Cyber Security Challenges in Smart Grids

Maria B. Line, Inger Anne Tøndel, and Martin G. Jaatun, *Senior Member, IEEE*

***Abstract*—The introduction of telecommunication in the energy grid, leading the way towards Smart Grids, challenges the way safe operations have traditionally been assured in the energy sector. New cyber security challenges emerge, especially related to privacy, connectivity and security management, and these need to be properly addressed. Existing cyber security technology and good practice mainly come from the traditional tele-communication environment where the requirements on safety and availability are less strict. For Smart Grids, lessons can be learned from the oil and gas industry on how they have dealt with security challenges in their implementation of integrated operations. Still, Smart Grids face a slightly different reality, due to their extensive geographical distribution and the enormous number of end-users. The contribution of this paper is a survey of cyber security challenges for Smart Grids, together with a roadmap of how these challenges must be addressed in the near future.**

***Index Terms*—Information security, cyber security, Smart grids, privacy.**

I. Introduction

THE introduction of telecommunication networks in the power grid results in a need to deal with cyber security threats. Cyber security experts need to understand the grid, including the importance of security solutions that are able to meet the strict requirements to availability, efficiency and scalability. However, developers and operators of the grid also need to understand the cyber security implications of the Smart Grid vision.

The vision of the Smart Grid implies moving from "a relatively small number of carefully controlled devices" to "an Internet-like distributed environment" with a high number of devices [1]. Though Cohen [1] refers to one presenter at an IEEE meeting on this topic that stated that "we know how to secure the Internet", not many at that meeting – or elsewhere for that matter – would agree. There are a lot of security problems associated with the Internet, though there are mechanisms in place that solve or reduce some of these problems. Examples of problems highlighted by Cohen include the routing infrastructure, the general purpose endpoints and the risk of denial-of-service attacks.

Fabro et al [2] 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 nation's critical infrastructure."

This paper presents cyber security challenges related to the concept of Smart Grids. It discusses the amalgamation of power grids and telecommunication networks, and points thereafter to the differences and similarities between traditional safety and information security. A set of actual incidents threatening the operation of power grids are referred to, before threats and vulnerabilities are discussed with respect to the energy value chain of the power grid. The paper ends with a roadmap discussing how the cyber security challenges should be met – by adapting good practice from the oil and gas industry and initiating important information security research tasks in the context of Smart Grids.

II. Process Control vs Telecommunication Networks: The Meeting of Two Traditions

Both power distribution and telecommunication networks are natural components of the critical infrastructure, and both are large-scale complex systems where the complexity is hidden from the user. Both have traditionally used the pay per use business model, and although some flat-rate (e.g. per-month) telecommunication services exist, the advent of Cloud Computing is revitalizing the metered usage paradigm also for general computing. Both were designed for reliability, and are based on a large body of standards.

On the other hand, these networks were clearly developed for quite different purposes, with quite different baseline requirements, and they experience different use and propagation.

In electric power transmission, incidents usually occur due to hardware failures, and lack of monitoring may make it difficult to identify the exact place for the failure. Electric power is generally perceived as a unidirectional, homogeneous service from a central supply, where scaling of capacity is expensive and time-consuming; it involves building new power plants and rigging high-power distribution lines.

In telecommunication networks, incidents more often occur due to software failures, directly or indirectly, and complexity

This work was supported in part by the Telenor-SINTEF research agreement, Smart Grid initiative.

M. B. Line is a PhD student at the Institute of Telematics, Norwegian University of Science and Technology, Trondheim, Norway (e-mail: maria.b.line@item.ntnu.no).

I. A. Tøndel is a Research Scientist at SINTEF ICT, Trondheim, Norway (e-mail: inger.a.tondel@sintef.no).

M. G. Jaatun is a Research Scientist at SINTEF ICT, Trondheim, Norway (e-mail: martin.g.jaatun@sintef.no).

.

makes it difficult to avoid and detect such failures. The telecom market is competitive, with several providers offering more or less equivalent services. This also implies that the supply is distributed, and the service that is offered is heterogeneous in the sense that multiple commodities are offered through the same channel. Furthermore, telecom networks are bi-directional, since users both consume and produce data. Scaling of telecommunications services might be quick and cheap, since this often involves measures such as replacing a server in a datacenter.

