The Cellular Approach Security of Micro Smart Grids

Gerhard Kleineidam[1], Georg Jung[2], Marco Krasser[3], Bernd Koch[4]

[1]Gerhard Kleineidam, University Bayreuth, ZET Zentrum für Energietechnik, Universitätsstraße 30, 95447 Bayreuth, gerhard.kleineidam@uni-bayreuth.de, [2]Georg Jung, University of Applied Sciences Hof, IISYS Institute of Information Systems, Alfons-Goppel-Platz 1, 95028 Hof, [3]Marco Krasser, SWW Wunsiedel GmbH, Rot-Kreuz-Straße 6, 95632 Wunsiedel, [4]Bernd Koch, Siemens AG, Von-der-Tann-Str. 30, 90439 Nürnberg

***Abstract*—The ongoing transition from a conventional energy supply towards an energy system based on renewable sources requires fundamental changes to the energy infrastructure. In particular, the move from a centralized and centrally stabilized network towards a distributed architecture significantly increases the demand for ICT-based management and control. Even in the current grid infrastructure ICT-based management is central, making the power supply vulnerable to cyberattacks. The necessary expansion and augmentation of ICT proliferation inside the power grid substantially multiplies this vulnerability, thus making a thorough risk assessment and mitigation unavoidable. The SWW Wunsiedel GmbH, a progressive, innovative, utility company in northern Bavaria, Germany, has been spearheading the transition towards renewable energy supply with a record of successful research projects and a consistent investment and renewal policy. The SWW area of operations provides a unique testing ground for cybersecurity related challenges under realistic conditions. This paper describes life safety and security assessment within the "Smart Grid Protection Against Cyber Attacks" (SPARKS) project.**

Keywords—security; smart grid; cyber attack; protection; field test; automation; SCADA; renewable energy generation; energy management; energy distibution; energy storage

The Energy Region Wunsiedel uses its area of operations to field test intelligently connected dezentralized systems to qualify and release secure solutions in energy supply.

All inventions, any change on existing solutions have to be field tested before releasing them to the public. The German energy saving and energy transition policy has initiated a large number of research programs stimulating innovations in energy supply. There are many valuable solutions in energy production, energy storage and efficient use of energy which are waiting for roll-out and thus need to be tested for proper functionality and quality, performance, safety and security. The University of Bayreuth with its "Zentrum für Energietechnik" (ZET) has installed a field test laboratory together with the "Insitute of Information Systems" (iisys) Hof University. Most of the infrastructure and testbeds of that field laboratory have been installed within the range of SWW Wunsiedel GmbH in northern Bavaria (Germany) financed by multiple research projects in order to life test various technologies focussing on biomass, power-to-heat, power-to-gas, and especially on automation & control (smart) energy systems including cyber security.

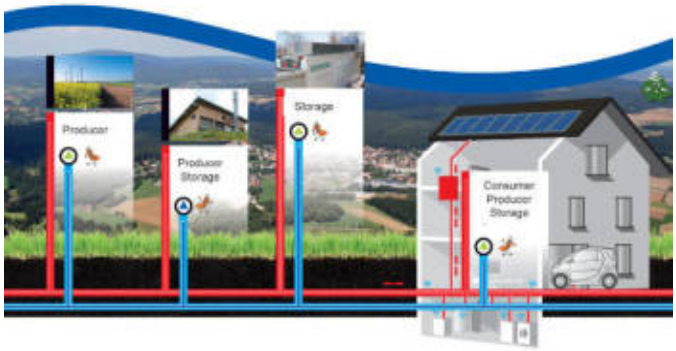

Fig. 1. Smart Energy Region means that communication among energy producers, consumers and storages allows to effectively manage fluctuating loads and demand

SWW Wunsiedel is a municipal, highly innovative, utility company and DSO[1] that ensures an affordable, highly environmentally responsible supply of the metropolitan area of Wunsiedel and seven other municipalities. The SWW Wunsiedel GmbH has set itself the goal of fully satisfying the energy demand by using renewable and regionally produced energy forms latest by 2030. Additionally they intend to be a supplier of balancing power for higher grid levels and external supply areas as well. With their "field laboratory of the energy transition" SWW is a model and pioneer for other utilities in Germany.

