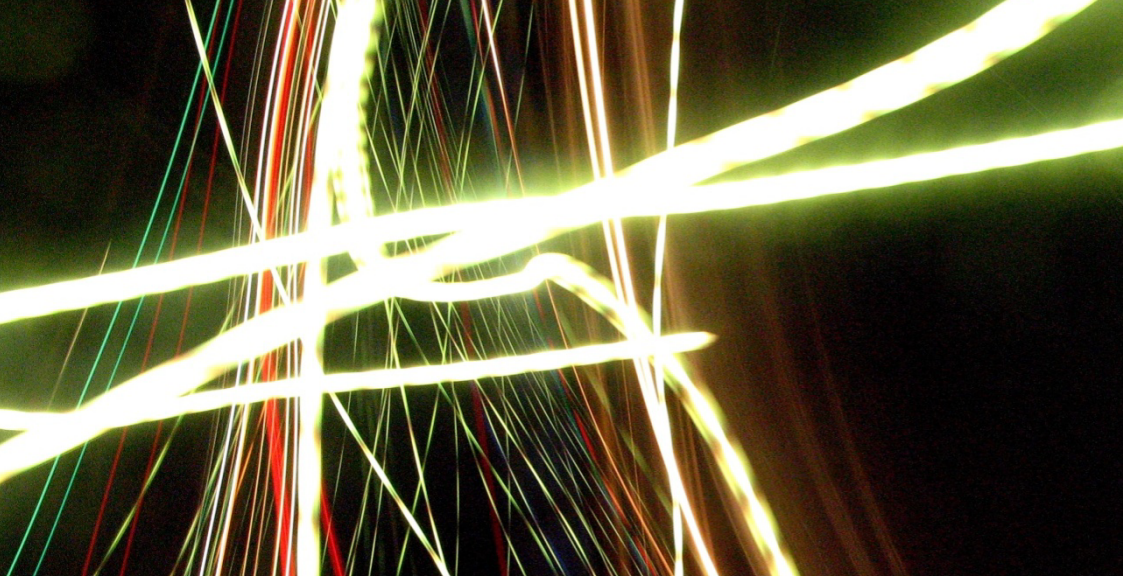


Tagungsband ComForEn 2014

5. Symposium Communications for Energy Systems

Workshops:	29. September 2014 Eschenbachgasse 9, 1010 Wien
Symposium:	30. September 2014 Eschenbachgasse 9, 1010 Wien
Industry Day:	01. Oktober 2014 Giefinggasse 2, 1210 Wien

OVE ÖGMA Mess- und Automatisierungstechnik

TU WIEN

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

OVE-Schriftenreihe Nr. 77
Österreichischer Verband für Elektrotechnik
Austrian Electrotechnical Association

ComForEn 2014
5. Symposium Communications for Energy Systems

29.-30. September 2013
Eschenbachgasse 9, 1010 Wien

Herausgeber:
Dipl.-Ing. Dr. techn. Friederich Kupzog

AIT Austrian Institute of Technology GmbH
Giefinggasse 2
1210 Wien

http://www.ait.ac.at

ISBN: 978-3-85133-083-0 Österreichischer Verband für Elektrotechnik

Inhalt

Geleitwort

Im Rahmen der ComForEn 2014 laden wir Sie als ExpertInnen aus Forschung und Industrie ein, die weiteren Herausforderungen auf dem Weg zu einem nachhaltigen Energiesystem zu diskutieren. Kommunikationstechnik und IT spielen bereits heute im täglichen Betrieb eine Schlüsselrolle in der elektrischen Energieversorgung. In zukünftigen Stromnetzen wird diese Rolle noch mehr an Relevanz gewinnen. Aktuelle Forschungsarbeiten beleuchten wesentliche Fragen rund um den Migrationspfad zu diesem Smart Grid. Architekturen, Protokolle, Regelungskonzepte, Security und Umsetzungsaspekte stehen dabei im Fokus.

Um den Charakter der ComForEn als wissenschaftliche Fachtagung zu Themen mit starkem Bezug zur Industrie und zu Infrastrukturbetreibern weiter zu schärfen, wurde das Format in diesen Jahr erweitert:

→ Neu ist die offene Einladung zur Einreichung wissenschaftlicher Beiträge mit Review durch das Scientific Board. Diese Einladung richtet sich vor allem an ForscherInnen, die ihre aktuellen Arbeiten vorstellen und mit der ComForEn Community diskutieren möchten.
→ Ebenfalls zum ersten Mal in dieser Form wird der ComForEn Industry Day (01. Oktober 2014) zum Thema „Smart and Secure Secondary Substation“ stattfinden. Auf der Fachmesse im AIT SmartEST Labor stellen fünf Aussteller ihre Hardware und Systemlösungen zum Thema Intelligente Ortsnetzstation vor.

Wir wünschen Ihnen eine informative Fachtagung und möglichst viele Anregungen für Ihre eigene Arbeit.

Dipl.-Ing. Dr.techn.
Friederich Kupzog

AIT Austrian Institute of Technology GmbH
Energy Department
Senior Scientist

Dipl.-Ing.
Thomas Leber

TU Wien
Institut für Computertechnik
Leitung Forschungsgruppe Energy&IT

Wir danken dem Organisationsteam

Birgit Sykora, Karl Stanka, OVE

Veronica Vana, AIT

Workshop-Programm

29. September 2014
Eschenbachgasse 9, 1010 Wien

Im Rahmen der ComForEn 2014 werden themenbezogene (Projekt-)Workshops abgehalten. Es bietet sich die einmalige Gelegenheit, mit den anwesenden Experten aktuelle Themen im Rahmen der Workshops zu diskutieren und die Tagung als Vernetzungskatalysator zu nutzen.

Weitere Details zu den einzelnen Workshops: http://energyit.ict.tuwien.ac.at/?p=501

Vormittag 9:30 – 13:00		
Projektworkshop EigenlastCluster Ziel des Workshops ist die Diskussion neuer Ansätze zur Steigerung des Eigenverbrauchs von Strom und Wärme in bereits datentechnisch erfassten Gebäuden der Gemeinde Großschönau. Gebäudecluster (Gemeindeobjekte, Gewerbe, Haushalte) werden gebildet und die Verbesserung der Eigennutzung mit und ohne Einsatz von zusätzlichen Batterie und/oder H_2-Speichern (Firma Fronius) bewertet. Organisation: Bettina Frantes, Sonnenplatz Großschönau Kompetenzzentrum	**Cybersecurity Risk Assessment in Smart Grids** (language: English) Future power grids come with a large cyber-attack surface, which makes cybersecurity risk assessment a major concern. The Austrian $(SG)^2$ and the EU FP7 project SPARKS will take a broader view and develop novel risk assessment methods for smart grids. The goals of this workshop are twofold: to understand the challenges of risk assessment for smart grids that are experienced by stakeholders, and to disseminate and gather feedback on the results from the $(SG)^2$ project. Organisation: Lucie Langer and Paul Smith, AIT Austrian Institute of Technology	**Projektworkshop ICT for Robust Grids** Für den stabilen Inselbetrieb und zur Gewährleistung des definierten und reibungslosen Übergangs zwischen netzgekuppeltem Betrieb und Inselbetrieb sind auch IKT-Strukturen notwendig, die diese Betriebsphasen ermöglichen und unterstützen. Dieser Workshop bearbeitet die Konzepte, die für die Inselfähigkeit von Microgrids auf Seiten der IKT und der Energietechnik erforderlich sind. Organisation: Wolfgang Gawlik, ESEA – Technische Universität Wien
Nachmittag 14:00 – 17:30		
Workshop Neighborhood Energy Management Dieser Workshop bearbeitet die Themen, die aus den Synergien einer offenen Nachbarschaft von aktiven Gebäuden entstehen können: Verteilte Nutzung erneuerbarer Energie, Demand Side Management, Gebäude als Energiedienstleister. Forschungsprojekte erzählen Erfolgsgeschichten und warnen vor Fallstricken in der Umsetzung von gebäudeübergreifendem Energiemanagement. Organisation: Gerhard Zucker, AIT	**Workshop RASSA-Prozess** Das Projekt RASSA-Prozess (Sept. 2014- Sept. 2015) bearbeitet die umfassende Konzeption eines Prozesses zur Entwicklung einer abgestimmten Smart-Grids-Referenzarchitektur für Österreich. Die Referenzarchitektur soll als „Blaupause“ für Smart-Grid-Lösungen dienen. Ziel des Workshops ist, zu identifizieren WER in einem Smart Grid WELCHE entscheidende Rollen WO spielt und WIE ein Kontakt aufrecht bleiben kann. Organisation: Marcus Meisel, ICT – TU Wien und Angela Berger, Technologieplattform Smart Grids Austria	**Intelligente Messysteme im Vergleich – Standardisierung, Spezifikation und Zertifizierung in Europa** In Österreich bereiten sich Verteilnetzbetreiber aktuell auf die Einführung intelligenter Messsysteme vor. Wir möchten die Gestaltungsspielräume der Branche deutlich machen und dabei helfen die Erfahrungswerte anderer Länder zu nutzen. Wir laden dazu ein, die Erfahrungen der europäischen Nachbarstaaten zu bewerten und darauf aufbauend Ideen für die Praxis in Österreich zu entwickeln. Organisation: Steffen Grüttner, DNV GL Energy

Industry Day

Smart and Secure Secondary Substations

01.10.2014, 10:00-17:00
AIT Austrian Institute of Technology GmbH
Giefinggasse 2, 1210 Wien, Austria

The ComForEn 2014 Industry Day brings together equipment providers and grid operators. The event aims to exchange experience and information on latest developments in the context of secondary substation technology. The Industry Day features both, deep conceptual insights from a moderated presentation panel and hands-on experience of innovative substation equipment at the smart secondary substation exhibition in the AIT SmartEST Laboratory.

While primary stations are closely integrated into distribution management systems, the vast majority of secondary stations are operated passively today. New operation paradigms for low voltage distribution networks caused by increasing connections of distributed generation, active demand, electric mobility and dedicated distributed energy storage will require on-line monitoring of more and low voltage substations. In order to manage the growing number of distributed generators, new functionalities have to be integrated at secondary substation level. Furthermore, IT security plays a vital role in the realisation of smart secondary substations due to the large number of connected devices in the field.

Talks (10:00 – 13:15)

10:00	Welcome
10:10	Friederich Kupzog, AIT Energy: Smart Secondary Substations: a modular approach
10:20	Steve Van den Berghe: International Experiences of Smart Secondary Substation Technology – Smart grid at the DSO Eandis (Belgium)
10:40	Manuel Sojer, Maschinenfabrik Reinhausen: Regelbare Ortsnetztransformatoren zur Verbesserung der Netzintegration von erneuerbaren Energien
11:00	Stefan Kämpfer, ABB Belgien: Applications for smart secondary substations based on selected pilot projects
11:20	Coffee Break
11:35	Tobias Gawron-Deutsch, Siemens AG Österreich: Die Intelligente Ortsnetzstation – Demonstrator
11:50	Hermann Bühler, Bühler GmbH: Smarte Kommunikation für Smarte Netze
12:10	Thomas Bleier, AIT Safety & Security: Security Challenges in smart distribution
12:30	Michael Mansholt, 3M: Why will physical security matter to PUs in the future?
12:50	Stefan Hoppert, a-eberle: LVRSys™ - das revolutionäre Niederspannungsregelsystem
13:15	Lunch

Exhibition (14:00 – 17:00)

Voltage control with MV/LV tap changer transformer
Maschinenfabrik Reinhausen

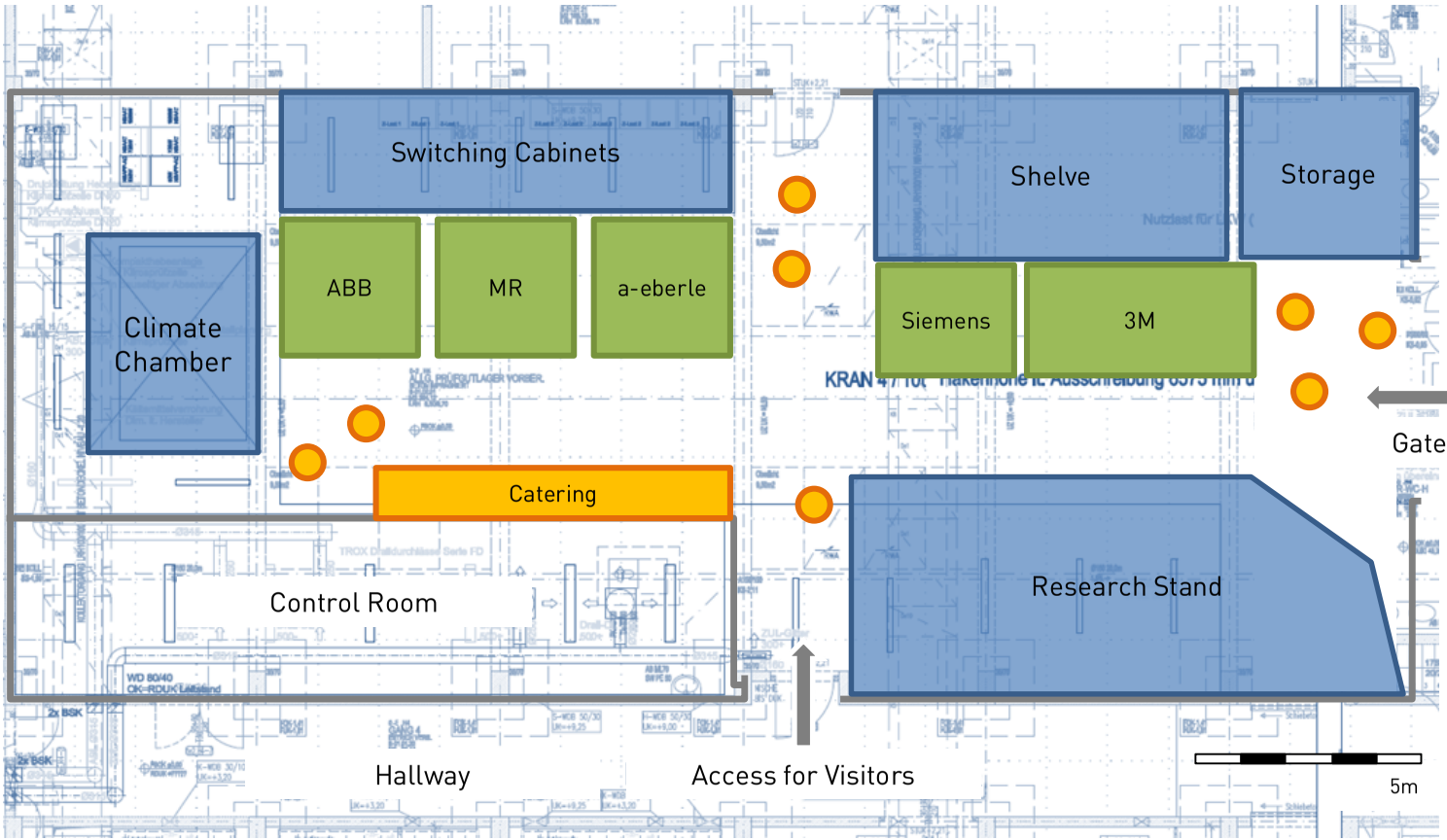
Feeder voltage control with LVRSys
a-eberle (inquired)

Demonstration Setup Intelligent Low Voltage Network
Siemens Cooperate Technology

Smart Secondary Substation Solutions
ABB

Smart Infrastructure Management System | Sensored Cable Accessories
3M Smart Grid - Connected, Efficient and Sustainable Energy

SmartEST – Smart Energy Systems and Technologies Laboratory
AIT Energy


Switching Cabinets
Shelve
Storage
Climate Chamber
ABB
MR
a-eberle
Siemens
3M
Gate
Catering
Control Room
Research Stand
Hallway
Access for Visitors
5m

Symposium Session 1

Wissenschaftliche Arbeiten

29. September 2014
Eschenbachgasse 9, 1010 Wien
9:40 – 12:00

Die für die ComForEn eingereichten wissenschaftlichen Arbeiten wurden durch das Scientific Board der Konferenz begutachtet. Vier von sechs Arbeiten wurden angenommen. Diese Arbeiten werden am Vormittag vorgestellt.

Scientific Board
Thomas Bleier, AIT
Mislav Findrik, FTW
Wolfgang Gawlik, TU Wien
Wolfgang Hribernik, AIT
Thomas Leber, TU Wien
Wolfgang Prüggler, TU Wien
Christine Rosinger, OFFIS
Andreas Schuster, ASCR
Hans-Peter Schwefel, FTW
Friederich Kupzog, AIT
Tanja Zseby, TU Wien

Communication Patterns for Demand Side Flexibility

Mike Pichler, Siemens AG Österreich, mike.pichler@siemens.com

Abstract – Controllable loads, storages and generators inside the building can be provided as flexibilities for the electrical energy system. These flexibilities can be used for higher-level optimization in markets or for technical grid operation. This paper introduces use cases for flexibilities from the building operator's point of view as well as some high-level communication patterns to implement them. Additionally, a comprehensive system architecture for a demand side flexibility system based on XMPP will be presented.

1. Introduction and Related Work

The EU Task Force Smart Grid (EG3) summarizes the need for demand side flexibility as followed: "Increased integration of distributed energy resources (DER) and the growing peak demand for electricity will drive the need for increased flexibility, customer engagement and empowerment in order to maintain an affordable energy system" [1]. Customer empowerment means to provide the technical equipment necessary for an active participation in flexibility markets to the customers. While most of the current research activities in the area of demand side flexibility focus on the use cases for energy suppliers, retailers, virtual power plant operators, balance responsible parties or grid operators, this paper focuses on the building operator's point of view.

"The *Extensible Messaging and Presence Protocol* (XMPP) is an application profile for the Extensible Markup Language (XML) that enables the near-real-time exchange of structured yet extensible data between two or more network entities" [2]. This makes XMPP perfectly suitable for information exchange in Smart Grids, which use Internet technologies for connecting the demand side into the overall system. The communication patterns introduced in this paper assume that the Internet Protocol (IP) and XMPP are used for communication between the demand side and external entities.

Various standardization groups and documents are related to demand side flexibility. The IEC 62939 TR "*Smart Grid User Interface*" [6] defines various use cases related to information exchange for demand response, lists standards and identifies gaps. The IEC/TS 62872 "*System interface between Industrial Facilities and the Smart Grid*" [7] focuses on the demand side flexibilities in industrial sides, mostly through direct load control. Finally, the IEC 62746 documents will de-

scribe the system interface between the customer energy manager and the power management system [8] – which is still work in progress. Data models and communication sequences are also introduced in the *OpenADR* protocol [9] and the *Facility Smart Grid Information Model* (FSGIM) [10].

2. Use Cases for Flexibility

From the building operator's point of view, flexibilities inside the building should be sold to the best price reachable. A so-called *Customer Energy Management System* (CEMS) should schedule the flexibilities based on different input signals like weather forecasts, dynamic price signals or flexibility orders from external entities. This section describes the different use cases for flexibilities. Each use case extends the previous one and possibly adds value for the provided flexibilities. The following use cases will be introduced:

- Self-consumption optimization: maximize self-consumption of produced energy while considering the overall energy efficiency
- Day-ahead pricing: using day-ahead price signals for cost optimization as extension to the previous use case self-consumption optimization
- Intra-day flexibilities: provide flexibility capabilities for market-based and/or physical demand response with lead times less than 24 hours
- Grid priority functions: provide emergency flexibilities, if technical limitations are violated

Energy efficiency (which means consuming as low energy as possible while considering the comfort needs of the customers) will be the basis for all these use cases. Optimizing energy efficiency while ensuring the comfort inside the building is the main functionality of today's building automation systems.

2.1 Self-consumption Optimization

More and more buildings are producing their own energy with local generators like wind turbines or photovoltaic plants. Most of these buildings use the produced energy by their own and feed power excesses into the public grid. Because the revenue for power feed-in is very low compared to consuming energy from the grid [3], optimizing self-consumption is a relevant business case for building operators. Nevertheless, energy efficiency sill must be considered. Because the generation from renewable energy resources strongly depends on climate influences like wind speed or solar radiation, predictive control algorithms can help to improve the efficiency of optimization algorithms significantly [12]. These algorithms need forecasts for the climate quantities from external service provides.

After receiving a climate forecast, the CEMS can calculate a generation forecast for the renewable energy resources. Additionally, a forecast of the electrical consumption of the building (called the base load) must be calculated. The difference between the base load and the energy generation shows the excesses for a certain time period. Storages and shiftable loads can be used to maximize the self-consumption by charging or supplying them with the excesses. By using flexibilities for

self-consumption optimization, these flexibilities get a certain price value depending on the savings from the optimization algorithm. This saving can be calculated by comparing the standard operation schedule with the schedule that comes from the self-consumption optimization.

2.2 Day-ahead Pricing

Day-ahead pricing allows the building operator to optimize energy consumption depending on a dynamic price signal. These signals are provided by the energy retailer at least 24 hours in advance. This allows the CEMS to use a full day-night cycle for optimization, which can be useful for thermal processes like heating or air condition. The use of flexibility in response to price signals for example has been described in [4].

The measurement for optimization based on day-ahead price signals is minimizing the energy procurement costs. This means, that e.g. controllable loads should be shifted into periods with low energy prices. The achievable incentives for this shift can be calculated by comparing the costs for the operation based on the original schedule with the costs based on the optimized schedule. The value of these incentives is important, if flexibilities should be sold during intra-day auctions as described in the next use case. As a response to day-ahead price signals, the CEMS can calculate an energy balance forecast for the grid connection point and send this forecast to interested parties like the grid management or an energy retailer.

2.3 Selling Intra-day Flexibilities

Intra-day flexibilities can be ordered with lead times less than 24 hours. The building provides these flexibilities by exposing a flexibility communication interface, which can be used by different external parties like *Flexibility Operators* or *Energy Pool Managers*. The entities involved in the communication patterns will be introduced in chapter 3.

A flexibility request looks similar like the following question: “How much flexibility can you provide today afternoon from 4 to 5pm?” The answer to this request is a relative power schedule, indicating the flexibility capabilities as well as “side effects” as introduced in [5]. The flexibility offer also contains a price value for this flexibility. The price depends on the generated revenue from the use cases self-consumption optimization and day-ahead pricing for the requested time period and flexibility. The building operator wants at least as much revenue from selling the flexibilities to external entities, as he would generate when using the flexibilities for self-consumption optimization and/or day-ahead pricing.

2.4 Grid Priority Functions

Grid priority functions take place in case of a “red grid state”, like defined in the German traffic light model. In this case, technical limitations are violated and the grid operation has the highest priority. Measurements from the building can be to reduce electrical production or consumption, or to produce reactive power instead of active power in case of voltage band violations. To ensure a proper reaction of all involved components in case of a communication blackout, P/U and Q/U characteristics are stored locally inside the building. Components like inverters or consumers (e.g. e-car charging stations) can operate autonomously based on these characteristics. Additional to the

mentioned characteristics, real-time commands like load-reduction signals can be sent to the CEMS in case of urgent problems.

3. Communication Patterns

In this section, communication patterns related to the use cases defined in chapter 2 as well as relevant projects will be presented. The first step is to define some entities involved in the communication patterns:

- CEMS – Customer Energy Management System; is situated inside a single household, building or campus; handles all communication issues with external entities. This entity also includes the Smart Grid Connection Point (SGCP) [6, 8].
- Tariff Server – provides day-ahead price signals for energy consumed from and/or feed into the public grid; usually is provided by the energy retailer.
- Energy Pool Manager – pools energy flexibility from a larger number of buildings to reach a "critical mass" for markets and to ensure the availability through statistical measures. This entity may also be called Virtual Power Plant (VPP) or Demand Response Automation Server (DRAS) [9].
- Flexibility Operator – supports the technical grid operation by generating grid state forecasts and uses flexibilities to avoid critical situations.
- SLVG-C – Smart Low Voltage Grid Controller; is responsible for a single secondary substation to control technical grid limitations like the voltage or maximum power consumption; sends grid priority signals to CEM-Systems in cases of violations of technical limits.

In the next chapter, an overall systems architecture based on XMPP will be introduced. XMPP allows delivering XML-based messages between clients using one or more centralized servers. Although the communication sequences in this chapter can be implemented using various communication protocols, it is assumed that the later introduced architecture will be used.