Table I [3] summarizes main differences between power grids and telecommunication networks.

TABLE I
A COMPARISON BETWEEN POWER GRIDS AND TELECOM NETWORKS

	Power grids	**Telecom**
Supply	Central	Distributed
Service type	Homogenous (single commodity)	Heterogenous (multi-commodity)
Direction	Uni-	Bi-
Scaling of capacity	Expensive and time-consuming	Quick and cheap
Infrastructure	Local monopoly	Competing market
Incidents	Hardware failures	Software failures

Today, we see that there are numerous interdependencies, in that telecommunications networks cannot function without electricity, and future power distribution systems will probably rely on telecommunications networks for control.

A. Safety vs Security

Safety usually describes the inability of a system to affect its environment in an undesirable way, and hence the main purpose of safety mechanisms is to protect life, health and the environment from damage. Security, on the other hand, can be seen as the inability of the environment to affect the system in an undesirable way [4]. An incident compromising a system's security can lead to the system acting in an unsafe way and such, a security breach can cause a safety breach. The two properties safety and security are closely connected and need to be addressed thereafter. Traditionally, the power grid has been more preoccupied by safety than security. With the introduction of Smart Grids, where telecommunication networks is a critical component, also security issues need to be considered.

This paper addresses information security, also denoted as cyber security. The concept of information security comprises the properties of confidentiality, integrity and availability, and is the most exact term compared to cyber security, network security and IT security. Accountability, privacy, audit and non-repudiation are other information security properties, although they are not included in the definition of the concept [5].

Wei et al. [6] point at four major differences between the power grid, or process control systems in general, and telecommunication networks, or the traditional IT systems, when it comes to security requirements and security mechanisms:

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

B. The close relative: Integrated operations

The introduction of Smart Grids is to the energy sector what the introduction of Integrated Operations (IO) was to the oil and gas industry. IO implied a change of technology from proprietary stand-alone systems in closed/physically separated networks to standardized commercial-off-the-shelf (COTS) systems integrated in communication networks. Such a transition makes remote control and support possible, and results in savings in both time and money, as a few persons can simultaneously monitor a large set of installations. Though this effect is valuable to the power industry, it also results in increased networking between supervisory control and data acquisition (SCADA) systems and the general ICT infrastructure, which means that two worlds are colliding with respect to requirements, vulnerabilities, threats and appropriate countermeasures. Proprietary systems offline have an attack surface equaling almost zero, as an attacker would have to be geographically at the same place as the target system and have detailed technical knowledge on the system in order to be able to do harm. COTS systems online are subject to a complete different set of attackers and threats, as they can be reached from anywhere. And although detailed technical knowledge is still required, there are far more experts in COTS systems worldwide than there are experts in proprietary systems. Also, existing vulnerabilities and exploitation methods for COTS systems are well known to a large community.

III. REAL-LIFE STORIES – INCIDENTS AND ATTACKS

Process control systems have already shown to be susceptible to failures and attacks due to ICT vulnerabilities. Control system security expert Joe Weiss is quoted in Computerworld [7] saying that at least 170 cyber-related incidents causing outages have occurred, three of which were major regional outages. However, it is almost impossible to

find publicly available details on these incidents. Some commentators [8] claim that they are documented in the so-called RISI[1] database, but access to the database is restricted to members, and membership seems unreasonably expensive. The Wall Street Journal wrote about Chinese hackers breaking into the US grid control infrastructure in 2009 [9], but also in this case there seems to be a lack of technical details.

A. Stuxnet

The most well-known attack appeared in July 2010; a new and advanced piece of malware was detected that targeted industrial control systems. Stuxnet's goal was to reprogram industrial control systems of a specific type and to hide any changes. Though the malware was detected in July 2010, it is confirmed to have existed at least one year prior to that. Stuxnet was targeted at five organizations, all with a presence in Iran, and most infections were found in Iran, but because of Stuxnet's ability to self-replicate, it has also infected machines outside the target organizations. Investigations performed by Symantec show that on Sept 29th 2010 there were approximately 100 000 infected hosts. They had also observed 40 000 unique external IP addresses from over 155 countries – approximately 60 % from Iran [10][11][12] .

