Cyber Security Challenges in Heterogeneous ICT Infrastructures of Smart Grids

Florian Skopik and Lucie Langer
Safety and Security Department, AIT Austrian Institute of Technology
Email: florian.skopik@ait.ac.at; lucie.langer@ait.ac.at

Abstract—A drastic change in modern power grids is underway. Conventional means of providing energy by centralized suppliers will not be sufficient to ensure the energy supply of our society in the future. Therefore, Information and Communication Technologies (ICT) are increasingly applied, for example, to allow a flexible integration of wind-, solar-, or biomass energy into the existing power grid. This integration of energy providers, consumers, producers and utilities by means of ICT is the cornerstone of a Smart Grid. With the increasing use of novel smart grid technologies, a comprehensive ICT network is established parallel to the electricity grid, which due to its large size, number of participants and access points will be exposed to similar hazards as the current Internet. However, the reliable energy supply of this system depends on the effective operation of ICT, and similar security problems such as in the current Internet would have severe consequences. Potential threats range from meter manipulation to directed, high-impact attacks on the critical infrastructure of the energy carrier that could damage or bring down parts of the national power grid. It is essential that security measures are put in place to ensure a future smart grid does not succumb to these threats, and to safeguard this critical national infrastructure at all times. One of the main challenges when building up smart grids is to cope with the heterogeneous character of applied technologies. Since product life cycles can span several decades, the overall system complexity will considerably grow in the next years due to the application of many different protocols and technical solutions. This heterogeneity eventually increases the attack surfaces to a smart grid and might also lead to an increased vulnerability. In this paper, we survey the most relevant protocols and standards today, and investigate their application and potential conflicts in future security-relevant smart grid use cases.

Index Terms—cyber attack scenarios, smart grid communication, smart grid ICT infrastructure, security.

I. Introduction

The smart grid promises solutions to many of today's challenges in energy provisioning. World-wide growing demands, the progressing integration of small distributed energy sources, as well as flexible energy usage patterns require a fundamental transformation of today's static power grid into a flexible and smart energy utility. This is especially true when changing from traditional sources with quite static energy output, such as nuclear power or fossil fuels, to comparatively unreliable green sources including solar power and wind power. Furthermore, the wide acceptance of electric cars in the near future will pose an additional challenge to the power grid. Eventually, appropriate solutions will be heavily based on information and communication technologies (ICT). Therefore, a complex ICT network is currently being established in parallel to the existing power grid in order to make it "smarter". This way, sensors can report operational data within fractions of seconds, and enable control loops to react much more dynamically to changing load conditions, and finally, enable more efficient energy distribution.

Unfortunately, this added complexity makes the power grid also more vulnerable to non-conventional attacks. While in the past utility providers and other grid stakeholders had to deal with safety concerns and physical security only, a widely distributed ICT network based on well known standard (such as TCP/IP) an having access points in almost every household (through smart meters) opens up entirely new attack surfaces. Many works therefore deal with novel architectures and sophisticated security models to address these issues. These works provide important insights and have even led to readily applicable technologies. However, one must not underestimate the comparatively long product cycles in this area. While in typical office environments ICT equipment is renewed every three to five years, in electric energy provisioning we are talking about life times of 20 years and even more for smart meters and other components, such as in the area of substation automation. As a consequence, novel security solutions cannot be applied directly in the entire grid, but need to be rolled out gradually over years. Often multiple generations of a component co-exist in the same setup. This aspect poses significant architectural design challenges in order to properly ensure the security of the power grid.

We therefore argue that, as an important step to gradually transform the current power grid into a smart grid that follows well-designed reference architectures [1], it is essential to review already applied technologies and protocols – especially in mixed systems consisting of legacy devices and smart components.

Eventually, the contributions of this paper are as follows:

- *Survey on Heterogeneous ICT Infrastructures in Smart Grids:* We revisit widely applied communication standards that are the fundamental pillars to build

Manuscript received April 18, 2013; revised June 11, 2013.
This work is supported by the Austrian security research program KIRAS and by the Austrian Ministry for Transport, Innovation and Technology through the project (SG)2 – Smart Grid Security Guidance.
Corresponding author email: florian.skopik@ait.ac.at.
doi:10.12720/jcm.8.8.463-472

up large scale heterogeneous ICT infrastructures. Here, we also provide an overview about smart grid stakeholders and their interconnections on a technical layer.

- *Definition of Cyber Attack Scenarios:* In context of the outlined infrastructure, we investigate (potential) attack scenarios to point out where further security relevant work needs to be carried out. In contrast to many others, here we do not only focus on smart metering but also on other important smart-grid relevant use cases and technology layers, such as the reliable operation of the distribution grid and the availability of e-mobility.
- *Security Challenges and Available Standards:* The cyber attack scenarios are the basis to survey (technical) security challenges for smart grids, and applicable security standards.

The remainder of the paper is organized as follows. Section II gives a brief overview about typical smart grid structures, their interconnections and communication technologies already in use. Section III then surveys attack scenarios on this structure with a special focus on the exploitation of applied protocols and standards. Next, Section IV highlights available cyber security standards to secure smart grid systems and mitigate the effects of attacks in the future. Section V deals with related work. Finally, Section VI concludes the paper.

II. The Evolution of Heterogeneous ICT Infrastructures in Smart Grids

The evolutionary development of the power grid itself, as well as its specific components in the areas of production, transmission, storage and consumption, has led to today's heterogeneous ICT architecture used to control the (smart) grid. In course of this evolution, numerous protocols have been introduced in recent decades. Unfortunately, many of them have been designed with widely different design goals in mind on security, flexibility and scalability than required today. And although many improvements have been proposed and are available, legacy technologies are still far away from being retired.

