks. Methods to identify attacks rely on *detection of known attack signatures* by firewalls or other techniques. However, the numbers of identified signatures are growing almost exponentially as is illustrated by the following Figure 17.

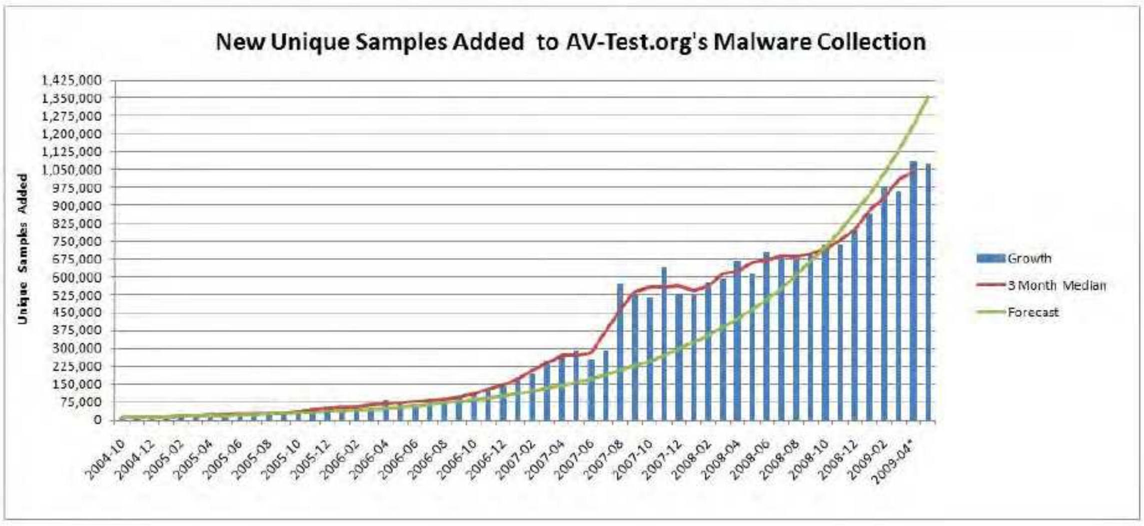


Fig. 17. A graph showing the number of unique new identified malware signatures over time.

The two last figures illustrate the potentially rapid increasing cyber number of attacks in general and more precisely the attacks on Smart grid infrastructures manifested by APT attacks based on RAT. Figure 17 illustrates also the increasing difficulties in pursuing threat analysis and/or attack detections by firewalls.

New technologies supporting increasing resilience of Smart grids include methodologies supporting *analysis and design of in-depth-defense* such as *Attack/Consequence Funnel* and *Last Line of Defense*.

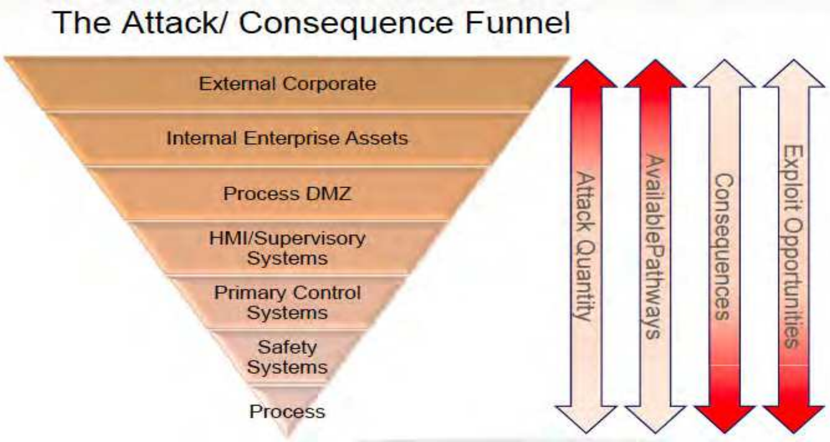


Fig. 18. The Attack/Consequence Funnel where the reddish arrow ends indicate increasing numbers.