There is a lot of speculation regarding who is behind Stuxnet. Estimates from Symantec however show that it would take months to develop, need several developers and realistic testing facilities. As a result, it is generally believed that nation states were behind the attack, and Israel and USA have been suggested as likely candidates. Nothing has been confirmed, but an Israeli security chief has taken some credit for the malware [13]. It is also not clear what the consequences of the Stuxnet attack have been. Experts have found that Stuxnet was able to control the speed of motors, and was thus able to send nuclear centrifuges out of control [14]. Some has suggested that it has slowed Iran's nuclear program and that they even may need to replace nuclear centrifuges to get rid of the malware, but Iran does not confirm this [15]. Reported consequences outside of Iran are also limited.

Stuxnet is important for many reasons, but maybe mostly because it demonstrates that it is indeed possible to perform cyber-attacks against critical infrastructure, and even infrastructure not connected to the Internet.

B. Night Dragon

In November 2009 an attack targeted at the energy sector (oil, power and petrochemical companies) was identified, which seemed to be originating from China and was given the name Night Dragon [16]. The attack was rather complex, compound of several techniques like social engineering, spear-phishing attacks, exploitation of vulnerabilities in the MS Windows operating system, compromising of MS Active Directory and remote administration tools. The goal seemed to be harvesting of sensitive information related to competitive proprietary operations and financial details regarding field bids and operations. McAfee has described their analysis in detail of the attack in their white paper [16] and foresees that similar attacks in the future will be more focused on theft of specific data and intellectual property, rather than "just" misusing processing power.

C. Power outage caused by hackers

Computerworld reports on hackers causing a power outage by hacking into computer systems [17]. This happened in January 2008, and the outage affected several cities in regions not being identified, and the motive seemed to be extortion. The disclosure of the attack was thoroughly considered with respect to both benefits and risks, and further details were not provided.

D. Target: the oil and gas industry

Already in 2003, Security Focus reported that the infamous Slammer worm penetrated a computer network at a nuclear power plant in Ohio, US, and disabled a safety monitoring system for nearly five hours [18]. This infection did not cause any damage, because the plant was actually offline. But the infected network was believed to be protected by a firewall, which turned out not to be true. This incident acted like an early warning for what is actually possible for an outsider to achieve with an attack towards a process control system.

In August 2009, an employee in a Californian offshore contractor company was charged for hacking into a communications network that detected oil leaks [19]. He was not getting full-time hire and wanted to get back at his employer. Fortunately, his actions did not lead to any leak, but he still caused damage for thousands of dollars. The article points at the fact that safety systems contain vulnerabilities like any other computer system, and it is possible to cause catastrophic damage by making those safety systems fail.

IV. The Energy Value Chain – Cyber Security Challenges

The energy supply value chain comprises four components; generation, transmission, distribution and load, as illustrated in Fig. 1. With the shift to Smart Grids, telecommunication will be introduced to each of these stages. And such, each of the components, and the power grid as a whole, will be exposed to a new set of threats.

Fig. 1. The four components of the energy value chain

Generation is production of energy, and *transmission* is the transportation of energy of high voltage over long distances; from the geographical location of production to the *distribution* central, where the voltage is lowered and adapted to end-users. *Load* denotes the end-users, where energy is

[1] RISI: The Repository of Industrial Security Incidents, by the Security Incident Organization.

consumed. With Smart Grids the consumers will also be producers, in that excess power will be available to other end-users, and then this is no longer a "simple", unidirectional chain.

In the following, a presentation of the most important cyber security challenges for Smart Grids is provided. The challenges range from threats towards the infrastructure needed to realize the Smart Grid vision to the privacy of homeowners. Problems related to management of security in a complex grid environment are also described. The challenges are well-known to the Internet in general, and in this paper it is especially discussed how they relate to Smart Grids.

A. Connectivity

As already mentioned, the introduction of the Smart Grid implies a transition towards an Internet-like distributed environment where there are a high number of devices that are interconnected. As a result of the increased connectivity, systems that used to be well protected, such as SCADA systems controlling power generation can now be reached by new types of attackers and from a distance. Relevant attackers to consider may be criminals wanting to disable alarm systems via groups of cyber attackers dealing with blackmailing, to hostile nation-states.

