# (Cyber) security in smart grid pilots

Dr. Francien Dechesne
Energy & Industry section
Department of Technology, Policy and Management
TU Delft, NL
f.dechesne@tudelft.nl

Final version. 12 December 2013

## Abstract

This report presents the findings of a series of interviews to investigate how security issues and novel vulnerabilities are seen and dealt with in the smart grid pilot projects in the Netherlands and Germany.

The report is a deliverable of the research project *Kwetsbaarheid en veiligheid van Intelligente Distributienetten (KID)*, conducted within the NGI-Alliander programme *Empowering Networks*, by the Department of Technology, Policy and Management of Delft University of Technology, and by Dutch DSO Alliander.

**keywords** smart grids; smart grid pilots (*proeftuinen*); risk management; sociotechnical systems; cybersecurity

## Summary

The energy system is in transition, in response to economic and ecological challenges, and employing technical developments. Renewable energy technologies are being added to our energy supply. The new energy infrastructure is multi-layered, multi-sectoral, and deeply socio-technical: human factors are an essential component in the effectiveness of the technology, and institutions need to be in place to balance different goals and stakes, and to regulate interactions between the different actors involved. The emerging new energy systems involves new roles, stakeholders, products, services. For example, households turn from mere consumers into producers of energy (through solar, wind), and of new commodities, in particular: data and flexibility.

Information and Communication Technology (ICT) is an important enabler for the operation and control of the new energy system. But the dependence on ICT also makes it susceptible for cybersecurity issues, and security issues that arise in the interaction between the cyber layer and the physical, institutional and human layers of the system. These vulnerabilities need to be addressed from an integrated engineering systems perspective, including policy, law and economics.

In the project *Vulnerability and Security for Intelligent Distribution Grids* (KID), the aim has been to make an inventory of the novel vulnerabilities that arise, and the changes in risk management that are required by the transition from traditional distribution grids to smart distribution grids. For this reason we have conducted a series of interviews with experts from DSOs (Alliander, Stedin) and research institutes (Fraunhofer, ENCS), involved in the smart grid pilots and smart meter roll out, to collect insight on the following questions:

- To give an operational definition of smart distribution grids, with an inventory of goals, functionalities, actors and values affected.
- What are novel technical, institutional and human vulnerabilities that arise in the (near future) smart grids?
- Which risk management strategies should be used to address these novel vulnerabilities, in particular those related to ICT?
- What are the expectations towards near future smart grid developments?

The interviews provide the following provisional answers to these questions:

There is no stable **definition** yet of what the smart grid will be exactly. What is common to the uses of the term, is that it is a supply system for electric energy based on a diversity of energy forms. The system is made economically, ecologically efficient and secure, and involves optimization functions. The system has at least the following two goals: to support the transition towards a significant share of renewable energy, and to use the electricity infrastructure more efficiently to accommodate growing electricity demands. Essential building blocks of the smart grid are generation technology, prediction algorithms, the integrated use of ICT, market design, and user participation. New roles and commodities emerge, such as shown in the role of flexibility aggregator.

**Technical vulnerabilities** are mainly to be expected in the use of remote operation and control, and in the increased complexity and interdependence of subsystems. These make smart grids vulnerable for cyberattacks and cascading failures. **Institutional vulnerabilities** are the fact that markets, standards and laws need to be in place. Also, scalability of the local-for-local approach to a national level is a challenge, as each location has different

characteristics. Smart grids require for their performance participation of the users. **Human vulnerabilities** are privacy and trust issues that may create resistance to this participation. Smart metering produces data from which individual behavior may be derived, and thereby become personal data. If *Big Data* practices, such as profiling, are introduced in connection to energy services, this will lead to more privacy issues and resistance. Other issues may be the education, lack of interest, lack of time needed for participation. Also, one has to be careful that the push for participation does not exclude certain population groups.

However, in the end, many vulnerabilities carry aspects of all three categories above and therefore require a **holistic approach**.

