SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2014; **7**:160–174
Published online 21 February 2013 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.703

SPECIAL ISSUE PAPER

Why securing smart grids is not just a straightforward consultancy exercise

Maria B. Line*

Department of Telematics, Norwegian University of Science and Technology (NTNU), N-7491 Trondheim, Norway

ABSTRACT

The long-term vision for modernization of power management and control systems, *smart grid*, is rather complex. It comprises several scientific traditions: supervisory control and data acquisition systems, automation systems, information and communication technology, safety, and security. Integrating information and communication technology systems and power management and control systems causes a need for a major change regarding system design and operation, in which security controls are required and implemented, and how incidents are responded to and learned from. This paper presents concerns that need to be addressed in order for the implementation of smart grids to succeed from an information security point of view: a unified terminology, a fusion of cultures, improved methods for assessing risks in complex and interdependent systems, preserving end users' privacy, securing communications and devices, and being well prepared for managing unwanted incidents in a complex operating environment. Copyright © 2013 John Wiley & Sons, Ltd.

KEYWORDS

information security; smart grids; advanced metering infrastructure; information and communication technologies; privacy

***Correspondence**

Maria B. Line, Department of Telematics, Norwegian University of Science and Technology (NTNU), N-7491 Trondheim, Norway.
E-mail: maria.b.line@item.ntnu.no

1. INTRODUCTION

Smart grids will result in increased instrumentation for monitoring and control in the low voltage distribution grid, distributed generation (micro wind turbines, solar panels, etc.), energy storage, and electric vehicles. The parts of the grid that include generation and high-voltage transmission of power are already modernized and do not need such large-scale investment in order to meet future demands. The distribution grid is the part of the power grid that transmits power from substations to end users such as companies and private households. Figure 1 shows the power grid value chain from the generation, via the transmission and distribution grids, to the end users [1].

The deployment of advanced metering infrastructures (AMIs) is the first big leap in the direction of the smart grid vision. This allows for automatic reading and gathering of customers' power consumption. The distribution system operators (DSOs) may use this data for both billing and grid management purposes. The customers can be charged more correctly than before; as the prices vary each hour throughout the day, the customers may be rewarded for using less power during the most costly hours. They may receive tariff information through the smart meter as a means to control their own power consumption. This pricing mechanism may contribute to reducing the consumption peaks that are expensive to both the customers and the DSOs. The DSOs will receive close-to-real-time information on power demand and consumption that they can use for managing production and response.

In addition to smart meters, the households may also be equipped with consumer appliances with web interfaces and remote control. The introduction of AMI will contribute to improving the utilization of the power grid, reducing restoration times, and giving users more control over their consumption and bill.

Several countries have started to roll out AMI. In Italy, the large DSO Enel SpA has rolled out AMI to more than 30 million customers, which makes this the largest AMI deployment so far. Canada, the UK, and the Netherlands are other countries that have started, and also, in Norway, there are demonstration and research activities in this area, especially through Demo Steinkjer (Nord-Trøndelag E-verk; www.demosteinkjer.no) and Smart Energy Hvaler (Fredrikstad Energi AS; www.smartenergihvaler.no).

With the AMI comes two-way communication between the DSOs' back-end systems and the customers' smart meters. This implies a tighter coupling between power automation systems and general information and communication technology (ICT) systems.

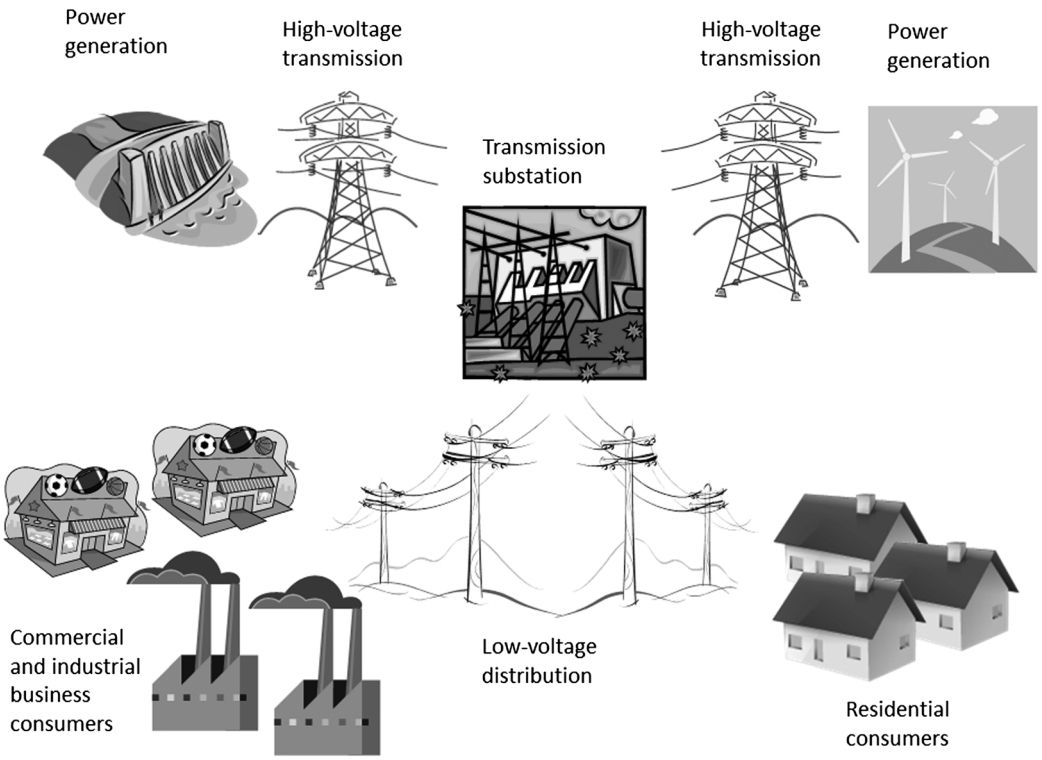

Figure 1. The power grid value chain.

Power automation systems have traditionally been based on proprietary technologies operating in closed networks. They have been designed to fulfill quite specific purposes and, by many, have not even been recognized as ICT, even though they are indeed a combination of hardware, firmware, and software. The information security objectives have been limited as connectivity and availability have been the most prioritized properties; confidentiality and integrity have not received the same attention. The attack surface has been quite limited as well, mainly because the systems have operated without network connections and they have not been connected to the Internet. Incidents usually occur as a result of hardware failures, and lack of monitoring may make it difficult to identify the exact location of the failure.

Information and communication technology systems, on the other hand, consist of commercial-off-the-shelf technologies operating on TCP/IP networks, and they are usually designed to fulfill multiple purposes. Such technologies are widely used, they frequently have quite open and accessible interfaces, and attackers find it attractive to exploit known and unknown vulnerabilities and cause minor or major damage. Incidents usually occur as a result of software failures, directly or indirectly, and complexity makes it difficult to avoid and detect such failures.

The vision of smart grids imposes the meeting of the two cultures of power automation and ICT.

This paper discusses information security challenges ahead and investigates how well current research addresses these challenges. Technical aspects as well as human and organizational aspects are covered, as the success of smart grids depends not only on technological innovations but just as much on changes in work processes, competence, and understanding. Future research and development needs are also pointed out.

The multitude of concepts and terminologies in this discipline is discussed in the following section, before reflections on culture and traditions within both power automation and ICT are provided in Section 3. Special considerations required during risk assessments for smart grids are presented in Section 4, and privacy issues arising with the AMI roll-out are described in Section 5. Existing recommendations for smart grid security architectures are provided in Section 6. Section 7 discusses information security incident management from a smart grid point of view, and examples of real-life information security incidents are provided. Section 9 looks beyond the limitations that information security usually poses and shows expected positive effects of smart grids, before further work is described and concluding remarks are given in Section 9.