3.1 Self-consumption Optimization

As described in the related use case in chapter 2, self-consumption optimization is based on climate forecasts for quantities like outside temperature, humidity or solar radiation. This information is provided by external service providers via the Internet and can be accessed using standard web technologies like the File Transfer Protocol (FTP), HTTP requests or webservices. Unfortunately, the data format of the information is not standardized. Even the forecast range, the time interval between values and the provided quantities vary largely between different providers, making it difficult to implement a generic communication client at the demand side. In research projects like *Building2Grid* or *Smart LV Grid*[1], clients for several specific service providers have been implemented. This works well for research projects, but has some disadvantages when using the clients in products. For example, due to different data models it is not possible to change the service provider

[1] See http://www.smartgridssalzburg.at/ for details

without modifications in the product's software. A solution for this problem could be a standardized data model and interface for providing and consuming climate forecasts.

3.2 Day-ahead Pricing

Day-ahead pricing means, that the building receives a dynamic price signal every day, indicating the price for the particular next day. The resolution of this price signal (interval between two prices), which is provided by a tariff server operated by an energy retailer, usually lies between 15 minutes and one hour. When using XMPP for communication, the tariff server is able to push prices signals to all or several clients when new prices are available. If other communication protocols are used, polling the tariff server from the clients may be necessary.

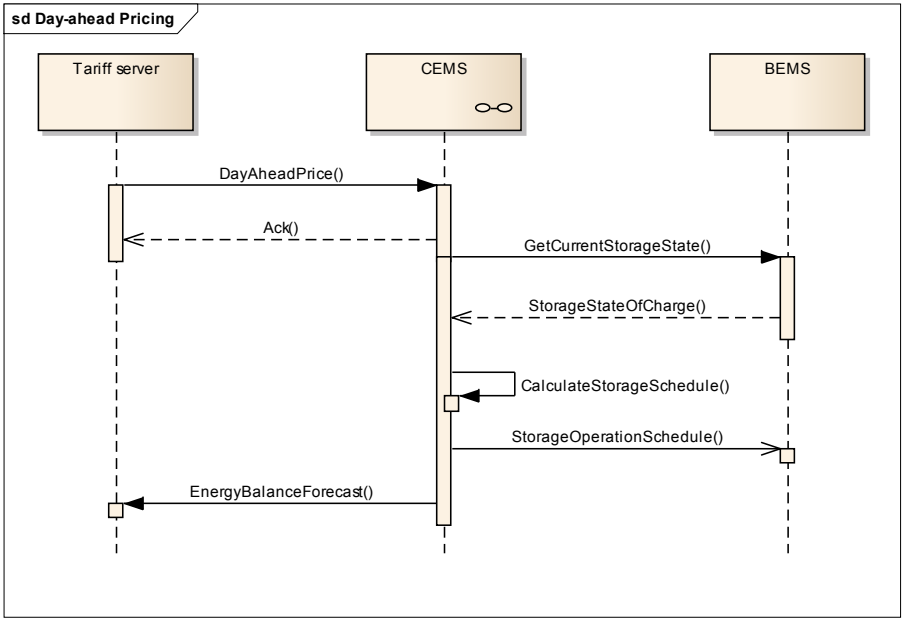


Figure 1. Sequence diagram for day-ahead pricing

Within a project called *HiT*[1] (German acronym for "Häuser als interaktive Teilnehmer"), a utility company has implemented a tariff server providing day-ahead price signals. The prices are generated from forecasts of the "EPEX SPOT" power spot market from the European Energy Exchange (EEX). Additionally, the utility added a virtual price for grid operation. After the CEM-system has received a new price signal, it runs an optimization algorithm that tries to minimize the energy costs for the provided period. This algorithm basically charges storages during low-price periods and uses the stored energy during high-price periods. Shiftable loads (e.g. heating domestic hot water in a boiler) are also scheduled for low-price periods. For each controllable load, storage and generator, the optimization algorithm generates an operation schedule for the next day. When comparing the

new operation schedules with the static standard schedules, the dynamic price signal usually causes changes in the energy balance at the grid connection point. Within the HiT project, these changes a reported to the tariff server by providing a relative energy balance forecast, compared to a "normal" operation forecast without the influence of a day-ahead price signal. This forecast is used by the energy retailer to optimize the portfolio management. The generated forecast can also be interesting for grid operation in order to predict shortages.
Figure 1 shows the communication pattern for day-ahead pricing, which has been introduced in the previous paragraphs. When a new price signal is available, the energy retailer broadcasts this signal to all known CEM-systems (which have a related contract with the energy retailer). The CEM-systems run their optimization algorithms and generate schedules for all controllable loads, storages and generators inside the building. These schedules are passed to the *Building Energy Management System* (BEMS). The BEMS is responsible for realizing the schedules, which means controlling all related parts and plants of the building's energy system. The CEMS can also be part of the BEMS, which possibly simplifies the configuration by reducing the number of interfaces inside the building. Beside the schedules, the optimization algorithm inside the CEMS also generates an (relative) energy balance forecast. This forecast is passed to the tariff server and optionally also to other interested entities like the Flexibility Operator.

3.3 Selling Intra-day Flexibilities

At this point, the CEMS created schedules for all controllable flexibilities inside the building on the basis of generation and consumption forecasts and day-ahead price signals. Nevertheless, the CEMS can still alter these schedules by providing intra-day flexibilities to external entities under the premise that the earnings are equal to or greater than before. Selling flexibilities is not a matter of optimization inside the building, but external entities can run other (higher-level) optimizations and use the flexibilities to realize optimization targets. In this paper, this higher-level optimization is not in focus. From the building operator's point of view, it doesn't matter for which purpose the flexibilities have been bought respectively sold. When a certain amount of flexibility is sold for a certain time span, this flexibility cannot be used for other optimizations during the corresponding period. This means, the optimization algorithms (e.g. for optimizing self-consumption) must be executed again after flexibility has been sold. The problem is, that this also causes a change in the energy balance forecast, which has been provided to the energy retailer and probably to other entities too. Depending on the contracts with these entities, violating the previously provided forecasts may cause penalty payments. These costs must be considered by the CEMS when offering flexibility as a response to a flexibility request.
Figure 2 shows a flexibility request, in this case sent by the Flexibility Operator. After the CEMS has received the request from the external entity, it calculates possible flexibilities for the requested period. The offer not only consists of the maximum available flexibility, but also possible quantization steps. For example, a boiler may be equipped with an electrical heating element that allows controlling it with two power steps, the first one with 5kW and the second one with 10kW (which is the maximum power of the heating element). The flexibility offer for a certain period could be 5kW or 10kW, but intermediate power steps like 7kW are not possible because of technical limitations. After receiving a flexibility offer, the external entity can send an empty order or an order for one

scenario. If an empty order has been received, the CEMS discards all scenarios of the recently sent flexibility offer. Otherwise, the ordered flexibility scenario will be scheduled by the CEMS and has to be considered in future flexibility requests. The final step is a flexibility release message for a scenario, which has been ordered before. After the CEMS has received the flexibility release, it integrates the related scenario into the storage schedules and passes these schedules to the BEMS. As mentioned before, finally a new energy balance forecast must be calculated.

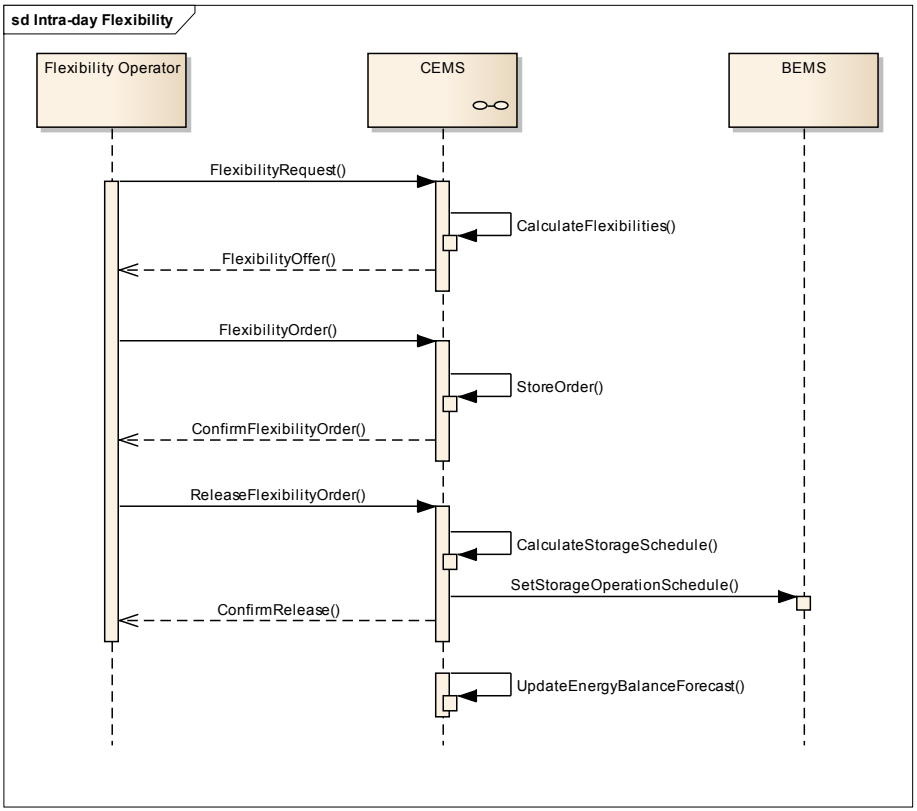


Figure 2. Sequence diagram for an intra-day flexibility request

3.4 Grid Priority Functions

If technical limitations of the (distribution) grid are violated, priority functions take place to protect the technical equipment and to ensure the overall grid stability. These functions can be managed locally or from a central controlling instance. Centrally managed functions assume the availability of a reliable communication infrastructure. This assumption can be avoided by implementing locally managed functions, which are rules based on measured conditions like the current voltage or

frequency. To avoid an oscillation behavior of the overall system, these rules should be slightly adopted for each CEMS or group of CEM-systems. Control strategies for voltage control in distribution grids for example has been introduced in [11].

4. Overall System Architecture

The communication patterns introduced in the previous chapter can be put together into an overall system architecture. This system architecture must fulfill some requirements, which are summarized in the following enumeration:

- From the building's point of view, the grid operator is the only static entity that cannot be changed. Thus, CEM-systems should be connected to an XMPP server provided by the grid operator.
- A grid operator may also operate entities like Smart LV Grid Controllers or Flexibility Operators, which are also connected to the XMPP server provided by the grid operator.
- An Energy Retailer provides one or more Tariff Servers and optional one or more Energy Pool Managers. These entities are connected to an XMPP server provided by the Energy Retailer.
- Energy Pool Managers may also be operated by several entities (which are not Energy Retailers), which are called Aggregators. Aggregators also provide an XMPP server.
- Various XMPP servers introduced in the enumeration items above are connected using XMPP server-to-server communication [2]. This enables all entities in the system to communicate with each other.
- Because a grid operator possibly connects a huge number of CEM-systems, it can operate a random number of XMPP servers. This makes the system very scalable while keeping initial costs down.

Figure 2 shows the overall system architecture. The figure shows two grid operators, two energy retailers and one aggregator role. The lines between the XMPP servers indicate that XMPP is not a multi-hop protocol, each server directly communicates with all other servers. In order to provide the IP addresses of the XMPP servers, a central registry from a trusted instance is necessary.

5. Outlook

As mentioned in chapter 1, the communication between CEM-systems and the power system will be standardized in IEC 62746 [8]. The communication patterns introduced in this paper will be presented to the working group IEC TC57 WG21, which elaborates the standard. Beside the main use cases from chapter 2, organizational use cases for adding CEM-systems, configuring entities and changing energy retailers or aggregators must be added and considered. Also, a security and privacy architecture together with a public key infrastructure must be established.

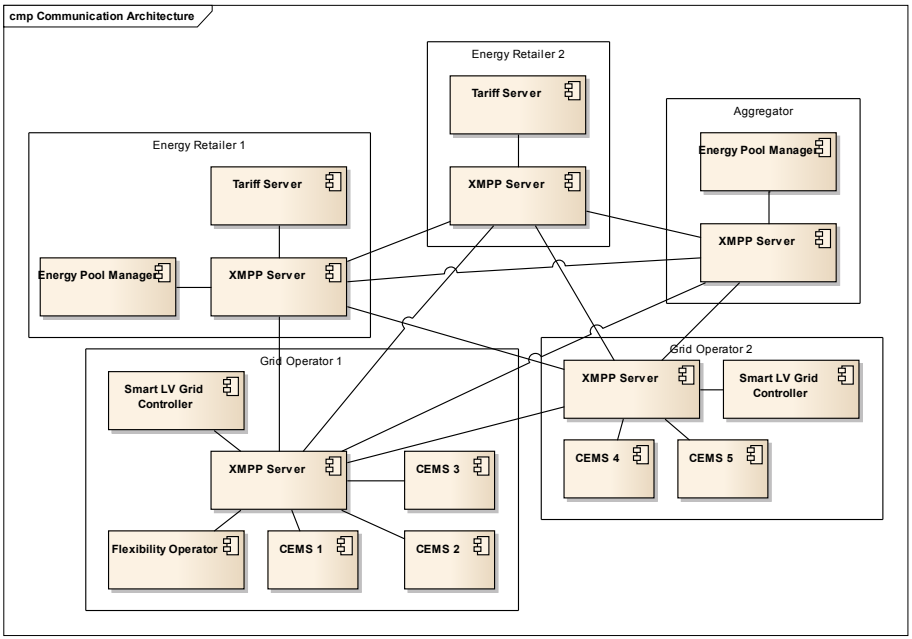


Figure 3. Overall system architecture for integrating the demand side into the Smart Grid.

6. References

[1] EU Task Force Smart Grid (EG3). (2014). Flexibility chapter.

[2] Saint-Andre, P. (2011). Extensible Messaging and Presence Protocol (XMPP): Core. Request for comments RFC, 6120.

[3] Bundesverband PHOTOVOLTAIC AUSTRIA. (2014). PVA-Plattform für Überschuss-Einspeiser. Retrieved July 28, 2014, from http://www.pvaustria.at/strom-verkaufen/. (in German).

[4] Joe-Wong, C., Sen, S., Ha, S., & Chiang, M. (2012). Optimized day-ahead pricing for smart grids with device-specific scheduling flexibility. Selected Areas in Communications, IEEE Journal on, 30(6), 1075-1085.

[5] Jungwirth, J., Mikulovic, V., Pichler, M. & Roessel, T. (2012). Smart Buildings: Flexible Teilnehmer in Smart Grids. In: Smart City. Vienna: Schmid Verlag.

[6] IEC, (2014), IEC 62939 Smart Grid User Interface.

[7] IEC, (2013), IEC/TS 62872 System interface between Industrial Facilities and the Smart Grid

[8] IEC, (2014), IEC 62746-2 System Interface between Customer Energy Manager and Power Management System (draft).

[9] Alliance, O. OpenADR 2.0 Profile Specification, A Profile.

[10] Bushby, S. T. (2011). Information model standard for integrating facilities with smart grid. ASHRAE Journal, 53(11), B18-B22.

[11] Einfalt, A., Kupzog, F., Brunner, H., & Lugmaier, A. (2012). Control strategies for smart low voltage grids-the Project DG DemoNet-Smart LV Grid.

[12] Oldewurtel, F., Parisio, A., Jones, C. N., Morari, M., Gyalistras, D., Gwerder, M., ... & Wirth, K. (2010, June). Energy efficient building climate control using stochastic model predictive control and weather predictions. In American Control Conference (ACC), 2010 (pp. 5100-5105). IEEE.

Smart Grid, Smart Charging, Smart Privacy?

An Empirical Investigation of Consumers' Willingness to Provide Smart Charging Information

Susen Döbelt, Technische Universität Chemnitz, Institute of Psychology, Cognitve and Engineeering Psychology, susen.doebelt@psychologie.tu-chemnitz.de
Bettina Kämpfe, Technische Universität Chemnitz, Institute of Psychology, Cognitve and Engineeering Psychology, bettina.kaempfe@psychoglogie.tu-chemnitz.de
Josef F. Krems, Technische Universität Chemnitz, Institute of Psychology, Cognitve and Engineeering Psychology, josef.krems@psychologie.tu-chemnitz.de

Abstract – The ability to balance electricity load efficiently has been highlighted as one of the biggest advantages of smart grids. However, the majority of smart grid scenarios require detailed settings of consumer consumption demand and the measurement of fine-grained consumption data. These data requirements provoke a conflict between the usage of sustainable smart grid appliances and the protection of individuals' privacy. While technical implementation of demand response appliances e.g. smart car charging have been well studied, there is still a lack of studies which address privacy issues of consumers in the electro-mobility context. Therefore, we conducted an empirical investigation of consumers' privacy concerns, as we asked $N = 73$ respondents of an online survey to indicate their willingness to provide smart car charging information. Results indicate differences in willingness between different information levels: consumers were "somewhat willing" to provide information evolving from raw and processed data of a smart car charging systems. In contrast, consumers rejected information provision including threat potential deduced from this data. To address consumers' privacy concerns, we advocate addressing data-minimization and data-avoidance principles to decrease the threat potential of smart appliances. Furthermore, we support to incorporate automated security mechanisms (e.g. data encryption, anonymization and decentralized data storage) to protect the privacy of the consumer.

1. Introduction

The restructuring of power grids from a centralized solution to a decentralized, demand-oriented smart grid is intended to be more energy efficient, sustainable and therefore meet central challenges of today's society. End-users may hope to save money when reducing their energy consumption, suppliers aim at a reduction of operational costs, and operators of the transmission system are interested in a flexible demand side to integrate the growing amount of renewable energy sources (McKenna, 2011). Least – the ability to balance load efficiently - has been highlighted as one of the

biggest advantages of smart grids (Erkin et al., 2013). Thus, demand response is supposed to be a promising strategy to reduce the amount of 'wasted green energy' (Raabe et al., 2011).
In a private application context, two demand-response-scenarios have been in the focus of previous research: 1. Smart homes and 2. Smart charging of electric vehicles (EVs): defined as "ad hoc charging systems interacting in real-time with smart grids in order to implement smart energy dispatching strategies aiming to overcome severe grid overload problems caused by a large [plug-in electric vehicles] PEV penetration" (Amoroso & Cappuccino, 2012, p.1). Here grid to vehicle (G2V) scenarios describe unidirectional loading of EVs, vehicle to grid (V2G) describes bidirectional energy flow (Langer et al., 2013). However, the majority of smart grid appliances require detailed settings of consumer consumption demand (time, amount of energy) and the measurement of consumption data. Thus, the possible inferring of personal information from demand response systems, which provide detailed information on occupants' activity (Lisovich, Mulligan & Wicker, 2010), provokes a conflict between the usage of sustainable, smart appliances and the protection of individuals' privacy.

2. Related Work

Energy consumption data, as well as long-term location and motion data are a rich source of information, whereof manifold information about daily activities, behavioral patterns, and individual lifestyles and can be extracted (Molina-Markham et al., 2010; Lisovich, Mulligan & Wicker, 2010; McKenna, 2011). Smart car charging includes the tracking, transmission, and processing of sensitive data, but privacy issues did not receive much attention in research yet (Langer et al., 2013).
The debate on smart grid privacy issues has been started with the installation of smart meters. Specific power consumption patterns of devices could be identified by fine-grained (a few seconds) data intervals (McKenna, 2011). Even less frequent measurements of half an hour allows to determine daily activities of consumers and presence (or absence) of occupants (Molina-Markham et al., 2010; Roßnagel & Jandt, 2010). Smart meter data is therefore justifiably viewed as sensitive personal data (McKenna, 2011). Smart car charging incorporates these difficulties, as the charging EV is usually another consumption device within a private household (Raabe et al., 2011).
Additionally the evolving data is not retrospective only, as the indication of user requirements e.g. time of departure (end of charging time) and the demanded charging amount provides prospective information of user consumption. Remote tracking of who, when, and where a user is connected to the grid is possible (Raabe et al., 2011). Therefore, location privacy, defined as the "claim and right to determine for themselves, when, how and to what extent location information about them is communicated to others" (Dunkham & Kulik, 1967, p. 2) is at risk. Moreover, these potential threats will be multiplied by the expected ubiquity of intelligent public charging infrastructure and the increasing installation of driver assistance systems in modern cars in the future. Because of the informative value of location data and the amount of additional actors involved in the context of e-mobility compared to smart metering, additional measures regarding data minimization and data avoidance should be taken into account (Raabe et al., 2011). Recently, Heuer (2013) claimed for the implementation of data minimization principle in assistance systems (driver assistance systems as well as smart homes).

A systematic collection of privacy issues for different charging use cases was provided by Langer, Skopik, Kienesberger and Li (2013). The authors sum up potential privacy invading information, which could be retrieved during four different charging use cases: combining 'in-house' (customer) vs. foreign charging and uncontrolled vs. controlled ('smart') charging. Especially information about users' location (presence or absence at home or workplace) and motion patterns (travelled distances and routes) are highlighted as privacy invading. Gosh, Thomas and Wicker (2011) identified similar privacy risks in V2G scenarios. They argue that long-term examination of consumers' charging profiles allows V2G controllers potentially to monitor travel behavior to a great extent and generate a reliable and detailed profile of the consumer. They propose secure mechanisms for planning, charging, and billing information, incorporating distributed information processing and cryptographic security. Further authors likewise highlight the importance of anonymizing data (Raabe et al., 2011, Efthymiou & Kaologridis, 2010).
Privacy enhancing technology features and security mechanisms which address privacy concerns at the very early design stage have been already suggested (Fhom & Bayarou, 2011; Metke & Ekl, 2010), but research studies including privacy issues of smart appliances are typically based on the analysis of potential threats (for an overview see McKenna et al., 2011). Just a few studies include empirical results on privacy concerns of consumers (e.g. Hargreaves, Nye & Burgees, 2010, Gerdenitsch & Döbelt, 2012). Recently, Jung et al. (2012) purposed a privacy preventing smart grid ICT architecture addressing the privacy concerns of consumers by facilitating decentralized data storage, local data processing, and using a service oriented architecture.

3. Research Question

While demand response applications have been well studied, there is still a lack of studies which address privacy issues of consumers (Shao, 2011). Therefore, we were interested in the following question: What is privacy sensitive information for consumers in a smart charging scenario?
To identify these specific privacy concerns we conducted an online survey asking for respondents' willingness to provide different kinds of information potentially arising in a smart car charging scenario. Therefore, we adapted the construct *willingness to provide data* according to Phelps, Novak and Ferell (2000), originally intended to study privacy concerns of consumers in the marketing sector. To separate specific information concerns from influence of personality, we additionally ask for *global information privacy concerns* (Malhorta et al., 2004; Smith et al., 1996). The aim of our study is to contribute to a privacy preventing ICT architecture design, which incorporates consumer privacy demands and information system requirements (Heuer, 2013).

4. Method

4.1 Procedure

Our online survey was conducted from December 2013 until April 2014 in Germany as one measurement within our research project "Gesteuertes Laden V3.0", investigating smart car charging in a

real world setting. This research project is funded by German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety and conducted by consortium partners: BMW AG, EWE AG, Fraunhofer-IOSB, Technische Universität Ilmenau, Vattenfall Europe Innovation GmbH, Clean Energy Sourcing AG and Technische Universität Chemnitz. Participants of our online survey were invited by several public announcements on project partners websites, a newsletter addressing an EV-interested audience, electro mobility related forum posts, and invitation of former respondents of e-mobility surveys of the Technische Universität Chemnitz. The completion of the survey took about 30min. The survey started with a description of the smart charging scenario, arranged like a storybook. Following essential (system-)components were part of the storybook: an EV user, a wall box at home, additional load peaks in the case of widespread of EVs, variable availability of renewables, EVs as one possibility to take up energy if production is higher than consummation, and information handling by an intelligent management system.

For a warm-up, respondents were asked to write down advantages and disadvantages of smart charging. Afterwards, further possibilities to set departure time and load preferences were described to deepen the understanding of the system application. The participants were asked to indicate their *willingness to provide* a total of 44 information items on a 4-point scale (1 = never, 4 = always willing). These 44 items incorporate three levels of informational content. Level 1: information on the basis of raw data, which is processed in the backend system (19 Items), level 2: information on the basis of already processed and long-term data, e.g. used for user feedback (e.g. consumption statistics, 9 items), and level 3: information deduced from level 1 and 2, focusing on possible threats of long-term generated and processed data (16 items). As information level 3 is deduced information from level 1 and 2, information levels are not disjunctive. These items incorporate the potential threats highlighted in the literature (Gosh et al., 2012; Langer et al., 2013) and are chosen to cover relevant topics for research on privacy in general. The existence of an item does not imply necessarily that this type of information will be inferred for smart charging. Our item set does not claim to be exhaustive and contains a self-centered formulation to increase personal relevance. All items have been presented in randomized order to avoid effects of order. Finally, we asked for demographics, experience with EV and smart charging, and *global information privacy concerns*.