The following Figure 19 illustrates means and reasons for securing the Last –Line-of-Defense of critical systems such as Smart Grids.

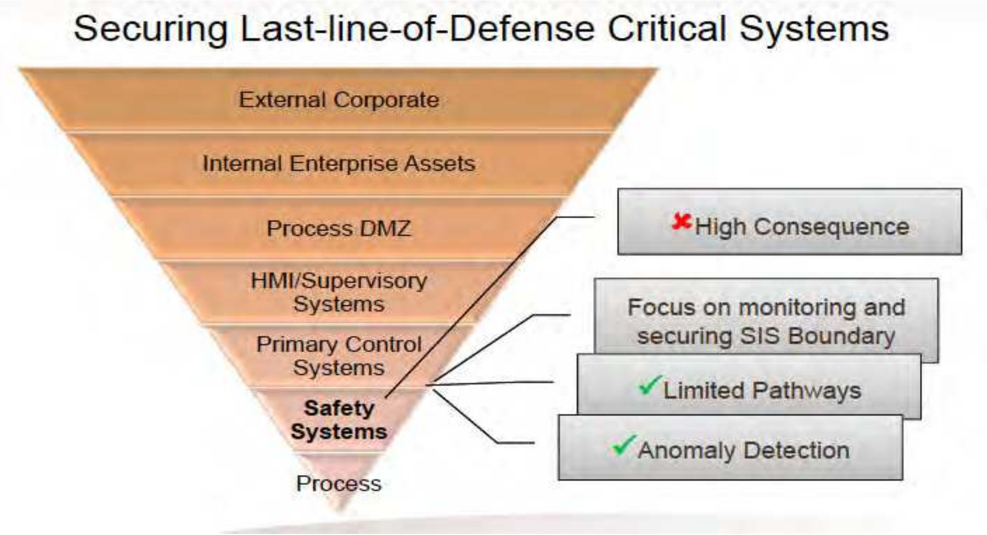


Fig. 19. Position and mechanisms enabling Last-line-of-Defense.

Figure 18 and Figure 19 gives a layered view of defense of critical systems. To implement those layers we could use the architecture given in the *standard ANSI/ISA-99* (now IEC 6222443.02.01 security standard of *"Zones and Conduits"*. The standard offers:

- A *level of segmentation* and *traffic control* inside the control system

- Control networks divided into *layers or zones based on control function*
- *Multiple separated zones* support *implementation* of a *defense in depth strategy*

Figure 20 illustrates the *overlay architecture of zones connected by conduits*. The information flows of the conduits are protected by carefully designed and implemented *firewalls*.

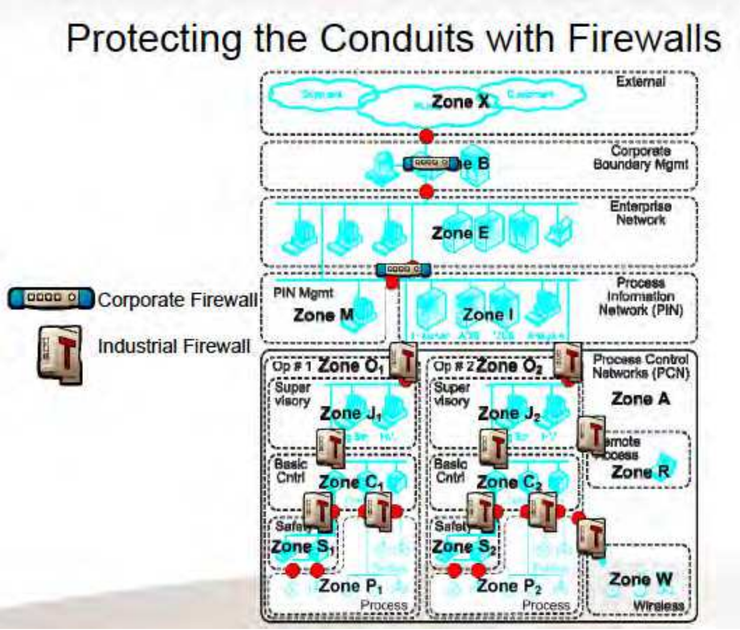


Fig. 20. The overlay security architecture of zones, conduits and firewalls.