2. CONCEPTS AND TERMINOLOGY

As the power industry is heading towards smart grids, more branches of science and engineering must be involved. There will be a need for new expertise, products, and solutions within fields such as communication infrastructures, hardware and software products and services, and information security solutions. Hence, there is a broad spectrum of

professionals addressing the topic of power automation systems. However, their approaches differ as they represent different traditions with different world views, cultures, terminology, work processes, and methods. To ensure a common understanding and efficient integration processes, a common terminology has to be established.

Thereafter, there needs to be a common understanding of the business processes and priorities in the power industry. Professionals being new to this industry must be open-minded and willing to learn about its traditions and, at the same time, bring in their own knowledge and experience, to enrich the industry. An efficient cooperation can then take place when this succeeds, when the main priorities are agreed upon and all professionals manage to contribute with their own specialties.

2.1. The system—which system?

There will be a tighter coupling between the power automation systems and ICT systems. But what does this really mean? Which systems are covered by the term *power automation systems*? And is this term the most appropriate and correct term to use? There are several terms denoting this kind of system; *power automation system* is one; others are *process control systems*, *control systems*, *supervisory control and data acquisition (SCADA)* systems, *distribution management system*, *energy management system (EMS)*, and *production systems*. Professionals working in this domain, performing monitoring and management of these systems in a control room, know what is meant by each of these terms and are able to explain the differences. However, ICT professionals who are now entering the power industry are usually not familiar with such systems, especially not to the level of detail needed in order to be able to "speak the language," which is an essential prerequisite for an efficient collaboration.

Ericsson [2] mainly uses the term *power control systems*, but he also mentions *SCADA/EMS* and *power system communication systems*. The latter refers to the fact that power control systems have been more integrated lately; SCADA systems and substations are now interconnected with other systems, and both a dedicated line and the Internet are used for communication. He does not distinguish between SCADA and EMS, but denotes them together, *SCADA/EMS*, without explaining what kinds of systems each of them refers to.

Wei *et al*. [3] use several terms, such as *power grid automation systems* and *power grid automation networks*, *automation and control systems*, *SCADA*, and *power automation systems*, but they mainly use the latter. They also include a figure illustrating how the different components and systems are connected. For the purpose of clarification, a similar figure is also presented in this paper (Figure 2). It shows a typical architecture for power automation systems, all systems related to monitoring and operation of the power grid. *SCADA/EMS* denotes the part of the system that is operated from a control room. One control room can manage several substations and also be connected to other control rooms. The upper part of the figure shows the corporate systems, which consist of what is usually denoted as regular ICT systems.

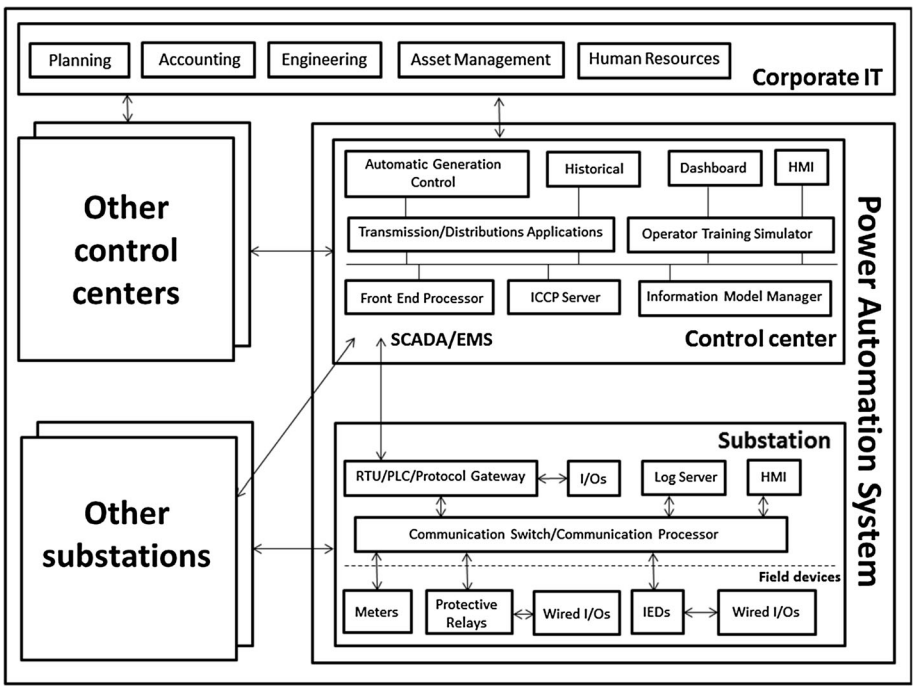

Figure 2. A typical power automation system. SCADA, supervisory control and data acquisition; EMS, energy management system; HMI, Human Machine Interface; IED, Intelligent Electronic Device.

Datta Ray *et al*. [4] speak of *industrial control systems (ICSs)*, *power grid control information systems*, and *power grid operation systems*. They distinguish between *operations technology (OT)* and *information technology (IT)*, and also denote these two systems as *control systems and IT systems*, and *legacy systems and corporate IT systems*. Their message would be clearer if they could stick to one set of terms and, if necessary, mention alternative terms in the beginning. At least, they state early in the paper that they will use the terms OT and ICS interchangeably. Khan *et al*. [5] speak of *SCADA* and *distributed control system*, but do not explain the differences or connections between these two.

For an ICT professional, it may seem like distribution management system, EMS, and SCADA are all parts of the larger power automation systems. However, it is not quite clear how they are connected and/or integrated. *Process control systems* and *production systems* are general terms used in several industries. Hence, they denote similar systems as the term *power automation systems*, but the latter is industry specific. Therefore, throughout this paper, the term *power automation systems* will be used to denote all systems and functionalities operated from the control center and substations related to management of the power grid, in accordance to Figure 2.

The terms *administrative systems* and *corporate systems* are often used as a counterpart to the power automation systems. They include all ICT systems needed to operate the corporate parts of the DSO: project management, contracts, financial information, human resources, and the like. Usually, the terms *ICT* and *IT* are used interchangeably, where both denote systems that are based on TCP/IP/Ethernet technologies. The term *ICT systems* will be used throughout this paper.

2.2. Security comes in many flavors

The term *security* is subject to several different interpretations depending on who are the sender and the receiver of the message. In the field of computer science, *security* usually means *information security*; although it could also denote the more limited concepts of *computer security* or *network security*. The term *cyber security* is used in some contexts, usually related to automation and control systems. This is a term that is not explicitly defined by International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000:2009 [6], which is the standard defining the most relevant terms within information security. However, in the literature, it seems like cyber security is a constructed term that mixes the fields of cybernetics and computer security, and hence, is widely used to denote ICT security in control systems.

Information security comprises the three attributes of confidentiality, integrity, and availability [6]. Also, the properties of non-repudiation, authentication, audit, and privacy are associated attributes, without them being part of the well-established definition. An information security event is defined to be an identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of controls, or to be a previously unknown situation that may be security relevant [6]. Then, an information security incident is defined as a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [6].

A related term to *security* is *dependability*, which usually describes the inability of a system to affect its environment in an undesirable way. The main purpose of dependability mechanisms is to protect life, health, and the environment from damage. It is also regarded as protection against random incidents [7]. Security, on the other hand, can be seen as the inability of the environment to affect the system in an undesirable way [8], or as protection against intended attacks. However, an incident compromising a system's security can lead to the system acting in an unfortunate way, and a security breach can cause a dependability breach. The two properties dependability and security are closely connected and need to be addressed accordingly. Traditionally, the power grid has been more concerned with dependability than security. With the introduction of smart grids, where ICT systems will be a critical component, security issues need to be considered.