4.2 Participants

All in all $N = 73$ respondents completed our online survey. The majority (96%) of participants was male and on average 40 years old ($M = 40.11$; $SD = 11.49$). With regard to the level of education, respondents' could be described as 'well educated': the majority (56%) of respondents holds a university degree, followed by 17% that holds a degree of a university of applied science. On average, respondents were in possession of one car ($Mdn = 1$) and had a high level of driving experience: the average possession of driver license was 22 years ($M = 21.91$, $SD = 12.02$). With regard to EV-experience, respondents indicate in mean that they 'occasionally drive an EV (e.g. a rented EV)'. Even one quarter of the respondents (25%) affirm to have experience with smart charging. Summing up our sample differs in gender distribution and level of education from the German population (49% male, 8% university degree; Statistisches Bundesamt, 2014).

4.3 Data Analysis

To obtain a comprehensive understanding of consumer concerns, we used a mixed method approach and combined qualitative and quantitative data collection. To analyze qualitative answers, a system of categories was educed bottom-up, raw data was categorized, and relative frequencies per category were enumerated. Demographic data was analyzed descriptively, means (*M* and *Mdn*), standard deviations (*SD*) and frequencies (in %) are reported. Distribution of quantitative data was tested and as data do not follow a normal distribution, in first instance nonparametric inference statistical tests used to analyze data regarding *willingness to provide data*. We further used parametric inference statistics to check the influence of individual differences in *global information privacy concerns*. Cancelled surveys were deleted from the set of analyzed data.

5. Results

After a first explanation of smart charging, the respondents were asked to name advantages and disadvantages. In total, respondents named 149 advantages vs. 115 disadvantages, indicating positive perception of smart charging. Most frequently, "stabilization of the grid" (32%), possible "financial compensation for consumers" (22%), and "increased integration of renewables" (19%) were mentioned as advantages. In contrast, concerns regarding constraints "for individual mobility, flexibility and spontaneity" (34%), "data protection and privacy" (16%) and "increased effort for planning" (18%) were mentioned. Example statements are listed in the table below.

	Categories	Example statement
+	stabilization of the grid	"*Positive for the electricity sector: if more EVs will be sold in the future, load peaks are avoided […]"*
	financial compensation for consumers	*"[…] in times of oversupply the customer could save money with a dynamical pricing or a bonus for charging."*
	increased integration of renewables	*"[…] Efficient use of renewable sources of energy by an adaption of energy demand on energy supply […]"*
-	constraints for individual mobility, flexibility and spontaneity	*"The EV is not available if it is not requested. What should one do in a case of emergency? Or if the kids are not in the mood for a short trip, then they agree, but not to the zoo, instead they want to go swimming."*
	constraints with regard to data protection and privacy	*"[…] Additionally, the user has to agree to the surveillance of his driving- and charging-behavior by a public agency or a company. Best regards from the NSA and G. Orwell."*
	increased effort for planning	*"An additional task is added […]. Additional to work, profession and leisure time […] I'm forced to consider my mobility to a greater extend."*

Table 1: Translated example statements for each category, illustrating respondents perspective on advantages (+) and disadvantages (-) of smart charging.

Afterwards, respondents were asked to indicate their *willingness to provide data* on the developed set of information evolving in a smart charging scenario. Respondents indicated that they were most unwilling to provide the level 3-information: "if my household is unattended" ($M = 1.14$;

SD = .509), "what I earn" (*M* = 1.27, *SD* = .629) and "who is part of my social network" (*M* = 1.30; *SD* = .617; descriptive results see Appendix 1). We used a Friedman ANOVA to investigate differences between the means of users' *willingness to provide* of the three information levels (Figure 1).

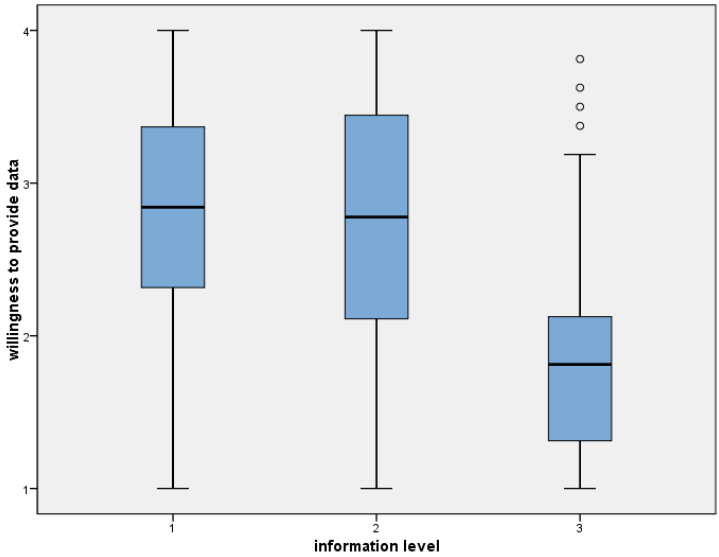


Figure 1: Mean willingness to provide information is lowered for level 3 information - focusing on possible threats of long-term generated and processed data.

Even if parametric ANOVA is known as robust to violations of normal distribution, the nonparametric test was used, because level 2 and 3 responses were not normal distributed (Kolmogorov-Smirnov: $D_{level2}(73) = .109$; $p = .03$; $D_{level3}(73) = .121$; $p = .01$). Results show that levels differ in willingness to provide information ($\chi^2(2) = 92.91$; $p < .000$). Ascending post-hoc pair tests (Wilcoxon signed-rank) were conducted to locate differences between levels. Differences were identified between level 3 (*Mdn* = 1.81, "not very willing") and 2 (*Mdn* = 2.78, "somewhat willing"; $W_s = 23.00$; $z = -6.86$; $p < .000$) indicating a lowered willingness to provide level 3 information. No differences could be identified between level 2 and 1 (*Mdn* = 2.84; "somewhat willing"; $W_s = 956.00$; $z = -1.14$; $p = .254$), indicating a comparably slight willingness to provide this information. These results became apparent in the same manner using a parametric ANOVA with repeated measures.

To investigate effects of personality, we conducted an additional ANOVA with the *global information privacy concern* scale as a covariate. One item of the scale was excluded due to a lack of reliability. The inclusion of *global information privacy concern* scale did not lead to a significant interaction effect of information level and *global information privacy concerns* ($F(1.47,104.68) = .33$; $p = .653$, Greenhouse-Geisser corrected), indicating that the results for *will-*

ingness to provide data do not differ for more or less concerned people. Again, the main effect of information level was confirmed ($F(1.47, 104.68) = 7.17$, $p = .003$, Greenhouse-Geisser corrected).

6. Discussion and Conclusion

The aim of our study was to investigate consumer privacy concerns within a smart charging scenario. Therefore, we contrasted consumer' *willingness to provide* different information levels: 1.) evolving from raw data (level 1), 2.) processed data (level 2), and 3.) based on threat analysis (level 3, highlighted by e.g. Gosh et al., 2012 or Langer et al., 2013). Qualitative statements of our respondents indicate a positive attitude on smart charging in general. Nevertheless, the invasion of privacy was one of most frequently named disadvantages of smart charging. Quantitative results showed that respondents of our survey were "somewhat willing" to provide information which evolved and processed in a smart car charging scenario (level 1 and 2 information). Probably this could be reflect the positive attitude on smart charging and respondents interest in this kind of information (e.g. statistics on covered distances or charging costs). Additionally, our results showed that consumers' *willingness to provide information* which incorporates threat potential (level 3) is significantly lowered. Consumers are "not very willing" to provide this kind of information. Furthermore, if a consumer is in general more or less concerned with regard to his/her privacy, seems to be not a decisive variable so far. Thus, we discovered a main effect for information level only. Moreover, as level 3 information is deduced from level 2 and level 1, but rejected by respondents, we assume consumers are probably not aware of inherent threat potential of level 1 and 2 information. Commonly, service providers inform users by consent forms or privacy policies about what kind of data is used by a certain application. Users could agree or deny these privacy policy forms. Hence the user is forced to take over responsibility for protection of privacy by his-/herself. But as our results indicate, the merely transparency of collected data seems not appropriate to identify secondary privacy threats. In other words, how collected (level 1 and 2) data could evolve to a possible privacy threat (level 3) is not obvious for consumers. Therefore and in line with Heuer (2013), we suppose to incorporate automated mechanisms (e.g. data encryption, anonymization and decentralized data storage etc.) into smart charging ICT architecture design to protect users' privacy by default. As Raabe et al. (2011) suggested already, the incorporation of data-minimization and -avoidance principles would decrease threat potential of smart systems per se.

Our results should be treated as empirical data of consumers with a high education, interest on and some experience with smart charging. Therefore results of our survey are probably overestimated. But for an exploration of consumers' perspective of a future scenario, we believe such respondents could provide valuable input. Additional methodological approaches such as repeated measurement and field trial studies with a broad range of representative consumers could provide further insights on privacy concerns related to smart charging. Especially the impact of increased personal relevance of evolving data on the *willingness to provide* this data is an interesting aspect to explore.

Acknowledgements

This study was conducted with in the research project "Gesteuertes Laden V3.0" funded by the German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety. We thank our consortium partners: BMW AG, EWE AG, Fraunhofer-IOSB, Technische Universität Ilmenau, Vattenfall Europe Innovation GmbH, and Clean Energy Sourcing AG supporting this study and furthermore Tobias Fritsche, Tilman Weyh, Claudia Mair, Franziska Bühler and Andreas Klein, who supported the development of the survey. Special thanks goes to Franziska Hartwich for motivating and this paper.

References

[1] Fhom, H., & Bayarou, K.: Towards a Holistic Privacy Engineering Approach for Smart Grid Systems, Proceedings of 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 234-241, 2011

[2] Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., & Irwin, D.: Private memoirs of a smart meter, Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building, BuildSys ´10, pp. 61-66, 2010

[3] Roßnagel, A., & Jandt, S.: Datenschutzfragen eines Energieinformationsnetzes, Alcatel-Lucent Stiftung Stiftungsreihe 88, Stuttgart, 2010

[4] Glancy, D. J.: The Invention of the Right to Privacy, Arizona Law Review, v.21, n.1, pp.1-39, 1979

[5] Duckham, M. & Kulik, L.: Location Privacy and Location-Aware Computing, J. Drummond, Dynamic & Mobile GIS: Investigating Change in Space and Time. Boca Raton, FL.: CRC Press, 2006

[6] Cavoukian, A., Polonetsky, J., & Wolf, C.: Smart privacy for the smart grid: embedding privacy into the design of electricity conservation, Identity in the Information Society, 2009

[7] Cavoukian, A.: Privacy by Design - Take the Challenge, Information and Privacy Commissioner of Ontario, Canada, 2009

[8] Langer, L., Skopik, F., Kienesberger, G., & Li, Q.: Privacy issues of smart e-mobility, Industrial Electronics Society, IECON 2013-39th Annual Conference of the IEEE, pp. 6682-6687, 2013

[9] Ghosh, D. P., Thomas, R. J., &Wicker, S. B.: A Privacy-Aware Design for the Vehicle-to-Grid Framework, System Sciences (HICSS), 2013 46th Hawaii International Conference on System Sciences, pp. 2283-2291, 2013

[10] Jung, M., Hofer, T., Döbelt, S., Kienesberger, G., Judex, F., & Kastner, W.: Access control for a Smart Grid SOA, Proceedings of 7th Conference for Inter-net Technology and Secured Transactions, 2012, pp. 281-287, 2012

[11] Wicker, S. B.: A Little Too Smart - The Loss of Location Privacy in the Celluar Age. 2011

[12] Cavoukian, A.: Privacy by design. Take the Challenge, Information and Privacy Commissioner of Ontario, Canada, 2009

[13] Raabe, O., Lorenz, M., Pallas, F., Weis, E., & Jahr, I.: Datenschutz im Smart Grid und in der Elektromobilität, Karlsruher Institut für Technologie, 2011

[14] McKenna, E., Richardson, I., & Thomson, M.: Smart meter data: Balancing consumer privacy concerns with legitimate applications. Energy Policy, 41, 807-814, 2012

[15] Erkin, Z., Troncoso-Pastoriza, J. R., Lagendijk, R. L., & Perez-Gonzalez, F.: Privacy-preserving data aggregation in smart metering systems: An overview, Signal Processing Magazine, IEEE, 30(2), 75-86, 2013

[16] Gerdenitsch, C., & Döbelt, S.: Who controls the switch?-Enhancing Residents Trust in Sustainable Building Technology, eNova12, 22.11.-23.11.2012, Pinkafeld, Online Available: http://www.fhpinkafeld.ac.at/enova/Tagungsband_2012.pdf, 2012

[17] Lisovich, M. A., Mulligan, D. K., & Wicker, S. B.: Inferring personal information from demand-response systems, Security & Privacy, IEEE, 8(1), 11-20, 2010

[18] Efthymiou, C. & Kalogridis, G.: Smart grid privacy via anonymization of smart metering data, International Conference on Smart Grid Communications, IEEE, pp. 238–243, 2010

[19] Heuer, A.: Forschung und Entwicklung zu Assistenzsystemen und Big Data – Vorsprung durch Datensparsamkeit, Tagungsband Fachkongress „Social Business“ Mittelstand Digital, pp.41-55, Online available: http://www.mittelstand-digital.de/MD/Redaktion/DE/PDF/fachkongress-social-business-5, 2013

[20] Phelps, J., Nowak, G., & Ferrell, E.: Privacy concerns and consumer willingness to provide personal information, Journal of Public Policy & Marketing, 19(1), 27-41, 2000

[21] Statistisches Bundesamt, Vorläufige Ergebnisse der Bevölkerungsfortschreibung auf Grundlage des Zensus 2011-Stand 10.4.2014. Online available: https://www.destatis.de/DE/Publikationen/Thematisch/Bevoelkerung/Bevoelkerungsstand/Bevoelkerungsfortschreibung.html, 2014

[22] Amoroso, F. A., & Cappuccino, G.: Advantages of efficiency-aware smart charging strategies for PEVs, Energy Conversion and Management, 54(1), 1-6, 2012

[23] Malhotra, N. K., Kim, S. S., & Agarwal, J.: Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model, Information Systems Research, 15(4), 336-355, 2004

[24] Smith, H. J., Milberg, S. J., Burke, S. J.: Information privacy measuring individuals` concerns about organizational practices, MIS Quart., 20(2), p.167-196, 1996

Appendix 1

Survey question: Please indicate below, to what extend you are willing to provide the following information...

	Level	Mean Willingess	SD
...if my household is unattended when I leave the house.	3	1,14	,509
...what I earn.	3	1,27	,629
...who belongs to my social network.	3	1,30	,617
...that I am not at home.	3	1,42	,798
...where my whereabouts are.	3	1,56	,850
...how my motion profiles looks like.	3	1,56	,866
My current vehicle location data	2	1,67	,929
...if I pursue a regular employment.	3	1,77	1,048
...who my employer is.	3	1,77	1,034
...how many people live in my household.	3	1,90	1,056
...when I arrive at home.	3	1,92	1,010
...when will I leave the house the next day.	3	2,00	1,080
My earnings through the participation in smart charging compared to other participants	2	2,08	1,102
...which route and distance I want to drive the next day.	3	2,11	1,048
My earnings through the participation in smart charging	2	2,12	1,079
...where my work is.	3	2,15	1,186
...where my main residence is.	3	2,23	1,185
Location of the wall box, where I have charged	1	2,38	1,150
My planned departure time(s) for the next week	1	2,48	1,094
My costs incurred per charging process	1	2,49	1,107
My planned departure time(s) for the day	1	2,56	1,118
Times, when my vehicle was connected to the wall box	1	2,59	1,091
...the distance to my work.	3	2,62	1,126
...how much I drove.	3	2,64	1,147
Deviation of my real departure times and my set departure times	2	2,66	1,145
Kilometers, that I've driven between two charging processes	2	2,79	1,130
My set flexibility of departure time	1	2,84	1,067
Identification, if I have charged on a wall box	1	2,84	1,080
Identification, if my vehicle was charged on a wall box	1	2,85	1,050
The energy provider of my wall box	1	2,86	1,084
Statistics of my charged energy amount per week	2	2,92	1,115
Statistics of my charged energy amount per day	2	2,93	1,058
Times, when electricity flows to charge my vehicle	1	2,93	1,045
My type of vehicle/vehicle brand	1	2,95	1,092
My set safety distance	1	3,00	1,080
Comparison of charged energy amount with other electric vehicle users	2	3,00	1,130
My charged amount of energy per charging process	1	3,00	1,054
Statistics of my charged energy amount per month	2	3,01	1,074
Statistics of my charged energy amount per year	2	3,01	1,047
State of charge/reach when connecting my vehicle to a wall box	1	3,03	,986
My set minimum range	1	3,05	1,012
Use of the function „preconditioning“ (preheating of the vehicle and the battery)	1	3,07	,977
My usage of the function "smart vehicle charging"	1	3,07	1,005
My usage of the function "load vehicle immediately"	1	3,12	,971

Table 2: Smart charging information (translated from German) ordered by ascending by mean willingness to provide the information. Additionally, information levels are added.

Cybersecurity Risk Assessment in Smart Grids

Thomas Hecht, Lucie Langer, Paul Smith

AIT Austrian Institute of Technology
Safety and Security Department
firstname.lastname@ait.ac.at

Abstract – Smart grids will make extensive use of information and communication technology (ICT) to enable the integration of renewable energy sources. Consequently, future power grids come with a much larger cyber-attack surface, which makes cybersecurity risk assessment a major concern. Due to their cyber-physical nature, risk assessment in smart grids is a challenging task. Moreover, the complex mix of legacy systems and new components in smart grids requires novel risk assessment methods that are able to cater for both. This paper surveys existing risk assessment methods for smart grids, addresses the key challenges, and presents ongoing research projects that aim to tackle these challenges.

1. Introduction

Future power grids will make extensive use of information and communication technology (ICT) to enable the integration of renewable energy sources and more efficient energy management. While ICT components are already part of today's power grid, they are used in a much more isolated fashion, with access restricted mainly to energy providers and grid operators. This paradigm will no longer hold in future smart grids: end-users will be connected to the grid via smart gateways, and electricity billing will be provided through smart meters, which means that every consumer (or prosumer) will have their own ICT-enabled entry point to the grid. The large number of access points introduces a much larger surface for cyber-attacks than there has been before. Possible attacks include large-scale meter tampering, spoofed measurement data leading to a misinterpretation of the current system status, or even targeted high-impact attacks on the critical infrastructure of grid operators. Moreover, recent events have shown that attacks on industrial control systems are becoming increasingly sophisticated. Consequently, assessing (and managing) the risk from cyber-attacks is of paramount importance for the security of future energy supply.

Risk assessment in smart grids is a challenging task for various reasons. First and foremost, due to the cyber-physical nature of smart grids, ICT-focused risk assessment methods are not readily

applicable, and safety aspects must be considered as well. Additionally, the complex mix of legacy systems and new components in smart grids requires novel risk assessment methods that are able to cater for both. This paper summarizes existing risk assessment methods applicable to smart grids, investigates the associated challenges, and summarizes ongoing research in this area.

2. Cybersecurity Risk Assessment

The primary objective of cybersecurity risk assessment is to identify vulnerabilities and threats, and determine their impact. The outcome of the risk assessment should be used in the specification of security requirements and the selection of security controls for smart grid. Both top-down (e.g., use case analysis and smart grid functionality) and bottom-up (e.g., authentication and authorization at substations, key management, intrusion detection, etc.) approaches should be used to implement risk assessment [1]. Furthermore, existing risk assessment methods are divided into quantitative and qualitative approaches. Quantitative methods use metrics that represent the probability and impact of a threat. As this often proves to be a difficult and subjective task due to the shortage of reliable data on incidents, qualitative approaches are widely used instead, which may also be able to take advantage of other sources of information that are not readily quantifiable, such as threat graphs and game-theoretic models. The European Network and Information Security Agency (ENISA) maintains a repository of risk assessment standards, methods and tools [2].

While risk assessment has been defined to address information security in conventional ICT systems, risk assessment for smart grids is still in its infancy. For system stakeholders, utility providers, manufacturers and system developers, risk assessment for smart grid remains a huge challenge for several reasons: current risk assessment frameworks are mostly focused either on conventional ICT systems (e.g., BSI Baseline Protection [3]), or on traditional power grids (from NERC [4] or ISA standards [5]). Little consideration has been given to smart grids and their specific attributes. While risks for traditional ICT systems focus on the confidentiality, integrity and availability of information (mostly in that order), in industrial control systems and, more specifically, smart grids, operational reliability is of utmost importance, and the priority therefore is on availability, followed by integrity and confidentiality [6]. This means that cybersecurity risk assessment for smart grids must be combined with safety aspects.

A small number of frameworks address risk assessment for critical (energy) infrastructures. The *Guidelines for Smart Grid Cyber Security* developed by NIST (NIST-IR 7628) [7] provide a set of high-level recommendations applicable to the proposed smart grid architecture for the U.S. However, a general approach for assessing cybersecurity risks is not provided. NIST-IR 7628 and ISO 27002 have been the basis for a report on smart grid security by ENISA [8]. It provides a set of specific security measures for smart grid service providers, aimed at establishing a minimum level of cybersecurity. The importance of performing a comprehensive risk assessment before selecting appropriate measures is pointed out, but no specific methodology is recommended. The Reference Security Management Plan for Energy Infrastructure developed for the European Commission [9] is intended to provide guidance for operators of energy grids or components thereof, and contains recommendations on performing a risk assessment, based on the *Performance and Risk-based Integrated Security Methodology (PRISM)*. The European standardization bodies CEN, CENELEC

and ETSI have issued a report on *Smart Grid Information Security (SGIS)* [10, 11] addressing cybersecurity and risk assessment in smart grids in response to the M/490 Smart Grid Mandate by the European Commission. It defines five *SGIS Security Levels* to assess the criticality of smart grid components by focusing on power loss caused by ICT systems failures. Moreover, five *SGIS Risk Impact Levels* are defined to classify inherent risks of smart grid assets. The risk assessment proposed by SGIS takes a clean-slate approach, assuming a future smart grid with no security controls in place. Consequently, this approach does not reflect the way that smart grids are being deployed, in which the present power grid undergoes an incremental transformation into a smart grid. Thus, a practical cybersecurity risk management approach must be able to deal with a complex combination of legacy systems and new technologies, which is only one among many challenges.

3. The Challenges of Risk Assessment for Smart Grids

In this section, we summarize a number of the key challenges associated with conducting a risk assessment for the smart grid. Some of these challenges exist in others contexts for different types of system; however, implementing a risk assessment in the smart grid is particularly difficult as all of these challenges are present.

3.1 Managing Safety and Security Risks

Cyber-attacks to an electric power grid have the potential to result in safety-related incidents, i.e., those that could result in a loss of life. For example, data injection attacks may be used to change measurement values of some devices, in order to hinder the operation of the grid [12]. Further challenges include data integrity attacks [13], which have the goal of inserting, changing or deleting data in network traffic, so that a management system takes incorrect decisions. Arguably, such attacks could result in safety-related incidents if they lead to the unsafe usage of plant equipment, for example. In the safety domain, a number of analysis techniques have been applied by the community for a number of years. Examples of these include the Hazard and Operability (HAZOP) [14] and Failure Modes and Effect Analysis (FMEA) [15] techniques, which can be used to identify hazard scenarios and the failure modes and their effect on a system, respectively. Similarly, in the security domain, a number of techniques exist for threat and vulnerability analysis, including Microsoft's STRIDE method [16] and attack trees [17]; the latter being very closely related to fault tree analysis [18], which is commonly used for safety analysis. Whilst these two classes of analysis methods are mature, their combined use to understand the safety-related incidents that could emerge from cyber-attacks is still in its infancy.

3.2 Analyzing Cyber-physical Risks

Closely related to the issue of safety in the smart grid, are the challenges associated with analyzing cyber-physical risks. The fact that the smart grid is a cyber-physical system has two major implications for risk assessment: *(i)* in addition to the cyber threats and vulnerabilities that must be considered, physical risks must also be assessed – this both increases the number of scenarios that have to be assessed and introduces the challenge of understanding the relative importance of cyber versus

physical risk; and *(ii)* the physical impact of an attack must be assessed, e.g., in terms of disturbance to energy supply, which can be particularly difficult to determine for cyber-threats. For instance, it is not readily apparent what effect cyber-attacks, such as a Denial of Service attack to a part of a smart grid's ICT infrastructure, could have on the physical operation of a grid – we anticipate this to be somewhat limited currently, as ICT services play an ancillary role, but this may change in the future as it is introduced to support increasingly critical functions of a grid.