Traditional firewalls are controlling the information flows at *system boundaries*. IT-based firewalls could handle IP-based traffic but not OPC based traffic that is the standard control system protocol, e.g., SCADA. Moreover, the more severe attacks are aiming at the *runtime environment* after the IT-based firewall. To remedy those shortcomings there are now products coming that could inspect OPC traffic. For instance *Hirschmann OPC Enforcer*[22] allows deep packet inspection of OPC. Stuxnet made extensive use of RPC (Remote Procedure Call) protocol, which is the basis for OPC. Also we have the *ECAT*[23] tool supporting *on-line monitoring of system memories* to address *APT threats*.

On-line monitoring as a basis for *system hardening* have been investigated in two thesis works [e, g] and several papers [8, 9, 10, 15, 25].

Finally, here are the following important recent reports addressing cyber security and Smart Grids by NIST Smart Grid[24]

- *Regulatory Recommendations* for Data Safety, Data Handling and Data Protection, issued by Expert Group 2 on February 16, 2011 [31].
- *Introduction to NISTIR 2628 Guidelines for Smart Grid Cyber Security* issued by Cyber Security Working Group in September 2010.

[22] Home page: http://www.hirschmann.com/en/Hirschmann_Produkte/Industrial_Ethernet/security-firewall/EAGLE20_Tofino_OPC/index.phtml

[23] Home page: http://www.siliciumsecurity.com/

[24] Home page: http://www.nist.gov/smartgrid/

Implementing defense-in-depth solutions, using architectures and standards mentioned above to monitor and protect data flows could be a way forward towards increased resilience of Smart grids. However, we need to investigate selected use cases and to develop suitable tool to pursue those efforts. This is the topic of next Sections.

7. Use cases

Use cases plays an important role in setting up and evaluate Smart grid scenarios. We have focused on use cases involving customers as stakeholders. Firstly, because *empowerment* of customers has been singled out as an important *enabler aiming at increased Energy Efficiency* (Section 1). Secondly, customers must be supported to *trustworthy collaborate* with other stakeholders of Smart grids (Figure 7), Thirdly, empowered *customers will require trusted cyber security and privacy* to accept Smart grid services.

We have advocated that setting up and monitoring Service Level Agreements (SLAs) provide a *structured methodology* to ensure Interoperability between stakeholders cooperating in delivering the services needed to fulfil the objectives and concerns related to the use cases at hand (Section 5). Typically, a *business case consists of related use cases*.

We have developed demonstrators of two customer empowerment related use cases in the areas of:

1. Smart homes
2. Green energy

The use cases are described in more detail in [12, 13, 26, 27, i]. The first use case aims at empowerment of customers to *change their profiles* to include more Renewable Energy Sources (RES), However, inclusion of RES will affect the energy balance of the (sub)grid to which the customer is connected. To have a minimal model of this sub grid we take into account the following three main stakeholders (Figure 3):

- A Distribution Grid Operator (DSO
- A Mediator/Facilitator (MF)
- Customers (C)

The Stakeholders participate in several SLAs coordinating the Business case based on changing the DER part of the power delivery to customer that is *empowered to change this amount*. In order to have a *separation of concerns* between the *business view* (buying power from RES) and the *grid view* (keeping energy balance of Voltage and Frequency) we model two types of SLAs (Figure 5):

- SLA_{MF-DSO}: Specifically addressing the coordination between MF and DSO maintaining the electricity balance within pre-set values.
- SLA_{MF-C}: Specifically addressing the requirements from C to change the amounts of RES to be delivered.

The two SLAs corporate in the following cycle:

1. Customer asks to change the DER amount with ΔDR during an interval Δ t.
2. The MF checks firstly if this allowable according to the SLA_{MF-C}, *if NO*, the request is *denied*.