The fields of dependability and security have different terminologies. As an example, a dependability breach may be denoted as a *fault* or an *accident*. Security breaches, on the other hand, may exploit what are denoted as *errors* or *bugs*. A *safety hazard* may correspond to a *security threat*. Avizienis *et al*. [9] thoroughly present concepts and taxonomies of dependability, which they see as a property that includes safety reliability, availability, integrity, and maintainability. They compare these to the field of security, which they see as quite related, but still different from, dependability, as it includes confidentiality, availability, and integrity, as also defined by ISO/IEC 27000 [6]. There are substantial differences when it comes to methods and methodologies between the two fields of dependability and security. Please refer to Line *et al*. [8] for an overview of common methods within each of the fields, including an analysis of similarities and differences.

Power security, on the other hand, is a quite different concept from information security. It usually refers to the ability of providing energy to customers. There is a certain parallel to the property of availability for ICT systems, but these two should still not be mixed up. It is therefore important to specify what kind of security one refers to. In this paper, information security is the main concern, and it will be denoted as information security, not just security, to make sure that confusions are avoided.

2.3. Current standards and guidelines

Several standards and guidelines exist that deal with different aspects of information security. Governmental organizations, academic institutions, industry, and interest groups are among the publishers. Two of the most recognized

publishers are ISO (www.iso.org), cooperating with the IEC (www.iec.ch), and the National Institute of Standards and Technology (NIST; www.nist.gov) at the U.S. Department of Commerce.

The ISO/IEC has published a set of standards and documents on information security matters in their 27000 series. Topics include information security management system, risk management, measurement and metrics, incident management, and network security. Cyber security and application security are two of the topics that are planned for the near future. It is natural to assume that the area of smart grids should be well suited for such joint standards.

Among the broad collection of documents from NIST, it is worth mentioning their Computer Security Incident Handling Guide [10], Guide to Industrial Control Systems Security [11], and Guidelines for Smart Grid Cyber Security [12–14]. As such, NIST considers security requirements for automation systems from an information security point of view, which is an important contribution in bringing information security expertise into the world of automation. In a survey of 104 energy security professionals [15], more than 70% of the respondents stated that security has not been adequately addressed in smart grid deployment and that smart grid security standards move too slowly to keep pace with smart grid deployment.

The aforementioned set of standards give directions on how information security could be organized, and a set of baseline requirements to both organizational and technical aspects. The general information security standards should indeed be adapted to a smart grid setting.

3. CULTURE AND TRADITIONS

Power automation systems and ICT systems have traditionally been operated separately. There have been limited, if not zero, logical connections between them, and they have served quite different purposes. The staff operating the two systems tend to have different backgrounds: electric power engineering and computer science. The technology bases are different and so are management routines. Wei *et al*. [16] point at four major differences between the power automation systems and ICT systems:

- Security objectives: whereas ICT aims at integrity, confidentiality, and availability, in that order, power automation is first and foremost concerned about human safety, before continuous operation and protection of physical components.
- Security architecture: whereas ICT has the central server with the highest security level in the middle of the network, power automation needs to protect all edge nodes just as well as the central control systems.
- Technological base: the variety of systems in use in ICT is limited compared with the number of proprietary systems and technologies used in power automation.
- Quality-of-service requirements: whereas rebooting is a common way of fixing an unstable office computer, this is not accepted in the power automation system as it results in disruption of operation, which usually has potentially huge financial consequences.

Power automation systems were built to run continuously without interruptions in quite specific operating environments. Information security measures were not among the requirements as there were no relevant threats in that category. Authentication, encryption, and detection of incidents are therefore usually not implemented in typical automation systems nor is the hardware designed with enough memory and processing capacity to support such mechanisms [17], which calls for new information security mechanisms that are specifically designed to fit the technical properties of power automation systems and still let them fulfill their operational requirements.

Incidents affecting power automation systems may however have severe consequences, both to business operation and even to life, health, and the environment. Such consequences are usually more associated with safety than security, and hence, the systems have been designed to meet safety requirements. This is also what characterizes the mindset of the staff operating power automation and distribution systems.

Fabro *et al*. [18] stress the need for understanding of cyber security as a fundamental condition for successful implementation of smart grids:

> *"(. . .) Without properly understanding the inherent risk in the Smart Grid, we risk either abandoning an exceptionally promising solution for energy issues or deploying a system that could be the Achilles heel of any industrialized nations critical infrastructure."*

3.1. Information security culture

Power automation staff are used to their proprietary systems not being connected to any external network and hence not used to think about the outside world as a possible threat towards their systems. They do not even necessarily recognize their systems as actually being ICT. ICT staff are used to computers failing from time to time, needing a reboot before they work all right again. Downtime is unfortunate, but sometimes necessary, and does not always have large financial consequences, especially not if it is planned. Testing and installing patches are quite common. In power automation, testing and installing patches are extremely difficult as they most probably lead to some downtime. *If it works, do not touch it*, is a tacit rule of thumb, which results in large parts of such systems being outdated and unpatched, and hence, vulnerable to a great number of known attacks.

Recognizing an information security incident is difficult if one is not trained for it. Experiences from the oil and gas industry show that a computer may be unstable for days

Security Comm. Networks 2014; **7**:160–174 © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/sec

and weeks without anyone recognizing it as a possible virus infection [19]. Ensuring that the organization detects and handles such an incident is a cultural challenge just as much as a technical one.

Even vendors of hardware and software within the domain of automation and control have a challenge ahead regarding information security culture. Information security needs to be a fundamental property of all products entering a networked environment, and vendors must accept their responsibility in these matters. They should ensure that their engineering processes include information security features from the beginning. In addition, they need to learn to appreciate feedback that they may have on vulnerabilities and bugs. Govindarasu and Hahn [20] discuss what the power industry has to learn about such vulnerability disclosure. There are some competent computer analysts out there testing software systems for flaws and vulnerabilities, merely because they think it is challenging and fun. Their purpose is usually not to misuse the weaknesses they might discover; they rather notify the system owner or system developer and give them the chance to fix the problems within a reasonable time frame before they eventually publish information on it to the public. This method is usually referred to as "responsible disclosure" [21]. Vendors should embrace such feedback rather than ignore it, as it is better to know about the vulnerabilities and be able to fix them, than experiencing directed attacks where the vulnerabilities are exploited.

3.2. Academia—islands of disciplines

In academia, there are quite clear divisions between departments such as computer science, electrical engineering, cybernetics, and electric power engineering, all of which need to be actively participating in the smart grid evolution. Such divisions are reflected in organizational structures, research projects, scientific publications, and teaching. When students graduate, they carry with them this mentality of isolated scientific traditions, and their future employers are most likely organized like the universities, with the same types of clear divisions. Also, there are differences between the disciplines regarding terminology, culture, and methods. Obviously, this challenges the success of smart grids, which depends on successful scientific and professional cooperation.

The industry is forced to integrate experts from different areas and minimize these established divisions. They have already realized that they will not succeed with their smart grid deployment without such collaboration. Academia, both universities and research institutions, needs to strive to overcome their existing divisions as well and overcome the multidisciplinary challenges to take part in the smart grid evolution.

Both computer scientists and electrical engineers contribute with papers within the domain of information security in smart grids. The authors' background has a great influence on which terminology is used in a paper. In many cases, it seems like the audience is assumed to be from within the same scientific area as the author. Authors should rather take into account that readers may have a different background than themselves and that several terms and concepts may have different meanings within different scientific fields. Within the topic of smart grids, experts from a broad range of scientific fields share the interest of reading each other's work. Papers should be written for a broader audience; hence, one should always specify concepts and terms to make sure that there will be no misunderstandings or room for personal interpretations, as discussed in Section 2.