Increased connectivity also opens up for new types of attacks as multiple components can be affected at once [1]. As an example, the high number of devices envisioned for the Smart Grid results in many sources for large-scale denial-of-service attacks. A successful attack may result in loss of control of (a high number of) system components during the attack, which can lead to physical damage, loss of efficiency, brown-outs, etc. [1]. In addition, failures, as well as attacks, may propagate from one system to another due to the high connectivity and use of standard components [20].

B. New trust models

People are used to viewing the control systems related to electricity as operating in a trustworthy environment. This has influenced design decisions. However, with the increased connectivity of the Smart Grid it is no longer safe to assume all participants are trustworthy [20]. As an example, it becomes important to take into account the homeowners who may not understand or follow all rules [1]. The consumers may even be interested in compromising the smart meters in order to save money, trying to make the smart meter report lower power consumption than what is actually real.

C. Security management

The number of devices that need to be managed, e.g. seen from a utility, will increase – possibly by several orders of magnitude. This poses challenges when it comes to maintenance, management of trust and monitoring for any cyber-intrusions [20]. One example of an area that is likely to pose challenges is that of key management. Many security measures will involve some sort of keys, e.g. for identifying smart meters and establishing cryptographic sessions. Managing such solutions requires staff resources, in addition to time and processing capacity at a level that may not be available (Khurana et al. [20] provide some estimates based on US conditions).

D. Software vulnerabilities – Malware attacks

Experience shows that software is crippled with security vulnerabilities. Though efforts have been made [21][22][23] to increase developers' understanding of how the number of software vulnerabilities and their criticality can be reduced, the number of software vulnerabilities stays high.

A large part of SCADA systems and other types of end points connected via the Smart Grid will consist of general purpose technology and solutions (e.g. MS Windows-based PCs). The use of general purpose components has many advantages, but also results in the risk that systems are subverted on a large scale by e.g. malware or erroneous or malicious updates [1]. General purpose systems are likely to have a number of well-known vulnerabilities that need to be patched. In addition, new vulnerabilities are commonly detected, and thus there is a need for a patching-regime that can make sure the system stays updated. However, patching is in general considered difficult in safety critical systems, as it is costly and may result in downtime – something that is generally not accepted. Some of these systems are also built on old versions of COTS systems that have not been patched – as they were not connected to the Internet – and where new patches are no longer provided.

The use of general purpose technology also opens up for new attackers. As there is a larger amount of attackers that have the expertise necessary and the motivation to identify new vulnerabilities. Thus the risks associated with directed attacks may increase. Cyber attacks have been part of several political conflicts lately [24][25][26], and it would be safe to assume that power grids are attractive targets for organized attacks in the future.

When it comes to custom made software, there is in general a rush to develop working solutions and a general lack of security testing. This leads to vulnerabilities in software, and Fabro et al. [2] provide several examples of how critical vulnerabilities have found their way into advanced meter infrastructure. They also point out that some of these vulnerabilities are well known in the PC community. In addition it has been found that the deployment of otherwise secure solutions has led to vulnerabilities. Thus, a challenge seems to be to communicate experiences from the ICT traditions to developers of solutions for the Smart Grid.

E. Consumers' privacy

On the consumer side, the introduction of smart meters and smart homes will be one of the most noticeable changes. The smart meter will automatically report back to the energy provider about the consumed amount of power, and the concept of smart homes will assist the consumer in controlling his power consumption, and also reducing it. The granularity of the collected consumption data will vary – everything from daily to sub-hourly intervals is likely, and the most advanced equipment can even provide data detailed enough to be able to identify appliance brands in use and malfunctioning appliances [27].