3. If YES, the change is allowed if the energy balance could be maintained, The SLA_{MF-C} sends a request to the SLA_{MF-DSO} with that question. If NO, the request is denied.
4. If YES, the request from Customer C is *granted*.

It should be noted that the reasons behind the denials or granting could be given according to the setting up of the SLAs. The message exchanges, driven by SLAs, are recorded in databases for billing, accountability and traceability.

Our next demonstrator focus on issues related to *building and maintaining trust* between stakeholders. The use case is curtailment of service offerings.

This use case has the following stakeholders; *RES* (Renewable Resources), *DSO* and *C*. The market is defined as follows:

1. The DSO provides, monitor and bills energy to C (the present situation).
2. RES can and will occasionally generate and distribute energy ΔDR to the DSO.

The use case is defined as follows:

1. C *asks* for ΔDR during an interval Δ t.
2. DSO *asks* RES if ΔDR can be delivered during Δ t.
3. RES *confirms* this and DSO *inform* C that the *request is granted*.

Normally, the agreement between RES, DSO, and C is settled with a SLA. However, we can *encounter a breakdown* leading to that DSO *curtails* the delivery of ΔDR! The reasons could be either of or a combination of the following three events:

- DSO *identifies* that inclusion of ΔDR will *unbalance the grid* (voltage). Since DSO is responsible for the proper functioning of the grid we have *curtailment*.
- C *discovers* that he *cannot receive* ΔDR . DSO is informed and we have curtailment.
- RES discovers that ΔDR *cannot be produced* during Δ t.

Obviously the curtailment could eventually generate *losses of revenue*, and/or *in trust* and/or *willingness to invest* in supporting infrastructures. The overall consequence can be *resistance to implement parts of Smart grids* unless *proper regulatory frameworks and trustworthy SLAs are in place*. In short, *Risk assessments and mitigation* of technical and economic nature have to be in place to enable acceptance of Smart grid solutions.

Our simple use cases illustrates that design, implementation, maintenance, and acceptance of Smart grids have to be *carefully engineered* along the lines outlined in this chapter. This in turn *requires suitable tools*. That is the topic of next section.

8. Tools and environments

We have implemented and assessed two types of tools related to design and development of Smart grid pilots and Field tests, that is tools supporting *SLA procurement* and tools supporting *configuration and implementation of experimental environments* [8, 9, 10, 11, 12, 13, 15, 22, 24, 25, 27, e, g, i].

The following Figure 21 gives a architecture of SLA design environment.

The SLA agreement is based on a *selected use case* (goal, stakeholders, goal architecture, tasks, non-functional requirements, KPIs, exception procedures, *etc*.). Functional and non-