Fig. 1 (as similarly shown in [3]) depicts an example of a smart grid and its (future) elementary components. On the left side are the grid stakeholders (on a rough organizational level), such as the energy stock market, transmission grid providers, energy suppliers and various operators. These actors communicate with each other already today using standard ICT systems, such as the Internet, e-mail and telephone, and are not further considered in this work. Here, we focus on the right side of Fig. 1 – the physical network and its actors on the different voltage level – and especially, how they are connected.

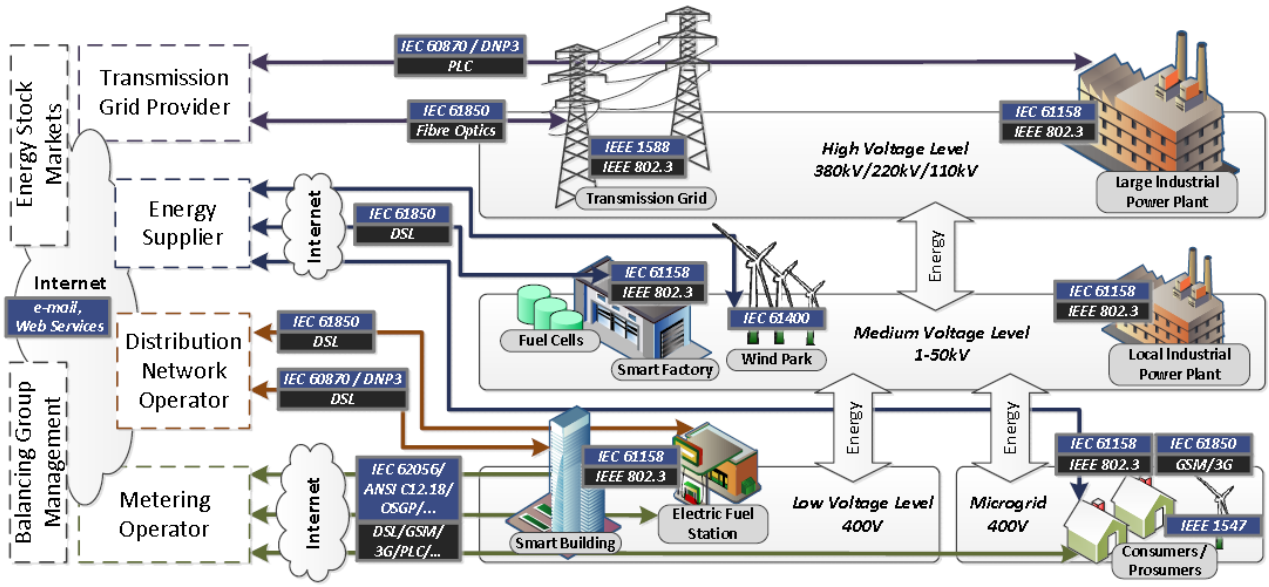

Figure 1. Overview of smart grid stakeholders, their communication paths and used protocols (not exhaustive).

On the highest/high voltage level, large-scale power plants and the transmission grid is located. While power plants make heavy use of local Field bus standards (IEC 61158, real-time Ethernet) to enable reliable and sophisticated control mechanisms, precise time synchronization is one of the tough technical challenges in the transmission grid in order to properly deal with phase shifts. The physical communication between transmission grid providers and power plants as well as the network infrastructure is often realized with power line carriers (PLC) [3], [4] or fiber optics. The communication protocol is currently often the telecontrol protocols DNP3 and IEC 60870-5-104 (Table I). (Notice, IEC 60870-5-101/102/103/104 are companion standards generated for basic telecontrol tasks, transmission of integrated totals, data exchange from protection equipment, and network access).

TABLE I: SOME OF THE MORE IMPORTANT PROTOCOLS IN (SMART) POWER GRIDS (AN EXHAUSTIVE LIST IS AVAILABLE IN [2]).

Protocol Name	Description
DNP3	A set of communications protocols used between components in process automation systems. It was developed for communications between various types of data acquisition and control equipment, such as SCADA systems, where it is used by master stations, remote terminal units and intelligent electronic devices.
IEEE 1547	A set of criteria and requirements for the interconnection of distributed generation resources into the power grid (in the United States).
IEEE 1588	Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems; implemented in PTP - Precision Time Protocol.
IEC 60870	Definition of systems used for telecontrol (supervisory control and data acquisition). Part 5 provides a communication profile for sending basic telecontrol messages between two systems, which use permanent directly connected data circuits.
IEC 61158	A family of industrial computer network protocols (Fieldbus) used for real-time distributed control in industrial network systems to connect instruments in a manufacturing plant.
IEC 61400(-25)	A set of design requirements made to ensure that wind turbines are appropriately engineered against damage from hazards within the planned lifetime; IEC 61400-25 provides uniform information exchange for monitoring and control of wind power plants.
IEC 61850	A set of standards describing the design of electrical substation automation. Data models defined here can be mapped to a number of protocols, including MMS (Manufacturing Message Specification) and GOOSE (Generic Object Oriented Substation Events).
IEC 62056	Data exchange protocol for meter reading, tariff and load control.

On the medium voltage level, wind parks, smart factories and even micro grids (though on the low voltage level) often use the IEC 61850 standard to connect to energy providers. Numerous different subsets define the structure and mapping of messages, e.g. see IEC 61850-8: Specific communication service mapping (SCSM) - IEC 61850-8-1: Mappings to MMS for the Manufacturing Message Specification (MMS). MMS uses well-known GOOSE messages to transfer switch commands between systems (e.g., substations) [5], [6]. For that purpose domain-specific object-oriented data models are used on the application layer (see IEC 61400-25 for wind parks).