Although current IT-security solutions help preventing and dealing with vulnerabilities within the cyber layer of smart grids, they are not sufficient for vulnerabilities in the interaction between the different smart grid layers. **Risk management strategies** on a general level that are expected to work are: 1) Zoneing: designing architecture of IT- and OT-layers in such way that in case of problems in the IT-layer, the problematic parts of the system of the system can be disabled, and the system can fall back on traditional operation. 2) Risk reduction through impact mitigation rather than prevention: because of the complexity of the system and the unpredictability of developments, it seems more effective to invest in anomaly detection and responding to reduce the impact, than in reducing probability of threats. With the non-tangible character of cybersecurity breaches, there is a need for a way of testing for (cyber)security. In order to incorporate cybersecurity issues, there is the need to learn to think like a hacker. For this either training (Red Hat/Blue Hat training, ENCS) or ficiton (the novel Black Out) seem more effective than models. For trust and privacy issues, transparency within the development and deployment of smart grids is key. This requires involvement of direct and indirect stakeholders, as demonstrated by the practice around the smart meter in the Netherlands.

The interviewees agree that the exact future development of the smart is hard to predict, for example depending on the order and speed of certain subdevelopments such as e-vehicles, smart appliances or new sustainable energy generation technology, but also depending on political decisions and agreement on standards. These developments are interdependent. This unpredictability provides an extra challenge to prepare for (cyber)security issues, especially a 'security by design' approach, which implicitly assumes stable functionalities and requirements. When smart grids move out of the experimental and tightly controlled pilot phase, into the more open real practice, (cyber)threats also become more realistic. It will help if awareness of vulnerabilities and threats has been incorporated as much as possible into the system design and the institutional environment. Organisations involved in the smart grid development are starting to 'build a culture of cybersecurity', to prepare for the new types of vulberabilities that will arise.

# Contents

# Chapter 1

# Introduction

The energy system is in transition. Growing global energy demands and ecological challenges, such as depletion of traditional energy sources and climate change, ask for renewable energy technologies. These are being developed and increasingly adopted, both on a local scale (solar panels on houses) and a larger scale (offshore wind farms in the North Sea generating up to 900MW each, totaling up to 6GW in 2023[1]). The growing demands, the diversity and dynamics of the different energy sources, and their partly decentralized character, ask for smarter use of existing infrastructure, and adaption of energy consumption patterns to align with the availability of energy.

Information and Communication Technology (ICT) is utilized to combine a greater variety of (sustainable) energy sources, a.o. to facilitate two-way loads, to monitor the components, and to balance production and demand optimally. On the one hand, performance data and communication will help prevent vulnerabilities within the grid, but they may also come with new threats [11]: the vulnerabilities within the ICT itself, but also those that arise in the interaction between the ICT and other layers of the grid, such as the "cyberphysical" vulnerabilities that also arise in SCADA and industrial control systems (ICS).

The new energy infrastructure is multi-layered, multi-sectoral, and deeply socio-technical: human factors are an essential component in the effectiveness of the technology. Institutions need to be in place to balance different goals and stakes, and to regulate interactions between the different actors involved. The emerging new energy systems involve new roles, stakeholders, products, services. Vulnerabilities will therefore not just be technical, but also human, and institutional.

The authors of this report are involved in two projects to develop a sociotechnical view on security of smart grids and corresponding tools: the EU-FP7 project *Securing the European Electricity Supply Against Malicious and accidental ThrEats* (SESAME[2]) on the transmission grid level (with the involvement of TSOs and regulators), and the Dutch project *Vulnerability and security of smart distribution grids* (KID), in collaboration with Dutch DSO Alliander. The overarching research interest in both projects is to investigate which vulnerabilities arise in the interaction between the different layers of smart grids, and to develop models and tools to support both the design and operation of secure smart grids.

[1] `http://www.tennet.eu/de/en/news/article/offshore-windenergie-gemeinsam-vorantreiben.html`, last checked 21 Nov. 2013.

[2] `https://www.sesame-project.eu/`

Both projects strive for more insight into the current status and practice of smart electricity grids in general. Part of the research is directed towards inventory of the changing vulnerability- and security aspects in the transition of a traditional (top-down) electricity grid towards a smart grid.

The role of ICT with respect to vulnerability and security in this development has (at least) two sides. On the one hand, the fast developing ICT provides new possibilities to gather and analyze performance data, making it possible to pre-emptively notice and remedy vulnerabilities in the system. On the basis of the information available, users can be stimulated to use electricity when available and suppress their demand when supplies are low. On the other hand, the interconnectivity associated with ICT brings in its own vulnerabilities.