Several scientific papers claim to present information security challenges or research related to smart grids. However, in many cases, the results are not really smart grid-specific. The authors just state that the results are applicable for the smart grid domain as well as the domain that was originally the objective of the research. This might very well be true but needs to be thoroughly justified. As the smart grid area is still quite new, papers that try to adapt well-known results from one area into this new one can be quite useful. As time goes by, it is expected that more research will be carried out with smart grids as the main focus. Results from this research will have more impact and provide more value than many of the papers published up till now.

4. RISK ASSESSMENTS

Several methods and tools exist to support risk assessments, some lightweight and some more comprehensive. Performing a comprehensive risk assessment may seem like an ordeal; therefore, it is usually a good idea to start with a high-level assessment to have a first impression of the system and the main threats and vulnerabilities. Then, some of the most interesting findings could be further elaborated through a more detailed assessment. The first phase of any risk assessment is to clearly define the object of consideration: which parts of the systems should be assessed and which parts should be left out.

Figure 3 [22] shows a conceptual model of the AMI, where the smart meter in a private home communicates directly with the front-end system at the DSO or via a concentrator in a substation. Different communication technologies can be used, depending on what is available and most suitable in the specific geographical area. Such a figure is a sufficient starting point for a high-level risk assessment. The next steps include identifying technical interfaces, possible technologies, participating actors, and preferably a set of scenarios or use cases for the system in focus. Thereafter, the assets of the systems (the values, what is to be protected) should be identified before threats (what can cause an incident) and vulnerabilities (what makes the system susceptible for the threats) are described. Possible consequences from an incident should then be documented. The resulting risk is then a product of the consequences and the probabilities of occurrence of unwanted incidents. This describes a regular risk assessment for any ICT system in general.

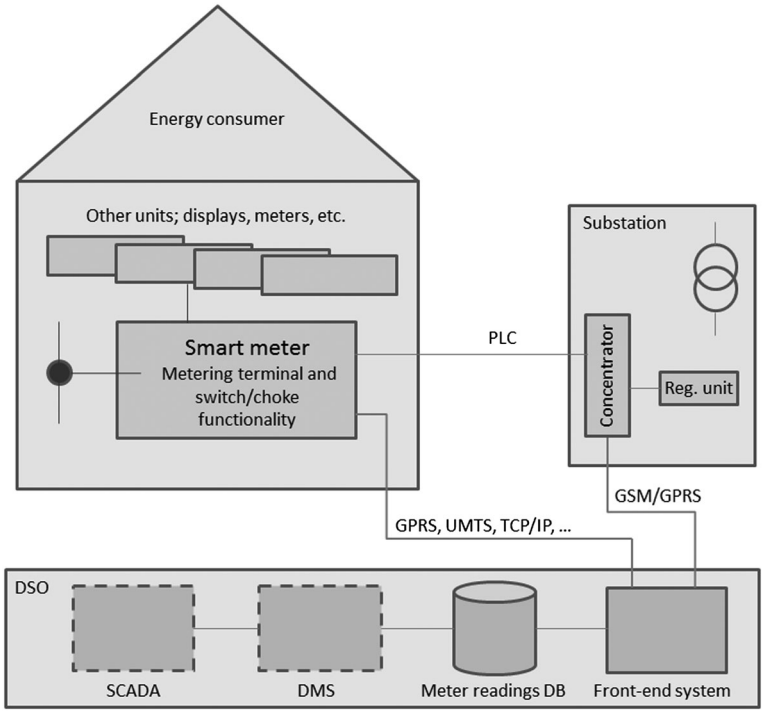

Figure 3. Advanced metering infrastructure [22]. SCADA, supervisory control and data acquisition; DMS, distribution management system; DSO, distribution system operator; GPRS, general packet radio service; UMTS, Universal Mobile Telecommunications System; PLC, Power Line Communication; DB, Database; GSM, Global System for Mobile Communication.

4.1. Cross-sectorial interdependencies

For each ICT system, there are usually some characteristics that need special attention. For the smart grids, there is the property of dependence. The power supply will depend just as vitally on ICT systems as ICT systems already vitally depend on power supply. As an example, an information security breach to the power automation systems may cause power outage. This outage may also affect the same power automation systems and put them out of function. Naturally, there should be extra power supply available, but it is quite important that this redundant supply last long enough to ensure availability for the power automation systems during a crisis. This two-way dependence must be recognized as it requires some extra thought when performing risk assessments. Methods exist that support such cross-sectorial assessments, as Kjølle *et al*. describe in [23].

Datta Ray *et al*. [4] discuss risk management approaches specifically tailored for smart grids. They recognize the challenges of studying ICT systems and power automation systems combined and provide a set of methods for modeling threats and vulnerabilities. They refer to the well-known models STRIDE for classification of the following threats [24]:

- spoofing,
- tampering,
- repudiation,
- information disclosure,
- denial of service, and
- elevation of authority or privilege;

and DREAD; for classification of the following vulnerabilities [24]:

- damage potential,
- reproducibility,
- exploitability,
- affected community, and
- discoverability.

However, they still point out the need for more research in the area of risk assessments for smart grids in order to obtain adequate support for viewing ICT systems and power automation systems in a correlated manner.

4.2. Measuring risks

The total cost for information security includes both investments on preventive mechanisms and financial consequences of unwanted incidents, both damage, and repair and recovery. These two need to be balanced. Standardized methods for calculating risks would help in determining where to put the investments. ISO/IEC 27004 [25] provides guidance on assessment of the effectiveness of an information security management system and controls. The

standard supports the requirements described in ISO/IEC 27001 [26]. It describes how attributes can be quantified and converted into indicators tailored for decision making.

Some research effort has been put into the topic of measuring risk and modeling vulnerabilities in smart grids as well. Hahn and Govindarasu [27] present a framework for analyzing the exposure of cyber attacks in a smartgrid. Their framework is based on access graphs, which relate to attack trees and attack graphs—techniques that are commonly used in vulnerability modeling. Each component and interface of a system is represented as nodes, and the edges represent possible ways for an attacker of entering and leaving nodes. Each edge is weighted, and the weight is set based on the level of effort that is needed to compromise that edge. The weights can be recomputed after a change to any security mechanism is performed to see how this change affects the total vulnerability of the system. Determining the weight, however, is no exact science, but some estimates would at least show which edges are more prone to be exploited than others. A general problem with access graphs, just like attack trees and attack graphs, is that it is almost impossible to include all possible attack vectors. Also, only known vulnerabilities can be used for modeling, which leaves out zero-day vulnerabilities, existing vulnerabilities that are not yet discovered. Zero-day vulnerabilities represent a great problem, as it might be attackers that make the first discovery. Ten *et al*. [28,29] have done quite extensive research in the area of measuring risk using both generalized stochastic Petri nets and attack trees for modeling vulnerabilities in and attacks to SCADA systems. Negrete *et al.* [30] present a method for evaluating the financial impacts of cyber attacks. They use a four-layer structure: physical network, communications/control, commodity market, and cyber security. The latter is the top layer, representing investment alternatives and upgrades to the security on the communications/control layer. It does not seem obvious why the cyber security layer is the top layer, as it might relate closely to the first two layers. Still, the authors show how the impacts of attacks change depending on different levels of security investments. The impacts may also be time variant, as an attack at noon may have different consequences for the market than an attack at midnight.