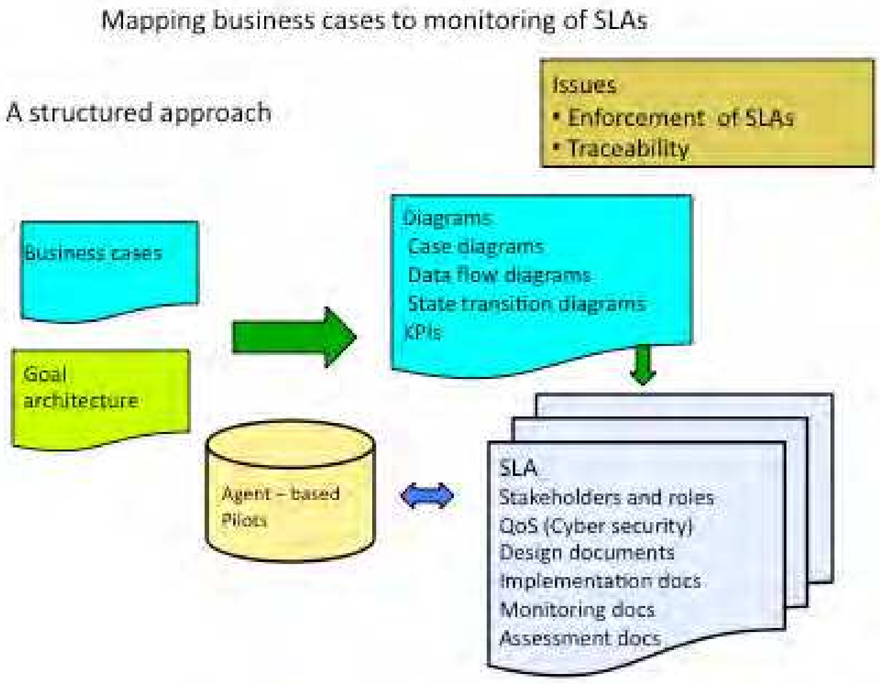


Fig. 21. Structured approach of setting up SLAs.

functional concerns are selected from *Interoperability Framework*, processed using our Framework supporting *Engineering trustworthiness* (Figure 10) and resulting in a *SLA footprint on the Interoperability Framework* (Figure 11).

During the SLA negotiation process, the stakeholders have *agreed on the terminology and meaning (semantics)*, the *KPIs and the conditions of the SLA*. Furthermore, issues related to *monitoring and data management* (including cyber security and privacy) have also been resolved. The SLA agreement is also a basis for assessing interoperability and simulations/pilots.

The *role of SLA agreements* is to map *use cases* into a *control and management structure* that *monitor the activities* (KPIs) *related to the use case*. Those activities are stored to enable billing, traceability and accountability. Furthermore, in cases of breakdowns, activities are recorded and eventually self-healing actions are activated according to the SLA. Furthermore a high-level *meta information* of the SLA agreement is kept to allow *reuse and adaptation* of use cases [6, 21, 23, a].

From Figure 3, Figure 4, Figure 5, Figure 6, and Figure 11 it follows that the *data flows* corresponding to the SLAs, firstly are *distributed and secondly have potentially large volumes*. Since the sets of SLAs are *overlays* of the infrastructure *into cells* of stakeholders and infrastructure components, we can form a *SLA-based data overlay* to address the challenges of data management in Smart grids [Figure 20, i].

Our *configurable experimental environments* have been evaluated in pilots aiming at:

- Hardening the execution environments (Software security)

- Designing experimental Smart grid environments by configuration of selected standard platforms.
- Evaluating tools supporting remote configuration and monitoring of pilots (France – Sweden)
- Evaluating tools supporting monitoring of data flows.

9. Conclusions and future work

Addressing the challenges of Future Smart grids poses several known and unknown challenges. In the Chapter we give a overview on identified challenges and promising routes toward solutions. We focus on the concept of Empowered customer of three reasons:

- *Active customers* have been identified as a key stakeholder to meet the expectations of the *EU 20-20-20 Energy Package*.
- *Other stakeholders in new business processes* of the Smart grid *must support active customers.*
- Active customers *will only accept and take up trustworthy services*.

In the Chapter we make a selection of key issues to address towards those ends. Firstly we emphasise the importance of *ensuring interoperability* of Smart grids. To that end, we advocate the use of the *Interoperability Frameworks* by NIST and GWAC, specifically addressing *interoperability between the Technical* (Syntax), *Informational* (Semantics), and *Organizational* (Pragmatics) Categories (Levels).

Interoperability assures that stakeholders can *coordinate their activities towards a common goal*. Our starting point of customer empowerment is that the customer is *empowered to change his/her energy-based services to meet individual goals*. To address this we propose *Service Level Agreements* (SLAs) as a mean to *coordinate different sets of stakeholders towards common goals that can be trusted, monitored, maintained, and billed*.

Information management (collect, store, access, process, distribute) is a key enabler of interoperability. Since the meaning of a given data item might be different to different stakeholders (system components) at different times we address these challenges briefly in the Chapter. Related to information processing is information sharing and information protection (e.g., privacy). Those important aspects of Cyber security and Privacy are outlined in the Chapter. We also illustrate some threats towards those non-functional concerns with some novel methods and techniques to implement a more resilient future Smart grid.

We also illustrate some use and shortcomings of present technologies in two use cases.