On the low voltage level, two essential functions are implemented: first, the distribution of energy, and second, the automatic (remote) metering. An efficient energy distribution is a vital part of the smart grid and can be optimized in numerous ways, especially when it comes to intelligent demand management of smart buildings (e.g., allow utility providers to switch off air condition for short periods to avoid peak loads). For these features the same protocols as on the upper level can be used (but are rarely applied today because most such setups exist only on a small scale within test pilots). For smart metering, a multitude of protocols and standards have been proposed in the past, such as IEC 62056 and OSGP.

A. Automatic Meter Reading (AMR)

Scope: The notion of AMR is not well defined; today we need to distinguish between (i) On-Site AMR, (ii) Walk-By/Drive-By AMR, and (iii) an actual real network solution. Referring to On-Site AMR, a meter reader carries a handheld computer or data collection device with a probe. The device automatically collects the readings from a meter by placing the read probe in close proximity. When a button is pressed, the probe signals the meter to send its readings. The software in the device matches the serial number to one in the route database, and saves the meter readings for later download to a billing or data collection computer. We say Walk-by/Drive-By AMR when a meter reader just carries a handheld computer with a built-in or attached receiver/transceiver to collect meter readings by just walking by the locations where meters are installed. With mobile meter reading, the reader does not normally have to read the meters on any particular route, but just moves through the service area until all meters are read. The network solution allows the metering operator to read out metering data from each single household completely remotely up to several times a day. The physical network is built either on wired telephony technology (such as DSL), wireless networks (including mobile standards such as GSM or 3G) or proprietary power line carriers (PLCs). The transport layer increasingly uses standard IP-based products.

Standards: An early but still widely used communication protocol in the European Union for smart meters is IEC 61107. Although it has been superseded by IEC 62056, it still remains in wide use because of its simplicity and thus high acceptance. Mainly used for on-site AMR, the physical media are either modulated light, sent with an LED and received with a photodiode, or a pair of wires, usually modulated by EIA-485 to send data to a nearby hand-held unit. On the logical layer it sends ASCII data using a serial port. IEC 61107 is related to the FLAG protocol. Ferranti and Landis+Gyr were early proponents of an interface standard that eventually became a sub-set of IEC 1107. The more modern IEC 62056 is a European meter protocol and superset of IEC 61107. The Open Smart Grid Protocol (OSGP) is a family of specifications published by the European Telecommunications Standards Institute (ETSI) used in conjunction with the ISO/IEC 14908 control networking standard for smart metering and smart grid applications. Millions of smart meters based on OSGP are deployed world wide.

B. Substation Automation

Scope: Substation Automation is essential to build up smart grids and essentially deals with three aspects: (i) Data acquisition refers to acquiring or collecting data.

This data is collected in the form of measured analog current or voltage values or the open or closed status of contact points. Acquired data can be used locally within the station where it is collected, sent to a neighboring substation to enable area-specific control tasks, or sent from the substation to one or several databases for use by operators, engineers, planners, and administration. (ii) Supervision refers to computer processes and personnel who supervise (i.e., monitor) the conditions and status of the power grid using the acquired data. This supervision is performed remotely. (iii) Control means sending commands to devices in substations to influence their operational states. Traditional supervisory control and data acquisition (SCADA) systems rely on operators to supervise the system and initiate commands from an operator console on the master computer. In the smart grid, many control tasks should run fully autonomic.

Standards: The application of SCADA systems in the field is basically not ground breaking, however the degree of automation is constantly growing. Several well-established standards are already in use. The most popular ones are IEC 60870-5, DNP3, and IEC 61850(-90-1) (see [2] for more details on the application context of these standards). Roughly, IEC-60870-5 defines the system for telecontrol, especially between two substations, including operating conditions, electrical interfaces, performance requirements and data transmission protocols. DNP3 was a comprehensive effort to achieve open standard-based interoperability among substation computers, remote terminal units, intelligent electronic devices, and SCADA master stations. Further key standards in this area are parts 1 to 10 of IEC 61850, which focuses on the station bus. These standards identify general and functional requirements of the substation communication system, an XML-based substation configuration language, common data and service models, mappings from abstract data objects into manufacturing message specifications (MMS).

C. Wide Area Situational Awareness

Scope: Wide Area Situational Awareness (WASA) refers to the implementation of a set of technologies designed to improve the monitoring of the power system across large geographic areas - effectively providing grid operators with a broad and dynamic picture of the functioning of the grid. The goals of situational awareness are to understand and optimize the management of power network components, behavior, and performance, as well as to anticipate, prevent, or respond to problems before disruptions can arise [7]. For that purpose, phasor measurement units (PMUs) play a crucial role. A PMU is a device which measures the electrical waves on an electricity grid, using a common time source for synchronization. Time synchronization allows synchronized real-time measurements of multiple remote measurement points on the grid. In power engineering, these are also commonly referred to as synchrophasors and are considered one of the most important measuring devices in the future of power systems. A PMU can be a dedicated device, or the PMU function can be incorporated into a protective relay or some other device.

Standards: IEEE C37.118-2005 defines the transmission format for reporting synchronized phasor measurements in power systems. It proposes a method for evaluating a PMU measurement and requirements for steady-state measurement. The standard further defines a total vector error which represents the measurement error allowed in different scenarios such as in the presence of harmonic distortions and out-of-band interferences. Another part of the standard deals with the structure of the different message and frame types (data, command, configuration etc.). Some extensions, such as C37.118.1 and C37.118.2, enable dynamic phasor measurement. Distributed phasor measurement requires high precision time synchronization, such as implemented through the IEEE 1588 Precision Time Protocol.