At any rate, placing such metering equipment in private homes has implications for the privacy of the citizens. Lisovich et al. [27] have shown that it e.g. will be quite possible to deduce when people are at home or away, and when they are sleeping, and to some extent which appliances are used. People may thus be right in considering their homes to be under surveillance by their energy service provider. This data needs to be well protected, during both transfer and storage, to avoid unauthorized persons or organizations gaining access. So, who may be interested in this type of private information? First, criminals can utilize consumption data to facilitate burglaries, e.g. by creating appliance lists and detecting occupancy patterns – even in the entire neighborhood. Secondly, marketers can utilize consumption data for targeted advertising. And third, law enforcement may wish to monitor home-based activities to e.g. detect criminal activity (like drug production) [27].

F. Human factors: cultural differences and lack of understanding

Experiences from the oil and gas industry when introducing integrated operations show that one of the main challenges regarding information security is on the human side [28]. Technical countermeasures are well known and well tested, so in this area it is more about choosing the appropriate mechanism related to cost and value for money than developing new mechanisms. But the well-known saying is still valid: A system's security level is not stronger than the weakest link. No matter how much is spent on technical protection mechanisms; if people who interact with the system lack knowledge and understanding, the system is not well protected.

Process control workers are used to proprietary systems not connected to any network, and hence not used to thinking about the outside world as a possible threat towards their domain. Their highest priority is keeping the system running in operation, because a fall-out usually means huge financial losses. "We don't have ICT," is a common perception among process control workers – also after the introduction of integrated operations [28].

IT workers are used to computers failing from time to time, needing a re-boot before they work all right again. Downtime is boring, but sometimes necessary, and does not always have large financial consequences. Testing and installing patches is quite normal. Ensuring confidentiality and integrity are often seen as more important than ensuring continuous operation – availability.

Integrating process control systems with IT systems require the two professions respectively working together and develop a common understanding. In process control, testing and installing patches is extremely difficult, as it most probably means some downtime. "If it works, don't touch it," is a safe rule of thumb; which results in large parts of process control systems being outdated and un-patched – and vulnerable to a great number of known attacks.

Recognizing a security incident is difficult if one is not used to it. Again, experiences from the oil and gas industry show that a computer may be unstable for days and weeks without anyone recognizing it as a possible virus infection [28]. Ensuring that the organization detects and handles such an incident is a cultural challenge just as much as a technical.

V. Addressing the Cyber Security Challenges – A Roadmap for Smart Grids

Chapter II. introduced the likeness between Integrated Operations (IO) and Smart Grids. Although the main technological changes are the same, there are still a few important differences that necessarily affect how the cyber security challenges are addressed. IO connect a few geographical locations for cooperation; typically offshore installations, onshore operation center and a few subcontractor offices, while Smart Grids connect power plants and system control centers with all households, businesses and buildings all over the country – and abroad. A limited number of nodes spread to a limited geographical area are much easier to secure than a network that spans a whole country. And as IO does not involve all citizens, privacy is less of an issue. Smart Grids, on the other hand, need to ensure privacy of all customers/end-users, and is also challenged by the fact that all customers will have physical access to equipment connected to the grid. Physical access to electronic components opens for much more advanced tampering and possible damage than network access only.

Even though Smart Grids faces more comprehensive cyber security challenges than Integrated Operations, transfer of useful experience and knowledge will have great value to the implementation of Smart Grids.

Power is the most fundamental infrastructure in a modern society; private households, health care, primary industries, finance, transport, telecommunication – they all depend on power in order to maintain normal operation [29]. The requirements for reliability and robustness are higher than for any other infrastructure, and it is therefore of utmost importance that the telecommunication networks that are used for monitoring and controlling each part of the energy value chain is secured appropriately.

PikeResearch [30] predicts that security will become the top Smart Grid concern and that serious investments will be required (worldwide spending on Smart Grid cyber-security is forecasted to $1.7 billion in 2013). Any actor wanting to be part of the Smart Grid needs to consider security issues.

As described in the previous chapter it is not sufficient to invest in technological security measures; one needs to include human factors as well as organizational aspects in order to achieve a secure system. In the following, a roadmap is presented containing both good practices, inspired by work carried out in the context of integrated operations, and research tasks ahead that need to be carried out in the near future.