Research approaches like these are praiseworthy attempts on using metrics for evaluating information security in smart grids, which is indeed a challenge. However, theoretical models and methods may seem like great ideas when initially described, but there is a lack of scientific papers thoroughly evaluating the actual use of such metrics more extensively than just as a proof-of-concept. There are some fundamental challenges that need to be overcome in order to make measurements work in practice. In some areas, estimating probabilities of occurrence of unwanted incidents is a mathematical or statistical exercise. For ICT systems, this is a complex and often impossible exercise [17]. Attackers' possible goals and strategies should be thoroughly considered, but it can be quite hard to grasp all their capabilities and motivations. The probability of someone wanting to attack a nation's power system may change from one day to the next because of political circumstances. Smart grids are just as complex as ICT systems alone—complex interdependencies in infrastructure combined with (quite often) incomplete documentation of systems and several possible threats. Probability estimation based on an experienced gut feeling may actually be the best possible alternative.

Another issue is ease of use. Implementing yet-another-process requiring personnel resources, documentation, a management system and attention from top management can be quite difficult to go through within an organization. Lightweight, not time-consuming, efficient, giving value, these are all properties of importance when designing the optimal measurement protocol.

4.3. ICT security threats—what's new?

In general, threats to ICT systems are well known, and there exist several well-known and well-functioning countermeasures. Limitations of these countermeasures are also well known, as well as how they still can be quite successfully implemented. If this was not the case, large-scale hacker attacks would succeed every day, resulting in totally unusable ICT systems and a major slowdown in efficiency in a large part of industry and public services worldwide.

Well-known threats and attacks are however continuously improved (from the attackers' point of view) to hit new types of computer systems, such as automation and control systems. The trend of connecting such systems to the Internet makes them vulnerable to attacks that can be remotely executed. With offline systems, the attacker needs to have physical access to the target systems in order to execute an attack. With online systems, targeted attacks can be executed from anywhere in the world. Also general, untargeted attacks may hit all kinds of systems as long as they are online.

Implementing all possible information security measures is never an optimal solution. This is quite costly and will not be worth the investment. Obtaining 100% security should therefore not be a goal but rather determining an appropriate level of security and implementing the measures needed to obtain this is far more realistic. Determining an information security level corresponds to determining what are the acceptable risks, and then being prepared to manage unwanted incidents.

5. PRIVACY

With the old metering technologies in place, each household reads their meters quarterly or monthly and reports to the utility company for billing. With the new smart meters implemented, the utility companies will automatically receive measurements collected much more frequently, several times a day. For billing purposes, hourly readings are needed, but for grid management purposes, the DSOs can make use of

per-minute readings or even per-second readings. These are huge amounts of data related to each household. Usage data must be kept confidential as they can tell a lot about the lifestyle and habits of the specific household. In its most simple form, it will clearly show when someone is at home and when the house is empty [31].

One week of readings will give quite clear indications on when the house will be empty during the next week, which is interesting information for someone planning robberies. More detailed readings can reveal information on which activities take place inside the house, as many household appliances have unique signatures that can be read from fine-grained metering data [32]. Such information can be of interest to house robbers looking for a specific TV or other specific household appliances; to commercial advertisers, who can personalize their messages and products when they know their receivers' habits; to the police, as certain criminal actions such as growing cannabis plants will leave their own fingerprint in the usage data; to employers wondering whether their employees are skipping work; and to insurance companies doing research on their customers before paying compensations. There is no doubt that usage data must be protected from unauthorized inspections, and there must be clear rules and guidelines in place describing what this data may be used for and who should have access, as there is for other similar large-scale collections of personal information, such as money transactions, phone calls, and broadband usage.

Much research is being carried out within the area of privacy in the smart grid, and then especially related to smart metering, as this is the area where the main privacy challenges arise.

5.1. Protection of consumption data

Non-intrusive appliance load monitoring techniques [32,33] can be used for decoding energy consumption data into which individual household appliances are in use. A reading frequency of 15 min can identify some of the most common appliances. An increase of the reading frequency will increase the accuracy of appliance identification. Efthymiou and Kalogridis [34] suggest a method for overcoming this privacy issue by giving each smart meter two different IDs: one anonymous ID, which is used for the most frequent metering reports used for management and network control purposes, and one known ID, which is associated with the household and used for billing purposes. Assuming that the anonymizing process including key and certificate exchanges and the suggested escrow third party can be trusted, this method will contribute to preservation of privacy, as the most frequent readings will be anonymized and hence not possible to track back to a specific household.

However, the utility companies are interested in knowing more than just the total energy consumption from each meter. For production planning and grid management, they find it quite useful to know what kind of household each meter reading belongs to. Fhom *et al.* [35] address this privacy issue by suggesting a different approach, introducing a user-centric privacy manager that allows each individual customer to control which and how much information is disclosed to which other smart grid parties. A smart energy gateway (SEG) should be the node connecting each home, including smart appliances and the meter itself, to the power supplier, distribution network supplier, billing provider, and other relevant actors. Each purpose, or functionality, will be represented by a corresponding software agent on the SEG, and the security architecture of the SEG should support secure multiplexing access to physical resources so that the different software agents would not interact in unfortunate and unsecure ways. Introducing such a privacy manager would give the end users access to inspect what kind of data is actually collected and by whom, including the possibility of having a certain amount of control over this data collection. This would provide a degree of transparency, which is not present today.

It should be carefully considered whether users would be interested in controlling their own privacy. Some should rather be protected from themselves, from being able to perform unfortunate choices. The majority of end users will most probably not be able to understand their privacy exposures and even less able to understand how to mitigate them. The services provided must therefore be privacy-preserving and trusted by default; the principle of privacy-by-design should be followed at all times during development and in operation, such that the customers do not have to be concerned about their own privacy.

In June 2011, the European Data Protection Supervisor (www.edps.europa.eu) provided an Opinion on the Commission Recommendation on preparations for the roll-out of smart metering systems [36]. He recommends that consumers should not be forced to install a smart meter if they do not want the advantages of time-of-use tariffs. Alternatively, the functionalities of granular readings and the remote on/off control should be disabled as a default setting, and an informed consent must be given before they are enabled.

This idea follows the privacy-by-design principle and lets the consumer choose whether he allows a privacy-invasive method being used for correct billing or accepts the risk of paying higher bills than strictly necessary. The DSOs would however still want to have more accurate readings than today in order to ease and increase the quality of grid management. Two methods to consider in this matter are to keep the reading frequency lower than every hour; it might suffice to read once or twice a day. If more detailed readings are strictly needed, meter data should be anonymized and preferably aggregated in order to preserve the privacy of the consumers.

5.2. Use of consumption data

Legislation on protecting personal information varies in different countries. In some countries, it is sufficient to notify the owner when the terms or purposes of use change, as opposed to ask for consent. The US-based NIST has provided guidelines for privacy and the smart grid [13],

Security Comm. Networks 2014; **7**:160–174 © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/sec

where they discuss the concept of privacy and how smart grids may pose privacy challenges. The guidelines contain recommendations for mitigations of smart grid privacy issues as well, and the intended readers include all entities that are involved with personal information related to smart grids in some way. A European Union (EU)-initiated Task Force on Smart Grids has also identified recommendations for data handling, data security, and data protection [37]. They provide an overview of the European legislation, identify potential risks in the handling of personal data, discuss data and access rights, and analyze how such issues should be handled. They also criticize the NIST report and state that it is too much based on end users' consent; the task force would rather see clear regulations on what kind of data may be collected and for which purpose.

In Norway, the Personal Data Act [38] is quite clear in stating that personal information may only be collected for specified purposes, and the owner of the information shall be informed and asked for consent if the collected information is to be used for other purposes than first planned. The data owner has the right to refuse, and an acceptance needs to be actively granted, as opposed to a tacit acceptance. The Norwegian Data Inspectorate has provided a guide specifically related to personal data in connection with smart metering [39]. This guide is intended to help the DSOs to fulfill the requirements stated in the Personal Data Act.