3.3 Understanding the Risks to Legacy Systems

The future smart grid will consist of existing *legacy* systems and new ones that, for example, implement novel control mechanisms. In this context, it may be beneficial to examine the security risks associated with new smart grid sub-systems when they are architectural concepts – for example, such an analysis at design-time can ensure secure architectural decisions are made. Examining this combination of legacy and new systems should be catered for when carrying out a risk assessment for the smart grid. For example, specific processes should be defined that support the architectural analysis of conceptual smart grid components that, e.g., identify topological vulnerabilities.
Alongside these forms of analysis, concrete threat and vulnerability assessment can be undertaken, e.g., via penetration testing, to understand the implementation-based risks that are related to legacy systems. However, it is widely understood that legacy industrial control systems can be fragile when subjected to active vulnerability scanning, which can result in the need for manual procedures, thus increasing the complexity of smart grid risk assessment. Similarly, the limited possibilities to perform active security tests may require expensive testing facilities that represent copies of the operational infrastructure, or limited passive tests being realized that are based on eavesdropping communication, for example.
Additionally, the impact on legacy systems from the introduction of new ones must be assessed, and vice versa. In some cases, the different technologies may not interact, e.g., because they use different protocols. When they do interact, there may be unclear security outcomes because of poorly documented legacy systems – such risks may be challenging to evaluate.

3.4 Complex Organizational Dependencies

The power grid is a complex system, which in the liberalized European energy market involves a number of different organizations, including Energy Producers, Transmission System Operators (TSOs), Distribution System Operators (DSOs), and Energy Suppliers. The smart grid has the potential to add more organizations such as telecommunications providers and cloud service providers, e.g., to support the implementation of an Advanced Metering Infrastructure (AMI). Energy customers in the smart grid have a potential role as an energy producer – operating their own equipment – potentially as part of a community of virtual energy producers. Additionally, a diverse range of equipment suppliers and solutions providers can be drawn upon to implement different sub-systems of the smart grid. This complex web of organizational dependencies and responsibilities has the potential to make risk assessment and management very challenging. For example, assessing the risks associated with third-party services and solutions is difficult, because of a lack of transparency. It is widely understood in the ICT sector that organizational boundaries are breaking down, making risk assessment problematic – the use of third-party cloud services by companies is a

good example of this phenomenon. With the widespread use of ICT solutions in the smart grid, these problems become inherent. Also, determining which organization is responsible for accepting the risk burden can be difficult.

3.5 Understanding Cascading Effects

The smart grid is a combination of ICT systems that are interconnected via communication networks, which support an underlying grid infrastructure. Incidents in each of these sub-systems of a smart grid have the potential to cause cascading effects that result in problems in another. This issue is closely related to the previously discussed challenge of cyber-physical impact analysis, i.e., that a cyber-attack to an ICT sub-system could result in an effect in the power grid. However, here we describe a more general problem, in which one attempts to analyze effects across multiple sub-systems that could be both cyber and physical. A particularly pathological case relates to the dependency between ICT systems and a supporting power infrastructure – a cyber-attack could result in a disturbance in its supporting power supply, such as a localized blackout, that could in return result in the ICT systems becoming unavailable when a battery-based uninterruptible power supply expires. To understand such cascading effects, appropriate models of the infrastructure must be developed, along with an understanding of how the impact of an attack could propagate through it.

4. Moving Forward: Addressing the Challenges of Smart Grid Risk Assessment

In ongoing research we will look to address the challenges of implementing a risk assessment for the smart grid via a number of related initiatives. Focusing on current and near-future distribution systems, the Austrian research project *Smart Grid Security Guidance (SG)*^{2} has developed a cyber-security risk assessment method that considers the evolving nature of the smart grid, as well as the given national context in terms of prevailing systems, regulatory constraints, or legal specifications. This method is based on the definition of a national reference architecture, and can be applied to both deployed legacy systems and near-term future developments. The risks to existing systems are evaluated through practical security assessments, which are complemented with a conceptual analysis of future developments. The latter involves threat modeling based on existing collections by the BSI [3] and ENISA [19], subsequently applying those threats to the architecture model, and assessing probability and impact in a semi-quantitative manner. The semi-quantitative analysis is achieved by developing possible attack scenarios and drawing on past experience of the DSOs in the project. Going beyond the activities in the (SG)^2 project, a number of initiatives are seeking to address many of the challenges that are outlined in Section 3**Fehler! Verweisquelle konnte nicht gefunden werden.**, although not necessarily in the context of the smart grid.

As part of the Artemis-funded *EMC*^{2} project (http://www.emc2-project.eu/), Schmittner *et al*. have developed an extension to the FMEA safety analysis technique, which can be used to analyze the likelihood and impact of cyber-attacks [20]. The EMC^2 project is applying this technique to embedded multi-core systems, such as those found in the automotive industry. This represents early work; further investigation is required, for example, to allow the direct comparison of security and safety-

related incidents, and support analysts determining the measures that are associated with threat actors, such as their incentive and capability. Whilst the EMC^2 project focuses on analyzing safety and security aspects for embedded systems, the techniques can be tailored to the analysis of specific smart grid components and sub-systems.

The EU-funded *HyRiM* project (*Hybrid Risk Management for Utility Providers*, https://www.hyrim.net/) is developing novel risk analysis techniques that can be applied to utility networks, e.g., gas, electricity and transport networks. An aspect they are investigating in the project relates to analyzing cascading effects, whereby incidents in the electricity grid result in effects in a transportation system, for example. In order to approach this problem, the project will seek to combine analysis methods that are based on game theory [21] with those related to network theory [22]. As mentioned earlier, parallels can be drawn with the investigations being undertaken in HyRiM and those needed for smart grids, which is comprised of multiple interconnected power and ICT networks and sub-systems.

The EU-funded *SECCRIT* project (*Secure Cloud computing for Critical Infrastructure IT*, https://www.seccrit.eu) is investigating how to support the implementation of high-assurance ICT services, such as those that underpin critical infrastructure services, in the Cloud. In this regard, they have developed a cloud-specific threat and vulnerability catalogue that can be applied when understanding the risks associated with migrating services to the Cloud [23]. The catalogue is organized into categories that relate to the usage of Cloud, such as the use of virtualization technology. Additionally, they have created an extension to an existing risk assessment process that supports the modeling of ICT services in the Cloud and the analysis of risk scenarios, based on the aforementioned catalogue. Assessing the risks associated with Cloud usage has similar challenges as those for the smart grid: there are a number of organizations involved with potentially complex responsibilities with respect to risk, for example. Our future work will seek to leverage the results from the SECCRIT project, especially with respect to the use of the Cloud to implement smart grid ICT services – a deployment model that could be applied.

Finally, the EU-funded *SPARKS (Smart Grid Protection Against Cyber Attacks)* project is investigating cybersecurity and resilience for the smart grid (https://project-sparks.eu). As part of the project's research activity, it will investigate suitable risk assessment methods. As a starting point to achieve this it will draw upon the findings from the projects that have been previously discussed. A specific contribution the project will make relates to the simulation and modelling of attack scenarios, which can be used to understand the potential physical impact of a cyber-attack on the smart grid. At the time of writing, the project is investigating existing tools that can be used to simulate communication networks, e.g., OMNeT++ (http://www.omnetpp.org), and power systems, e.g., GridLAB-D (http://www.gridlabd.org/). The goal is to combine these tools and develop suitable models that simulate attack behaviour, for example. Furthermore, the project will seek to develop models that can be used to analyze the impact that tampering with measurement signals have on the control algorithms that will be realized for the smart grid. This activity will build on previous research carried out in the EU-funded Viking project, which investigated this issue for transmission systems [24]; an initial study is seeking to learn what will be the important control algorithms for the smart grid.

An overview of how these projects address the different challenges that are outlined in Section 3 is presented in Table 3. A further aim of the SPARKS project is to develop an overarching risk as-

sessment framework that can be used to address these challenges, drawing on results from the aforementioned initiatives. A starting point for reaching this objective will to examine the SGIS toolbox – a risk-driven approach to incorporating security into a use case analysis framework – which is described in the CEN-CENELEC-ETSI Smart Grid Coordination Group's *Smart Grid Information Security* documentation [11].

Table 3 Overview of the major contribution of the different initiatives with respect to the challenges outlined in Section 3. SS – Managing Safety and Security Risks, CP – Analyzing Cyber-physical Risks, LS – Understanding the Risks to Legacy Systems, CO – Complex Organizational Dependencies, CE – Understanding Cascading Effects.

Project Name	SS	CP	LS	CO	CE
Smart Grid Security Guidance $(SG)^2$			✓		
EMC^2	✓				
HyRiM					✓
SECCRIT				✓	
SPARKS		✓			

5. Conclusion

Future power grids will have to cater for many new requirements that can only be met through the support of a comprehensive ICT infrastructure. This changes the significance of cybersecurity issues: while safety and reliability aspects have been in the focus of security considerations for power grids so far, risks emerging from cybersecurity attacks must be considered in the future as well. However, cybersecurity risk management in smart grids is not a straightforward matter. ICT-focused risk frameworks cannot be readily applied to smart grids, due to their cyber-physical nature. While smart-grid-specific security recommendations do exist, they often fail to understand the particular challenges related to cybersecurity risk assessment in smart grids, such as the interrelation of safety and security risks, the mix of legacy and novel systems, or the potential of cascading effects. These challenges are currently being addressed in various research projects. The common goal of these efforts is to support smart grid stakeholders in understanding and assessing vulnerabilities and cybersecurity threats in smart grids, and to provide guidance on effective risk management by integrating cybersecurity and power systems security assessment approaches.

References

[1] NIST, Smart grid cyber security strategy and requirements, NISTIR 7628.
[2] ENISA, Inventory of risk management/risk assessment methods and tools http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory.
[3] Federal Office for Information Security (BSI), IT Baseline Protection Catalogs, http://www.bsi.bund.de/gshb, 2013.
[4] NERC, Security guidelines for the Electricity sectors: vulnerability and risk assessment.
[5] ISA, Security for industrial automation and control systems: concepts, terminology and models.

[6] IEC62443-2-1, Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program.
[7] NIST, NISTIR 7628 – Guidelines for Smart Grid Cybersecurity, 2013.
[8] ENISA, Appropriate security measures for smart grids, Dec 2012.
[9] A Reference Security Management Plan for Energy Infrastructure. Prepared by the Harnser Group for the European Commission under Contract TREN/C1/185/200. 2010. Available at http://ec.europa.eu/energy/infrastructure/studies/doc/2010_rsmp.pdf.
[10] CEN-CENELEC-ETSI Smart Grid Coordination Group, Reports in response to Smart Grid Mandate M/490, 2012.
[11] CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Information Security, December 2013.
[12] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen: Smart attacks in smart grid communication networks, Communications Magazine, IEEE, vol. 50, no. 8, pp. 24–29, August 2012.
[13] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu: Securing smart grid: cyber attacks, countermeasures, and challenges, IEEE Communications Magazine, vol. 50, no. 8, pp. 38–45, August 2012.
[14] Tyler, Brian, Crawley, Frank & Preston, Malcolm (2008). HAZOP: Guide to Best Practice (2nd Edition ed.). IChemE, Rugby. ISBN 978-0-85295-525-3.
[15] Department of Defense: MIL STD 1629A, Procedures for Performing a Failure Mode, Effect and Criticality Analysis, November,1980.
[16] Shawn Hernan, Scott Lambert, Tomasz Ostwald, Adam Shostack, Uncover Security Design Flaws Using The STRIDE Approach, MSDN Magazine, November, 2006.
[17] Bruce Schneier, Attack Trees, Dr. Dobb's Journal, December, 1999.
[18] David J. Mahar and James W. Wilbur, Fault Tree Analysis Application Guide, Reliability Analysis Center, 1990.
[19] ENISA, Smart grid threat landscape and good practice guide, Dec 2013.
[20] Christoph Schmittner, Thomas Gruber, P.P., Schoitsch, E.: Security Application of Failure Mode and Effect Analysis (FMEA). 33rd International Conference on Computer Safety, Reliability and Security (SafeComp) 2014 (September 2014), (in press).
[21] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Bacşar, and Jean-Pierre Hubaux. Game theory meets network security and privacy. ACM Computing Surveys. 45(3), July 2013).
[22] Saray Shai and Simon Dobson. Coupled adaptive complex networks. Physical Review E 87(4). April 2013.
[23] Jerry Busby, Lucie Langer, Marcus Schöller, Noor Shirazi, Paul Smith .Deliverable: 3.1 Methodology for Risk Assessment and Management. December 2013. Available online at: https://www.seccrit.eu.
[24] György Dán, Henrik Sandberg. Stealth attacks and protection schemes for state estimators in power systems. 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm). Gaithersburg, Maryland, USA, October 2010, pp. 214 – 219.

A Survey of Control Strategies Applied in Worldwide Microgrid Projects

Yi Guo, Vienna University of Technology, guo@ea.tuwien.ac.at
Wolfgang Gawlik, Vienna University of Technology, gawlik@ea.tuwien.ac.at

Abstract **–** A growing amount of distributed energy resources are integrated into the medium and low voltage level. This does not only bring a series of benefits, but also causes severe problems in power systems. The technologies of microgrids, including their architecture, distributed generation, storage, and control schemes, are widely researched across the globe, because of the increasing requirement of power quality and reliability and security of energy systems. This paper, focused on the technologies of operation systems and available control approaches, illustrates the review of diverse research projects and activities of microgrids around the world. It presents existing microgrid projects in Europe, America and Asia. It also illustrates the current state of control strategies and the correlation between volatile distributed generation and storage systems, and between loads and storage systems.

1. Introduction

To improve the reliability and security of electrical power systems and the power quality, as well as to decrease greenhouse gas emissions, the concept of microgrids (MG) has been introduced. The MG is a decentralized electricity network comprising distributed generators (DG), such as wind, photovoltaic (PV), biomass and diesel generation, local loads, and energy storage systems that can operate in grid-connected or island mode.

The most compelling characteristic of a MG is that it has the possibility to separate itself from the utility network when faults occur either in the overall grid or in the local network, and when the fault is cleared, the MG can reconnect to the utility grid. Distributed power generators are typically located closer to the side of consumers than centralized power plants. The energy then can be generated and stored near the consumption points, which can improve the stability and reduce the losses caused by large power lines [1].

2. State-of-the-art

While an increasing amount of distributed energy resources (DERs), i.e. decentralized generation capacity and decentralized energy storage, are integrated into overall grids, it is important to develop a safe and efficient control technique for the MGs operation. The control strategies of MGs face a series of challenges. This section introduces some existing control strategies.

2.1 Centralized control

A hierarchical control structure consists of a MG central controller (MGCC), which controls all the components of the MG, and local controllers (LC). The local controllers provide the locally measured data to the MGCC and receive instructions from the MGCC, such as setting points of voltage, active and reactive power. This centralized control concept was applied in large utility power systems for years to control the frequency of a large-area electrical network and has been applied to MGs for voltage and frequency restoration in the recent years [2]. An example of hierarchical control architecture is shown on the upper-left side in Figure 1.

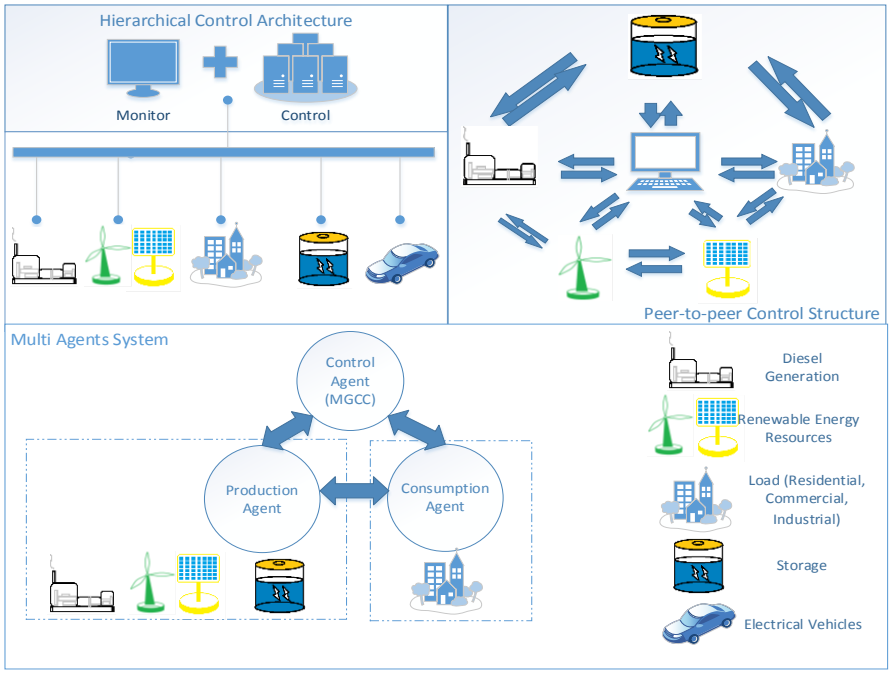


Figure 1. Hierarchical Architecture (Upper Left), Decentralized Control Structure (Upper Right) and the MAS (Bottom)

2.2 Decentralized control

Peer-to-peer control architecture was proposed by Piagi and Lasseter in [3] for the "plug and play" MG. In decentralized control, each microsource is equivalent, and no single component, such as the central controller or the central storage unit, is essential for the operation of the MG. A central controller may exist for the purpose of monitoring the system, but its presence is not necessary for the peer devices to operate. The MG can continue operating while any generator is connected or

disconnected, if the energy requirements are still satisfied [4]. The upper-right picture in Figure 1 shows a peer-to-peer control structure.

2.3 Multi agents System (MAS)

A multi agents system [5] is a compromised structure between the centralized control and entirely decentralized control structure. To some extent, agents, which can make decisions and commands without the MGCC, have autonomy, and they are able to communicate with each other to exchange information. Also, there is an agent acting as the MGCC in the MAS, coordinating local tasks and recording power exchanges between the agents periodically. The structure of the MAS is shown at the bottom in Figure 1.

3. Overview of Microgrid Projects

With growing interest in MGs, plenty of projects regarding the operation of MGs have been carried out worldwide. In this section, some surveyed MG projects are presented, and some of their characteristic features are compared.

3.1 Microgrid Projects in EU

3.1.1 Isle of Eigg, Scotland

The Isle of Eigg near the Scottish coast, with a population of about 100, was without grid electricity before 2008. In 2004, a hybrid renewable energy system was proposed and completed in 2008. The MG system comprises a 30 kWp PV system, hydro plants of 112kW, four 6kW wind turbines, and diesel backup capacity of 160 kW. It now provides power limited to 5 kW for households and 10 kW of electricity for businesses 24 hours each day. The decentralized control approach is applied in the system. The whole system can be automatically controlled by means of calculating the state of charge (SOC) of the batteries and controlling the power via the grid frequency [6]. This MG is an example of a MG that is constantly operated in the island mode without any external grid.

3.1.2 CESI RICERCA DER test microgrid, Italy

The pilot microgrid is connected to the medium voltage (MV) grid through an 800 kVA transformer. It includes various DG sources, energy storage systems, and several controllable loads. A Supervision and Data Acquisition System (SCADA), which provides remote monitoring and control of all the DERs and the controllable loads, is used for centralized control. [7]. This MG structure is an example of a MG test bed featuring several DER technologies.

3.1.3 The virtual microgrid in Eberstalzell

The virtual MG in Eberstalzell, a municipality located in Upper Austria, is investigated in the ongoing research project “SORGLOS” led by the Institute of Energy System and Electrical Drives, TU

Wien. While the project "SORGLOS" investigates the possibility and requirements of MG operation, it is currently not planned to actually operate the grid in island mode.
Eberstalzell is a municipality located in Upper Austria. The MG is connected to a 20 kV MV grid via one 630 kVA transformer. PV systems with total peak output of nearly 300 kWp are installed in the network. Due to the high volatility of PV systems in the virtual MG system, therefore a backup diesel generator and storage would be required. The maximum load demand is about 450 kW, and the annual energy consumption of this region is approximately 1,350 MWh. The MAS will be implemented in the virtual MG system. Technologies, like Power Line Communication (PLC), radio and cable & wireless communication, are considered to be used for the communication system.

3.1.4 Other projects in EU

Diverse MG projects for control optimization of operation are under development in EU, for instance, the commercial feeder of LABEIN located in Spain [8] with a certain level of ability to reconfigure will be used to test out both centralized and decentralized control schemes. MG systems with central battery storage systems, like flywheel, normally use centralized control architecture, for example, the University of Manchester Microgrid/Flywheel energy storage laboratory prototype, DeMoTec Microgrid, Germany [9], the MG in Bronsbergen Holiday Park, Zutphen, Netherlands [7], and a benchmark low voltage (LV) microgrid network [10]. There are also a large size MG on Bornholm island [11, 12] and EDP Frielas feeder, Portugal, only operating one microturbine with a capacity in excess of the maximum load demand [13] utilizing the centralized control strategy.
In medium and large MG systems, like the residential MG, with a ring configuration, of Am Steinweg in Stutensee, Germany [7], decentralized control approach was planned.
The MAS is implemented in a residential MG in Mannheim-Wallstadt, Germany [14, 15], for controlling the loads, monitoring the production and storage systems, as well as in the laboratory-scale test microgrid in the National Technical University of Athens, Greece [7], and the rural off-grid on Kythnos Island, Greece [16].

3.2 Microgrid Projects in America

3.2.1 Santa Rita Jail CERTS Microgrid Demonstration, USA

Santa Rita Jail is the fifth largest county jail of the USA, requiring around 3 MW of reliable and secure electricity 24 hours each day. The MG system, with high penetration of DGs, a storage system, and a power factor correcting capacitor bank, is a demonstration of CERTS microgrid concepts. In this MG system, a localized control scheme is implemented for each component [17]. Another demonstration of the CERTS testbed is CERTS American Electrical Power. [18].

3.2.2 Joint Base Pearl Harbor Hickam, USA

The MG system of Joint Base Pearl Harbor Hickam, USA, is developed for military application. The most important characteristic of a military MG, unlike other applications, is the energy security in comparison to the economical aspect and energy efficiency. This MG, includes two electrically isolated generators, which ensures that the system can be operated without renewable resources,

serves critical loads. A cyber-secure control system is used to achieve the seamless transition from or to the utility network. More military microgrid projects can also be found in [19, 20].

3.2.3 Other projects in the USA

The MG project of Allegheny Power, West Virginia Super Circuit intends to demonstrate the reliability benefits of the dynamic feeder reconfiguration across two adjacent feeders. The MAS and advanced wireless communication will be applied in the system [21].
Likewise in Europe, MG projects in the USA with battery energy storage systems at substations, such as the microgrid in the University of California, San Diego [22], SDG&E Borrego Springs Microgrid Demonstration Project [23] and Maui Smart Grid Project, Hawaii [24], and the Illinois Institute of Technology Perfect Power System Prototype equipped with Uninterruptible Power Supply (UPS) flywheels and batteries [25] use the centralized control architecture.

3.2.4 Research Projects in Canada

The MG projects in Canada are focused on the MV level and mostly implement hydro generation. The Hydro Boston Bar MG system and Hydro-Québec distribution system are prepared for planned islanding operation. Centralized control is used in the system [26]. The MG in the village of Hartley Bay, British Columbia, is an off-grid MG utilizing the centralized control technology [27].

3.3 Microgrid Projects in Asia

3.3.1 MG projects in Japan

Japan is the leader in MG demonstration projects. The New Energy & Industrial Technology Development Organization (NEDO) has started four demonstrations in 2003, namely, Hachinohe MG, Aichi MG, Kyotango MG and Sendai MG [7]. NEDO projects have a control target to maintain the operation of network between production and consumption over a certain period when errors occur. Meanwhile, many private MG projects, like Shimizu Corporation MG, Tokyo Gas Yokohama Techno Station MG, and Roppongi Hills, are carried out. From 2010, NEDO supported their first overseas Los Alamos MG project, and Albuquerque Building MG conducted in the USA [28] to research advanced technologies of DERs and energy security. All the listed MG projects in Japan with high penetration of DERs and a big amount of energy storage systems utilize the centralized control approach.

3.3.2 MG projects in China

The research of MGs in China, focusing on bulk DERs interconnection with the power system and the influence on the utility network, started around 2004. The MG research includes from laboratory-scale MG, like Microgrid testbed in Hefei University of Technology (HFUT), to medium and large scale MG, such as Tianjin eco-city Smart Grid Demonstration [29] and Turpan New District Sustainable Development City Project [30]. Since the foundation of microgrid technology in China is weak, it needs a long process to realize commercial operation, especially cooperating with national policies, laws and regulations.

4. Comparison of MG projects

The comparison between the power of maximum load demand and total installed capacity of DG sources in logarithm is presented on the left side in Figure 2. The surveyed MGs can be classified into three groups according to the maximum load demand as the following.