In its region SWW supplies about 20,000 people with electricity, heat, water, gas, and communi-cation services based on fiber optics. SWW has developed the roadmap "WUNSiedler Weg – Energie" where (a) the extension of renewable energy generation, (b) the integration of various energy storage technologies, and (c) a generic, modular smart grid ICT architecture based on self-controlled smart micro-grids guide SWW to the vision of the "Energieversorgung 4.0" (Energy Supply 4.0) – see figure 2.

[1] DSO - Distribution System Operator (regarding electricity distribution)

Changing from centralized power plants to a complex system of distributed renewable energy sources requires the balancing of fluctuating loads and power profiles.

Local supply forms the basis of SWW's approach. Within the SWW supply area it shall be proven that balancing local generation and consumption at the lowest viable level e.g. districts within MV power distribution rings or branches (cells), could decrease fluctuation within the whole area. This requires the integration of electrical storages or power-to-x transformation capacity. The intergration and combination of electrical and thermal power plays a key-role in the concept. So the first R&D projects which have been started in 2012 have dealt with buildings used as thermal storage. In future it will be possible to shave and shape load profiles by using electrical heaters (or coolers) in households [1], [2].

In Germany there are so far only a few regional utility providers, such as the SWW Wunsiedel GmbH, that focus excusively on renewable forms of energy. The main challenge in this context was and still is the management of the volatility of electricity generation and consumption in a distributed power grid. The complexity to manage and control such a distributed power grid can be reduced by accurate forecasts for power generation and the provision of reliable load profiles from every unit in the system. The solution SWW develops is based on the segmentation of their area into smaller units consisting of integrated micro-power-plants, intelligent consumers and energy storage capacity to form so called microgrids. Where such microgrids provide isolated operation capability in case of emergency, stability and an energy buffer to other external grid segements. Segmentation into autonomous microgrids also increases security.

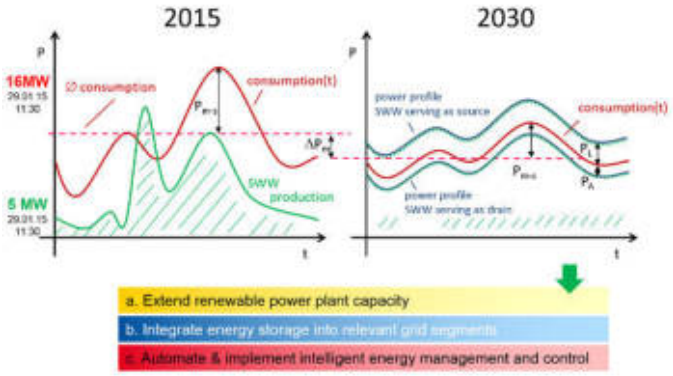

Fig. 2. The vision is not only to shape load profiles and balance energy consumption or supply but also to provide a bandwidth of power source or drain capacity to external territories

Automation and communication form the platform of a cellular approach which requires secure ontime interaction of independently operating energy islands.

Due to the permanently increasing portion of distributed energy generation, energy management systems become more important to allow a stable operation of the grid at its limits. Distribution grids are often sparsely monitored and an upgrade of measuring technology is associated with high costs. However, information about load behaviour at the nodes of a grid is essential for grid state identification and load forecasting. Future Smart Grid ICT systems shall be able to monitor behaviour and to predict the utilization and the state of the grid more precisely than today – see: Handschin and Wedde [3], [4].