The European Data Protection Supervisor is looking into whether further legislative action is needed on an EU level. He would specifically like to see more guidance on retention periods and recommends that the use of privacy-enhancing technologies and similar techniques for data minimization is made mandatory. He also points out that each consumer should have direct access to their energy usage data.

Guidelines and recommendations from institutions like NIST and EU-initiated working groups, in addition to data protection supervisors and data inspectorates, are indeed necessary for helping DSOs and other parties in preserving consumers' privacy when implementing smart metering. Privacy is an important principle that should not be sacrificed for the interest of efficiency and new technological possibilities and solutions, and having the consumers' trust is essential for smart grids to be a success.

Large amounts of personal information have been stored for a long time by several actors; securing such storage can be obtained without large research efforts. However, research is needed to fully investigate how the privacy-by-design principle can be followed in practice when developing smart meters and implementing an AMI. The development and use of privacy-enhancing technologies, anonymization, aggregation, and possibly new and still unknown techniques are indeed required.

6. SECURITY ARCHITECTURE

A thorough modernization of the aging power grid infrastructure implies the need for an appropriate information security architecture. In each device, the communication channels and the interfaces between them need to be secured, privacy issues for the consumers must be addressed, the strategy of defense-in-depth should be obeyed, and the large geographical spread of the network must be carefully taken into account. Both a high-level holistic view and in-depth focused investigations are needed in order to decide on an appropriate information security architecture.

The operational requirements governing power automation systems today cannot be circumvented. Performance must be maintained; continuous operation as well; and the properties of hardware and software already in use must be regarded when designing new mechanisms, as described in Section 3.

The worldwide approved ISO standards represent the best starting point. They could be supplemented with the comprehensive documentation published by NIST—a set of guidelines on smart grid cyber security strategy, architecture, and high-level requirements [12]. Their architecture includes a set of domains, a high-level view on actors, and a logical reference model for the smart grid, in addition to a thorough list of high-level information security requirements. The Advanced Security Acceleration Project has provided a more focused document, describing a security profile for AMI [40]. It addresses the complete AMI from the smart meter at the consumer's side to the meter data management system at the DSO's side. This documentation is also quite comprehensive and is aimed for organizations developing or implementing AMI solutions. These reports describe current good practice, although local adaptations of the recommendations, based on risk assessments and actual incidents, if any, are needed when they are put into use.

Ericsson [2] describes how the power automation grid started out as "islands of automation" and became more integrated as time went by. The utility companies have been asking for more openness—commercial-off-the-shelf products and more integrated systems. This seems to be the future for the power industry. Ericsson suggests to decouple the operational SCADA/EMS system from administrative systems to ensure an appropriate information security level. This, however, is a step backwards and does not appear as a future-oriented solution. He then discusses the approach of studying SCADA/EMS systems in terms of domains, where business operations are grouped together and each domain has an information security policy, a set of requirements, mechanisms, and one responsible "authority". It is claimed that this will ensure a minimum security level for all systems within the same domain.

Wei *et al*. [16,3] propose a novel security framework for power grid automation systems. This is designed to meet the requirements of integration in a non-intrusive fashion, performance in terms of modularity, scalability, extendibility, and manageability, and also alignment to the Roadmap to Secure Control Systems in the Energy Sector [41]. The framework consists of three layers (power, automation and control, and security), and the three major conceptual components in the framework are as follows:

- *Security agents*: protection at the networked device level, firmware or software, access control, and IDS.

- *Managed security switch*: for protection of bandwidth and prioritizing of data, used across the automation network.
- *Security manager*: in the center of the power automation network, a security agent master; obtains and downloads patches to security agents, and collects data from agents.

Test results show that the security agents did not imply significant reduction of performance on SCADA communication, some vulnerabilities were mitigated or partially mitigated, and the IDS reported some findings.

Boroomand *et al*. [42] address the topic of deciding the optimal level of automation in a SCADA setting, thereby mitigating cyber security risks. The authors motivate their work by pointing out the new security challenges following the implementation of smart grids, where security and reliability are not always aligned. The concept of varying the level of automation based on current threat level is intriguing, and finding the optimal balance between human responsibilities and automatic processes also related to incident detection and response is an interesting idea. However, it is not always the case that a system based on human decisions and actions is more secure than fully automated systems, as it seems to be assumed by the authors. Humans make mistakes, and the higher complexity of the system and tasks, the higher probability for wrong decisions or at least minor mistakes, which in the worst cases may have quite severe consequences.

Proving that certain information security mechanisms do not affect SCADA performance is a rather hard exercise. Performing tests and evaluations in smaller lab facilities may show good results, but the real world is usually a bit more complex than what we manage to set up in the lab. Also, some of the stated operational requirements are difficult to test extensively no matter how realistic the test facilities are.

7. INCIDENT MANAGEMENT

Potential computer break-ins, industrial espionage, malware attacks and denial-of-service attacks are some of the threats to ICT systems that companies face today. As smart grids are complex systems consisting of complex power grids that interact with equally complex ICT systems, these threats will in the near future also be highly relevant for the power industry as well. The ability to appropriately prepare for, and respond to, information security incidents is essential for companies that need to ensure and maintain continuous operation of their systems.

Incident management is the process of detecting and responding to incidents, including supplementary work as learning from the incidents, using lessons learned as input in the overall risk assessments, and identifying improvements to the implemented incident management scheme. ISO/IEC 27035 incident management [43] describes the complete incident management process. This is a fairly new standard (2011) but is based on a technical report that was produced in 2004. The process comprises five phases: plan and prepare, detection and reporting, assessment and decision, responses, and lessons learned. The guideline is quite extensive and will indeed be costly to adopt to the letter, but it is a collection of practical advice, key activities, and examples, and is indeed useful for companies establishing their own security incident organization. The ISO standard addresses corporate systems in general and does not contain any considerations related to power automation systems. There is a need to delve into the standard and adopt it for a smart grid setting, where corporate systems and control systems are connected in different ways.

In their Guidelines for Smart Grid Security (NISTIR 7628), NIST describes a set of high-level requirements for incident response for a smart grid information system [12]. All requirements are however on the governance, risk, and compliance level, and are therefore more high level than what the ISO standard provides. They contain no practical advice; hence, they are more useful in a planning process than during business operation. They also contain no specifics related to the cooperation of corporate systems and control systems. In part 3 of their Guidelines [14], NIST however points out the need for research on incident response for the cross-domain of ICT and power systems. More specifically, the issues of response and containment, intrusion detection and prevention, and event and impact prediction are emphasized.

NIST 800-61 [10] addresses computer security incident handling, whereas NIST 800-82 [11] contains several recommendations for securing ICSs, including a comprehensive overview of vulnerabilities. The security profile on AMI [40] that contains a large number of security concerns, guidance, and controls related to AMI also includes a separate section on incident response. The requirements are quite high level, similar to those listed in the ISO standard and NISTIR 7628 as well, but at least, they are directly addressing AMI, which is an important part of smart grids.

There are not many scientific papers describing real-life experiences regarding incident management. The Annual FIRST Conference Forum for Incident Response Teams (www.first.org) brings together such expertise worldwide, and one or two presentations each year seem to cover real-life experiences. These presentations are however not publicly available afterwards. A large amount of available publications from relevant venues are concerned with the technical reporting systems in use, vulnerability registration, establishing response teams, and computer forensics—topics that are indeed relevant but not as interesting as experience papers would be. Metzger *et al*. [44] present their real-life experiences, covering the complete process from detection, response, reporting, and even some short notes on how lessons learned were used in the improvement process at the end of the incident handling cycle.