In this report, we distinguish three categories of vulnerabilities associated with smart grids:

**Technical vulnerabilities** For example, the possibility of remote operation has made it very attractive for operators to connect previously isolated networks to the internet. However, with the development of dedicated search engines such as Shodan[3], control systems become increasingly vulnerable to hackers, especially so since many components have security mechanisms that were designed for local only networks. This makes it also easy for backdoors to be exploited.

**Human vulnerabilities** Consumer participation is a crucial element in load balancing for the smart grid. While the energy usage information provided by smart metering is essential, the gathering of such information also raises privacy, Big Data and information security concerns. Not addressing these consumer and societal concerns, or the usability of security measures, leads to non-acceptance and non-participation. [1]

**Institutional vulnerabilities** One characteristic of the smart energy systems, is the transition from the centralized architecture of TSOs and DSOs, to open, decentralized systems of 'prosumers', consumers who also produce energy, e.g. through solar panels or a locally co-owned wind turbine. As holds for the internet, the roles of the public and government are changing, and legislation (institutions) have to adapt. Who is responsible for which aspect of the security of supply and the information security?

The transition towards smart grids is a gradual development that has already started, e.g. with the increasing share of decentralized electricity generation (solar- and wind energy). In the Netherlands, experiments with smart grids are conducted in a number of different pilot project, the so-called "Proeftuinen" of the Innovatieprogramma Intelligente Netten IPIN (innovation program smart grids).

As part of the aforementioned research projects, we aim to map out how, in the (experimental) practice of smart grids, vulnerability and security of smart grids are dealt with. In this report, we present an overview of current practices in the Netherlands and outside (Germany) with smart grids and smart grid pilots. We specifically focus on vulnerability and (cyber)security issues.

[3] `http://www.shodanhq.com/`, last checked 23 July 2013.

## 1.1 Interview set-up

We have conducted interviews with eight experts involved in pilot projects involving smart grids, in order to gain insight on the following points:

- An operational definition of the notion of smart grids as it transpires from the current (experimental) practice, and an inventory of actors within the smart grids pilots
- An inventory of technical, human and institutional vulnerabilities, and current approaches to risk management.
- Visions on directions of development of smart grids and necessary policy with respect to vulnerabilities and security.

These insights should serve as a basis for the development and review of vulnerability models for (non-experimental) smart grids. The interview plan can be found in Appendix A.

As mentioned above, the Dutch innovation programme smart grids (*Innovatie Programma Intelligente Netten*, IPIN) coordinates a number of pilots, called "proeftuinen". These pilots aim at gathering experiences with, and insights into, new technologies, partnerships and cooperation structures, both in the light of the current situation and of the foreseeable developments. For our interviews, we targeted experts, from within and outside of the Dutch experimental settings who are involved in design and/or monitoring of the setting (for the overview of actors and procedures), and/or in the area of Risk Management, and/or in the area of ICT integration into the electricity infrastructure.

We thank Harry van Breen (Alliander), Harold Veldkamp (Alliander program manager pilot projects), Dipl.-Ing., Dipl.-Oec. Patrick Selzam (Fraunhofer-Institut), John Hodemaekers (Stedin) for helping us to get in touch with the following experts:

| **Organization** | **Name** |
|---|---|
| Fraunhofer-Institute for Wind Energy<br>and Energy System Technology (IWES) | Jan Ringelstein<br>Marco Portula |
| Alliander (Liander) | Lineke Goorix |
| Alliander (Liander Infostroom) | Franke Gosliga |
| Alliander (Liandon) | Ben Kootstra |
| Stedin | Milo Broekmans |
| Alliander (Liandon) | Ben Tubben |
| European Network for Cybersecurity (ENCS) | Rob van Bekkum |

## 1.2 Background of the interviewees and their organizations

We have interviewed experts in different roles with respect to smart grid pilot projects and smart grid developments. A majority of the interviewees come from a background in IT, but they all have worked for a significant number of years in the electricity sector. The organizations they work for have different roles.

We have spoken to four people working for Dutch DSOs who are involved in different smart grid pilots.