A. Cooperation

Actors representing all sides of the power industry should cooperate on developing a set of baseline requirements for information security in Smart Grids [2]. Cooperating does not

mean exchanging business sensitive information, but discussing expectations and fundamental operational requirements, and agreeing on a minimum level of security requirements for all components and systems that are to be connected to the grid. The ISO/IEC 27001 – Information Security Management System – Requirements [5] could be used as a starting point. Such work has been carried out in the Norwegian oil and gas industry, resulting in an official guideline published by the Norwegian Oil Industry Association (OLF) [31].

In a societal perspective, there is a need to increase the understanding of dependencies between power and other infrastructures. Methods for performing risk assessments for critical infrastructure, considering the complete picture, need to be further developed and tested [32].

The NIST Smart Grid Interoperability Panel Cyber Security Working Group [33] had identified a number of other topics which can only be solved through cooperation between several organizations:

- Solutions for detecting security events across domains (power and telecom), and the analysis and response to such events.
- Resilience against denial of service attacks
- Auditing and accountability solutions that fit the complex grid environment.
- Privacy and access control solutions that allow effective communication without having businesses risk leakage of trade secrets, strategies or activities. It will also be important to reduce the implications and threats related to residences being monitored by the energy service provider [20].

B. Network mapping and risk assessments

Each actor should map their own computer networks – all components, systems and networks, including all network connections, internal and external, should be documented. An important part of this work is to recognize process control systems as ICT and include them in the mapping. One needs to know *what* to protect in order to protect it appropriately.

Risk and criticality assessments of all parts of the computer networks should be performed to support selection of the appropriate level of security measures. If critical components cannot be patched, they should be protected such that software vulnerabilities cannot be exploited remotely.

Advanced risk-based approaches is needed that make it possible to analyze potential cyber attacks and their consequences, that offer improved measurements of risk and that helps measure the mitigation effect of security solutions [33].

C. Security architecture

A security architecture should be developed that addresses all requirements – both operational and security [1]. The onion model [34] where several security layers are defined and there are different security requirements to each layer can be used as an inspiration. Access rules can be defined for each layer, both who has access and from where (geographical and from which systems). Research is still needed in order to develop an appropriate architecture that can evolve and is able to tolerate failures. Specific research challenges include [33]:

- security solutions that are able to meet real-time requirements
- interaction with legacy systems
- efficient composition of mechanisms, avoiding introduction of security problems

Another important research challenge is whether commercial off-the-shelf components and public networks actually can be used in a safe manner in the grid, and it must be considered whether alternative network technologies (independent of the Internet protocols) and architectures are needed, and how security can be built into prospective solutions.

Also, research is necessary for creating device architectures (e.g. for smart meters) that are scalable and cost effective, and at the same time tamper resistant and allow for secure remote recovery. This is important for reducing the risk that local attacks become distributed and affect the system at a larger scale [33].

D. Cryptography and key management

Cryptography and key management is a necessary research topic in order for Smart Grids to become reality [33]. Large-scale, economic key management is needed, that is efficient and has reduced requirements to centralization and persistent connectivity. There is also a need for cryptography solutions that take into account limitations on space and computation. Solutions must fit an environment with limited physical protection and various organizations that need to interact. This research topic addresses the challenge of security management.

E. Incident response

As mentioned earlier, there is a need for cross-organizational cooperation in order to develop the technical solutions for incident detection. Research is also recommended to improve intrusion detection in embedded systems [33]. But each organization must also prepare for the processes following such detection.

A scheme for responding to security incidents should be developed and the organization needs to train to ensure that the scheme will work in case of an actual incident [28]. Such a scheme needs to define how an incident should be recognized and reported, who is responsible for actions, how experiences from incidents can lead to improvement and prevent repetitions of similar incidents.

Crisis management systems exist already today, but they are generally lacking in decision support systems to specifically handle the effects of cyber attacks [33].

F. Awareness training

Awareness raising and training are crucial for addressing the issue of human factors. Employee and end-user

participation and two-way communication are success criteria for building a security culture [35]. ICT personnel need to understand the requirements and operation within the traditional power grid, while process control personnel need to understand the threats and vulnerabilities that actually are of great relevance to their proprietary components, systems and networks [1].

VI. Conclusion

An important part of the Smart Grid concept is introducing telecommunication as a means to manage the power grid. This makes the power grid vulnerable to a large set of new threats – new in the context of the power grid, but not new in the context of telecommunication. This provokes the need for security mechanisms addressing the threats appropriately while supporting the operational requirements, especially for availability, in the power grid.