- Small Scale Microgrids: 1W < P_{load} < 30 kW
- Medium Scale Microgrids: 30 kW < P_{load} < 1 MW
- Large Scale Microgrids: P_{load} > 1 MW

From the picture, the majority of MGs have enough installed capacity of DGs for islanding without load shedding and the rest needs to be supported by the utility network for covering the full load. Among all the investigated MG projects, the installed capacity of the DG sources cooperated with the backup diesel generation and batteries are sufficient for the demand of consumers in the off-grid MG projects. Most of on-grid projects are able to use the DG sources to support their local loads, and some exceptions need to get the energy supply from the utility grid.

Existing control techniques have offered a lot of possibilities for the operation of MGs. Parameters like power quality and stability, installed storage capacity, requirement of a communication infra-structure, and types of installed distributed generators affect the choice of control strategies. The right picture in Figure 2 shows the percentage of the utilization of applied control strategies in the surveyed MG projects.

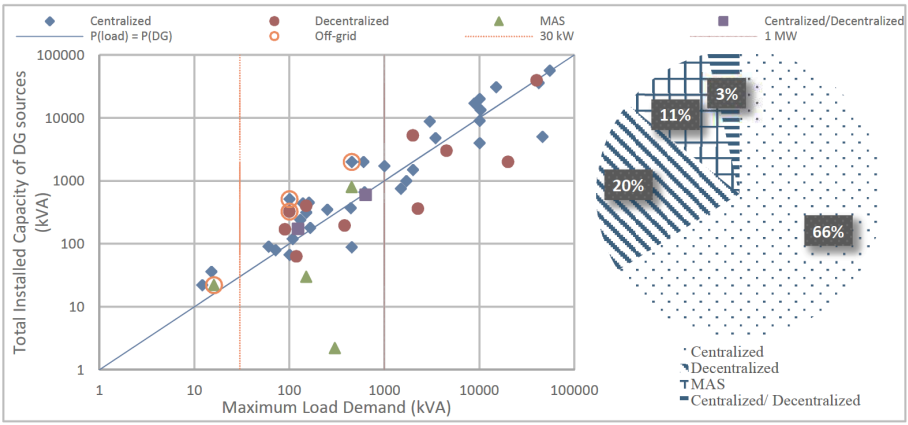


Figure 2. Comparison between the power of maximum load demand and total installed capacity of DG sources in logarithm (Left) and applied control strategies in the surveyed MG projects (Right) [Self-created]

The centralized control approach is widely adopted, when there is a central storage system in the MG, from the small scale MGs to the large scale MGs. The MAS is implemented mostly in the small and medium scale MGs, as long as there are controllable loads and controllable generation. The decentralized control technology is applied in medium and large MGs. For medium and large systems with complex grid structure, utilizing the decentralized control strategy is easy to achieve

the plug-and-play function of MGs and would not influence architecture and the communication structure of energy systems. There are also test fields, which have the ability to reconfigure, allowing to test out both centralized and decentralized control strategies for their systems.
The analysis of the correlation between volatile DG sources, like PV and wind power plants, and the storage capacity is also made based on the available data of the survey. The more volatile DG sources are installed, the larger the capacities of the storage systems are used, as it can be seen in Figure 3. Most storage can be fully charged within 6 hours and provide energy to the customers for at least one hour. In case of failure during the period, which is lack of volatile DG sources, those MGs would only last for a blackout of several hours, but surely not days.

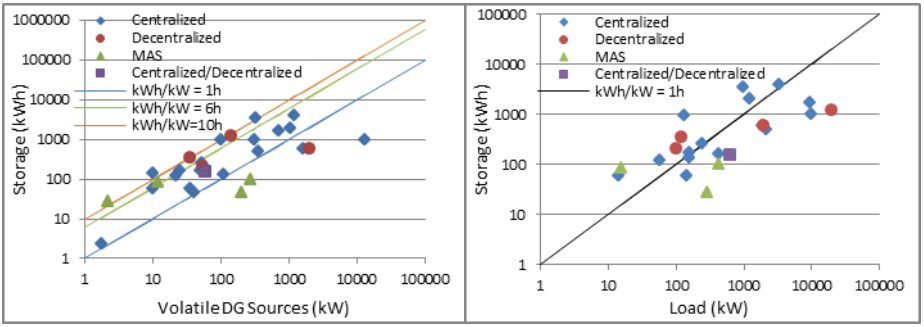


Figure 3. The correlation between capacity of installed volatile DG sources and storage (Left), the correlation between load demand and storage (Right) [Self-created]

5. Conclusions and Findings

Although there are differences among microgrid control structures, they all intend to ensure the reliability and security of networks when a plenty of DGs are integrated into utility grids. According to the surveyed MG projects, centralized control is currently dominant. In off-grid MGs, total installed capacity of DG sources usually exceeds maximum load demand, while in around 38% of on-grid MGs, load shedding would be necessary at a situation of reaching maximum load demand and depleted storage. Storage capacity rating related to installed volatile DG sources is usually between 1 and 10 kWh/kW. The data of MGs is collected and made into a summary table and is allowed for further research applications. Due to the page limit, it cannot be shown in the paper.

References

[1] Lasseter, R. H., et al. "The CERTS microgrid concept." White paper for Transmission Reliability Program, Office of Power Technologies, US Department of Energy (2002).

[2] Hou, Chaoyong, Xuehao Hu, and Dong Hui. "Hierarchical control techniques applied in micro-grid." Power System Technology (POWERCON), 2010 International Conference on. IEEE, 2010.

[3] Piagi, Paolo, and Robert H. Lasseter. "Autonomous control of microgrids."Power Engineering Society General Meeting, 2006. IEEE. IEEE, 2006.
[4] De Brabandere, K., et al. "Control of microgrids." Power Engineering Society General Meeting, 2007. IEEE. IEEE, 2007.
[5] Dimeas, Aris, and Nikos Hatziargyriou. "A multi-agent system for microgrids."Methods and applications of artificial intelligence. Springer Berlin Heidelberg, 2004. 447-455.
[6] Thim, Frank, Stratis Tapanlis, and Steve Wade. "CONCEPTION AND OPERATION OF A UNIQUE LARGE-SCALE PV HYBRID SYSTEM ON A HEBRIDEAN ISLAND."
[7] Lidula, N. W. A., and A. D. Rajapakse. "Microgrids research: A review of experimental microgrids and test systems." Renewable and Sustainable Energy Reviews 15.1 (2011): 186-202.
[8] http://www.microgrids.eu/index.php?page=kythnos&id=1
[9] Barnes, M., et al. "MicroGrid laboratory facilities." Future Power Systems, 2005 International Conference on. IEEE, 2005.
[10] Tsikalakis, Antonis G., and Nikos D. Hatziargyriou. "Centralized control for optimizing microgrids operation." Power and Energy Society General Meeting, 2011 IEEE. IEEE, 2011.
[11] Jorgensen, J. M., et al. "Ecogrid EU—A prototype for european smart grids."Power and Energy Society General Meeting, 2011 IEEE. IEEE, 2011.
[12] Østergaard, Jacob, and John Eli Nielsen. "The Bornholm Power System an Overview." (2008).
[13] Barnes, Mike. "Real-world MicroGrid-an overview." IEEE International Conference on System of Systems Engineering, San Antonio, USA, 2007. 2007.
[14] http://building-microgrid.lbl.gov/mannheim-wallstadt
[15] http://www.microgrids.eu/documents/661.pdf
[16] Chatzivasiliadis, S. J., N. D. Hatziargyriou, and A. L. Dimeas. "Development of an agent based intelligent control system for microgrids." Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE. IEEE, 2008.
[17] Alegria, Eduardo, et al. "CERTS Microgrid Demonstration With Large-Scale Energy Storage and Renewable Generation." (2013): 1-7.
[18] Eto, J., et al. "Overview of the CERTS microgrid laboratory test bed." Integration of Wide-Scale Renewable Resources Into the Power Delivery System, 2009 CIGRE/IEEE PES Joint Symposium. IEEE, 2009.
[19] http://www.apec-conf.org/wp-content/uploads/2013/09/is2.5.4.pdf
[20] http://der.lbl.gov/sites/der.lbl.gov/files/weir.pdf
[21] Hatziargyriou, Nikos, ed. Microgrids: Architectures and Control. John Wiley & Sons, 2013.
[22] http://www.sunspec.org/wp-content/uploads/2014/02/Sunspec-UCSD-Microgrid-final.pdf
[23] http://energy.gov/sites/prod/files/30_SDGE_Borrego_Springs_Microgrid.pdf
[24] http://www.hawaiicleanenergyinitiative.org/storage/media/4.HCEI%20Plenary%20Update_5.02.11_HNEI%20Maui%20Smart%20Grid.pdf
[25] Kelly, John F., Don Von Dollen, and I. L. Oak Brook. "The Illinois Institute of Technology Perfect Power System Prototype "." Grid-Interop Forum. Vol. 137. 2007.
[26] Asano, H., et al. "Microgrids: an overview of ongoing research, development, and demonstration projects." IEEE Power Energy Magazine (2007): 78-94.
[27] http://der.lbl.gov/sites/der.lbl.gov/files/Wrinch_2010.pdf
[28] http://www.ct-si.org/events/APCE2013/program/pdf/YasuhiroShimizu.pdf
[29] Wu, Xing, et al. "Research on Microgrid and its Application in China." Energy and Power Engineering 5.04 (2013): 171.
[30] http://der.lbl.gov/sites/der.lbl.gov/files/jeju_yu.pdf

Session 2

Projektberichte

29. September 2014
Eschenbachgasse 9, 1010 Wien
13:15 – 17:00

In der Nachmittagssession stellen eingeladene Vortragende aktuelle Ergebnisse aus laufenden Forschungsprojekten vor.

DG DemoNetz – Smart LV Grid: Rapid Prototyping vernetzter Smart Grid Regelungssysteme

Mario Faschang, Energy&IT–Forschungsgruppe am Institut für Computertechnik der Technischen Universität Wien, faschang@ict.tuwien.ac.at

Abstract – Der steigende Anteil an Einspeisung erneuerbarer elektrischer Energie aus verteilten Erzeugungsanlagen, sowie die zunehmende Integration volatiler Starklasten in Niederspannungsnetzen verursacht neue Herausforderungen zur Aufrechterhaltung der Versorgungssicherheit und Spannungsqualität. In den Feldtestgebieten des Forschungsprojektes *DG DemoNetz – Smart LV Grid* wird mit Hilfe intelligenter Regelungsansätze versucht, vorhandene Aktoren – wie Elektrofahrzeugladestation, Photovoltaik-Wechselrichter und Transformator-Stufensteller – so zu beeinflussen, dass eine Maximierung der Aufnahmekapazität für Photovoltaik und Elektromobilität ohne konventionellen Netzausbau möglich ist. Ein entscheidendes Element dieses Ansatzes ist neben den verteilten Sensoren und Aktoren das zentrale Regelungssystem. Die Entwicklung und Einführung solcher vernetzter Smart Grid Regelungssysteme ist eine neuartige Aufgabe für Verteilnetzbetreiber und Ingenieure. Diese Arbeit präsentiert den neuartigen Entwicklungs- und Einführungsprozess, der im Zuge des genannten Forschungsprojektes entwickelt wurde, sowie dessen Umsetzung.

6. Einleitung und Umfeld

Im kürzlich vorgestellten Österreichischen Sachstandsbericht Klimawandel 2014 [1] wird abermals die globale Erderwärmung in Verbindung mit dem fortwährenden Anstieg der Treibhausgaskonzentration in der Atmosphäre thematisiert. Mit 78 % verursacht die Nutzung fossiler Energieträger in Österreich den größten Anteil dieser Emissionen [1, S.74f]. Etwa die Hälfte dieses Anteils wird bedingt durch die energetische Umwandlung in Kraftwerken und durch den Verkehrssektor.
Das österreichische Forschungsprojekt *Smart LV Grid* (FFG 829867) der Projektgruppe *DG DemoNetz* zeigt in seinen Feldtestgebieten die Umsetzung technischer Möglichkeiten, um den Anteil elektrischer Energieversorgung aus, in Niederspannungsnetzen verteilten, solaren Erzeugungsanlagen zu maximieren, sowie Elektromobilität in diesen Netzen zu integrieren. Die Herausforderung dabei ist – ohne die Niederspannungsnetze konventionell und damit kostenintensiv auszubauen – diese mit einer großen Dichte hausgebundener Photovoltaik (PV)-Anlagen, sowie Ladestellen für Elektrofahrzeuge (EV) auszustatten. Diese zusätzliche Integration großteils einphasig angebundener Starklasten und Einspeiser verursacht Asymmetrien, sowie Schieflasten und kann aufgrund der fluktuierenden Charakteristik zu Verletzungen des Spannungsbandes nach EN 50160 [2] führen [3].

Um dem entgegenzuwirken, werden in den Niederspannungsnetzen Smart Meter als verteilte Sensoren [4], sowie aktiv steuerbare Aktoren zur Beeinflussung des Spannungsniveaus und des Leistungsflusses verbaut. Dabei handelt es sich konkret um unter Last schaltbare Stufensteller an den MV/LV-Ortsnetztransformatoren, steuerbare Elektrofahrzeugladestationen und PV-Wechselrichter mit adaptiver Wirk- und Blindleistungsanpassung [5]. All diese Aktoren sind, gemeinsam mit den Smart Metern angebunden an ein, dem Stromnetz überlagerten PLC-, TCP/IP-, und ModBus-basiertem Kommunikationsnetz. Zur koordinierten Ansteuerung dieser Netzelemente auf Basis der Messwerte aus dem Netz ist es nötig, zentrale Regelungssysteme zu entwickeln [6] und zu verbessern [7]. Diese kommen nun in den genannten Feldtestgebieten erfolgreich zum Einsatz.
Da es sich beim elektrischen Energieversorgungsnetz um kritische Infrastruktur handelt, ist es nicht möglich die Reglerentwicklung mittels Falsifikation („Trial and Error“) im realen Netz durchzuführen. Vielmehr ist es nötig, die neue Disziplin der Reglerentwicklung für vernetzte, aktiv gesteuerte Niederspannungsnetze nach dem „Divide and Conquer“-Paradigma in mehrere Schritte aufzubrechen. Das Ziel dieser koordinierten, schrittweisen Reglerentwicklung ist die stufenweise Reduktion des Risikos am Weg von der ersten Spezifikation und dem ersten Reglerentwurf bis hin zum fehlerfrei lauffähigen Regelungssystem im Feld.

7. Agiler Prozess für Rapid Prototyping des Regelungssystems

Die Reglerentwicklung für vernetzte Smart Grid Regelungssysteme ist aufgrund mehrerer Einflussfaktoren eine hochkomplexe Aufgabe. Dazu zählt die Tatsache, dass es aufgrund der Neuheit von Smart Grids und der Regelung verteilter Niederspannungsnetzelemente erst wenig Erfahrung gibt und es somit schwer ist, eine konkrete Spezifikation für den Regelansatz zu entwickeln, bzw. sich diese im Projekt- und Entwicklungsverlauf immer wieder ändert. Des Weiteren handelt es sich bei Smart Grids um komplexe Systeme von Systemen [9] die nur schwer ganzheitlich modellierbar sind. Teilweise sind eingebettete Sub-Regelungssysteme (z.B. in PV-Wechselrichtern), sowie andere zu berücksichtigende Domänen (Kommunikationsverzögerungen, Kopplungen zu anderen Energiesystemen) und implizite Abhängigkeiten (z.B. Leistung von Netzparametern) vorhanden, die kaum (formal) berücksichtigt werden können. Somit ist auch eine formale Verifikation der entwickelten Regelungsansätze, wie in der klassischen Reglerentwicklung üblich, unmöglich.

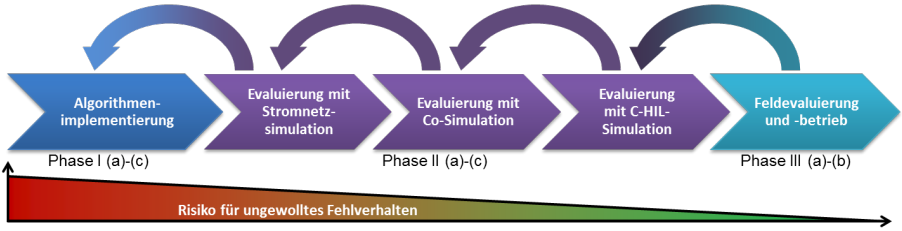


Fig. 1 Agiler Entwicklungsprozess zur Risikominimierung für vernetzte Smart Grid Regelungssysteme

All diese Herausforderungen führten zur Einführung des in Fig. 1 dargestellten agilen Entwicklungsprozesses für vernetzte Smart Grid Regelungssysteme. Er ist abgeleitet aus der agilen Softwareentwicklung (z.B. Scrum, Extreme Programming oder Feature Driven Development) und hat zum Ziel, mit möglichst geringem Aufwand das Entwicklungsrisiko zu minimieren. Dazu bietet der Prozess gegenüber den klassischen Entwicklungsmethoden (z.B. V-Modell) folgende Vorteile für komplexe Systeme mit variierenden oder unklaren Anforderungen:

- Für die erste Spezifikation muss nicht im Vorhinein das Verhalten des gesamten Systems (von Systemen) bekannt sein.
- Es kann früh ein erstes funktionales Regelungssystem ausgeliefert werden, welches
- nach kontinuierlicher Reflektion und Bewertung
- iterativ erweitert, angepasst und verbessert werden kann.
- Nachträgliche Änderungen können einfach berücksichtigt werden.

Der Entwicklungsprozess in Fig. 1 besteht grundsätzlich aus drei Phasen die üblicher-, jedoch nicht notwendigerweise von vorne nach hinten durchlaufen werden:

Phase I ist die Implementierungsphase. Sie besteht aus der Erstellung der ersten Spezifikation (Phase I-a) auf Basis des zu diesem Zeitpunkt verfügbaren System- und Expertenwissens und des gewählten Regelungsansatzes. Aufbauend auf der Spezifikation erfolgt die Entwurfsphase (Phase I-b) für den Regelungsalgorithmus (z.B. mittels UML-Struktur- und -Verhaltensdiagrammen, bzw. Struktogrammen). Anschließend folgt die eigentliche Implementierung (Phase I-c) in Programmcode.

Phase II ist die Evaluierungsphase. Ihre drei Sub-Schritte sind in Fig. 1 aufgrund ihrer Relevanz explizit dargestellt. Der erste Schritt der Evaluierung (Phase II-a) erfolgt nach Kopplung des Reglers mit einer Stromnetzsimulation. Dafür ist im Idealfall bereits ein Modell des Netzes vorhanden, in das das fertige Regelungssystem nach erfolgreicher Entwicklung ausgeliefert werden soll. Anschließend erfolgt die Evaluierung des Reglerverhaltens unter Berücksichtigung weiterer Umfeldeinflüsse (z.B. der Eigenschaften des Kommunikationssystems) in Phase II-b. Da hierbei eine Simulatorkopplung zur parallelen Simulation unterschiedlicher physikalischer Domänen erfolgt, spricht man von Co-Simulation [9]. Im letzten Evaluierungsschritt (Phase II-c) kommt bereits die Ziel-Hardware ins Spiel, auf welcher der entwickelte Regler nach einer erfolgten (Cross-)Kompilierung betrieben wird. Das so entstandene Regelungssystem wird nun ebenfalls mit der Co-Simulationsumgebung verbunden um das Verhalten der Regel-Software auf der Ziel-Hardware zu evaluieren. Man spricht dabei von Controller-Hardware-in-the-Loop (C-HIL) Simulation [10].
Ab dem ersten Schritt der Phase II ist ein Rücksprung in einen vorherigen Schritt bzw. die vorangegangene Entwicklungsphase des agilen Entwicklungsprozesses jederzeit möglich um die Spezifikation, den Programmcode oder Parameter des Reglers aufgrund von entdeckten Fehlern oder neuer Erkenntnisse anzupassen.

Phase III ist die Feldphase. Diese Phase ist die kritischste und wird erst nach umfangreicher Prüfung der Regler-Soft- und -Hardware (in Phase II) mit der Installation des Regelungssystems im Feld (z.B. im Ortsnetztransformator) begonnen (Phase III-a). Hierbei erfolgt zuerst ein Betrieb ohne Weitergabe der Steuerbefehle des Reglers an die Aktoren. Die Feststellung der fehlerfreien Übertragung der Messwerte aus dem Feld und deren Verarbeitung steht hier im Vordergrund. Die Regelschleife ist also nicht geschlossen – man spricht von einem Open-Loop-Betrieb (Phase III-b). Nach Prüfung der, durch das Regelungssystem auf Basis der Messwerte aus dem Feld erzeugten Steuerbefehle, wird der Open-Loop-Betrieb beendet und das Regelungssystem in den aktiven Betrieb (Phase III-c) versetzt.

8. Rapid Prototyping im Projekt DG DemoNetz – Smart LV Grid

Die drei Phasen des agilen Prozesses für Rapid Prototyping kamen im Projekt *DG DemoNetz – Smart LV Grid* erfolgreich zum Einsatz [11]. Die konkrete Umsetzung wird in den folgenden Unterkapiteln und den referenzierten Publikationen erläutert.

8.1 Anwendung der Phase I – Implementierung

Zu Beginn des Projektes wurde durch ein interdisziplinäres Konsortium bestehend aus Experten der Netzbetreiber, Forschungseinrichtungen und Industriepartner ein fünfstufiges Reglerkonzept erstellt [7]. Die Spezifikation sieht, wie von Einfalt et al. in [7] dargestellt, als einfachste Regelstufe eine unabhängige, lokale Regelung der einzelnen Aktoren (Transformator mit Stufensteller, PV-Wechselrichter und EV-Ladestationen) vor, um die Grenzwerte der EN 50160 nicht zu verletzen. Die zweite darauf aufbauende Regelstufe verwendet Messwertübertragungen von AMIS Smart Metern zum zentralen Regelalgorithmus um damit ggf. eine Stufenstellung am Transformator zu veranlassen. Als nächste Erweiterung der Regelstrategie werden in der dritten Ausbaustufe an die verteilten Aktoren (PV-Wechselrichter und EV-Ladestationen) mittels Broadcast-Nachrichten Stellbefehle (z.B. zur Beeinflussung des Bildleistungsverhaltens) ausgesandt. Die weiteren beiden Ausbaustufen erweitern den Regelansatz um individuelle Stellbefehle an Aktoren, sowie die Fähigkeit die Netztopologie in die Regelstrategie miteinzubeziehen. Die Implementierung selbst erfolgte anschließend mit MS Visual Studio in C++.

8.2 Anwendung der Phase II – Evaluierung

In der zweiten Entwicklungsphase erfolgt die Kopplung des zuvor implementierten Regelalgorithmus mit dem Stromnetzsimulator DIgSILENT PowerFactory um die grundlegende Funktionalität der Regelung zu evaluieren (vgl. Fig. 2). In DIgSILENT PowerFactory wurden für die Evaluierung die beiden relevanten Niederspannungsnetze (Eberstalzell und Köstendorf), sowie deren aktive Netzkomponenten modelliert. Zur Anbindung der entwickelten Regelalgorithmen an den Netzsimulator musste zuerst eine Software-Middleware (der Simulation Message Bus – SMB) zur Kopplung mehrerer Simulationseinheiten [12], sowie ein Interface dazu für DIgSILENT PowerFactory [13] entwickelt werden. Mit Hilfe dieser Middleware und der Schnittstelle ist eine Anbindung der Regelalgorithmen an den Stromnetzsimulator wie in Fig. 2 dargestellt möglich. Durch den nachrich-

tenbasierten Austausch von Spannungsmesswerten und Steuerbefehlen zwischen der Netzsimulation und dem Regler kann eine erste Evaluierung des Verhaltens angestellt werden.