D. Interconnection of Distributed Energy Resources (DERs)

Scope: DERs are small, modular, decentralized, gridconnected or off-grid energy systems located in or near the place where energy is used. They are integrated systems that can include effective means of power generation, energy storage, and delivery. With the increasing adoption of privately owned renewable energy sources, e.g., small solar panels or wind turbines, distributed generation allows the collection of energy from many sources and may give lower environmental impacts and improved supply security.

Standards: IEEE 1547 is a series of standards, published since 2003, providing criteria and requirements for the interconnection of distributed generation resources into the power grid. The standard is intended to be universally adoptable, technology-neutral, and cover DERs as large as 10 MVA [2]. As an extension of IEC 61850, IEC 61850-7-420 is an international standard that defines the communication and control interfaces for all DER devices [8].

III. Smart Grid Attack Scenarios

A critical review of Figure 1 leads to a multitude of security-relevant smart grid use cases. We shortly outline some of the most important ones here and especially focus on the types of attacks and the technological challenges to mitigate their effects.

A. Cyber Attacks on Smart Metering and Demand Side Management

Scenario Setting: We argue that attacks to the metering infrastructure will be one of the most prominent threats in the smart grid. Although attacking other critical nodes, such as substations, will usually be more effective (in terms of impact), there is one property which makes the smart meter such an attractive target: its distribution. Shortly, a smart meter will be located in each and every

household – and virtually no or only weak physical barriers will prevent its exploitation. Publicly available information on the Internet about metering interfaces and access methods may motivate malicious activities. One of the main questions in this regard is about how well these meters are protected and what harm could be caused by an attacker once he has compromised a meter.

Types of Attacks: Attacks on smart metering are manifold and have been discussed extensively in [9], [10]. They usually aim at the exploitation of metering data on the one side (which also affects privacy), or at causing malfunction and denial of service on the other side. Especially on the lower levels, i.e., the home area network and neighborhood area network, cheap devices are used in sometimes improperly secured designs [11], [12] which often lack computing power for complex encryption techniques. Thus, sniffing of smart meter readings is one of the most distinct threats to privacy. However, once an attacker is able to decrypt and understand messages on the metering network, the next level of attacks is active message tampering. The consequences of fabricated meter messages might range from little impact (such as wrong billing) to severe impact, including incorrect control actions in the grid if wrong energy consumption data is reported to the utility. This situation is aggravated if demand side management comes into play. Here, the utility provider is allowed to control a customer's non-critical appliances (under certain service level agreements), for instance, switch off the air condition in case of peak loads. This feature could be exploited to attack a customer selectively and cause harm of unknown degree depending on the appliances used.

Technical Challenges: Adequate countermeasures to these attacks are available encryption technologies [13], [14] to prevent the illegal access to sensitive data and the fabrication of spoofed messages in the metering network. However, two major challenges remain here: The first one is the actual implementation of these technologies on small and cheap devices. The second one deals with maintenance of firmware and periodic updates of keys. Since we are talking about embedded and autonomic devices, a concept to exchange keys over potentially unsecure communication paths is required. Additionally, the whole key management infrastructure in the utility backend must be secured against illegal access. OSGP already foresees encryption and authentication of all messages, but is therefore demanding to hardware devices.

B. Cyber Attacks on Distributed Energy Resources

Scenario Setting: The integration of small distributed renewable energy sources is one of the cornerstones of the smart grid. Besides bio reactors and solar power, especially wind turbines are an emerging technology to ensure future energy supply. For optimum operation of wind turbines and entire wind farms respectively, they need to communicate among each other and with the power grid. For instance, if too much energy is in the grid or the weather forecast predicts a storm, wind turbines must be switched off remotely for safety reasons. Furthermore, the application of reactive power is essential in order to control the voltage level and energy flows in the grid. Modern wind turbines are capable of generating reactive power and are thus a vital part to the whole energy infrastructure [15]. Thus, a wind turbine can be seen as a controllable generator. Within a wind park typically some kind of real time communication is used, such as Ethernet combined with IEC 61158 Industrial Ethernet or IEC 61850. In some recent work we also showed the application of time triggered protocols in such scenarios [16].

Types of Cyber Attacks: One potential attack deals with manipulating the carefully specified settings for the production of active and reactive power (and their relation respectively). A targeted attack towards this function may cause local overloads and an imbalance in the grid. This would lead to partial shutdowns to ensure safety for the rest of the grid, but at the same time compromise the availability and stability of energy supply. One can have multiple reasons for a deliberately provoked blackout, such as economic reasons and vandalism. Furthermore, willfully caused power fluctuations could be used to exploit current pricing models for networked power market participants and bring multiple economic benefits.

Technical Challenges: Because many of today's communication solutions use IP on the lower levels [17], [18], simple Denial of Service Attacks are quite effective for successful attacks to the availability of remotely controlled energy supplies. Effects can be mitigated by implementing secondary interfaces, using (virtual) private networks and network filter devices (e.g., IDSs) on strategically important nodes in the grid. Another alternative is to switch to non-IP-based technologies, such as (secure) time triggered protocols (TTPs) [16]. TTP, although limited in its expansion, has a quite effective mechanism to avoid simple DoS attacks through the application of monitoring bus guards.