Moving towards a Smart Grid is a long term investment and expensive process. Thus the grid should be built "future-proof" – also meaning that it should be able to survive future malicious attacks. As Smart Grids is just in the early beginning, it is possible to do things right from the beginning instead of rushing forward and return to the security challenges afterwards.

VII. References

[1] Fred Cohen, "The Smarter Grid," *IEEE Security & Privacy*, January/February 2010, p. 60-63, 2010.

[2] Mark Fabro, Tim Roxey and Michael Assante, "No Grid Left Behind", *IEEE Security & Privacy*, January/February 2010, p. 72-76, 2010.

[3] Poul Heegaard, "The power grid meets the Internet", Presentation at the Smart Grid Workshop, NTNU, Trondheim, 2011.

[4] Maria Line, Odd Nordland, Lillian Røstad and Inger Anne Tøndel, "Safety vs. Security?," in *Proceedings from Probabilistic Safety Assessment and Management (PSAM)*, New Orleans, 2006. ISBN 0-7918-0245-0.

[5] *ISO/IEC 27001:2005 Information security management systems – Requirements*, ISO/IEC 2005.

[6] D. Wei, Y. Lu, M. Jafari, P. Skare and K. Rohde, "An Integrated Security System of Protecting Smart Grid against Cyber Attacks," *Proc. Innovative Smart Grid Technologies (ISGT)*, Gaithersburg, Maryland, January 2010.

[7] Computerworld, "Stuxnet renews power grid security concerns", Jul 26, 2010: http://www.computerworld.com/s/article/9179689/Stuxnet_renews_power_grid_security_concerns?taxonomyId=17&pageNumber=1

[8] Andy Bochman, Jack Danahy, "Stuxnet marks the emergence of real-world SCADA security challenges", The Smart Grid Security Blog, July 27, 2010: http://smartgridsecurity.blogspot.com/2010/07/with-stuxnet-utilities-confront-new.html

[9] The WallStreet Journal, "Electricity grid in U.S. penetrated by spies", Apr 8, 2009: http://online.wsj.com/article/SB123914805204099085.html

[10] Nicolas Falliere, Liam O. Morchu and Erik Chien, "W32.Stuxnet Dossier," Symantec, Version 1.4 (February 2011)

[11] David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?," Institute for Science and International Security, December 22, 2010, http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

[12] David Albright, Paul Brannan, and Christina Walrond, "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report," Institute for Science and International Security, February 15, 2011, http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf

[13] The Telegraph, "Israeli security chief celebrates Stuxnet cyber attack", Feb 16, 2011: http://www.telegraph.co.uk/technology/news/8326274/Israeli-security-chief-celebrates-Stuxnet-cyber-attack.html

[14] New York Times, "Worm was perfect for sabotaging centrifuges", Nov 18, 2010: http://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.htm

[15] New York Times, "Report suggests problems with Iran's nuclear effort", Nov 23, 2010: http://www.nytimes.com/2010/11/24/world/middleeast/24nuke.html?ref=stuxnet

[16] McAfee® Foundstone® Professional Services and McAfee Labs™, "Global Energy Cyberattacks: "Night Dragon", Feb. 10, 2011. Available: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

[17] Computerworld, "CIA says hackers pulled plug on power grid": http://www.computerworld.com/s/article/9057999/CIA_says_hackers_pulled_plug_on_power_grid

[18] Kevin Poulsen, "Slammer worm crashed Ohio nuke plant network", SecurityFocus, Aug 19, 2003: http://www.securityfocus.com/news/6767

[19] Foreign Policy, "The New Threat to Oil Supplies: Hackers", Aug 25, 2009: http://www.foreignpolicy.com/articles/2009/08/25/the_new_threat_to_oil_supplies_hackers

[20] Himanshu Khurana, Mark Hadley, Ning Lu and Deborah A. Frincke, "Smart-Grid Security Issues," *IEEE Security & Privacy*, January/February 2010, p. 81-85, 2010.