**Alliander** is a Dutch DSO, "responsible for a large share of the energy pipeline grid in the Netherlands. [...] Alliander consists of two business units: **Liander** manages the gas and electricity grids in many areas of the Netherlands. **Liandon** works on energy infrastructures for high-voltage, complex medium-voltage and industrial installations.”[4]

*Franke Gosliga* is data protection officer at Liander Infostroom. He is responsible for privacy and security in the smart meter domain.

*Lineke Goorix* is coordinator on behalf of Liander in the pilot project **CloudPower Texel**. After some startup issues, the project is currently conducted by three partners, viz. TexelEnergy (cooperative energy provider for Texel), CapGemini (ICT company) and Liander (DSO for Texel). The project works with two technical systems: a display for all relevant information for the consumers (developed by Quby), and an overall platform (Siemens DEMS).

*Ben Kootstra* is projectmanager in the pilot project in Lochem. The **Lochem** pilot involves LochemEnergie, a cooperation of citizens, with collective ownership of solar panels and collective buyers of energy. Locamation is a company specialized in automation of high and middle voltage stations and produces sensors for the operational technology. Eaton Industries is a producer of technical parts used in the grid. Research partner is Universiteit Twente (CTIT). Besides its role as DSO, Liander is also involved int he pilot with the new smart charging concept.

*Ben Tubben* is business project manager Liandon, and also involved in the pilot project in Lochem, as well as the **Houthavens** pilot (EU FP7): this is the development of a newly built area, with a focus on research and realisation of low energy buildings.

**Stedin** is also a Dutch DSO. We have spoken to *Milo Broekmans*, who is enterprise architect with a focus on general picture of the role of DSOs in smart grid situation. Stedin is involved in pilot projects such as Couperus (apartments in Ypenburg).

Besides the DSOs, we have spoken to experts from two research institutes that also focus on the (experimental) practice of smart grids.

**Fraunhofer** is Europe’s largest application-oriented research organization, with “66 institutes and independent research units at locations throughout Europa.”[5] The interviewees *Jan Ringelstein* and *Marco Portula* work in the department “Energy Management” of the Instut für Windenergie und Energiesystemtechnik (IWES). This department consists of two subgroups: the Energy Management Applications group, of which Jan Ringelstein is the head, and the Software Development group, in which Marco Portula is scientific employee.

IWES has been involved in broad range of experimental smart grid research projects, with participation of industry. Examples are:

- The Open Gateway Energy Management Alliance “OGEMA 2.0” project, concerning software development for middleware for residential gateways.[6]
- The INEES project (Intelligente Netzanbindung von Elektrofahrzeugen zur Erbringung von Systemdienstleistungen - Smart Grid Connection of Electric Vehicles Enabling Ancillary Services) investigates technical requirements for ancillary services for the transmission network, delivered by electric car battery storage, as well as their effect and value. Based on this, business processes including required communication interfaces

[4] http://www.alliander.com/en/alliander/about-alliander/key-data/

[5] http://www.fraunhofer.de/en/institutes-research-establishments.html.

[6] http://www.ogema.org/

between driver, vehicle, grid operator and utilities are worked out and turned into corresponding IT solution. [7]

- Project EMSE: implementing an energy management system at a German agricultural site.
- Project REV2020: a field test in a small village near Kassel
- BEAMS: European project energy management in public buildings like football stadiums.
- STARGRID (European project FP7): standardization for smart grids[8]

The **European Network for Cyber Security (ENCS)**, located in The Hague, is a research institute as well. It states as its mission to “improve the resilience of European critical infrastructures. [They] do so by bringing together the best R&D resources in Europe to address the needs of your business. [Their] initial objective is to raise the cyber security bar for the electricity supply.” [9]

The ENCS is an independent cooperation, not for profit, which collect its income from membership fees of the participating companies. The responsibility for cybersecurity lies with the companies themselves, and ENCS can serve as an advisor. Organizations like ENCS aggregate, anonymize and generalize knowledge of their partners as input for standards, good knowledge, best practices, white papers etc. The ENCS is not directly involved in the Dutch pilot projects, but there is a connection to them through its founding member Alliander.