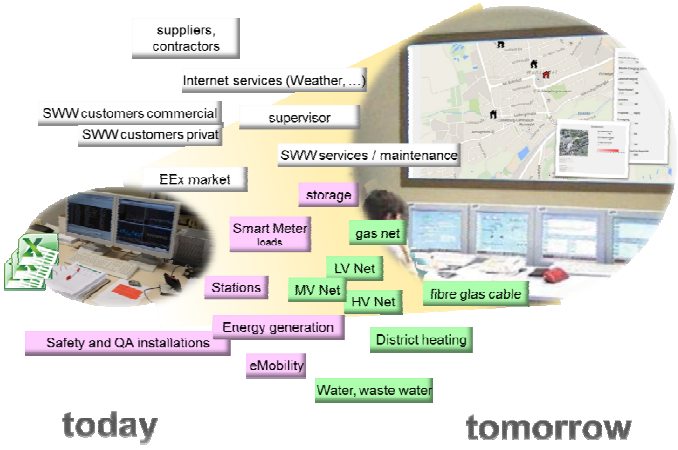

Fig. 3. The future energy control center shall integrate all relevant business processes and monitor utilities with minimum of interference but efficient exception handling mechanism

Following this idea, SWW has decided to develop a new energy management system to not only handle the volatility of electricity generation and consumption in a distributed power grid by 2020 but also to manage all other services provided by a utility company. The future solution shall be based on Siemens SPECTRUM Power™ 5 software, which in the first step shall be installed and tested as a clone to the existing master control system. Functionality, performance, reliability and use of said clone can be developed and tested with non-critical components, such as research systems or smart meters (read only components). Figure 4 shows an example for a generic smart grid ICT architecture which is able to provide load balancing by a cellular approach based on self-controlled smart microgrids.

While distributed autonomous systems provide a higher level of reliable supply by nature, a higher degree of automation in combination with an increasing number of communicating field devices in a smart grid also mean a higher cyber security risk– see potential target for cyber attacks in figure 4.

At the core of the change in grid management is an increased use of ICT to implement enhanced monitoring and control in the distribution network at medium and low-voltage levels. The future smart grid represents a significant evolution in the way electric grids function. Ensuring the cybersecurity and resilience of smart grids is of paramount importance. This challenge has motivated to participate in and contribute to the EU FP7 funded project "Smart Grid Protection Against Cyber Attacks – SPARKS" [5]. The project aims to provide innovative solutions in a number of ways, including approaches to risk assessment and reference architectures for more secure smart grids.

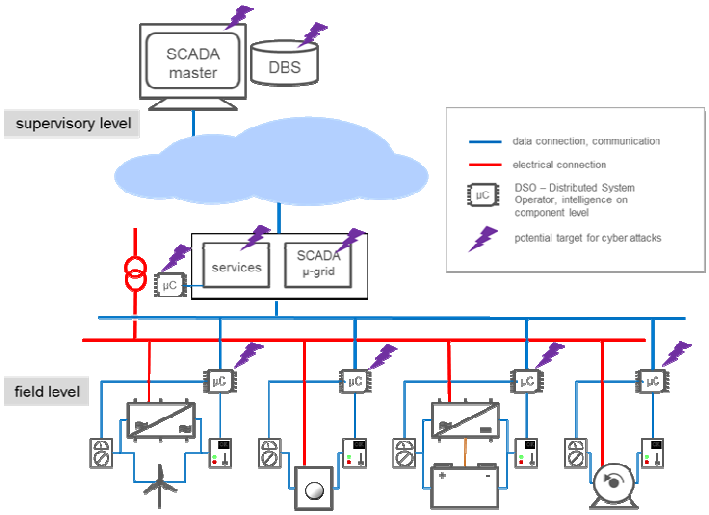

Fig. 4. The example of a cellular smart grid / smart microgrid architecture (using the example of "WUNSiedler Weg – Energie") shows the potential targets for cyber-attacks (SCADA = Supervisory Control And Data Acquisition, DBS = data base system)