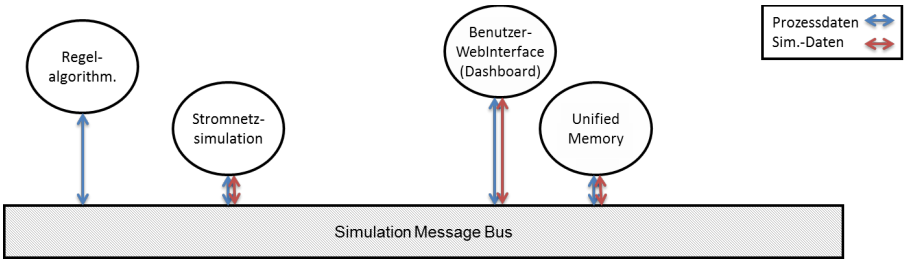


Fig. 2 Simulationsmodule zur Evaluierung der entwickelten Regelalgorithmen durch Kopplung an einen Stromnetzsimulator (Phase II-a)

Die Übertragung der Messwerte und der Steuerbefehle der komplexeren Regelalgorithmen erfolgt über einen schmalbandigen PLC-Kanal. Um dessen Auswirkungen auf das Regelverhalten ebenfalls in die Analyse miteinfließen zu lassen, wurde das Evaluierungs-Setup um eine Kommunikationsnetzsimulation zur Co-Simulation erweitert (Phase II-b – siehe Fig. 3). Das Modell des Kommunikationskanals basiert auf statistischen Auswertungen von Nachrichtenübertragungen der realen Netze. Für den Betrieb der Co-Simulation ist eine Simulationssteuerungs- und Koordinationseinheit entwickelt worden, welche die Simulatoren im Sekundentakt synchronisiert und unterschiedliche zuvor definierte Testfälle an die Simulatoren sendet. Das Benutzer-Webinterface dient ebenfalls zur Simulatorsteuerung, sowie zur Überwachung der Simulation. Alle Simulationsdaten werden in einer Speichereinheit (dem Unified Memory) für den späteren Export und die Auswertung abgelegt.

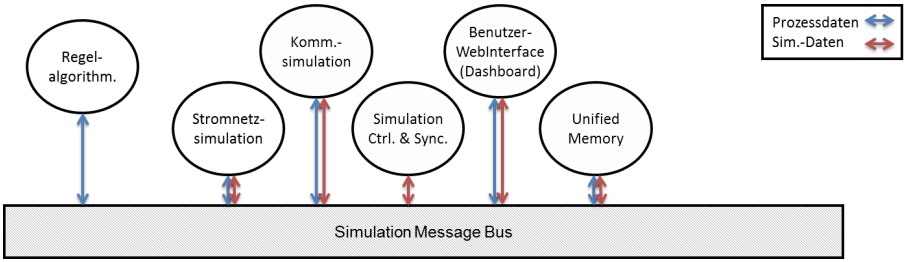


Fig. 3 Simulationsmodule zur Evaluierung der entwickelten Regelalgorithmen durch Kopplung an einen Stromnetzsimulator und eine Kommunikationssimulation (Phase II-b)

Der letzte Schritt der Entwicklungsphase II unterscheidet sich grundlegend von den beiden vorangegangenen, da hier der Regelalgorithmus nicht mehr auf dem Entwicklungs- bzw. Simulationssystem betrieben wird, sondern nach erfolgter Kompilation auf die Regel-Hardware, einem Unix-Industrie-PC, übertragen wird, um damit via TCP/IP-Sockets zum Co-Simulationssystem verbunden zu werden (vgl. Fig. 4). Die dadurch entstandene Controller-Hardware-in-the-Loop Evaluierung [10] liefert einen wesentlichen Beitrag zur Risikominimierung im Entwicklungsprozess.

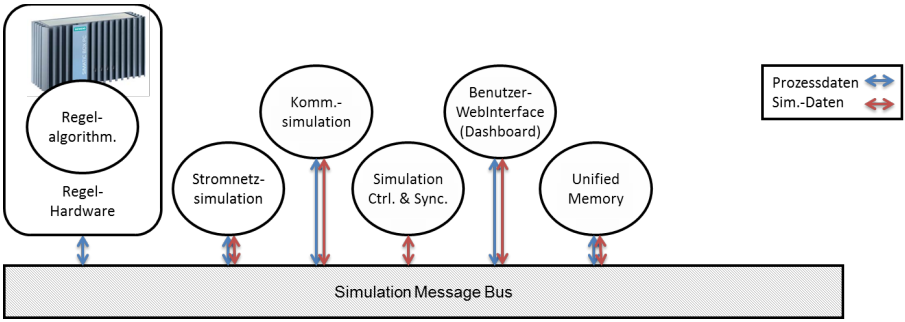


Fig. 4 Regel-Hardware und Simulationsmodule zur C-HIL-Evaluierung des entwickelten Regelungssystems durch Kopplung an einen Stromnetzsimulator und eine Kommunikationssimulation (Phase II-c)

8.3 Anwendung der Phase III – Feldeinsatz

Nach der erfolgreichen ausführlichen Evaluierung der Eignung des entwickelten Regelungssystems mittels Strom- und Kommunikationsnetz-Co-Simulation, sowie der C-HIL-Evaluierung erfolgt die Installation und der Betrieb in den Feldtestgebieten. Die Anbindung des Regelungssystems ist in Fig. 5 dargestellt. Aufgrund der geschickten Wahl der Schnittstellen und der plattformunabhängigen Architektur der SMB-Middleware ist die Portierung mit sehr geringem Aufwand möglich. Das Grund-Setup – mit SMB, Regelalgorithmen, Benutzerinterface und Unified Memory – bleibt bestehen und wir lediglich nicht mehr auf dem Entwicklungs- bzw. Simulationssystem betrieben, sondern direkt auf der Unix-Ziel-Hardware. Die simulierten Komponenten (Strom- und Kommunikationsnetz) werden ersetzt durch einen IEC 60870-5-104 Kommunikations-Stack, der als Field Automation Gateway fungiert und damit die Kommunikation zu den Feld-Komponenten aufbaut. Bevor das Regelungssystem in Produktivbetrieb (Closed-Loop) geht, werden seine Stellbefehle mit Hilfe des Web-Interfaces im Open-Loop-Betrieb abgefangen und durch Experten überprüft. Dies ist der letzte Schritt zur Risikominimierung vor dem operativen Betrieb.

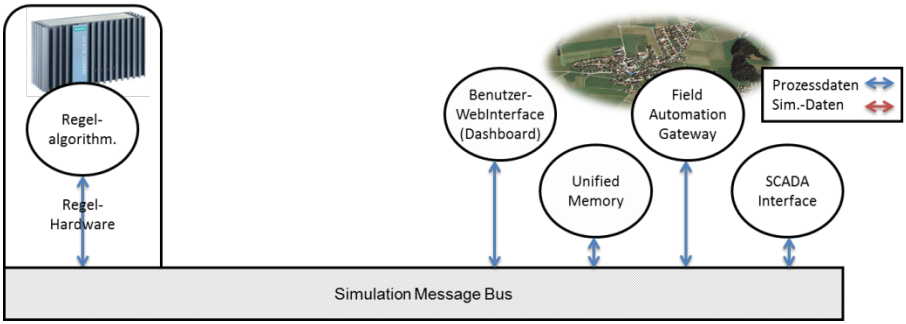


Fig. 5 Betrieb des entwickelten Regelungssystems (Regelalgorithmen auf Regel-Hardware) im Feld mit Anbindung von Senoren, Aktoren, SCADA-, Benutzer-Schnittstellen und Datenpersistierung

9. Zusammenfassung und Ausblick

Die Möglichkeit, die sich durch die Einführung von Smart Grids ergibt, aktiv in den Betrieb von Niederspannungsnetzen einzugreifen führt auch zur neuen Herausforderung adäquate Regelungssysteme zu entwickeln. Im Projekt *DG DemoNetz – Smart LV Grid* wurde erfolgreich ein solches mehrstufiges Regelungssystem für die Maximierung der Aufnahmekapazität von Niederspannungsnetzen für PV-Anlagen und Elektrofahrzeugen mithilfe eines agilen Entwicklungsprozesses entwickelt. Es hat sich gezeigt, dass speziell für solch eine komplexe Aufgabe, wie der Regelungssystementwicklung für cyberphysikalische Systeme, die Methoden der agilen Softwareentwicklung aus der Informatik ebenfalls zielführend angepasst und eingesetzt werden können. Um auch in Zukunft und für ähnliche Aufgabenstellungen schnell und mit geringem Risiko Regelungslösungen entwickeln zu können, ist die Verwendung normierter Schnittstellen für cyberphysikalische Modelle, Simulatoren und andere Co-Simulationswerkzeuge nötig. Auch könnte die Aufnahme des Entwicklungsprozesses in abstrahierter Art und Weise als (High-Level)-Use-Case im SGAM-Modell eine einheitliche Sicht und Vorgehensweise für diese Aufgabenstellung fördern.

Danksagung

Das Forschungsprojekt *DG DemoNetz – Smart LV Grid* ist Teil des Forschungs- und Technologieprogramms Neue Energien 2020 und wird gefördert durch den Österreichischen Klima- und Energiefond.

Referenzen

[1] Kromp-Kolb, H., N. Nakicenovic, R. Seidl, K. Steininger, B. Ahrens, I. Auer, A. Baumgarten, B. Bednar-Friedl, J. Eitzinger, U. Foelsche, H. Formayer, C. Geitner, T. Glade, A. Gobiet, G. Grabherr, R. Haas, H. Haberl, L. Haimberger, R. Hitzenberger, M. König, A. Köppl, M. Lexer, W. Loibl, R. Molitor, H. Moshammer, H-P. Nachtnebel, F. Prettenthaler, W. Rabitsch, K. Radunsky, L. Schneider, H. Schnitzer, W. Schöner, N. Schulz, P. Seibert, S. Stagl, R. Steiger, H. Stötter, W. Streicher, W. Winiwarter (2014): Synthese. In: Österreichischer Sachstandsbericht Klimawandel 2014 (AAR14). Austrian Panel on Climate Change (APCC), Verlag der Österreichischen Akademie der Wissenschaften, Wien, Österreich.

[2] EN 50160, Voltage characteristics of electricity supplied by public electricity networks, March 2011, CENELEC

[3] B. Bletterie, S. Kadam, M. Stifter, A. Abart, R. Pitz: "Optimisation of LV networks with high photovoltaic penetration - balancing the grid with smart meters"; in: "IEEE Powertech 2013", IEEE, Grenoble, Frankreich, 2013.

[4] M. Stifter, P. Palensky, "Smart Meter Data as a basis for Smart Control in Low Voltage Distribution Networks," in Proc. IEEE International Symposium on Industrial Electronics (ISIE), May 2013

[5] M. Heidl, C. Winter, B. Bletterie, A. Abart: "Advanced Grid Features - Lokale und ferngesteuerte Funktionen in PV-Wechselrichtern zur besseren Netzintegration"; Vortrag: Proceedings IEWT, Wien; 12.02.2013 - 15.02.2013; in: "Proceedings IEWT", TU Wien, (2013).

[6] Kupzog, F.; Brunner, H.; Prüggler, Wolfgang; Pfajfar, T.; Lugmaier, Andreas, "DG DemoNet-Concept - A new Algorithm for active Distribution Grid Operation facilitating high DG penetration," Industrial Informatics, 2007

5th IEEE International Conference on , vol.2, no., pp.1197,1202, 23-27 June 2007, doi: 10.1109/INDIN.2007.4384946

[7] Einfalt, A; Kupzog, F.; Brunner, H.; Lugmaier, A, "Control strategies for smart low voltage grids — The project DG DemoNet — Smart LV Grid," Integration of Renewables into the Distribution Grid, CIRED 2012 Workshop , vol., no., pp.1,4, 29-30 May 2012, doi: 10.1049/cp.2012.0824

[8] IEEE Smart Grid, Smart Grid Conceptual Model, http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model (besucht am 21.09.2014)

[9] F. Kupzog, P. Dimitriou, M. Faschang, R. Mosshammer, M. Stifter, F. Andren: "Co-Simulation of Power- and Communication-Networks for Low Voltage Smart Grid Control"; Vortrag: D-A-CH-Konferenz Energieinformatik 2012, Oldenburg; 05.06.2012 - 06.06.2012.

[10] M. Faschang, A. Einfalt, R. Schwalbe, R. Mosshammer: "Controller Hardware in the Loop Approaches Supporting Rapid Prototyping of Smart Low Voltage Grid"; Innovative Smart Grid Technologies Europe (ISGT EUROPE), 2014 5th IEEE/PES (to be published)

[11] Faschang, M.; Kupzog, F.; Mosshammer, R.; Einfalt, A, "Rapid control prototyping platform for networked smart grid systems," Industrial Electronics Society, IECON 2013 - 39th Annual Conference of the IEEE , vol., no., pp.8172,8176, 10-13 Nov. 2013, doi: 10.1109/IECON.2013.6700500

[12] Mosshammer, R.; Kupzog, F.; Faschang, M.; Stifter, M., "Loose coupling architecture for co-simulation of heterogeneous components," Industrial Electronics Society, IECON 2013 - 39th Annual Conference of the IEEE , vol., no., pp.7570,7575, 10-13 Nov. 2013, doi: 10.1109/IECON.2013.6700394

[13] Stifter, M.; Schwalbe, R.; Andren, F.; Strasser, T., "Steady-state co-simulation with PowerFactory," Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2013 Workshop on , vol., no., pp.1,6, 20-20 May 2013, doi: 10.1109/MSCPES.2013.6623317

INTEGRA: The Possible Role of a Flexibility Operator in the Transition From Market Oriented to Grid Oriented Operation

Tobias Gawron-Deutsch, Siemens AG Österreich, tobias.gawron-deutsch@siemens.com
Alfred Einfalt, Siemens AG Österreich, alfred.einfalt@siemens.com

Abstract – Current approaches to operation of a low voltage smart grid usually differ between two states – market and grid oriented operation. In case of the first one, connected consumers and producers are unrestricted in their behavior as long as they meet the general grid connection conditions (e.g. maximum current "supervised" by the fuse). The latter one introduces the possibility to restrict operation for the grid operator. Thus, in case of grid quality problems measures like mandatory reduction of photovoltaic power generation can be used. This results in a hard transition from market to grid oriented operation. A possible approach to eliminate it is to introduce a new entity – the Flexibility Operator – that uses market mechanisms to stimulate grid friendly behavior. Thereby, red state measures are either avoided or delayed and a smoother transition from market to grid oriented operation is in effect.

1. Introduction

Sustainable regions and cities are using renewable energy sources to satisfy their energy demand. An important part play photovoltaic power generator that are installed on residential buildings. Together with local energy storages (e.g. dedicated batteries, electric vehicles) they supply the residential building with energy. Building energy management systems (BEMS) optimize power consumption in respect to forecasted generation, available storage capacities, and, in case of flexible pricing energy, costs are considered. The resulting load profile is very dynamic and can hardly be compared with a standard load profile due to its sensitivity to weather conditions and price signals. New technologies and components are necessary to integrate these smart buildings with their dynamic behaviors into a Smart Grid.

These new participants in the low voltage grid provide new possibilities for grid operation to the distribution system operator (DSO). In case of grid quality problems like voltage band violations the following measures were available: changing the tap-position of the transformer, reduction of consumption or production, and reaction of appliances to price signals (heating is delayed as long as

possible in high-price-situations). A BEMS as described above has to be able to integrate weather forecasts and has to have a model of the comfort zone demands of the residents. Based on this information a schedule is generated and adapted regularly. Thereafter, such a building can react to new situations and affordances.

In this new situation, two questions arise for a DSO: *How can we avoid problems in the reliable operation of the regional infrastructure by a flexible usage of available resources in the distribution grid? And how can this be motivated?*

The two aspects that are the core of these questions are:

a) Technical aspect: The distribution network must work correctly and provide the required power to the consumers at any time.
b) Economical aspect: The energy should be provided in the most efficient and most economic way.

The task for the DSO is to operate its low voltage grid in respect of these two – partly mutually exclusive – aspects. A grid with no technical restrictions for any kind of market oriented operation is not economical feasible due to oversizing and the resulting reserves. A grid specified regarding economical aspects from the DSO point of view only might interferes with the idea of using renewables as energy source for a sustainable city. A solution for this dilemma is to dimension the grid to be sufficient for most of the time and to introduce active and passive concepts that take place otherwise – the smart grid.

Similar to the two aspects, two different approaches to grid operation exist in current concepts: Market and grid oriented operation. In case of the first one, connected consumers and producers are unrestricted in their behavior as long as they meet the general grid connection conditions. For example, maximum current is enforced by a fuse at the connection point. The latter one introduces the possibility to restrict operation for the grid operator. Thus, in case of grid quality problems measures like mandatory reduction of photovoltaic power generation can be used. This type of operation interferes directly with internal processes and business models of the building operators.

In the traffic-light-model these two states can be mapped to the green (market oriented) and red (grid oriented) traffic light. For the yellow state different approaches exist. A straight forward implementation would be to use the same mechanisms as for the red state but with relaxed thresholds and measures.

As soon as the first threshold has been reached grid oriented operation is in charge. Recently, market based mechanisms have been introduced as a possibility for the yellow state. The grid operator provides incentives to the connected consumers and producers to stimulate grid friendly behavior.

The traffic light model of the Austrian Smart Grids Technology Platform (Figure 1, [1]) defines three roles that are necessary for such a market based yellow state: the Flexibility Operator (FlexOp), an object manager, and an automation system. A BEMS can incorporate both roles: the object manager and the automation system. In the green state the grid is in normal operation and unrestricted function of all market mechanisms is in place. The next state – Yellow – has the needs for optimization and market based optimization considering technical constraints are installed. Finally – in the red state – some limits are exceeded and local restrictions of market mechanisms are active limited in time. Further, the DSO can send priority signals to the automation unit directly to prevent further problems.

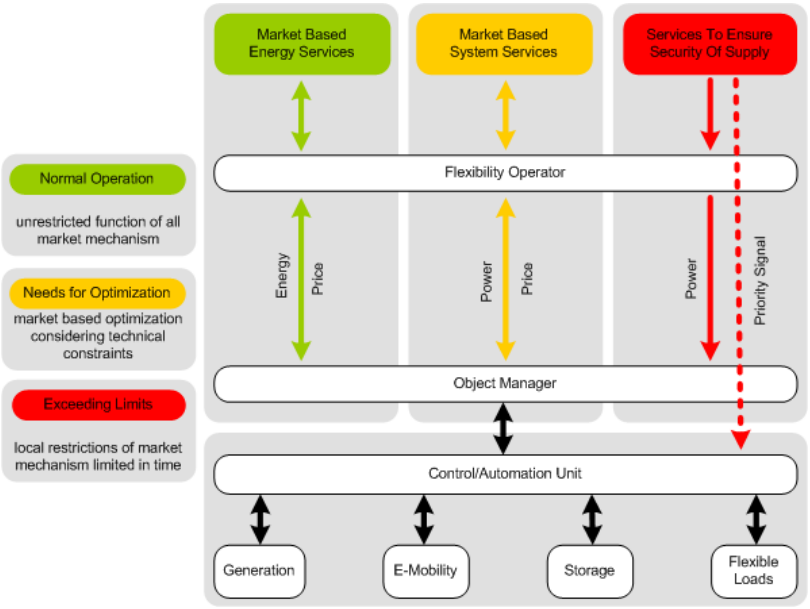


Figure 2 - Traffic Light Model from the TP Smart Grids Austria [1]

In [2] a concept for the yellow state is discussed. To motivate participation lower grid connection tariffs are offered. Further, an opt-out mechanism is defined to increase acceptance – customers can decline flex-requests. The grid operator has to be able to detect that a problem exists. Thus, monitoring is necessary; whereas forecast and prediction of future problems are not considered. A simple approach has been chosen as example: If the problem can be solved with registered „flexible customers" the grid state is yellow; otherwise it is red.

<table>
<tr><th></th><th>Green</th><th colspan="2">Yellow</th><th>Red</th></tr>
<tr><td rowspan="2">Planning phase</td><td rowspan="3">Neither yellow nor red</td><td colspan="2">Forecast detects red grid state at some point in the future.</td><td rowspan="3">Currently, some (or all) grid nodes are exposed to active power restrictions.</td></tr>
<tr><td>Yellow-Yellow
Offered flexibilities will be sufficient.</td><td>Yellow-Red
Offered flexibilities are insufficient to prevent red state.</td></tr>
<tr><td>Operative phase</td><td colspan="2">Flexibilities are called upon to prevent red grid state.</td></tr>
</table>

Figure 3 - Traffic Light Model for a Flexibility Operator [4]

A different concept has been developed in the public funded research project INTEGRA [3]. In a planning phase forecasts from connected smart buildings / BEMS are collected and integrated into a grid state estimation. If a future problem is predicted the FlexOp tries to reserve the necessary flexibilities. In case the problem occurs the operative phase is entered. Reserved flexibilities are called upon to prevent the red grid state. The two main differences are that participants can opt-in and the proactive behavior. Each customer can set the price and the amount for a flex-request; if no flexibilities are available for the period in question no offer will be set. If the forecast predicts a problem, the necessary amount of flexibility is bought from customers. The advantage is that more flexibility might be available – the customers can adapt their schedules in advance and not on a short term notice. Thus, customers and grid controller can use their resources more efficiently. A more detailed discussion of these two concepts can be found in [4].

2. The Flexibility Operator

The task of a FlexOp is to avoid red grid states with market mechanisms. To achieve this goal, it generates forecasts based on information provided sensors, smart meters, energy management systems, and external sources (e.g. weather forecast, information from the SCADA). For each identified problem an auction is opened and fitting candidates are invited to place their offer (amount of flexibility and price). Based on the problem description technical ideal candidates can be identified. No guarantees exist that they will participate in the auction (opt-in) or that they have the right amount of flexibilities available. Thus, "suboptimal" but still fitting candidates are invited as well. They might need to provide more flexibility to solve the problem. Nevertheless, they provide as solution for a certain price. Thereafter, inviting less optimal candidates from a technical point of view makes it more likely that the FlexOp can prevent a red grid state.

Distributed energy resources (DER) can be connected to the priority signal as described above if they are not connected to a BEMS to perform self consumption optimization or have to follow a schedule. DERs that are connected to a virtual power plant (VPP) and smart buildings that perform self consumption optimization and can react to external price signals are equipped with all necessary means to interact with a FlexOp in principle. On a long term base they are trading with the VPP/energy retailer (day-ahead) and intra-day they trade with the FlexOp using the same communication interface. The interaction between BEMS and FlexOp happen without humans-in-the-loop. The buildings operators and the DSO can parameterize their system in advance.

Reusing the existing infrastructure reduces the operation expenses for the building owners. Conceptually, the FlexOp detects problems infrequently; it aims at reducing peaks. Thereafter, the volume of bought flexibilities is small compared to regular trades between the buildings and a VPP. In case of very frequent problems grid enhancements might be more cost efficient. The FlexOp needs to pay more than the VPP to motivate buildings to participate in auctions. Note that the FlexOp is not participating in other markets. Its sole purpose is to avoid local grid problems. The relative few situations when the FlexOp is in concurrence to a VPP have to be compared with a system without a FlexOp. Here the problem can definitively not be avoided and the free trading between VPP and smart building is overruled by the red state.

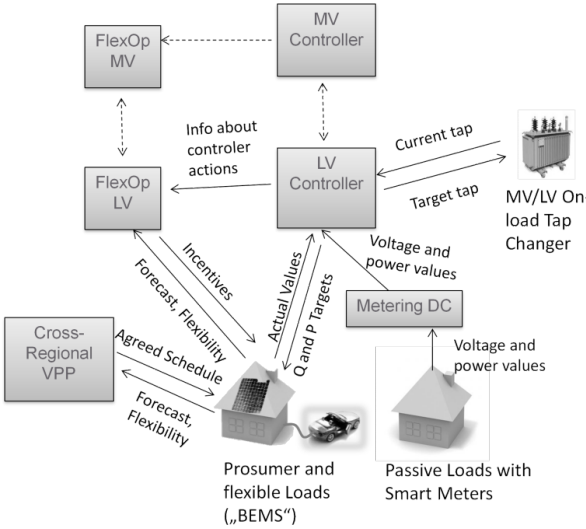


Figure 4 - System Architecture [5]

Figure 3 depicts the system architecture of a low voltage smart grid with a FlexOp. The low voltage controller [6] is responsible for the on-load tap changer transformer, collection of smart meter readings from passive loads/generators, and for red state measures like restricting generation of a prosumer. The prosumers and flexible loads are trading with cross-regional VPPs and the FlexOp. The correct operation of a FlexOp depends on many factors like working communication channels. This is mirrored by the fact that the low voltage controller is an independent instance from the FlexOp. Thus, even if the FlexOp cannot operate due to communication delays, the low voltage controller is fully functional.

The concept of the low voltage architecture can be extended towards the medium voltage level. The low voltage FlexOp acts towards the medium voltage FlexOp the same way as the smart buildings acts towards the low voltage FlexOp. One possible use-case would be that the medium voltage FlexOp helps the balancing group. Deviations in one low-voltage-feeder can be balanced by the other low-voltage-feeders that are connected to the same substation.

3. Example

In the following the concept of the FlexOp is discussed with the help of a simplified example. It consists of a small low voltage grid and excludes the low voltage controller and the cross-regional VPP.