We have spoken with general director *Rob van Bekkum*, who has working experience in IT and Telecom at different companies, among which energy company Nuon and later as business project manager at Alliander. Within the Liandon business unit of Alliander, he has 4 years of work experience in smart meter projects.

In the interviews, all interviewees have expressed their personal experiences and opinions, and do not represent official company or organization policy.

[7] http://www.erneuerbar-mobil.de/projekte/foerderung-von-vorhaben-im-bereich-der-elektromobilitaet-ab-2012/kopplung-der-elektromobilitaet-an-erneuerbare-energien-und-deren-netzintegration/inees

[8] http://stargrid.eu/

[9] https://www.encs.eu/contact/about-encs/

# Chapter 2

# Part I: Current smart grid practice

## 2.1 Definition of the term ‘smart grid’

All interviewees agree that no commonly valid definition of smart grid can be given. In particular, the term ‘smart’ is overloaded and almost meaningless. For example, the term ‘smart’ is sometimes used in reference to a more or less traditional grid to which remote operation is added, only because human presence is replaced. In the interviews, there was agreement that the term ‘smart grid’ refers to a next generation energy infrastructure that should realize a number of technical, environmental and societal goals and values. Several of these goals and values are highlighted by the interviewees.

Ringelstein has looked into some definitions given by organizations. It is hard to find one that is satisfactory. The International Electrotechnical Commission (IEC) states that ‘smart grid’ is more like a marketing term. “The general understanding is that the Smart Grid is the concept of modernizing the electric grid.” [1] The *Bundesverband der Energie- und Wasserwirtschaft* (BDEW) states that “a Smart Grid is an energy network, that integrates the consumption- and supply behavior of all market participants that are connected to it. It ensures an economically efficient, sustainable power system with low losses and high availability.”[2] This definition is not very descriptive in what is *smart* about a smart grid; for example, it would include the current grid.

A definition from Ringelstein’s personal view would be:

> A smart grid is a supply system for electric energy, that takes into account a diversity of energy forms. It enables to connect all equipment in the energy supply system, especially generators and nodes, such that the whole system is economically, ecologically efficient and secure (security of supply would be at least as good as in the current grid). It involves optimization functions that ensure the efficiency of the system. The ultimate *goal* of the system would be that it facilitaties the energy transition towards 100% renewable energy supply. For achieving this, according to current research, you need several *building blocks*:
>
> - Generation technology, with controllable loads.

[1] http://www.iec.ch/smartgrid/background/explained.htm

[2] http://www.bdew.de/internet.nsf/id/smart-grids--smart-meter-de

- Prediction algorithms for generation and loads. These have to be different from the classical system, which relies on control of centralized generation. Management of renewables requires predictions.
- ICT is primarily necessary for the optimization. There are enormous amounts of data involved, and ICT is needed for transmission and processing of the data. However, according to Ringelstein, part of the solution of a smart grid must be to reduce complexity, to avoid problems with data integrity, data security etcetera.
- And a number of other building blocks, including (but not limited to) market design, business models, maybe most important: end users.

*Smartness*, according to Ringelstein, will not be in the technology. The smartness lies in the way we use the technology towards our goals: towards a system based 100% on renewables, and at the same time as secure as today's system and free of cyber threats. A truly smart solution would in the end reduce complexity rather than increase it, so we should try to resort to the most simple solutions available.

Tubben agrees that 'The Smart Grid' as a notion is too broad to be descriptive. Just introducing a feedback system like Toon (the smart thermostat of Eneco[3]) is already called a smart grid. It is important to be clear which one of the layers or components of a smart grid one is referring to, especially when using words like "platform". These words easily lead to miscommunications. From a restricted data/information perspective, a smart grid consists of three layers: the operational layer (OT, this is where SCADA systems are increasingly used for smarter use and management of the grid), an IT-layer with a bridging function between OT and IT, and finally, the virtual IT layer (where apps and services, such as feedback systems, are developed for demand side management).

Broekmans sketches Stedin's general smart grid vision under the name of *Intelligent net management*, with has four pillars:

1. Intelligent Technology. This includes ICT, but also 'power electronics', e.g. technology for stabilizing the local grid (voltage control) or using DC instead of AC.