The work reported is promising but still in its infancy. We will continue our investigations and explorations is some on going and planned projects with involvement of KTH. Examples include:

- KIC InnoEnergy[25]
- Stockholm Royal Seaport[26]
- EU Grid4EU (new)[27]

[25] Home page: http://www.kic-innoenergy.com/

[26] Home page: http://www.stockholmroyalseaport.com/

10. Acknowledgements

The author acknowledge the importance of fruitful discussions and work in national and international collaborative projects and within the research groups at BTH and KTH as reported in the references.

11. References

[1] Energy Efficiency in SmartGrids, (2011) Download from http://seesgen-ict.rse-web.it.

[2] Akkermans, J.M., Ygge, F., Gustavsson, R.: Homebots: Intelligent decentralized services for energy management. In Proceedings of The Fourth International Symposium on the Management of Industrial and Corporate Knowledge, ISMICK '96, Rotterdam, The Netherlands, 21-22 October 1996. (1996).

[3] Gustavsson, R.: Agents with power. Communications of the ACM. March 99/Vol. 42, No. 3, pp. 41–47 (1999).

[4] Gustavsson, R.: Ensuring dependability in service oriented computing. Proceedings of The 2006 International Conference on Security & Management (SAM06) at The 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing, Las Vegas (2006).

[5] Gustavsson, R.: Proper use of Agent Technologies in Design and Implementation of Software Intensive Systems. The Second International Workshop on Integration of Software Engineering and Agent Technology (ISEAT 2006) at The Sixth International Conference on Quality Software (QSIC 2006) (2006)

[6] Gustavsson, R., Fredriksson, M.: Process algebras as support for sustainable systems of services. Applicable Algebra in Engineering, Communication and Computing. 16, 179–203 (2005).

[7] Gustavsson, R., Fredriksson, M., Meilstrand, P.: The proper role of agent technologies in design and implementation of dependable network enabled systems. Weyns, D. and Holovet, T. (eds.) Multiagent Systems and Software Architecture, Proceedings of the Special Track at Net.ObjectDays, Erfurt, Germany, September 19, 2006, pp. 49-58. (2006)

[8] Mellstrand, P., Gustavsson, R.: An Experiment Driven Approach Towards Dependable and Sustainable Future Energy Systems. Proceedings of the 3rd International Conference on Critical Infrastructures (2006).

[9] Mellstrand, P., Gustavsson, R.: Experiment based validation of Critical Information Infrastructure Protection (CIIP). Critical Information Infrastructures Security, First Inter-national Workshop, CRITIS 2006, Samos, Greece, August 31 - September 1, 2006. Revised Papers in Lecture Notes in Computer Science, Springer Verlag, Volume 4347/ 2006, 15-29, DOI: 10.1007/11962977_2 (2006).

[10] Ståhl, B., Le Thanh, L., Caire, R., Gustavsson, R.: Experimenting with Infrastructures. Proceedings of 5th International Conference on Critical Infrastructure (CRIS 2010). Beijing, pp. 1 – 7, (2010).

[11] Pepink, G., Kok, K., Dimeas, E., Hatzpargyrious, N., Hadjsaid, N., Caire, R., Gustavsson, R., Salass, R., Niesing, J., Hamilton, L., others: ICT-platform based

[27] Home page: http://www.enel.com/en-GB/innovation/smart_grids/european_initiatives/grid4eu/

Distributed Control in electricity grids with a large share of Distributed Energy Resources and Renewable Energy Sources. Proceedings of the First International ICST Conference on E-Energy–E-Energy 2010. Athens, October 14–15, 2010. (2010).

[12] Hussain, S., Gustavsson, R.: Coordinating Energy Business Models and Customer Empowerment in Future Smart Grids. ICST Conference on E-Energy. E-Energy, 2010. Proceedings of the First International ICST Conference on E-Energy–E-Energy 2010. Athens, October 14–15, 2010. (2010).