C. Cyber Attacks on E-Mobility

Scenario Setting: One important feature of the smart grid is load compensation, especially when integrating highly volatile renewable energy sources with dynamically changing outputs. Load compensation needs to take place through controllable loads. Here, the utility provider is allowed to reduce or increase load based on available energy in the grid, and thus effectively avoid overloads on the one side and burn surplus energy on the other side. Basically, we distinguish between direct and indirect load management. According to the indirect model, energy suppliers set energy prices dynamically several times a day and inform their customers about the current costs (e.g., either via PLC or via the Internet). Smart appliances are individually configured to change their power consumption at different price levels

automatically; in other words a smart appliance decides itself based on its configuration if it increases or decreases its load. This makes especially sense for sluggish devices which can vary their energy consumption over a wide range in short time intervals, such as water boilers, or air condition systems. In contrast to that direct models foresee utility providers who are allowed to switch on/off devices and adapt power consumption directly. This model offers better predictability of energy requirements and thus a more efficient grid management to utility providers. A particular directly controllable load in the future will be charging stations for electric cars. Here, assume the charging process takes approximately three hours, while a car is usually being plugged to the grid for the whole night (or a whole working day). Thus, there is the need to schedule these charging processes over a longer time period where the car is connected to the grid in order to balance energy withdrawal. From an organizational point of view three major parties of the smart grid will be involved in this use case: (i) the grid provider will "tell" the charging station when and how much energy it can withdraw (e.g., using IEC 61850 protocol over PLC); (ii) the metering operator will monitor the charging cycles (collect meter readings at short time intervals for instance via OSGP) and bill (iii) the right customer, even when plugged to a socket at a friend's premises (unique IDs of appliances).

Types of Cyber Attacks: Previous Works [3] identified three different types of attacks: (i) abuse of meter readings; (ii) sabotage of mobility; and (iii) sabotage of the grid. The abuse of meter readings has been discussed before but needs to be extended here: Since the concept of e-mobility assumes that someone can plug in his car also on foreign premises and still gets billed, it follows that the car needs to identify and authenticate itself towards the grid and also report amounts of withdrawn energy. This data can be used to track people and create detailed mobility profiles. Sabotage of mobility means that an attacker is able to interrupt or massively distort the charging cycles and, thus, that the expected battery capacity at a certain point in time (e.g., the next morning) is not provided. The last attack case refers to losing the control over multiple charging stations and thus the ability to dynamically control the load on the grid. This would have similar effects as losing influence on controllable generators (see wind park case) and might lead to instabilities and blackouts on the grid.

Technical Challenges: Numerous challenges remain unsolved in this use case, mainly because this is a quite complex and somewhat futuristic scenario compared to the others. Especially the privacy of customers due to misuse of sensitive movement data is at stake. So on the one hand we require a secure federated identity management approach, which means people (or their cars) need to be equipped with unique identifiers for billing purposes. However, important lessons learned from e-government initiatives dealing with identity management will be of great value when implementing a country-wide e-mobility scheme. Another foundational pillar could be OpenID [19]. Besides identity management, other challenges closely connected to those outlined before exist, i.e., a working end-to-end security layer for the underlying communication system.

D. Cyber Attacks on the Transmission Grid

Scenario Setting: The basis for the efficient control of energy flows in the grid is a precise knowledge of the network state, the utilization of transformers, transmission lines and the operation reserve (i.e., the generating capacity available to the utility operator within a short interval of time to meet unpredictable demands). Phasor measurement units (PMUs), also known as synchrophasors, play a vital role in this setup, since they determine the phase angle between current and voltage with absolute reference to a measurement time. Therefore, phase angles can be synchronously measured at distributed locations across the whole grid. This provides a consistent view on the grid status. The whole approach just works because of the highly precise clock synchronization mechanisms, which uses GPS data to establish a consistent time base for all PMUs. For the synchronization of substations, switching stations and power plants, which are connected through IEEE 802.3 Ethernet (as part of the transmission grid), the popular IEEE 1588 precision time protocol is often applied.

Types of Cyber Attacks: Since highly precise time synchronization between geographically distributed equipment (usually the relative time deviation must be less than one microsecond) is the basis for the usability of the measured data, a manipulation of this time base is the most obvious attack in this smart grid use case. If a time synchronization message is not received correctly, or clocks are drifting too fast, measured values are not usable for control tasks. In the worst case, measured values need to be discarded. This happens in case of system faults, and fault tolerant mechanisms are applied to avoid or at least safely detect such scenarios. However, if an attacker manages to manipulate the time base by either GPS spoofing [20] or injection of tampered messages in the IEEE 1588 protocol [21] in such a way that the manipulation is not noticed, the grid's control mechanisms will not work properly and can lead, in the worst case, to heavy damage of equipment.

Technical Challenges: Since disturbing/jamming the clock synchronization is in the main interest of attackers, the development of robust mechanisms to prevent such manipulations is fundamental. Highly reliable clock synchronization protocols, such as IEEE 1588, are already in use today, however, have been largely designed with just safety aspects in mind. This means such protocols can greatly deal with glitches due to hardware/software faults, but often fail at preventing malicious attempts with a carefully planned attack strategy. Intelligent GPS spoofing counter measures [22] can help to protect systems using existing technologies,

including signal strength monitoring and intelligent reasoning over received data. Of course, such methods require again more complex systems designs which might impact both price of units and performance. Eventually, future systems need to be designed and implemented with a consistently combined safety and security perspective.

IV. Cyber Security Standards

Many different standards, guidelines and recommendations on smart grid cyber security have been promoted to date. In the following we summarize the most important ones, with a focus on European initiatives.

IEC 62351: IEC 62351 Parts 1-8 (Information Security for Power System Control Operations) define security requirements for power system control operations. The focus is on security standards for the communication protocols defined by IEC Technical Committee (TC) 57, in particular IEC 60870-5 including its derivative DNP, IEC 60870-6 and IEC 61850. The security requirements include authentication, prevention of eavesdropping, playback and spoofing as well as intrusion detection [23].