The project will make recommendations regarding the future direction of smart grid security standards. Furthermore, key smart grid technologies will be investigated, such as the use of big data for security analytics in smart grids, and novel hardware-supported approaches for smart meter (gateway) authentication. All of these contributions and technologies will be assessed from a societal and economic impact perspective, and evaluated in real-world demonstrators. Specifically, the SPARKS project has the following objectives:

- Promote the awareness of existing and emerging smart grid cyber-security risks to stakeholders, including energy network operators, industry and policy makers.
- Develop procedural and technical countermeasures, and provide cost assessments of the developed technologies via business cases.
- Investigate privacy issues related to smart grid development, especially in the areas related to customers like smart metering, taking into account existing legislation and providing guidance for future activities.
- Control systems research will investigate the relationship between key control loops in a smart grid, and propose designs that enable semi-autonomous islands of control, which maintain stable operation in the face of attack or disruption.
- Real-time network monitoring and data analysis is essential for building advanced SCADA-specific intrusion detection systems – SPARKS will develop innovative technologies in this area.

The following table lists the various nodes / components of a power grid which may be a potential target of cyber attacks and thus have to be secured and tested for cyber security when integrated into a smart grid in a real world environment (see figure 4) the risks are categorized based on the CIA criteria (Confidentiality, Integrity and Availability).

POTENTIAL TARGETS FOR CYBER ATTACKS

Power Grid Components and Risks			
Component	***communi-cation capability***	***type of controller, operating system***	***key risks***
Supervisory Level			
Master controller station with SCADA[a], database management functionality	IP and all required protocols	Extended server architecture including several process	Major target. Key risks are in the area of integrity, confidentiality and availability (e.g. Denial of Service attack or brute force attack)
SCADA[a] on microgrid level (=matter of research)	Standardi-zation efforts ongoing	Controller architect	Key risks in integrity, confidentiality and availability (e.g. Denial of Service attack or brute force attack)
Field level			
(micro) power plants, storages	field bus IP, hard-wired signal processing	Mostly PLC[b] or Soft PLCs on PC	Key risks are in the ara of integrity and availability (e.g. unauthorized access through (remote) service interfaces or injection of malware)
Protection & Control device	IP, field bus, hard-wired signal processing	Integrated programmabl e logic function	Key risks are in the area of integrity and availability (e.g. unauthorized access or misuse of administration rights)
Consumer components including smart meters	smart meter protocols	µControllers	Key risks are in the area of confidentiality (privacy) and integrity (e.g. changed meter data)
Power transformer stations	signal processing	Industrial PC, PLC[b] or mini PLCs	Key risks are in the area of integrity (e.g. caused by changed data from SCADA[a] or wrong data send to SCADA[a])
Others: circuit breakers, switched capacitor banks, earth contact, monitoring or metering systems, etc.	-	-	Requires a detailed risk assessment on the reference architecture.

[a] SCADA = Supervisory Control and Data Acquisition
[b] *PLC = Programable Logic Controller*