2. Smarter customer interaction. This is about coming to agreements with consumers on power consumption. Here responsibilities are clearly shifting to outside the traditional borders of the role of DSOs (and the current law). Such contracts could also be offered by other market parties.

3. Intelligent area planning. This is about taking local resources and the energy environment into account when managing the net, and installing grids in newly built areas.

4. Intelligent utilization and extension of the net capacity. Given the increasing demand for energy, in particular electricity, net extensions seem necessary. However, it is also possible to utilize the current capacity more efficiently. For example, while gas demand is decreasing, we could start using gas for storage and transportation (*power to gas* technology). Also, intelligent congestion management can help to postpone the need for physical extension of the grid.

[3] http://www.eneco.nl/Toon/

In a general sense, the smartness is to make smarter use of the physical technology: to use "intelligence" to prevent reinforcements of the physical network. Part of that intelligence comes from ICT and software, for example such as the Powermatcher algorithm, initially developed by ECN, and now further developed by TNO. [4]

## 2.2 What is the role of the smart meter in the smart grid?

The smart meter is arguably the most visible and tangible component of smart grids for the average citizen: Italy and Sweden have already connected households through smart meters on a large scale before 2010. Roll outs in most European countries are currently ongoing or in preparation. The smart meter also connects closely to broader discussions about cybersecurity and privacy in ICT intensive infrastructure systems (such as transportation cards and electronic health records). This may explain why societal discussions and big parts of the research community on smart grids focus on security and privacy issues of the smart meter. In the Netherlands, a law for mandatory roll out for all households to be executed before 2013, was suspended in the senate in 2009 because of privacy and security issues raised by consumer organizations and academics.[3]

Despite the smart meter being such a tangible and visible element of smart grid developments, some experts would not consider the meter to be a true part of the smart *grid*. According to them, the smart grid may be restricted to the medium voltage grid. This is a conceptual discussion, showing again that the term 'smart grid' has no fixed meaning (yet). Smart meter expert Gosliga takes the term 'smart grid' broadly, so considers smart meters and its privacy/security issues to be part of it, as well as all medium voltage stations and -grid.

Gosliga points out that the smart meter is a necessary enabling component to come to a smart grid, and that is why it is the aspect where we currently have the steepest learning curve. This is also the reason why the smart meter is the part of smart grids of which we have the highest awareness of vulnerabilities and security issues. The bigger picture of the smart grid is lagging far behind in terms of requirements, standards, use cases, what we can do and want to do with it - despite many ideas and expectations.

The Dutch smart meter has been defined (in the Dutch Smart Meter Requirements DSMR, cf. Section 2.6) to have quite restricted functionality, and according to Gosliga the functionality probably will not change soon: Alliander will invest massively in order to satisfy the aim of having 80% of connected households supplied with a smart meter by 2020 (this is a European objective). The life span of a meter is 15 years, so it would be a gigantic disinvestment to make essential changes. The radical change will be higher up in the chain, where the smart grid information technology is used to manage and control the grid.

## 2.3 Current smart grid pilots and developments

Tubben lists the three pillars that DSO Alliander distinguishes for its activities in the practice of the pilot projects Lochem and Houthavens:

1. Technical (energy architecture)

[4] http://www.powermatcher.net/, last checked: 21 Nov. 2013.

2. Behavioural (feedback systems, customer participation)

3. Demand-side management (demand-supply/load balancing)

The Houthavens pilot concerns the development of a newly built area, with a focus on research and realisation of low energy buildings. The central aspect for Alliander's involvement is the technical one: it is a research project aimed at designing the most efficient energy architecture. But the other two categories of Alliander's pilot activities are also represented, in the questions how to present and share consumption information, and in the implementation of *demand side management*. Currently, everything is still done on paper and in simulations. The first inhabitants of the Houthavens area are expected in 2015.

In the Proeftuin Lochem (which is part of the IPIN programme), the main focus is on the second pillar: feedback systems and consumer participation. Also, the role of e-vehicles for supply-demand balancing (3) is investigated: can charging schemes for e-vehicles help deal with temporary surpluses of energy. On the technical side (1), the main question is how to integrate solar energy in the existing grid.