[21] OWASP – The Open Web Application Security Project: www.owasp.org

[22] Build Security In – sponsored by DHS National Cyber Security Division, US: http://buildsecurityin.us-cert.gov

[23] CWE/SANS: Top 25 Most Dangerous Software Errors 2011, Sep 13, 2011: http://cwe.mitre.org/top25/

[24] E. Tikk, K. Kaska, K. Rünnimeri, M. Kert, A.M. Talihärm, L. Vihul, "Cyber Attacks Against Georgia: Legal Lessons Identified", Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2008. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

[25] Wired Magazine, "Hackers Take Down the Most Wired Country in Europe", Aug 21, 2007: http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all

[26] BBC News, "Hacktivists target Egypt and Yemen regimes", Feb 4, 2011: http://www.bbc.co.uk/news/technology-12364654

[27] Mikhail A Lisovich, Deirdre K. Mulligan, Stephen B. Wicker, "Inferring Personal Information from Demand-Response Systems," *IEEE Security & Privacy*, January/February 2010, p. 11-20, 2010.

[28] Martin Gilje Jaatun, Eirik Albrechtsen, Maria B. Line, Inger Anne Tøndel, Odd Helge Longva, "A framework for incident response management in the petroleum industry," *Intl. Journal of Critical Infrastructure Protection 2 (2009) pp. 26-37*, Feb. 2009.

[29] Håvard Fridheim, Janne Hagen, Stein Henriksen, "En sårbar kraftforsyning – sluttrapport etter BAS3", FFI/RAPPORT-2001/02381 (in Norwegian only).

[30] Bob Gohn and Clint Wheelock, "Smart Grid: Ten Trends to Watch in 2011 and Beyond", PikeResearch Research Report, 4Q 2010, http://www.pikeresearch.com/research/smart-grid-ten-trends-to-watch-in-2011-and-beyond

[31] 104 - OLF recommended guidelines for information security baseline requirements for process control, safety and support ICT systems, 2007. http://www.olf.no/no/Publikasjoner/Retningslinjer/Integrerte-operasjonerIntegrated-operations/104/

[32] Maria B. Line, Dag Bertelsen, Håvard Fridheim, Per Hokstad, Gerd Kjølle, Jon Røstum, Ingrid B. Utne, Gunhild Åm Vatn, Jørn Vatn, "Metode og verktøy for en samlet risikovurdering av kritiske infrastrukturer", SINTEF report (in Norwegian only), ISBN 978-82-14-04814-8, 2009.

[33] The Smart Grid Interoperability Panel – Cyber Security Working Group, "Guidelines for Smart Grid Cyber Security," NISTIR 7628, August 2010 – Vol 3: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

[34] Jaatun, M. G., Grøtan, T. O., Line, M. B.; *Secure Remote Access to Autonomous Safety Systems: A Good Practice Approach*, International Journal of Autonomous and Adaptive Communications Systems, Vol. 2, No. 3, 2009, ISSN 1754-8632, pp 297-312.

[35] Eirik Albrechtsen, “Friend or foe? Information security management of employees”, Ph.D. Thesis, NTNU, 2008:101, Norway, 2008.

VIII. BIOGRAPHIES

Maria B. Line holds a MSc from the Norwegian University of Science and Technology, Institute for Telematics, 2002. Since then Line has been a Research Scientist at SINTEF in Trondheim. Line is currently a PhD candidate at the NTNU, Institute for Telematics. She is looking into Smart Grids as a critical infrastructure. Her scientific interests include privacy, intrusion detection, security awareness and risk assessments.

Inger A. Tøndel received her MSc degree from the Norwegian University of Science and Technology in 2004, and has since then been a Research Scientist at SINTEF ICT. Mrs. Tøndel’s research interests include electronic privacy, access control, threat modeling and security requirements engineering.

Martin G. Jaatun (M’01, SM’11) received his MSc degree in Telematics from the Norwegian Institute of Technology in 1992, and has been a research scientist at SINTEF ICT since 2004. Previous positions include scientist at the Norwegian Defence Research Establishment (FFI), and Senior Lecturer in information security at the Bodø Graduate School of Business. His research interests include security in cloud computing and security of critical information infrastructures. He is vice chairman of the Cloud Computing Association (cloudcom.org).