NISTIR 7628: The Smart Grid Interoperability Panel Cyber Security Working Group (SGIP-CSWG) launched by the U.S. National Institute of Standards and Technology (NIST) has come up with a three-volume report on Guidelines for Smart Grid Cyber Security. The first volume defines a high-level architecture categorizing the interfaces in a smart grid, and presents an approach to identify security requirements for these interface categories [24]. The second volume focuses on privacy risks that arise in customer premises due to sensitive information being generated and processed in the smart grid, and gives high level recommendations on mitigating these risks [25]. The third volume provides supportive material, such as classes of potential vulnerabilities for the smart grid [26].

BSI-CC-PP-0073, BSI-CC-PP-0077 and BSI-TR-03109: The German Federal Office for Information Security (BSI) has come up with a Common Criteria Protection Profile for the Gateway of a Smart Metering System and its Security Module: BSI-CC-PP-0073 [27] defines minimum security requirements for a Smart Metering Gateway based on a threat analysis. The underlying Evaluation Assurance Level (EAL) is four, which means that in order to receive a Common Criteria certification based on [27], a Smart Metering Gateway must have been "methodically designed, tested, and reviewed" [28]. An according certification will become mandatory for Smart Metering devices deployed in Germany [29].

The security requirements for the Security Module, which stores sensitive material such as cryptographic keys and secures the communication between the Smart Metering Gateway and connected entities, are laid down in a separate Protection Profile BSI-CC-PP-0077 [30]. BSITR-03109 [31] defines functional (especially interoperability) requirements for Smart Metering components and elaborates on the security requirements defined in [27] and [30]. Each component is addressed in a separate module of this Technical Guideline.

CEN-CENELEC-ETSI M490: In Europe, the CENCENELEC-ETSI Smart Grid Coordination Group has come up with a comprehensive framework on smart grids in response to the EU Smart Grid Mandate M490 [32]. The framework consists of several reports: "first set of standards" [33] provides a list of relevant smart grid standards to be considered for an efficient deployment of smart grids in Europe, including an overview of the current Cyber Security Standardization landscape. Based on an adaptation of the NIST Conceptual Model [34] to the European scenario, "smart grid reference architecture" [1] defines a three-dimensional technical reference architecture which consists of domains, zones and interoperability layers. Information data flows within a smart grid can be visualized through the reference architecture, which can thus support a security analysis of a given system setting. It also provides a method to analyze information security use cases in smart grids. "sustainable processes" [35] gives a prioritized list of high-level use cases which are characteristic for the operation of a smart grid, and which can provide a basis for further developments such as investigations in risk analysis for information security or functional safety. Finally, "smart grid information security" [36] provides smart grid cyber security requirements and recommendations on their implementations: it defines security levels to bridge the gap between electrical grid operations and information security, and provides related data protection levels to classify data in the grid and to define according protection requirements.

V. Background and Related Work

Smart Grid technologies have received major attention in both academia and industry in recent years. Various works discuss the basics of the smart grid, such as its structure, application, and potential impact [37], [38]. Others cover established and recently developed technical standards [13]. The European Union plans to replace traditional electricity meters with smart meters until 2020 to a large extent, which basically motivates us to take a detailed look at privacy and security threats of this technology [39].

The electric grid is perhaps the most critical infrastructure today, and thus safety, i.e., reliability and availability, is a top priority. Many works investigate how smart meters and related technologies can contribute to an even more reliable grid, e.g., by applying novel self-healing mechanisms [40]. Moreover, in the last months – after starting considerable roll outs of this technology – security and privacy issues have become the focus of many discussions [41]. Threats to and vulnerabilities of smart metering systems are widely discussed topics [14], [41], [42]. Data communication security controls (e.g., cryptographic functions such as encryption, message authentication codes, and digital signatures) provide

standard security services in terms of confidentiality, integrity, and accountability of messages and their origin [13]. Some particular research deals with effective key distribution [43] and management for devices with very limited computational power [14] to enable efficient encryption of meter readings and access control (similar to Pay-TV access control systems [43]).

A key success factor for many smart grid features is the extensive monitoring and logging of consumption data. The prediction of the amount of electric energy required is important to avoid overloads and blackouts in the system. However, by observing the consumers' electricity consumption behavior, major privacy issues arise [44]. An important official first step towards a privacy-enabled smart grid has been made by the NIST [25], who defined problems related to privacy protection and legal constraints. Technical solutions deal either with the anonymization of metering data [45], metering data obfuscation [46], [47] or privacy-preserving metering data aggregation [48], [49]. Finally, SmartPrivacy ('privacy-by-design') [50] focuses on a more holistic view, instead of considering technical aspects only. This concept is an umbrella that offers the complete suite of protections to ensure data privacy. It consists of multiple measures ranging from regulatory protections to education and awareness.

From the industrial side, efforts have been made to set up security guidelines and best practices, e.g., by the Advanced Meter Infrastructure (AMI) security task force [51]. Due to the fact that the electric power grid is a strategic target in case of wars, investigations on the reliability and resilience of smart grids [52] are necessary, and essential to devise security architectures against cyber attacks [42]. Furthermore, novel security mechanisms [53] require sophisticated threat models in order to verify and validate their implementation.

VI. Conclusion and Future Work

In this paper, we highlighted the most common communication protocols of today's power grids. Due to their wide distribution and expected complex and time-consuming migrations, many of those standards will survive the transformation of today's power grid into the future smart grid, and eventually co-exist for decades. However, some of these protocols will be extended to meet new requirements (such as security) and to enable smart services; on the other hand, others will be completely replaced. It is important to keep this co-existence of a wide variety of different protocols in mind when assessing the security of future smart grids. Eventually, the smart grid will not be designed from scratch with the best and most sophisticated security mechanisms well integrated. It will rather be established on existing works and gradually be transformed to a future energy utility. Moreover, security (and privacy!) challenges in this environment do not only highly depend on the technical layer, but also on the actual application scenarios. For instance, the security challenges to enable a secure efficient energy distribution are different from an e-mobility scenario. A detailed discussion regarding future application scenarios is therefore essential.