Hennin described in 2008 the Cyber Attack Alert Tool project [45] that aimed at developing an industry standard protocol for sharing information about control system

cyber incidents across all critical infrastructure sectors. The project idea seemed promising, as it was going to focus on early warnings, as opposed to the Repository of Industrial Security Incidents (www.securityincidents.org) database, which contains reports written in the aftermath of incidents and where a quite costly membership is required to gain access. However, it has turned out to be difficult to find papers describing results from the Cyber Attack Alert Tool project, so it is not known whether the project led to a breakthrough.

Although standards and recommendations exist on the area of incident management, also with respect to smart grids, there is a lack of documented research and experience related to managing incidents in an operating environment where automation systems and ICT systems are closely integrated. An efficient incident management process is just as important as technical information security measures when continuous operation is a governing requirement.

7.1. Real-life incidents

Information and communication technology security incidents are indeed not science fiction, they are already happening. During the last 10 years, there have been several examples of power outages or other types of damage to automation and control systems caused by hackers, untrusted employees, or software failures. The most famous attack up till now is Stuxnet [46–48], which appeared during summer 2010 as an advanced piece of malware created to target ICSs. Such systems have been attacked before, but not with this kind of specifically designed malware. Stuxnet is important mostly because it demonstrated that it is indeed possible to perform attacks against critical infrastructure and even infrastructure not connected to the Internet. Quite recently, it was announced that the USA and Israel were behind Stuxnet, and the intention was to attack Natanz, an Iranian power plant [49]. Natanz was indeed attacked, but a minor bug in the Stuxnet exploit made Stuxnet go "in the wild" and hit several other systems worldwide.

Another recent attack, Night Dragon [50], was identified in November 2009 as an attack targeted at the energy sector. The goal was harvesting of sensitive information related to competitive proprietary operations and financial details regarding field bids and operations. A similar attack was also discovered in Norway 2 years later [51]; 10 large companies within defense, oil, and energy experienced industrial espionage attacks where communication were being monitored, and the goal was to capture sensitive information. These two cases did not specifically target automation and control systems, but it shows that the energy sector is an attractive target for attackers, and smart grids imply that the attack surface increases; there will be more ways of attacking a company or the industry as a whole, subsequently causing damage that impact larger parts of the society.

Duqu and Flame are two pieces of malware that have similarities to Stuxnet, and researchers therefore believe that all three of them were created by the same authors [52-54]. They were detected in September 2011 and May 2012, respectively, but they are both believed to date from 2007. Duqu is a reconnaissance tool, and Flame is an espionage tool, and both have Iran's nuclear program as the main target, just like Stuxnet did. Flame has hit private companies, academic institutions, governmental systems, and home users, not automation and control systems specifically. It has been around for a long time without being detected; antivirus suppliers have therefore not provided any functionality for detecting nor removing a Flame infection [?].

Flame and its relatives represent the kind of threats that the power industry need to be prepared for. A planned and directed attack towards the industry should be assumed to comprise attempts to cause physical damage together with attempts to gather confidential information.

8. NOT JUST NEGATIVE PROSPECTS

Information security is more often seen as a limitation than an enabler. This might be due to the nature of security; there is usually a trade-off between security and properties such as functionality, user-friendliness, performance, efficiency, and cost. Still, the fact is that many services cannot be set to life without at least a basic level of security. In the case of smart grids, which is a critical infrastructure, or more correctly a combination of two critical infrastructures (power and ICT), information security issues must be addressed appropriately.

When critical information security challenges are overcome, the smart grid represents a huge potential for the industry. It will provide for more efficient management of the grid, real-time monitoring of demand response, efficient error detection and repair, and the possibility of affecting end users' energy consumption in such a way that a major investment in upscaling the grid capacity may be avoided, or at least postponed. End users may contribute to environmental advantages if they are able to exploit the smart grid in the right way; with more correct billing—a clear connection between consumption and the bill—they might reduce their total consumption, and they may take part in power production by having their own windmill, solar panel, or the like, and hence contribute to increasing the amount of renewable energy.

It is easy to point out many challenges, both security-wise and other, when talking about smart grids. However, when two or more scientific fields meet, there are great possibilities ahead. Cross-discipline cooperation makes people see their own field in new ways, which can lead to results and innovations that otherwise would not be discovered.

9. CONCLUSION AND FURTHER WORK

Successfully adapting good ICT security practice to power automation, distribution, and control systems, while at the

same time fulfilling the current requirements for power grid operation, is a huge step in the direction of successfully securing the smart grid. Local adjustments are however needed in order to comply with existing solutions and local laws and regulations. Still, there are smart grid-specific challenges that need to be addressed that are not possible to solve through existing measures.

Technical measures are not sufficient for obtaining secure smart grids. Increased understanding, knowledge, and awareness are needed among both ICT staff and power automation staff. They need to cooperate more extensively than today, and they need to understand each other's mindsets, terminology, needs, and information security objectives. The whole organization needs to be onboard, and organizational and cultural changes cannot be bought. Neither should they be expected to have a "quick fix"; a careful and long-term approach is required. Otherwise, there is a risk of ending up with two opposites—the ICT people and the power automation people—both fighting for their views and their priorities, and both being afraid of being redundant. The top management must recognize organizational and cultural measures as a major priority area and lead the way by truly showing that collaboration and mutual understanding is needed in order for smart grids to be a success.

Securing the smart grids is therefore not just another security project. It takes more than time and money to succeed.

A large part of smart grid research today concerns AMI specifically, even though there are many uncertainties ahead regarding smart grids: are the smart meters a kind of a smart grid, will there be more to it, when will the concept of smart grids be achieved, who will do it, what are the benefits, and so on. AMI is just the beginning of the smart grid roll-out. While the industry fully focuses on implementation of the AMI, researchers should contribute looking forward to what comes next.

We plan to study how ICT security incidents are being detected and responded to—both by technical measures and by human actions—and how the aftermath is handled—information sharing, lessons learned, and how experiences are transferred into the overall work with information security in companies operating power automation and control systems. This must be studied with respect to both ICT systems and the power automation and control systems in order to identify cooperation, possible synergy effects from future cooperation, and the management system in general. This will require a socio-technical approach, as the field of research is neither only technology nor man but indeed a combination of the two. It will be impossible to improve anything without addressing both. The results of this work will hopefully contribute to efficient and successful incident management in smart grids environments, where the worlds of ICT and automation meet.

ACKNOWLEDGEMENTS

I would like to thank Professor Svein J. Knapskog (NTNU), Senior Scientist Martin G. Jaatun (SINTEF), Professor Poul E. Heegaard, and PhD student Jonas Wäfler (both NTNU) for providing invaluable input and comments and participating in fruitful discussions.

REFERENCES

1. Kluza J. Status of grid-scale energy storage and strategies for accelerating cost-effective deployment. PhD Thesis, MIT 2009.
2. Ericsson GN. Cyber security and power system communication—essential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery* 2010; **25**(3):1501–1507.
3. Wei D, Lu Y, Jafari M, Skare PM, Rohde K. Protecting smart grid automation systems against cyberattacks. *IEEE Transactions on Smart Grid* 2011; **2**(4): 782–795.
4. Datta Ray P, Harnoor R, Hentea M. Smart power grid security: a unified risk management approach. *IEEE International Carnahan Conference on Security Technology (ICCST)*, 2010; 276–285.
5. Khan H, Xu Z, Iu H, Sreeram V. Review of technologies and implementation strategies in the area of smart grid. *Australasian Universities Power Engineering Conference (AUPEC)*, 2009; 1–6.
6. ISO/IEC 27000:2009 Information security management systems—overview and vocabulary 2009.
7. Idsø ES, Jakobsen ØM. Objekt- og informasjonssikkerhet: metode for risiko- og sårbarhetsanalyse (in Norwegian). *Technical Report*, Norges Teknisk-Naturvitenskapelige Universitet (NTNU) 2000.
8. Line MB, Nordland O, Røstad L, Tøndel IA. Safety vs security? *Eighth International Conference on Probabilistic Safety Assessment and Management (PSAM)*, Stamatelatos M, Blackman H (eds). ASME Press: New York, 2006.
9. Avizienis A, Laprie JC, Randell B, Landwehr C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing* 2004; **1**(1):11–33.
10. NIST. 800-61: Computer Security Incident Handling Guide 2008.
11. NIST. Guide to Industrial Control Systems (ICS) Security 2011.
12. NIST. 7628-1: Guidelines for Smart Grid Cyber Security 2010.
13. NIST. 7628-2: Guidelines for Smart Grid Cyber Security 2010.
14. NIST. 7628-3: Guidelines for Smart Grid Cyber Security 2010.
15. nCircle, EnergySec. 2012 Smart Grid Cyber Security Survey. *Technical Report*, nCircle 2012. URL http://