[13] Gustavsson, R., Stahl, B.: The empowered user - The critical interface to critical infrastructures. Proceedings of 5th International Conference on Critical Infrastructure (CRIS 2010). Beijing, pp. 1 – 7, (2010).

[14] Kok, K., Karnouskos, S., Nestle, D., Dimeas, A., Weidlich, A., Warmer, C., Strauss, P., Buchholz, B., Drenkard, S., Hatziargyriou, N., others: Smart houses for a smart grid. Electricity Distribution-Part 1, 2009. CIRED 2009. 20th International Conference and Exhibition on. pp. 1–4 (2009).

[15] Gustavsson, R., Ståhl, B.: Self-healing and resilient critical infrastructures. Proceedings of 3rd International Workshop on Critical Information Infrastructures Security Rome, (2008).

[16] Törnqvist, B. and Gustavsson, R.: On Adaptive Aspect-Oriented Coordination for Critical Infrastructures. In Proceedings of the First International Workshop on Coordination and Adaptation Techniques for Software Entities, Oslo, 2004, (2004)

[17] Van Craenenbroeck, T., De Wispelaere Vreg, B.: Service level agreements and regulatory aspects of data communication between DGO's and suppliers. Electricity Distribution, 2005. CIRED 2005. 18th International Conference and Exhibition on. p. 1–4 (2005).

[18] Vrba, P.: Java-based agent platform evaluation. Holonic and Multi-Agent Systems for Manufacturing. 1086–1087 (2004).

[19] Barwise, J., Perry, J.: Situations and attitudes. CSLI Publications MIT Press 1983 (reprint 1999).

[20] Devlin, K.: Infosense: Turning Information Into Knowledge. W.H. Freeman (2001).

[21] Malik, K., Choudhary, P.: Business Organizations and Collaborative Web: Practices, Strategies and Patterns. Igi Global (2011).

[22] Lundberg, J., Gustavsson, R.: Challenges and opportunities of sensor based User empowerment. Engineering principles for open socio-technical systems. Proceedings of 8th IEEE International Conference on Networking, Sensing and Control, April 11-13, 2011, Delft, the Netherlands (ICNSC2011). (2011).

[23] Fakhfakh, K., Chaari, T., *et.al.*: A Comprehensive Ontology-Based Approach for SLA Obligations Monitoring. The Second International Conference on Advanced Engineering Computing and Applications in Sciences. p. 217–222 (2008).

[24] Gustavsson, R. and Mellstrand, P. : Dependable Virtual Power Plants. In *Proceedings of CRIS Workshop 2006 - Influence of Distributed and Renewable Generation of the Power System Security (DiGeSEC´06),* Magdeburg, Germany (2006).

[25] Gustavsson, R. and Ståhl, B.; Self-Healing and Resilient Critical Infrastructures, In *Proceedings of 3rd International Workshop on Critical Information Infrastructures Security, October 13-15, Rome.* Selected to be published in a special issue on *CRITIS´08 by Springer Verlag (2008).*

[26] Hussain, S., Honeth, N., Gustavsson, R., Sandels, C., and Saleem, A.: Trustworthy Injection/Curtailment of DER in Distribution Networks Maintaining Quality of Service. In *Proceedings of 16th International Conference on Intelligent System Applications to Power Systems ISAP 2011* (2011).

[27] Gustavsson, R., Hussain, S., and Nordström, L.; Engineering of Trustworthy Smart Grids Implementing Service Level Agreements. In *Proceedings of 16th International Conference on Intelligent System Applications to Power Systems ISAP 2011* (2011).

[28] *The Future of Cloud Computing. Opportunities for European Cloud Computing Beyond 2010.* EC Expert Group Report, Public Version 1.0 (Eds . Jefferry, K. (ERCIM) and Neidecker-Lutz, B. (SAP)).

[29] *Introduction to NISTIR 7628 - Guidelines for Smart Grid Cyber Security.* The Smart Grid Interoperability Panel, Cyber Security Working Group. September 2010, NIST.

[30] *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, Release 1.0, NIST Special Publication 1108.