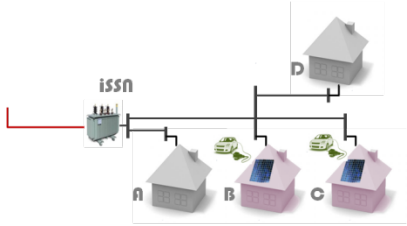


Figure 5 - Example Grid With one Intelligent Secondary Substation Node, two Regular Buildings and two Smart Buildings

The low voltage grid is depicted in Figure [4]. An intelligent secondary substation node supplies four buildings. Two of them are regular, passive consumers (A, D). Buildings B and C are smart buildings equipped at least with photovoltaic power generators and controllable heat pumps.
The example is placed at an arbitrary summer weekend. The tap position of the transformer is already on the highest level due to low medium voltage. Influence of the low voltage controller is now excluded. Day-ahead-weather forecast predicts undisturbed sunshine during the whole day. The BEMS of B and C come to the conclusion that they will be using the excess energy from the solar panels for the heat pumps at noon from 10:00 to 13:00. On Sunday morning at 9 a new weather forecast is available. It predicts a cloudy sky from 12:00 am to 13:00. As the heat pumps need to be operated anyway no change to their operation schedule is done by B and C. Nevertheless, they need the draw energy from the grid to fulfill their plans. The new schedules lead to a new grid state estimation for the timeslot at noon.

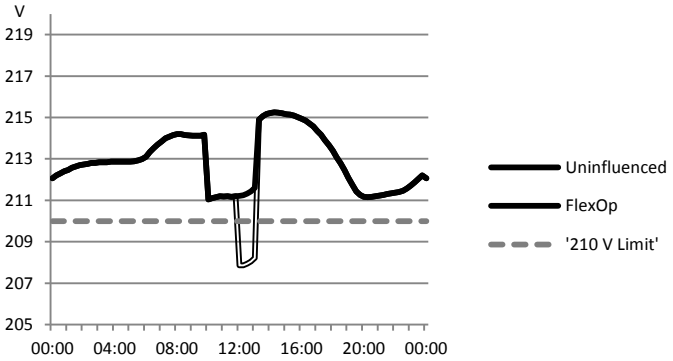


Figure 6 - Voltage at the Transformer

Without intervention of the FlexOp (see Figure 5 – uninfluenced curve) the voltage would drop below 210 V. Each connected building acts according to their connection conditions. Nevertheless, the overall system state would result in a red grid state and the priority signal would interfere with the planned heat pump usage.

Based on the generated forecast an auction is started at 9:15. The grid state estimation has identified the buildings B, C, and D as fitting. Buildings equipped with fitting infrastructure are invited to place their offer. Thus, building D is excluded from the auction. B is offering to shift heat pump usage to from 12-13 to 13-14 at a low price. The other building – C – is offering to reduce heat pump usage during 12-13 at a high price. Due to internal restrictions shifting is not possible and this could result in comfort loss for the residents. FlexOp closes the auction and accepts the offer from building B. B adapts its schedule and shifts the heat pump usage to 13-14. The result is not only less power drawn from the grid – there is even some generation overhead that can be fed back into the grid.
Overall, the voltage drop at the transformer level has been avoided by influence of the FlexOp (cp. Figure 5). The DSO was able to fulfill its task to guarantee grid quality, building B earned some money without interfering with comfort parameters, and the other three buildings were able to continue their market oriented behavior.

4. Conclusion

The discussed concept of a FlexOp provides a sound solution for a smooth transition from market to grid orient operation of a low voltage grid. By combination of "low-hanging-fruits" a powerful approach to the yellow state is possible from the technical as well from the economic perspective. Smart buildings need to be able to bargain with energy retailers/VPPs and they need to be able to make forecasts and schedules and to adapt them to new situations. Smart secondary substations need meter readings for their work in the red state – they can be used for state estimation as well. Rural areas usually have voltage problems, urban areas currency problems – for the latter some kind of grid state estimation is necessary. The step to integration all these components into the FlexOp is comparatively small.
The necessary incentives for the auctions don't need to be money. They can also be virtual credits that are defined in the contract. The connected building needs to earn a certain amount of credits per month and gets a reduced connection fee in return. This substitution results in predictable long-term costs for the DSO. Also reduced concepts like information based cooperation instead of auction based are possible. The problem with this approach is how to motivate building operators to participate.
A proof-of-concept for the example has been performed successfully. Thus, the technical possibility has been shown. The next task in project INTEGRA is to perform an economic feasibility study.

5. Acknowledgements

The presented work conducted in the SGMS INTEGRA project is funded and supported by the Austrian Klima- und Energiefonds (KLIEN) and the Austrian Research Promotion Agency (FFG).

References

[1] A. Lugmaier, H. Brunner, W. Prüggler, N. Glück, H. Fechner, F. Kupzog, "Smart Grid Roadmap Austria: „Der Weg in die Zukunft der elektrischen Stromnetze“", NTP Smart Grid Austria, 2010

[2] BDEW-Roadmap „Realistische Schritte zur Umsetzung von Smart Grids in Deutschland“, Bundesverband für Energie- und Wasserwirtschaft, Berlin, 11. Februar 2013

[3] Mattle, P., Neureiter, C., Kupzog, F. (2013): Projekt SGMS – INTEGRA: Übergang zu netz- und marktgeführtem Betrieb im Smart Grid. In Tagungsband ComForEn 2013, Vierte Fachkonferenz Kommunikation für Energiesysteme, OVE, Wien, 26. September 2013.

[4] T. Gawron-Deutsch, F. Kupzog, A. Einfalt, “Integration von Energiemarkt und Verteilnetzbetrieb durch einen Flexibility Operator”, e & i Elektrotechnik und Informationstechnik, Volume 131, Number 3, pp. 91-98, 2014

[5] T. Gawron-Deutsch, F. Kupzog, A. Einfalt, S. Ghaemi, „AVOIDING GRID CONGESTIONS WITH TRAFFIC LIGHT APPROACH AND THE FLEXIBILITY OPERATOR“, CIRED Workshop, Paper 0331, 2014

[6] A. Einfalt, A. Lugmaier, F. Kupzog, H. Brunner, "Control strategies for smart low voltage grids — The project DG DemoNet — Smart LV Grid," Integration of Renewables into the Distribution Grid, CIRED 2012 Workshop, 29-30 May 2012

Communication Protocols for virtual Power Plants
The eBADGE message bus

Alexander Lurf, cyberGRID, alexander.lurf@cyber-grid.com

Abstract – eBADGE is an EU funded FP7 project with the objective of proposing an optimal pan-European Intelligent Balancing mechanism, which is also able to integrate Virtual Power Plant Systems. This article compares several existing communication protocols and explores their usability as a universal standard for Demand Response both on Smart Grid and Market level and furthermore introduces the eBADGE data model and message bus. Currently, the data standards related to the field or end customer level communications and those related to the market level are completely different. For the communication between all the stakeholders in the pilot project a common eBADGE data model and encoding is being defined. The first version of the eBADGE message bus consists of a default RabbitMQ installation and a reference implementation of the eBADGE data standard. This data model will be continuously updated and refined within the course of the eBADGE project.

1. Introduction

The 3rd Energy Package clearly boosts the development of an Integrated European balancing mechanism. In this context, ACER[2] has in 2011 started the development of the Framework Guidelines on Electricity Balancing. It is expected from the ACER statements that Demand Response (DR) will play significant role in the future integrated balancing market allowing Virtual Power Plants (VPP), comprising Demand Response and Distributed Generation (DG) resources to compete on equal ground.

eBADGE is an EU funded FP7 project with the objective of proposing an optimal pan-European Intelligent Balancing mechanism, which is also able to integrate Virtual Power Plant Systems by means of an integrated communication infrastructure that can assist in the management of the electricity Transmission and Distribution grids in an optimized, controlled and secure manner.

In order to achieve the above overall objective the eBADGE project will have four objectives focusing on:

[2] Agency for the Cooperation of Energy Regulators

- Developing the following components: simulation and modelling tool; message bus; VPP data analysis, optimisation and control strategies; home energy cloud; and business models between Energy, ICT and Residential Consumers sector;
- Integrating the above components into a single system;
- Validating these in lab and field trials;
- Evaluating its impact.

This article compares several existing communication protocols and explores their usability as a universal standard for DR both on Smart Grid and Market level and furthermore introduces the eBADGE data model and message bus.

2. Communication Protocols

Currently, the data standards related to the field or end customer level communications and those related to the market level are completely different. The field level only started evolving with the Smart Grid initiatives, thus the standards are relatively recent and in line with modern software patterns and technologies. On the other hand, the market level is currently a mix of various legacy and more modern protocols, many of which are defined by individual software/system vendors rather than a standardization consortium.

2.1 Overview of existing standards

This section analyses the applicability of the most important existing standards to eBADGE. Unfortunately, as it turns out, no existing standard fits the requirements perfectly, thus any of them would have to be extended to the point of losing direct compatibility. Additionally, many of the existing standards are quite complex to implement, and it makes little sense to spend development time on implementation of large standards without the compatibility benefits. Finally, many smart grid approaches, data standards and middlewares are competing and it is far from certain which ones will prevail [1].

2.1.1 Smart Grid Data Standards (Examples)

- OpenADR, OpenADR 2.0
- Open Smart Grid Protocol
- OPC
- OPC UA

2.1.2 Energy Market Standards (Examples)

- IEC 60870-5-101, 60870-5-104
- IEC 61850
- Proprietary Market Interfaces

3. eBADGE data model

For the communication between all the stakeholders in the pilot project, such as a home energy hub - where metering data is collected, individual demand-response commands are sent, etc. - sending usage data to its VPP operator and receiving curtailment commands, or a TSO collecting balancing energy bids and sending activation commands when needed, a common eBADGE data model and encoding is being defined.

The required communication in the eBADGE pilot can be divided into multiple levels where different entities communicate:

- Energy resources, energy storage, smart meters, home energy hubs (gateways), VPPs, microgrids, DSOs, energy providers exchange messages with home energy usage profiles, VPP activation commands and similar,
- VPPs and other balancing service providers (BSPs), e.g. traditional generators, send bids to their TSO, who send activation commands back,
- In an international balancing market based on the TSO-to-TSO model, TSOs forward bids to a common merit order list and coordinate balancing energy allocation from this list.

No messages pass the level border (for example, the home energy hub never communicates directly with a TSO). Each higher level contains less message volume but must be more resistant to attacks and failures.

4. eBADGE message bus

The eBADGE message bus [2] has been built using off-the-shelf open source components and the message payload will be the eBADGE messages, as defined in the data model [3].

The best possible ways have been analysed to connect the stakeholders, either through direct stakeholder-to-stakeholder connection or through some kind of a proxy/message server. We found out that the latter option is preferable in order to meet the project goals within the foreseen development effort. Accordingly, multiple message bus technologies were evaluated both by consulting the literature and by conducting hands-on analysis using actual test messages as defined by the eBADGE data standard.

The following requirements have been enumerated for the communication software:

- Technical requirements:
  - High performance
  - Two-way communication through firewalls
  - Security
- Sustainability:
  - Open-source with commercial support available,

- Stability, as proven through a wide base of deployments and a large community, which also ensures that it will not go out of fashion and out of support prematurely,
- Lively community with active developers on all software layers.

The first version of the eBADGE message bus consists of a default RabbitMQ installation, an open source AMQP 0.9.1 implementation, and a reference implementation of the eBADGE data standard. The latter is implemented as a Python library that provides a two-way mapping between eBADGE messages and Python objects and a simplified AMQP-like API for sending and receiving messages. Together they provide an easy-to-use, high performance, secure, scalable and reliable message bus.

The Python library is publicly available under a free software license [4].

5. Next Steps

This data model will be continuously updated and refined within the course of the eBADGE project.

Firstly, certain features that have already been foreseen but are not essential for the development of first prototypes will be added, such as the ability to report non-electricity metering data (e.g. water usage, heat generation) or communication with additional types of entities (e.g. DSOs, energy providers).

Secondly, we will keep following the development of new and existing relevant standards. If a new standard emerges that covers our use cases very well or, more likely, an existing standard is updated in such manner, we will re-consider adopting it.

Finally, as the project progresses and the pilot is implemented, the data model will almost certainly need to be changed due to requirements that we were not able to be captured in the first year, both from the perspective of content (e.g., a previously unforeseen market mechanism may require additional message types) as well as from the technical perspective (e.g., potential decision for another type of message bus may require adding explicit sender and/or receiver fields to each message).

References

[1] Comparison of Demand Response Communication Protocols, Scott Coe, UISOL, http://canmetenergy.nrcan.gc.ca/renewables/smart-grid/publications/3045
[2] The eBADGE Message Bus – First Intermediate version, eBADGE project deliverable D3.2.1, September 2013.
[3] The eBADGE Data Model Report – First Version, eBADGE project deliverable D3.1.1, September 2013.
[4] https://dev.xlab.si/ebadge/ebadge-svn/wp3/message-bus/releases/1.0/

SmartWebGrid: User Acceptance of New Services of a Smart Grid IT Infrastructure

Sebastian Prost, AIT Austrian Institute of Technology, sebastian.prost@ait.ac.at
Marcus Meisel, Vienna University of Technology, meisel@ict.tuwien.ac.at
Manfred Tscheligi, AIT Austrian Institute of Technology, manfred.tscheligi@ait.ac.at

Abstract – The SmartWebGrid (SWG) project researched user interactions, technology, economic feasibility, as well as safety, security, and privacy of a universal information platform for future Smart Grid applications. The implemented proof-of-concept of the platform and selected use cases were evaluated with focus on user acceptance of private and business customers. The findings of the qualitative study with stakeholder workshops highlighted specific privacy concerns, acceptance considerations for the use cases, and an underlying distrust in current privacy protection measures. For increased acceptance of Smart Grid applications we give recommendations to better communicate benefits of Smart Grids, ensure privacy and transparency, give consumers freedom of choice, and create independent supervision authorities.

1. Introduction

Future Smart Grids applications will include considerably more explicit interactions between the power grid and its participants, such as consumers, energy producers, or electric vehicle users. This not only allows a more efficient use of available infrastructure, but also creates an active relationship between the power grid and its users. As part of the Smart Grid Modellregion Salzburg (SGMS), the SmartWebGrid (SWG) project [1,4,5] developed a platform for customers and third party service providers that enables such user interactions for various Smart Grid applications in a universal, interoperable, and secure way.

SWG researched user interactions, technology, economic feasibility, security, and privacy of such a platform. The SWG concept was implemented as a proof-of-concept for selected Smart Grid use cases and evaluated with private and business consumers. A central focus of the evaluation was privacy and trust and its relation to user acceptance [3]. In this paper we detail the SWG concept and use cases (Section 2), describe the evaluation procedure and findings (Section 3), and conclude with recommendations to increase user acceptance of Smart Grid services in the future (Section 4).

2. SmartWebGrid Concept

The SWG concept consists of two major components: The *SmartWebGrid core* that manages customer-data access and authenticity of third-party service providers, and five *use cases* that illustrate how potential service providers can integrate into the SWG core and provide valuable products and services after customers granted access to their data without sacrificing privacy at any point.

2.1 SmartWebGrid Core

The SWG core was designed and implemented in the SWG project by following the principles of security-by-design and privacy-by-design [2]. The architecture of the core allows customer data to remain at the local (decentralised) data source. However, it also allows third party service providers to access the data, but only as long as the customer actively grants this access (opt-in). Secure communication channels encrypting the transmitted data in transit, combined with a certificate authority providing authenticity to the registered service providers, are only two of the mechanisms of the SWG core to centrally manage data access. Figure 1 shows example apps offered on the platform and how users can customize access to optional data sources.

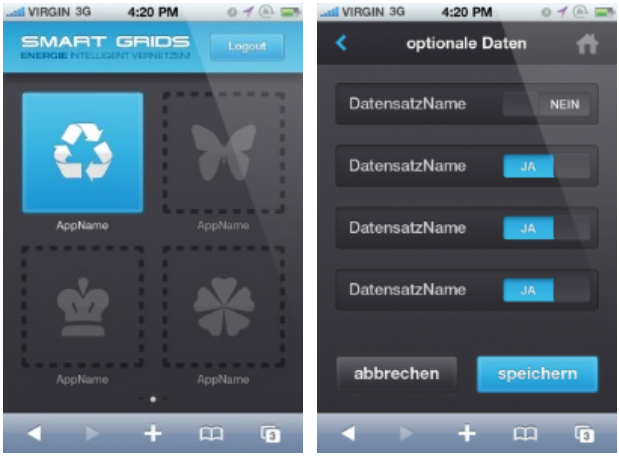


Figure 1. The SWG core provides a platform for service providers to offer their apps (left screen) and for customers to manage access to their data (right screen); courtesy of Salzburg AG.

New service providers can register their company, receive a certificate and access to available data descriptions (using Web Services Description Language files – WSDLs) to develop their services without viewing or manipulating any customer data. The third party company developers download the WSDLs of data sources they intend to use in their apps (e.g. weather, solar generation power level in 1 hour granularity, etc.) and develop against those definitions. To hand in their app, they log in with the company certificate at the SWG core, provide necessary app information (e.g. name, image, app URL, etc.), and receive a signed app certificate. Customers on the other hand browse the SWG platform, select apps from any provider and log in or register at a service provider offering

the app. At this point the mapping of customer information and offered services takes place in the background without revealing any privacy related data.

2.2 SmartWebGrid Use Cases

Five relevant use cases were identified and implemented as web applications: energy feedback, e-car charging, photovoltaic (PV) system monitoring, municipal energy balance feedback, and home automation. Figure 2 shows sample screenshots of each app.

Energy feedback: This app allows a customer to review electricity, gas, and water consumption across various time frames. The user can also view current usage and set upper limits. When an upper limit is reached, customers can be informed via app, e-mail, or SMS.

E-car charging: This app allows a user to control how his or her e-car is charged. It offers an economy and express type of charging with different pricing options. It also gives information on tariffs, charging stations nearby, the current charging level and the amount of CO_2 saved compared to a standard car.

PV system monitoring: This app allows the owner of a private PV system to review the daily power curve to see how much power is currently produced. It also includes weekly statistics and alarms that can be triggered for certain events.

Municipal energy balance: This use case represents the municipal energy monitoring developed in the SGMS project 'Modellgemeinde Köstendorf' in Salzburg, Austria. The app allows the inhabitants to view the current energy balance, which consists of PV production, general electricity consumption and e-mobility consumption. It also visualises the share of solar energy in the energy consumption and how much CO_2 could be saved by this.

Home automation: This app allows inhabitants of equipped homes to regulate room temperature, view sensor data (temperature, humidity, CO_2 concentration), and activate a so-called eco button. With one touch, the eco button turns off dedicated power outlets and reduces room temperature.

Opening an app is only possible through the SWG core, which presents customers with a privacy prompt that lists what data sources the app *must* access to provide basic functionality and what data sources the app *can* access on top of that to offer additional features (see Figure 1), before being redirected to using the app. Only at this point the app has received SWG core-granted access and directions to the data it requires to perform its service.

Figure 2. The apps implementing the SWG use cases, from left to right: a) energy feedback, b) e-car charging, c) PV system monitoring, d) municipal energy balance, e) home automation; a)-e) courtesy of Salzburg AG, e) courtesy of Siemens.

3. User Acceptance Evaluation

For evaluation of the user acceptance of the SWG core and the use cases three stakeholder workshops with potential users were conducted. Two groups of users were invited: private customers that use electricity in their household and business customers that use electricity for their small or medium-sized enterprise.

3.1 Method

We conducted two workshops with private customers (P1 and P2) and one workshop with business customers (B). The workshops took place in Vienna, Austria and lasted about 3.5 hours each. Participants received 50 € as compensation for their participation.

First we introduced participants to Smart Grids and the SmartWebGrid project. In particular we answered the questions of 'What is a Smart Grid?', 'Why do we need it?', 'What potential risks come along?' and 'What solutions does SWG provide to overcome these risks?' Following this, we conducted a brainstorming session about potential privacy risks in a Smart Grid. For each risk we identified what data is concerned, what would be the motivation to collect the data, and what threats this causes to an individual or a business. Next, we asked participants to subjectively rate whether they believe that the security and privacy measures implemented in SWG can solve the collected privacy problems.

In the second part of the workshop we presented the SWG use cases and the apps that implement them. In particular, we highlighted what data sources each app must and can access in the current implementation of SWG. Following each presentation, users were asked what type of data they would allow each app to access in which granularity. For example, we discussed if energy usage data should be available anywhere between real-time and a single yearly value. We also asked how likely it is that they would use each app.

In the third part of the workshop we played a so-called *innovation game.* Innovation games are a creative tool to uncover more subtle or unconscious aspects [6]. We chose the game 'my worst nightmare', which is particularly designed to address problems and negative aspects connected to a product or service. The task in this game was to draw the worst nightmare in connection to Smart Grids on a flipchart. This could be a person, a monster, or just a collection of characteristics. As an example, people were told, if this workshop was about a refreshment drink, in the nightmare this drink could make people vomit. Participants worked in groups of two or three for about 20 minutes and then presented their nightmare to the others. The audience was instructed to note down positive, negative, or surprising elements about the dream and discuss it afterwards. One particular aspect of the discussion was the question if SWG has the ability to prevent such nightmares.

In a concluding discussion benefits and disadvantages, as well as potential future use and costs were discussed.

3.2 Participants

In total 21 persons (9 female, 12 male) were recruited to participate in the workshops (9 in P1, 7 in P2, 5 in B). All participants were responsible for the topic of energy use and energy supply in their household or company. During recruitment participants we screened for their interest in the topic of energy and their interest in privacy. P1 included people that stated energy is an important topic for them; P2 included those who said it is not (that) important. All the participants in B said energy is important to them. In P1 and P2 a strong majority stated that privacy is important to them; in B, 3 of the 5 participants said it is not (that) important.

3.3 Findings

In this results section first we will outline present privacy concerns regarding Smart Grids and how participants perceived the ability of SWG to overcome them. Then we will discuss how participants perceived the SWG use cases, and finally present the innovation game 'my worst nightmare'.

3.3.1 Privacy Concerns and SWG Potentials

During the brainstorming of privacy concerns the following issues were identified:

- When is energy used? (presence/absence, holidays)
- How much energy and what type of energy is consumed or produced? (tariff, PV)
- When is how much energy used? (peaks)
- How is energy used across time? (statistics)
- What device is using energy?
- Where is energy used? (address, location)
- How does energy use compare with others?
- How is energy paid for? (banking details)

These concerns were then discussed in the light of the privacy protection measures implemented in SWG. Private customers expressed distrust in smart meters and private businesses (this includes the energy provider) to manage their data. They much rather trust the state or independent organisations. Furthermore they expressed concerns regarding manipulation and hacker attacks. They are also afraid of their personal data being sold to third parties to create personal profiles for targeted advertising, or being used to penalise them for overconsumption, or that low-income groups become second-class citizens. However, the possibility of variable tariffs was seen as having the potential to create more energy awareness and energy solidarity.

Privacy concerns were discussed in the light of a general distrust that is not restricted to Smart Grids, as privacy has not been addressed seriously enough in the past in other domains. For example, participants doubted that data they at some point agreed to share with a company is really deleted in case of revocation. Privacy measures without supervision were seen as pointless. Again, the state was seen as the required authority to control enforcement of privacy protection measures.

Business customers also pointed out the problem of transparent individuals, abuse, and hacker attacks. However, privacy measures of SWG were regarded as sufficient to protect them. They also expressed concerns that electricity prices will rise and certain old devices might be banned. Most important for business customers was the aspect of decentralised data storage. In particular they wanted to avoid that certain devices that constitute company secrets can be identified. Furthermore they highlighted the need to communicate potential risks so that customers can understand them to allow them to act accordingly.

3.3.2 Acceptance of the SWG Use Cases

The **home automation** use case received absolute acceptance. Additionally, the benefit of the **energy feedback** use case was clear to most participants and a future use seen as likely. Participants assumed saving potentials and increased energy awareness. Regarding **PV system monitoring** opinions were split. Some participants thought of the information as interesting and useful, but

others saw little benefit, as solar radiation can't be influence anyway. **Municipal monitoring** was seen interesting for comparing different regions, but deemed more relevant to local governments, not individual customers. The **e-car charging** use case was regarded as most hypothetical, which can be attributed to the fact that e-mobility is not yet a common form of transport. None of our participants was planning to buy an e-car in the near future. In case they would, the charging app was, however, seen as interesting, as they valued the option to charge the car economically.
The discussion on what data users would grant access to, showed that for private customers the real-time information is valuable, but is also seen as potential total surveillance. The risk to abuse data was seen as lower if data was much older, e.g. half a year old. Business customers stated that daily consumption feedback can be useful but risky, weekly feedback is more acceptable. Access to some specific data, such as e-car consumption data, name, address, and gender were regarded as too risky in terms of privacy. In general it can be summarised that participants rejected sharing data when the benefit was not immediately visible to them.
Regarding coverage of the costs of such as system, opinions were divided. Some stated that those customers who want such an infrastructure should pay for it. Others argued that the SWG core and its functionality should be free and customers could pay for additional services. In this case, the grid operators should carry the costs of the infrastructure, as they also enjoy benefits and savings.