The combination of legacy protocols with new cutting-edge technologies raises new security challenges. Therefore, future work deals with the technical and scientific steering of pilot cases to learn about the best strategies for large-scale smart grid roll-outs. Eventually, we plan to develop new risk assessment models to quantify the risks due to the integration of ICT-supported components. Here, especially the mixture of legacy technology with "smart" components and the resulting heterogeneous structures are in the center of interest. We will study related aspects in context of realistic use cases, including those described in this paper.

References

[1] CEN-CENELEC-ETSI Smart Grid Coordination Group. Smart Grid Reference Architecture. (Nov. 2012). Version 3.0. [Online]. Available:http://ec.europa.eu/energy/gaselectricity/smartgrids/doc/xpert_group1_reference_architecture.pdf

[2] M. G. Kanabar, I. Voloh, and D. McGinn, "Reviewing smart grid standards for protection, control, and monitoring applications," presented at IEEE PES Innovative Smart Grid Technologies, 2012.

[3] S. Schriegel and J. Jasperneite, "Sicherheits-und datenschutzan-forderungen an smart grid-technologien," *Elektrotechnik & Informationstechnik*, vol. 129, no. 4, pp. 265–270, 2012.

[4] A. Zaballos, A. Vallejo, M. Majoral, and J. M. Selga, "Survey and performance comparison of AMR over PLC standards," *IEEE Transactions on Power Delivery*, vol. 24, no. 2, pp. 604–613, 2009.

[5] K. Brand, V. Lohmann, and W. Wimmer, *Substation Automation Handbook*. Utility Automation Consulting, 2003.

[6] J. Ekanayake, N. Jenkins, K. Liyanage, J. Wu, and A. Yokoyama, *Smart Grid: Technology and Applications*, 1st ed. Wiley, 2012.

[7] R. F. Nuqui, "State estimation and voltage security monitoring using synchronized phasor measurement," Ph.D. dissertation, Virginia Polytechnic Institute and State University, 2001.

[8] F. Cleveland, "IEC 61850-7-420 communication standard for distributed energy resources (DER)," in *Proc. IEEE Power and Energy General Meeting*, 2008, pp. 1–4.

[9] F. Skopik, Z. Ma, T. Bleier, and H. Grneis, "A survey on threats and vulnerabilities in smart metering infrastructures," *International Journal of Smart Grid and Clean Energy*, vol. 1, no. 1, pp. 22–28, 2012.

[10] P. D. McDaniel and S. E. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy*, vol. 7, no. 3, pp. 75–77, 2009.

[11] M. C. Travis Goodspeed and Joshua Wright. (2008). Hacking AMI. [Online]. Available: http://inguardians.com/pubs/090202-SANS-SCADA-Hacking%20AMI.pdf

[12] J. Wright. (2009). Killerbee: Practical zigbee exploitation framework. [Online]. Available: http://inguardians.com/pubs/090202-SANS-SCADA-Hacking%20AMI.pdf

[13] R. DeBlasio and C. Tom, "Standards for the smart grid," in *Proc. IEEE Energy 2030 Conference*, 2008, pp. 1–7.

[14] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, 2010.

[15] I. Erlich, W. Winter, and A. Dittrich, "Advanced grid requirements for the integration of wind turbines into the german transmission system," presented at IEEE Power Engineering Society General Meeting, 2006.