[31] *Regulatory Recommendations for Data Safety, Data Handling and Data Protection*. Task Force Smart Grids. Expert Group 2. Report June 22, 2010.

[32] Ådahl. K. and Gustavsson, R.: Decision Support by Visual Incidence Anamneses for increased Patient Safety. In *Efficient Decision Support Systems: Practice and Challenges – From Current to Future*. InTech – Open Access Publisher (2011). ISBN: 978-953-308-63-9.

Thesis works

a. Fredriksson, M.: *On the nature of open computational systems – Online Engineering*. PhD Thesis, Dissertation Series No. 2004:5, Blekinge Institute of Technology. ISBN 91-7295-045-5.

b. Rindebäck, C.: *Designing and Maintaining Trustworthy Online Services*. PhL Thesis, Licentiate Dissertation Series No. 2007:8, Blekinge Institute of Technology, ISBN 978-91-7295-129-4.

c. Brandt, P.: *Information in Use – Aspects of Information Quality in Workflows.* PhD Thesis, Dissertation Series No. 2007:04, Blekinge Institute of Technology. ISBN 978-91-7295-111-2.

d. Östlund. L.: *Information in Use – In- and Outsourcing Aspects of Dogital Services.* PhD Thesis, Dissertation Series No. 2007:05, Blekinge Institute of Technology. ISBN 978-91-7295-110-2.

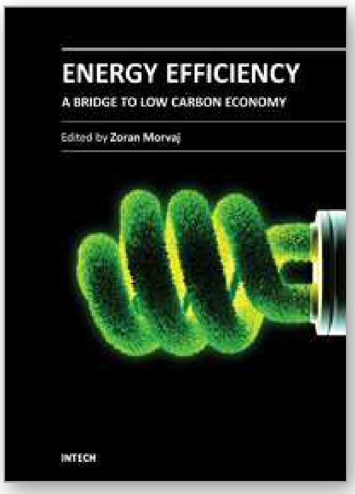
e. Mellstrand, P.: *Informed System Protection*. PhD Thesis, Dissertation Series No. 2007:10, Blekinge Institute of Technology. ISBN 978-91-7295-106-8.

f. Lundberg, J.: *Engineering Principles for Open Socio-Technical Systems*. PhD Thesis, Dissertation Series No. 2011:01, Blekinge Institute of Technology. ISBN 978-91-7295-103-9.

g. Ståhl, B.: *Exploring Software Resilience*. PhL Thesis, Licentiate Dissertation Series No. 2011:05, Blekinge Institute of Technology, ISBN 978-91-7295-206-5.

h. Ådahl K.: *On Decision Support in Participatory Medicine supporting Health Care Empowerment.* PhD Thesis, Dissertation Series No. 2011:01, Blekinge Institute of Technology. ISBN 978-91-7295-221-8

i. Hussain, S: *Coordination and Monitoring Servises Based on Service Level Agreements in Smart Grid*s. PhL Thesis, Licentiate Dissertation Series No. 2012:01, Blekinge Institute of Technology, ISBN 978-91-7295-224-9.



Energy Efficiency - A Bridge to Low Carbon Economy
Edited by Dr. Zoran Morvaj

ISBN 978-953-51-0340-0
Hard cover, 344 pages
Publisher InTech
Published online 16, March, 2012
Published in print edition March, 2012

Energy efficiency is finally a common sense term. Nowadays almost everyone knows that using energy more efficiently saves money, reduces the emissions of greenhouse gasses and lowers dependence on imported fossil fuels. We are living in a fossil age at the peak of its strength. Competition for securing resources for fuelling economic development is increasing, price of fuels will increase while availability of would gradually decline. Small nations will be first to suffer if caught unprepared in the midst of the struggle for resources among the large players. Here it is where energy efficiency has a potential to lead toward the natural next step - transition away from imported fossil fuels! Someone said that the only thing more harmful then fossil fuel is fossilized thinking. It is our sincere hope that some of chapters in this book will influence you to take a fresh look at the transition to low carbon economy and the role that energy efficiency can play in that process.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821