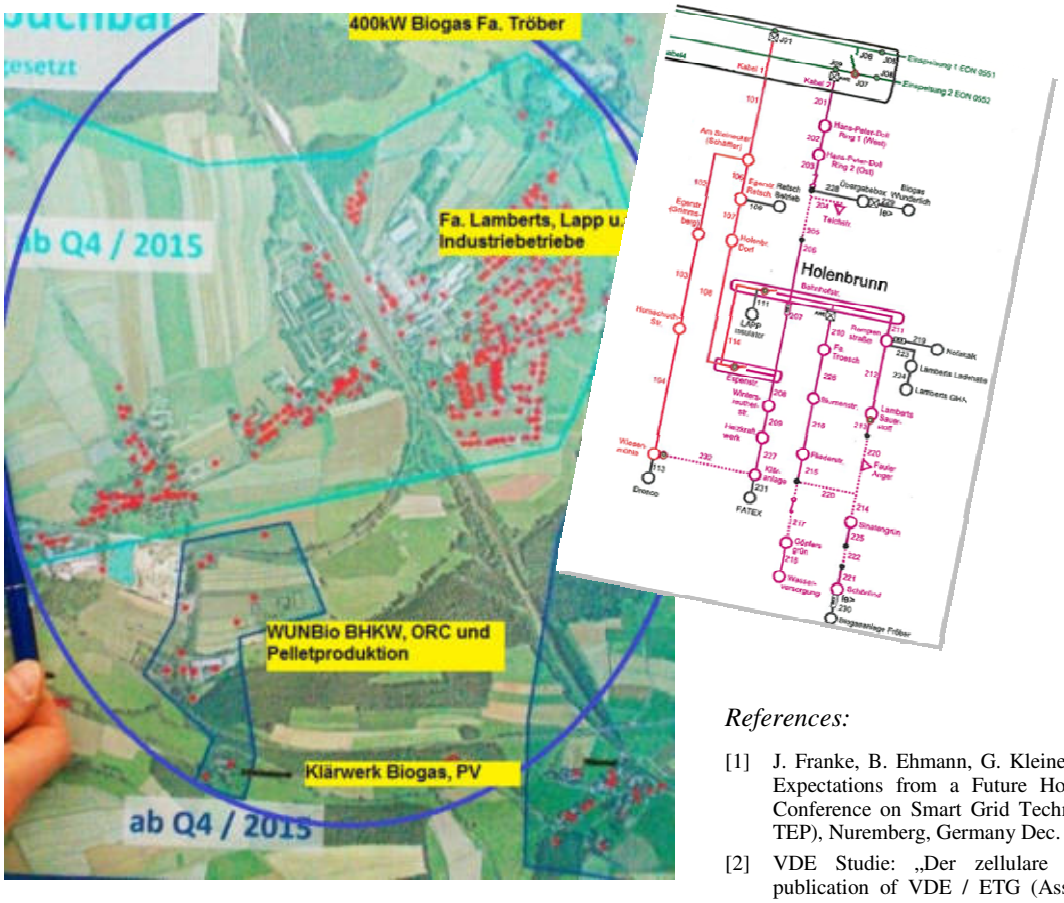

Fig. 5. The cellular approach shall be tested in Wunsiedel Holenbrunn by installation of various energy storage technologies and intelligently acting and communicating field devices

In addition to the new master controller the grid segment Holenbrunn within the area of SWW will be technically upgraded to an autonomuous functioning energy island (micro-grid) with black-start capability. This requires the installation of various storages and intelligently interacting grid components (see figure 5).

References:

[1] J. Franke, B. Ehmann, G. Kleineidam: „Smart Grid Requirements and Expectations from a Future Home Perspective“, IEEE International Conference on Smart Grid Technology, Economics and Policies (SG-TEP), Nuremberg, Germany Dec. 3-4. 2012.

[2] VDE Studie: „Der zellulare Ansatz” (The Cellular Approach), publication of VDE / ETG (Association for Electrical, Electronic & Information Technologies), Munich, Germany June 16, 2015.

[3] E. Handschin, C. Rehtanz, H. F. Wedde, O. Krause, S. Lehnhoff; „On-Line Stable State Determination in Decentralized Power Grid Management“, 16th PSCC, Glasgow, Scotland, July 14-18, 2008.

[4] H. F. Wedde; S. Lehnhoff, C. Rehtanz, O. Krause; „Bottom-Up Self-Organization of Unpredictable Demand and Supply under Decentralized Power Management“, Second IEEE International Conference on Self-Adaptive and Self-Organizing Systems, Venice, Italy Oct. 20-24, 2008.

[5] P. Smith et.al. , SPARKS – Smart Grid Protection Against Cyber Attacks, EU FP7 funded project Contract No. 608224, www. project-sparks.eu, Vienna April 01, 2014.