3.3.3 Innovation Game: My Worst Nightmare

The innovation game revealed a number of topics that represent underlying concerns that are relevant to Smart Grids. The most common theme is that of decreased transparency on the side of corporations and increased transparency on the side of customers.
In Figure 3 (left) the transmission tower with many eyes illustrates this fear of surveillance and screening of private life impressively. Another topic that came up was the complete breakdown of the energy system. Connected with this is a fear of regress, as illustrated in Figure 3 (left) by a leaking fridge, a cold stove, and a dark city. Another important topic is abuse, sabotage and exploitation. This could be the "bad neighbour" that steals electricity as well as data theft by corporations and state organisations. However, even though participants had the explicit task to think of their worst nightmares, one group drew a balanced view, by pointing out environmental benefits due to reduced energy consumption (Figure 3 right).

Concluding, participants had the view that Smart Grids is a development they cannot stop anyway, but they want at least influence its direction to protect their privacy. The following quote illustrates this: "If the train is already running, one can at least steer it onto the right track."

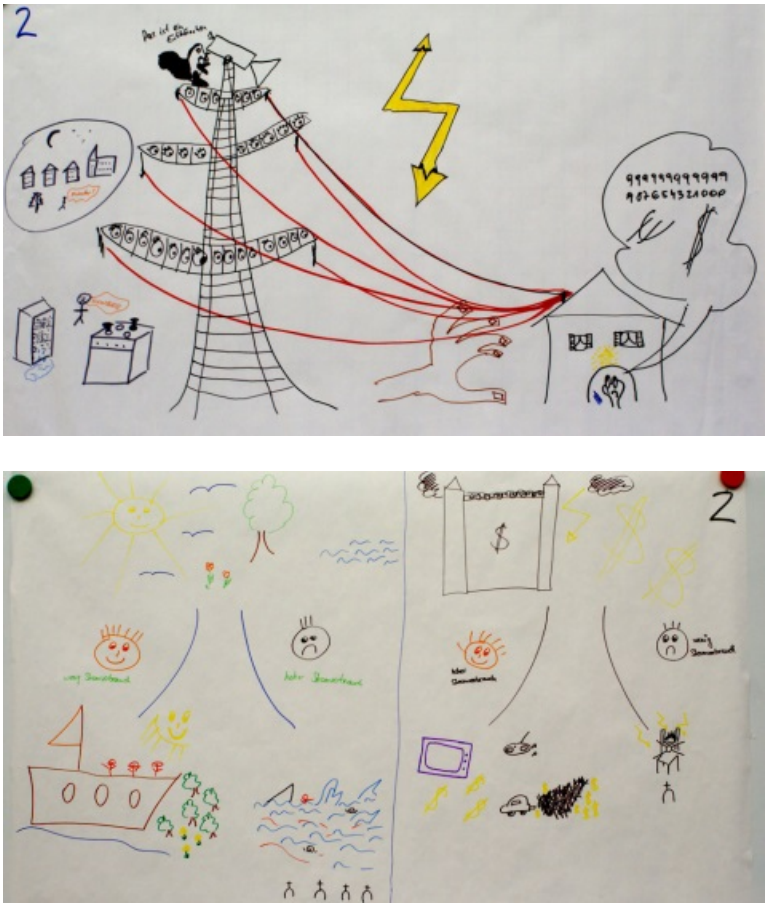


Figure 3. Examples of worst nightmares: A negative vision of surveillance and breakdown (left), and a more balanced vision that acknowledges environmental benefits (right).

3.4 Discussion

The results of the workshops highlight that trust-building actions and better communication are needed in order to improve acceptance of Smart Grids in the population. Participants were not fully aware of environmental benefits and possibilities to save costs. Furthermore, a lack of trust in current privacy protection measures became evident. Smart meters in particular are judged very sceptically. Additionally, the lack of transparency of how data is treated and who has access to it is criticised. Business customers expressed this concern even more so than private customers.

A second major point of criticism was the compulsory introduction of smart meters without asking the citizens. Participants expressed the willingness to participate in the design and creation of their

energy future. An important element for the future is the creation of independent supervision authority that ensures transparency for data security and privacy. This should also be understood as an appeal to the legislator. The solution developed in the SWG project can form a technological reference to build a Smart Grid infrastructure, deserving the trust and acceptance of the population.

4. Recommendations for Increased Smart Grid Acceptance

Based on the findings of the SWG evaluation, we can give the following recommendations to increase user acceptance of Smart Grids:

Communicate benefits: Benefits of Smart Grids for the end user, such as reduction of energy consumption and thus environmental protection, cost savings, or educational effects. There exists both a great lack of knowledge and at the same time great interest. Therefore, the benefits of Smart Grids should be communicated more clearly.

Ensure privacy: The apparent lack of trust in current privacy protection measures and the perceived risk of abuse of smart meters illustrate the need for better privacy protection. This includes building trust in those stakeholders that operate in the Smart Grid and creating transparency of the type and purpose of data collection. Only then the demands for data security and privacy in households and businesses can be met.

Give choice: The participants disliked in particular the idea of regulations "from outside" due to the obligatory introduction of smart meters. They showed willingness to participate in how Smart Grids take shape in their community or town. These collaboration aspects should be strengthened to enable citizens to make their own choices.

Create independent supervision authorities: Currently, trust in energy providers is rather low. Based on this we recommend to install supervision authorities and support citizens to develop trust in them. The authorities should be as independent as possible, and should have the power to prosecute violations against privacy. This, of course, also needs to be reflected in legislation.

The SWG project also developed a number of **other recommendations** that are based on technological, scientific, and economic considerations. We can only briefly mention them here; they are addressed in more detail in the final project report [1]. Technological recommendations include: following the principals of security-by-design and privacy-by-design, scalability, integration in to existing infrastructure, openness of the architecture, transparency, decentralised data storage, and state-of-the-art access control. Scientific recommendations include: the development of a holistic, standardised reference architecture, inclusion of additional privacy-enhancing technologies (PETs), public key infrastructures and digital certificates, as well as standardised authentication, authorisation, and data transmission. Economic recommendations include the creation of an open stakeholder exchange platform and specific recommendations for the use cases.

5. Summary and Conclusions

Summing up, the SWG evaluation revealed several areas of concerns in the public that potentially prevent wide-scale acceptance of Smart Grid infrastructure. The concerns include distrust in exist-

ing privacy protection measures that need to be addressed both technologically and organisational. Building on a strong technological basis, further action, such as independent supervision authorities can be enabled. Furthermore, the lack of trust and knowledge in the population needs to be addressed with transparent communication of both benefits and risks. Going beyond communication, users expressed the wish to participate in the creation of future Smart Grid solutions. Finally, future service providers in the Smart Grid need to carefully respect privacy and connect any access to customer data with a clear benefit for the customer.

User acceptance is critical for viable new services in a Smart Grid IT infrastructure. For further developments, the recommendations given in this paper can help to increase trust and acceptance in the Smart Grid. Future research has to explore how security and privacy can be enabled and communicated in a holistic Smart Grid architecture and should monitor how real-life, large-scale developments of Smart Grids affect user acceptance and trust.

Acknowledgements

SmartWebGrid has partly been funded by the Klima- & Energiefonds (FFG #829902) and the Smart Grids Modellregion Salzburg. We thank our project partners Salzburg AG and Siemens.

References

[1] M. Berger, T. Hofer, F. Judex, M. Jung, G. Kienesberger, M. Meisel, M. Pichler, S. Prost, W. Prüggler, K. Röderer; „Smart Grids Modellregion Salzburg - Konzeption eines Informationsmodells für webbasierten Zugriff auf Smart Grids Daten", Wissenschaftlicher Endbericht, Erstellt für Klima- und Energiefonds, FFG, Wien, April 2014.

[2] A. Cavoukian, J. Polonetsky, and C. Wolf, "SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation," in Identity in the Information Society, 2009.

[3] C. Gerdenitsch, and S. Döbelt, Who Controls the Switch? Enhancing Residents' Trust in Sustainable Building Technology. In e-nova internatioal Conference, 2012.

[4] M. Jung, W. Kastner, and S. Döbelt, „Smart Web Grid", In smart city: Wiener Know-how aus Wissenschaft und Forschung, Wien: Schmid, 2013, pp. 184-190.

[5] G. Kienesberger, T. Hofer, M. Jung, and S. Döbelt, "Smart Web Grid - Eine serviceorientierte Informationsdrehscheibe für Smart Grids," in ComForEn, 2012, pp. 1–6.

[6] L. Hohmann, Innovation Games: Creating Breakthrough Products Through Collaborative Play. Boston, MA: Addison Wesley, 2006.

Approaching Verification and Validation Challenges in Smart Grids

Tobias Gawron-Deutsch, Siemens AG Österreich, tobias.gawron-deutsch@siemens.com
Josef Widder, TU Wien – Formal Methods in Systems Engineering Group, widder@forsyte.at

Abstract – The aim of this paper is to present some challenges found in the design and implementation of smart grids from a computer scientist's perspective. We discuss selected aspects in the design of smart grids, and then give some pointers to related research results that have been achieved in computer science research in the last decades. We hope that this short paper will lead to collaboration of smart grid designers and computer scientists from the related areas.

1. Challenges in Smart Grids

The technologies used in the context of generation, transportation, and consumption of electric energy are changing currently. The large facilities have competition from a huge number of tiny, decentralized generators that use renewable energies as their primary energy source. Top-down distribution of energy from the high voltage grids down to the consumers at the low voltage level is facing reverse power flows.

To be able to cope with these challenges, the control of the power grid and its components, have to be automated, and the components must be able to communicate with each others in order to achieve the required tasks. Hence, compared to classic power grids, the new grids will be less hierarchical and more distributed in nature. This distribution adds new challenges due to concurrency, which makes the task of system design more complicated and inherently more error-prone. A grid with passive, not connected components is well understood and can be operated very reliably. Blackout times in developed countries are counted in minutes per year. The new systems have to match this number. Thus, new methods have to be introduced into the domain that guarantee that the system reliably operates as intended, despite its more complicated nature.

We would like to highlight several components with specific requirements:

Communication protocols: There are many European and U.S. American standards for communication protocols that are relevant for smart grids. Often, details in these standards contain parts that are left unspecified on purpose, and should be designed/implemented by the vendor. Inherently, protocols and communication protocols are difficult to design, and it is easy to overlook corner cases that lead to bugs [1,3], e.g., to livelocks or deadlocks. Hence, a systematic way for correct protocol design is required.

Different Voltage Levels: A power grid is usually divided into three voltage levels. Until now, each level has been treated independently from the control point of view; respectively, low voltage

grids were operated statically. With the advent of automated distributed controls for each level, the mutual influence of the controllers on the same level as well as on different levels has to be considered. Guarantees for the stability of the whole system are crucial for the acceptance of the new technology.

Load Balancing by Command: Projects like the intelligent secondary substation aim at enforcing grid quality constraints in volatile situations (e.g. [15]). They are granted priority control power over relevant devices like production (e.g. photovoltaic) and consumption (e.g., heat pumps). In case of need, they are allowed to reduce production/consumption to ensure, e.g., that voltage is within the required bandwidth. Methods that help to demonstrate that the design behaves "well", even in the presence of message loss or partial failure of the system, should be developed.

Load Balancing by Cooperation: To reach the goal of the grid operator – e.g., lower voltage – a node can influence its production or its consumption. It receives the command from the grid controller and decides whether production should be reduced or consumption increased. Internal processes and requirements of the connected node are unknown to the grid operator. As the grid operator has no direct control over the devices – a mediator that translates the grid request to the possibilities of the node is necessary. Motivation to act accordingly is limited to abiding contracts on node side. The challenge is that the operator should detect whether and how has been reacted.

Load Balancing by Markets: Given that smart grids have many participants that produce and consume electric power, it is natural to view the system as market place, where the mechanisms of the market shall motivate the participants to behave in a way that is beneficial for undisturbed operation of the grid. Participants can be motivated to behave beneficial by providing incentives. However, as in all markets, issues such as fraud and unstable periods should be avoided. Hence, implementations of robust market mechanisms are required.

2. Approaches Towards Reliability in Computer Science

As discussed in the previous section, it is crucial to design distributed computer systems for smart grids in a way that ensures that they do not fail. To do so, one has to address two challenges: on the one hand, we have to design means that tolerate partial failure that is outside the control of a system designer (such as hardware faults or bit-flips due to radiation), and on the other hand, find design faults (bugs) in order to fix them. The former is classically addressed by means of replication and fault-tolerant distributed algorithms, while the latter is dealt with by rigorous system and software engineering methods, such as model checking. In this section we will give a very brief introduction into these two well-established research-fields.

2.1 Fault-tolerant Distributed Algorithms

In contrast to a centralized computing system, a distributed system (such as the Internet) should not stop to operate in the case where one of its components fails. At the same time, the mentioned applications in smart grids require that many components are actually cooperating quite tightly. Consequently, we require the system to stay operational despite close cooperation and partial fail-

ure. Such problems have been considered in the area of distributed computing theory [5,6] since the early 1980s. Lamport et al. [4] considered the consensus problem of agreeing on a common value in the presence of unrestricted (Byzantine) faults, that is, processes may fail by sending faulty, or even conflicting information to other processes, or processes may crash prematurely, etc. The problem of agreeing on a common value is the paradigm of establishing some global view of the distributed system, and lies at the heart of many solutions to different distributed computing problems. Although in the early 1980s, and still today, it is often believed that a majority of correct processes is sufficient to keep systems operational, Lamport et al. showed that less than a third of the processes may be faulty. Moreover, they provided an algorithm that works in synchronous systems, that is, in systems where the processing and communication times are predictable and a priori known. The second seminal work is the one by Fischer et al. [7] that considers, in some sense, the opposite of the spectrum, that is, "well-behaved" faults, that is, faults that just lead to a process crash (without sending erroneous messages), while the timing is unpredictable. There, quite surprisingly, it was shown that it is impossible to design a protocol that allows to agree on a common value. We thus see that the interplay of concurrently running processes with uncertain timing and faults leads to complications, both from a theoretical viewpoint as well as from a protocol design viewpoint: Theory tells us that certain problems cannot be solved without adding assumptions on the underlying system, and thus provides us a guideline what we should not even try to develop. At the same time, even in the cases where theory tells us that we can solve problems, the combinatorial explosion of possible executions of a protocol due to concurrency, uncertain timing, and faults are challenging for the human mind.

An example where ignoring such issues during the system design and implementation phase had severe consequences is the accident of a Qantas Airbus in October 2008 that caused serious injuries of twelve persons (and light injuries of many more). The control system of the Airbus is a cyber-physical system that collects physical environment data such as speed, altitude, or the "angle of attack," and controls the actors that operate the aircraft. As reported in [18], the angle of attack was measured wrongly by a single faulty computing component, which resulted in erroneous commands that lead to dramatic altitude drops; this all happened in the presence of two redundant correctly working components. We conclude that when a system should be designed to be highly reliable, underestimating the complexity of the problem, and ad-hoc solutions, can have severe consequences.

We shall conclude this section, by mentioning work on fault-tolerance that considers game theory, and can thus be used to address the market challenges mentioned above. Halpern [8] gives an overview on work that extends classic equilibria concepts to ones that tolerate several adversarial participants, and to design mechanisms that motivate participants to behave in order to achieve some global goal. In particular, mechanisms for robust and resilient equilibria have been introduced. This means that (coalitions of) participants are prevented from destabilizing the market. In addition, more refined cost models that incorporate the cost of computing better strategies or changing between strategies has been considered in the literature. Finally, the standard game theoretic assump-

tion that all participants have complete knowledge about the relevant details of the game is unrealistic. There exists literature that considers limited knowledge.

2.2 Computer Aided Verification

We have discussed in the previous section that reasoning about the correctness of distributed algorithms is inherently difficult. Hence, system designers might easily miss bugs that are due to the concurrency, or the unpredictable timing. Well-known examples of such bugs are race conditions, or deadlocks. Computer aided verification techniques, in particular model checking [11,12], have matured in the recent years into tools that are used in industry to verify hardware designs, e.g., microprocessors and cache coherence protocols [1], sequential software [9,10], e.g., device drivers, and network protocols [11].

The research area of model checking considers efficient procedures to evaluate a formal specification (of the correct system behavior) over a system description (the implementation of the system, roughly speaking). In contrast to testing, that can only cover a limited number of test cases, and thus cannot establish the correctness of a system, model checking is a complete method, which ensures that the system is correct if the verification procedure has a positive outcome. In case the system contains a bug, model checking finds it, and returns an error trace to the user. Such error traces are very useful to fix bugs during the system design and implantation phases.

In order to maximize the reliability, one should deploy fault-tolerant distributed algorithms that have been verified by model checking. In the recent years, this research area received attention, and several research projects (forsyte.at/software/bymc/) at TU Wien are devoted to that subject [13,14]. Moreover, a recent Dagstuhl seminar on Formal Verification of Distributed Algorithms in April 2013 (http://www.dagstuhl.de/13141/), and a follow-up workshop FRIDA during the Vienna Summer of Logic (http://vsl2014.at/frida/) were devoted to that subject.

3. Conclusions

In this paper we sketched design challenges for smart grids. As human operators cannot in sufficiently short time perform the tasks required in modern systems, new autonomous distributed computing systems have to be developed. Moreover the sheer size of the systems (large number of components), as well as the mentioned issues due to concurrency and faults, call for a rigorous approach toward system design and engineering.

We have discussed results from computer science that can be used in such a rigorous approach. These results come from well-established sub-areas of computer science, which as is proven by Turing awards (“Nobel price in computer science”) given to leading figures in this research, namely to Lamport (for his work on distributed and concurrent systems), and Clarke, Emerson, and Sifakis (for their work on model checking).

The discussed set of tools from computer science is rendered in respect to the list of components given in the introduction. We have mentioned approaches to make communication protocols more

stable and reliable. Fault tolerant distributed algorithms make the distributed and vertical control solutions for smart grids better suitable for their main task – undisrupted supply of energy. The third topic we emphasized is load balancing. It not only incorporates challenges from communication protocols and control solutions, but adds the question of fair cooperation. To design a suitable system methods from the important scientific field game theory have to be used as well.

The first years in smart grid oriented research were devoted in understanding the domain and thus driven by a power engineering centered view. Recently, research and development efforts are shifting towards computer science topics. To name but a few examples: Security and safety are becoming core topics of large project (e.g. [16]), formal methods are applied to smart grid applications (e.g. [2]), research funding calls are explicitly asking for this shift (e.g. [17]). In an interdisciplinary research field like smart grids, it is important to understand what results and methods from the different fields can be applied to the problems at hand. We hope to convince the community that is concerned with the design and development of state-of-the-art power grids that existing results in computer science can help them in their difficult task to design highly reliable distributed computing systems.

Acknowledgements

The presented work conducted in the ICT4RobustGrid project is funded and supported by the Austrian Klima- und Energiefonds (KLIEN) in the program “IKT der Zukunft“.

References

[1] Clarke, E., Grumberg, O., Hiraishi, H., Jha, S., Long, D., McMillan, K., and Ness, L. Verification of the future-bus+ cache coherence protocol. Technical report, DTIC Document, 1992.

[2] Shravan Garlapati and Sandeep K. Shukla. Formal verification of hierarchically distributed agent based protection scheme in smart grid. SPIN 2012.

[3] Yifei Dong, Xiaoqun Du, Gerard J. Holzmann, Scott A. Smolka: Fighting livelock in the GNU i-protocol: a case study in explicit-state model checking. STTT 4(4): 505-528 (2003)

[4] Leslie Lamport, Robert E. Shostak, Marshall C. Pease: The Byzantine Generals Problem. ACM Trans. Program. Lang. Syst. 4(3): 382-401 (1982)

[5] Nancy A. Lynch: Distributed Algorithms. Morgan Kaufmann 1996

[6] Hagit Attiya and Jennifer Welch. Distributed Computing. Wiley, 2nd edition, 2004.

[7] Michael J. Fischer, Nancy A. Lynch, Mike Paterson: Impossibility of Distributed Consensus with One Faulty Process. J. ACM 32(2): 374-382 (1985)

[8] Joseph Y. Halpern: Beyond nash equilibrium: solution concepts for the 21st century. PODC 2008: 1-10

[9] Beyer, D., Henzinger, T. A., Jhala, R., and Majumdar, R. The software model checker Blast: Applications to software engineering. Int. J. Softw. Tools Technol. Transf., 9:505–525, 2007.

[10] Ball, T., Levin, V., and Rajamani, S. K. A decade of software model checking with SLAM. C. ACM, 54:68–76, 2011.

[11] Grumberg, O. and Veith, H., editors. 25 Years of Model Checking - History, Achievements, Perspectives, volume 5000 of LNCS, 2008.

[12] Clarke, E., Grumberg, O., and Peled, D. Model Checking. MIT Press, 1999.
[13] Annu John, Igor Konnov, Ulrich Schmid, Helmut Veith, Josef Widder. Parameterized model checking of fault-tolerant distributed algorithms by abstraction. In FMCAD, pages 201-209, 2013.
[14] Annu John, Igor Konnov, Ulrich Schmid, Helmut Veith, Josef Widder. Towards Modeling and Model Checking Fault-Tolerant Distributed Algorithms. In SPIN, volume 7976 of LNCS, pages 209-226, 2013.
[15] Ralf Mosshammer, Alfred Einfalt, Mario Faschang. Smart Low Voltage Grid Controller. Smart Grids Week, Graz, 2014
[16] Lucie Langer, Friederich Kupzog, Markus Kammerstetter, Thomas Kerbl, Florian Skopik. Smart Grid Security Guidance (SG)2 – Empfehlungen für sichere Smart Grids in Österreich. In ComForEn, pages 17-21, 2013.
[17] Programm IKT der Zukunft – Ausschreibungleitfaden 1. Ausschreibung 2012. FFG, 2012.
[18] In-flight upset 154 km west of Learmonth, WA; 7 October 2008; VH-QPA; Airbus A330-3-3. Australian Transport Safety Bureau, Aviation Occurrence Investigation AO-2008-070 Final, 2011.

ComForEn 2014 – Programm der Tagung 30.09.2014

9:00	**Anmeldung, Get Together, Kaffee**
9:30	Begrüßung
9:40	**Session 1: Wissenschaftliche Arbeiten** Keynote: Kein Smart Grid ohne Energietechnik: neue Komponenten für die Verteilernetze der Zukunft – Wolfgang Hribernik, AIT
10:20	Communication Patterns for Demand Side Flexibility, Mike Pichler, Siemens
10:45	Smart Grid, Smart Charging, Smart Privacy? An Empirical Investigation of Consumers' Willingness to Provide Smart Charging Information, Susen Döbelt, Bettina Kämpfe, Josef F. Krems, TU Chemnitz, Institut für Psychologie
11:10	Cybersecurity Risk Assessment in Smart Grids, Thomas Hecht, Lucie Langer, Paul Smith, AIT
11:35	A Survey of Control Strategies Applied in Worldwide Microgrid Projects, Yi Guo and Wolfgang Gawlik, TU Wien, ESEA
12:00	**Mittagspause**
13:15	**Session 2: Projektberichte** Keynote: Strommärkte, -netze und Flexibilität: Ein notwendiges Dreieck zukünftiger Versorgungssysteme? Wolfgang Prüggler, TU Wien
14:00	DG DemoNetz – Smart LV Grid: Rapid Prototyping vernetzter Smart Grid Systeme, Mario Faschang, TU Wien
14:20	INTEGRA: Die mögliche Rolle eines Flexibility Operators beim Übergang von Markt- zu netzgeführten Betrieb , Tobias Gawron-Deutsch, Alfred Einfalt, Siemens
14:40	Kommunikations-Protokolle für Virtuelle Kraftwerke, Alexander Lurf, Cybergrid
15:00	**Kaffeepause**
15:30	SmartWebGrid: Benutzerakzeptanz von neuen Dienstleistungen über die Smart Grid IT-Infrastruktur, Sebastian Prost, Manfred Tscheligi, AIT, Marcus Meisel, TU Wien ICT
15:50	Approaching Verification and Validation Challenges in Smart Grids, Tobias Gawron-Deutsch, Siemens und Josef Widder, TU Wien
16:30	Diskussionsrunde: Technische Ausgestaltung des Ampelmodells: lohnt sich der Einbau zusätzlicher ICT-Komponenten um Einspeisebeschränkungen zu vermeiden?
17:00	**Abschluss**