www.ncircle.com/index.php?s=resources surveys Survey-Smart Grid-2012
16. Wei D, Lu Y, Jafari M, Skare P, Rohde K. An integrated security system of protecting smart grid against cyber attacks. *IEEE Innovative Smart Grid Technologies (ISGT) 2010*, 2010; 1–7, doi:10.1109/ISGT.2010.5434767.
17. Rativa LCT. Risk assessment for power system security with regard to intentional events. PhD Thesis, Institut Polytechnique de Grenoble 2008.
18. Fabro M, Roxey T, Assante M. No grid left behind. *IEEE Security & Privacy* 2010; **8**(1):72–76.
19. Jaatun MG, Albrechtsen E, Line MB, Tøndel IA, Longva OH. A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection* 2009; **2**:26–37.
20. Govindarasu M, Hahn A. What the power industry has to learn about cyber vulnerability disclosure. IEEE Smart Grid Newsletter January 2012. URL http://smartgrid.ieee.org/newsletter/january-2012/479-whatthe-power-industry-has-to-learn-about-cyber-vulnerability-disclosure?utm_source=IEEE+Smart+Grid&-utm_campaign=f4bc47e6e9-January_2012_Smart_-_Grid_Newsletter1_17_2012&utm_medium=email
21. Shepherd SA. Vulnerability disclosure. *Technical Report*, SANS 2003.
22. Line MB, Johansen GI, Sæle H. Risikovurdering av AMS. Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS. *(In Norwegian)*. *Technical Report*, SINTEF 2012.
23. Kjølle GH, Utne IB, Gjerde O. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. *Reliability Engineering and System Safety* 2012; doi:10.1016/j.ress.2012.02.006. URL http://www.sciencedirect.com/science/article/pii/S09518320120 0021X.
24. Swiderski F, Snyder W. *Threat Modeling*. Microsoft Press: Redmond, Washington, 2004.
25. ISO/IEC 27004:2009 Information technology—Security techniques—Information security management—Measurement 2009.
26. ISO/IEC 27001:2005 Information security management systems—Requirements 2005.
27. Hahn A, Govindarasu M. Smart grid cybersecurity exposure analysis and evaluation framework. *IEEE Power and Energy Society General Meeting*, 2010; 1–6.
28. Ten CW, Liu CC, Manimaran G. Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, Nov 2008; **23**(4): 1836–1846, doi:10.1109/TPWRS.2008.2002298.
29. Ten CW, Manimaran G, Liu CC. Cybersecurity for critical infrastructures: attack and defense modeling. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans* 2010; **40**(4):853–865. doi:10.1109/TSMCA.2010.2048028.
30. Negrete-Pincetic M, Yoshida F, Gross G. Towards quantifying the impacts of cyber attacks in the competitive electricity market environment. *IEEE PowerTech Bucharest*, 2009; 1–8.
31. Lisovich MA, Mulligan DK, Wicker SB. Inferring personal information from demand-response systems. *IEEE Security and Privacy* 2010; **8**(1):11–20.
32. Hart G. Residential energy monitoring and computerized surveillance via utility power flows. *Technology and Society Magazine, IEEE* 1989; **8**(2):12–16. doi:10.1109/44.31557.
33. Drenker S, Kader A. Nonintrusive monitoring of electric loads. *Computer Applications in Power, IEEE* 1999; **12**(4):47–51. doi:10.1109/67.795138.
34. Efthymiou C, Kalogridis G. Smart grid privacy via anonymization of smart metering data. *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2010; 238–243, doi:10.1109/SMARTGRID.2010.5622050.
35. Simo Fhom H, Kuntze N, Rudolph C, Cupelli M, Liu J, Monti A. A user-centric privacy manager for future energy systems. *International Conference on Power System Technology (POWERCON)*, 2010; 1–7, doi:10.1109/POWERCON.2010.5666447.
36. The European Commission Recommendation on preparations for the roll-out of smart metering systems (2012/148/EU) 2012.
37. Task Force Smart Grids Expert Group 2: Regulatory recommendations for data safety, data handling and data protection 2011.
38. LOV-2000-04-14-31 Lov om behandling av personopplysninger (personopplysningsloven) (in Norwegian), Ministry of Justice and Public Security 2000.
39. The Norwegian Data Inspectorate: guide for processing of personal data in connection with automatic metering systems within the energy sector 2011.
40. ASAP-SG. Security profile for advanced metering infrastructure 2010.
41. Roadmap to secure control systems in the energy sector 2006.
42. Boroomand F, Fereidunian A, Zamani M, *et al*. Cyber security for smart grid: a human-automation interaction framework. *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES*, 2010; 1–6, doi:10.1109/ISGTEUROPE.2010.5638949.
43. ISO/IEC 27035:2011 Information technology—Security techniques—Information security incident management 2011.
44. Metzger S, Hommel W, Reiser H. Integrated security incident management—concepts and real-world experiences. *Sixth International Conference on IT Security Incident Management and IT Forensics (IMF)*, 2011; 107–121.

45. Hennin S. Control system cyber incident reporting protocol. *IEEE Conference on Technologies for Homeland Security*, 2008; 463–468.
46. Falliere N, Murchu LO, Chien E. W32.Stuxnet Dossier. *Technical Report*, Symantec February 2011.
47. Albright D, Brannan P, Walrond C. Did Stuxnet take out 1000 centrifuges at the Natanz enrichment plant? *Technical Report*, Institute for Science and International Security (ISIS) 2010.
48. Albright D, Brannan P, Walrond C. Stuxnet Malware and Natanz: update of ISIS December 22, 2010 Report. *Technical Report*, Institute for Science and International Security (ISIS) 2011.
49. Sanger DE. Obama order sped up wave of cyberattacks against Iran 2012. URL http://www.nytimes.com/2012/06/01/world/middleeast/obama-orde red-wave-of-cyberattacks-against-iran.html?_r = 1
50. Global energy cyberattacks: "Night Dragon". *Technical Report*, McAfee 2011.
51. Johansen PA. Stjeler kontrakter, tegninger, passord og hemmelige data (in Norwegian) 2011. URL www.ap.no/nyheter/iriks/Stjeler-kontrakter-tegninger-passord-og-hemmelige-data-6698674.html
52. Perlroth N. Researchers find clues in malware 2012. URL http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html
53. Plikk N. Massivt cyberangrep pågår i Midtøsten (in Norwegian) 2012. URL http://www.aftenposten.no/digital/Massivt-cyberangrep-pagar-i-Midtosten-6838800.html
54. Greenberg A. New research shows Flame malware was almost certainly a U.S. or Israeli creation 2012. URL http://www.forbes.com/sites/andygreenberg/2012/06/11/new-research-shows-flame-malware-was-almost-certainly-a-u-s-or-israeli-creation/

DOI: 10.1002/sec