[16] F. Skopik, A. Treytl, A. Geven, B. Hirschler, *et al.*, "Towards secure time-triggered systems," in *Proc. SAFECOMP Workshops*, 2012, pp. 365–372.
[17] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, *et al.*, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Industrial Informatics*, vol. 7, no. 4, pp. 529–539, 2011.
[18] J. Wang and V. C. M. Leung, "A survey of technical requirements and consumer application standards for ip-based smart grid ami network," in *Proc. International Conference on Information Networking*, 2011, pp. 114–119.
[19] OpenID Foundation. (2013). Openid foundation website. [Online]. Available: http://openid.net
[20] T. Humphreys, B. Ledvina, M. Psiaki, B. O'Hanlon, and P. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in ION GNSS, The Institute of Navigation, 2008.
[21] A. Treytl, G. Gaderer, B. Hirschler, and R. Cohen, "Traps and pitfalls in secure clock synchronization," in *Proc. Int. Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, 2007, pp. 18–24.
[22] J. S. Warner and R. G. Johnston. (2003). GPS spoofing countermeasures. [Online]. Available: http://lewisperdue.com/DieByWire/GPS-Vulnerability-LosAlamos.pdf
[23] F. Cleveland, "Enhancing the reliability and security of the information infrastructure used to manage the power system," in *Proc. IEEE Power Engineering Society General Meeting*, 2007, pp. 1–8.
[24] The Smart Grid Interoperability Panel Cyber Security Working Group. (2010). Guidelines for smart grid cyber security: vol. 1, smart grid cyber security strategy, architecture, and high-level requirements. [Online]. Available: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628 vol1.pdf
[25] The Smart Grid Interoperability Panel Cyber Security Working Group. (2010). Guidelines for smart grid cyber security: vol. 2, privacy and the smart grid. [Online]. Available: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628 vol2.pdf
[26] The Smart Grid Interoperability Panel Cyber Security Working Group. (2010). Guidelines for smart grid cyber security: vol. 3, supportive analyses and references. [Online]. Available: http://csrc.nist.gov/publications/nistir/ir7628/ nistir-7628 vol3.pdf
[27] Federal Office for Information Security. (March 2013). Protection profile for the gateway of a smart metering system, V.1.2. [Online]. Available: https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html.
[28] (Sept 2012). Common criteria for information technology security evaluation, part 3: security assurance components, version 3.1, revision 4. [Online]. Available: http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf
[29] K. J. Muller, "Verordnete sicherheit-das schutzprofil fur das smart metering gateway-eine bewertung des neuen schutzprofils," *Datenschutz und Datensicherheit*, vol. 35, no. 8, pp. 547–551, 2011.
[30] Federal Office for Information Security. (March 2013). Protection profile for the security module of a smart metering system, V.1.0. [Online]. Available: https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Security/security module node.html
[31] Federal Office for Information Security. (March 2013). Technische richtlinie BSI-TR-03109, V.1.0. [Online]. Available: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/index htm.html
[32] European Commission. (2011). Standardization mandate to European standardisation organisations (ESOs) to support European smart grid deployment. [Online]. Available: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf
[33] CEN-CENELEC-ETSI Smart Grid Coordination Group. (Nov. 2012). First Set of Standards, Version 2.0. [Online]. Available: http://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/First%20Set%20of%20Standards.pdf
[34] US National Institute for Standards and Technology (NIST). (2010). Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. [Online]. Available: http://www.nist.gov/public_affairs/releases/upload/smartgridinteroperability final.pdf
[35] CEN-CENELEC-ETSI Smart Grid Coordination Group. (Nov. 2012). Sustainable Processes, Version 1.0. [Online]. Available: http://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Sustainable%20Processes.pdf
[36] CEN-CENELEC-ETSI Smart Grid Coordination Group. (Nov. 2012). Smart grid information security. [Online]. Available: http://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf
[37] S. M. Amin and B. F. Wollenberg, "Toward a smart grid: Power delivery for the 21st century," *IEEE Power and Energy Magazine*, vol. 3, no. 5, pp. 34–41, Sep 2005.
[38] L. H. Tsoukalas and R. Gao, "From smart grids to an energy internet: Assumptions, architectures and requirements," in *DRPT*, 2008, pp. 94–98.
[39] European Regulators Group for Electricity and Gas (ERGEG), *Ergeg-Public Consultation: Position Paper on Smart Grids no. e09-eqs-30-04*, Berlin, 2010.
[40] M. Amin, "Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid," *PES General Meeting*, pp. 1–5, 2008.
[41] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, 2010.
[42] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in *Innovative Smart Grid Tech.*, Jan 2010, pp. 1–7.
[43] S.-Y. Wang and C.-S. Laih, "Efficient key distribution for access control in pay-tv systems," *IEEE Transactions on Multimedia*, vol. 10, no. 3, pp. 480–492, 2008.
[44] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy Magazine*, vol. 7, no. 3, pp. 75–77, 2009.
[45] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. IEEE International Conference on Smart Grid Communications*, 2010, pp. 238–243.
[46] D. P. Varodayan and A. Khisti, "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage," in *Proc. International Conference on Acoustics, Speech, and Signal Processing*, 2011, pp. 1932–1935.
[47] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proc. International Conference on Smart Grid Communications*, 2010, pp. 232–237.
[48] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the smart-grid," in *Proc. International Conference on Privacy Enhancing Technologies*, 2011, pp. 175–191.
[49] F. Li, B. Luo, and P. Liu, "Secure and privacy-preserving information aggregation for smart grids," *Int. J. Secur. Netw.*, vol. 6, no. 1, pp. 28–39, Apr. 2011.
[50] A. Cavoukian, J. Polonetsky, and C. Wolf, "SmartPrivacy for the smart grid: Embedding privacy into the design of electricity conservation," *Identity in the Information Society*, vol. 3, no. 2, pp. 275–294, Aug 2010.

[51] AMI-SEC. Advanced metering infrastructure security task force, homepage. (2013). [Online]. Available: http://osgug.ucaiug.org/utilisec/amisec
[52] K. Moslehi and R. Kumar, "A reliability perspective of the smart grid," *Innovative Smart Grid Technologies*, vol. 1, no. 1, pp. 57–64, 2010.
[53] A. P. A. Ling and M. Masao, "Selection of model in developing information security criteria for smart grid security system," in *Proc. Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops*, May 2011, pp. 91-98.

Florian Skopik joined AIT in 2011 and is currently working in the research program ICT Security, focusing on diverse security aspects of distributed systems and service-oriented architectures.
Current research interests include secure smart grids and the security of critical infrastructures, especially in course of national cyber defense. Before joining AIT, Florian received a bachelor degree in Computer Science 2006, and master degrees in Computer Science Management and Software Engineering from the Vienna University of Technology in 2007. He was with the Distributed Systems Group at the Vienna University of Technology as a research assistant and post-doctoral research scientist from 2007 to 2011, where he was involved in a number of international research projects. In context of these projects, he also finished his PhD studies. Florian further spent a sabbatical at IBM Research India in Bangalore for several months.
He published around 50 scientific conference papers and journal articles, and is member of various conference program committees and editorial boards. In parallel to his studies, he has been working in the industry as firmware developer for microcontroller systems for more than 10 years.

Lucie Langer joined the Safety & Security Department of AIT Austrian Institute of Technology in 2012. She is currently working on projects related to the security of critical infrastructures and smart grids. Before joining AIT she has been working as a Technology Consultant in the private sector for two years, focusing on access rights and infrastructure management in large-scale IT projects. As a Research Assistant with the Cryptography & Computer Algebra Group at Technische Universit ̈at (TU) Darmstadt she participated in several security-related research projects on e-government between 2006 and 2010. In 2010 she received her PhD from TU Darmstadt's Computer Science Department for a thesis on privacy and verifiability aspects of electronic voting. She holds a master's degree in Mathematics from TU Darmstadt (2006) and Darmstadt University of Applied Sciences (2004).