Kootstra explains that in Lochem, the performance data are gathered, and sent to the management database LiveLab. This is a management environment for the middle voltage stations, in order to proactively respond to imbalances. The physical network will always be closely monitored. Once you have insight in these measurements, one can respond better to certain demand balancing questions, for example, by making certain fast charging options for e-vehicles impossible. What one measures in the net, is interpreted into a certain power quality assessment, which translates into the proposed demand-response mechanisms and incentives. If things go really wrong, simple interventions should be enough to solve the problem (e.g. shutting parts of the net down).

This involves only a limited number of new components in the net: sensors in the low voltage range, sensors on the middle voltage, such sensors are already currently on the market and being employed. The Powermatcher however is truly new, as are all apps. It must be evaluated how well this will work. For this, the project also uses the simulation tool TRIANA[5] of the University Twente [2].

Goorix explains the general structure of the Texel pilot. An overall system (which has been chosen to be Siemens Decentralized Energy Management System, DEMS) gathers all information from the displays, and monitors the balance between generation and consumption. In the future (but outside of this pilot), alternative power generator units, such as wind turbines, could be added. The overall system could then be seen as an IT-layer over the grid which could autonomously balance the load by switching on and off connected generator units (supposing you would have a large number of generation units). The system that has been purchased is over-dimensioned for the current situation in anticipation of that future application (the existing generation units lag a bit behind the IT-infrastructure). In the current situation, the system can already send information about weather conditions for that day and related energy availability (”tomorrow afternoon will be sunny and would be a good moment to use your washing machine”).

Broekmans is involved in the Smart Energy Collective (SEC). This is a Dutch consortium of 26 partners: network operators (including Stedin, Alliander, TenneT), power generators and

[5] `http://www.utwente.nl/ctit/energy/simulator/`, last checked: 23 Oct. 2013.

suppliers, service providers and technology suppliers, manufacturers of electrical equipment, project developers, financial institutions, installers, energy consultants and last but not least the energys end-users.[6] SEC is currently developing the Universal Smart Energy Framework (USEF) that will be tested and evaluated in several smart grid pilots, among which the pilot in Heerhugowaard (cf. page 16). It is working towards doing more and more what Tennet does for the transmission grid, but then on a local level for distribution: predict loads, balance production and consumption, taking grid constraints into account.

To do this, aggregators are necessary on the lower levels of the distribution grid: only the aggregated consumption and flexibility for a bunch of households can make a difference, a single household cant. The current grid will require such management and control when the situation changes to more distributed and flexible generation, like when entire streets decide to place solar panels.

**Smart metering practice in the Netherlands** Gosliga, as data protection officer for smart meters, is not directly involved in one or more of the Proeftuinprojecten, but his team (of three people) is involved in making the privacy and security assessments of smart meters in a large number of (pilot) projects. This involves a risk analysis with respect to privacy and security of the process and underlying systems, and a proposal for measures to be taken to mitigate the risks. The team has been installed by Liander Infostroom, the department that is responsible for the smart meter rollout. Because of the societal discussion that emerged around 2009 regarding the mandatory rollout for all Dutch households, which resulted in the corresponding law being suspended, the board decided to take measures to prevent a similar course of events in the future.

Therefore, Alliander wants to achieve a very high level of privacy and security guarantees with respect to smart metering. It works with a model that includes three (or four) phases of compliance, with information security and privacy regulation: (1) unconscious compliance - (2) conscious compliance - (3) certified compliance. The experimental phase (0) precedes phase 1: in this phase technology and systems are tried out partly outside of existing regulations and standards (for example because it is not clear which regulations should apply, or because standards have not settled yet). With respect to Privacy and Security, most energy companies and DSOs operated in phase 1, or just starting phase 2 in 2009. The rejection of the rollout law has been a catalyst. Alliander now aims for phase 3, under monitoring of accountancy firm PricewaterhouseCoopers.

Tubben indicates that this model is also used in the later stages of the pilot projects such as Lochem, to prepare the systems for going from experimental to operational, taking privacy and information security into account.

## 2.4 Local for local

Germany has achieved the goal of dramatically increasing the ratio of sustainable energy, supported by very attractive (and expensive) financial incentives. However, Tubben claims Germany was not prepared for the impact of large scale integration of decentralized generation on the network. So now, Germany needs to catch up in the infrastructure, which is very costly. In contrast, the Netherlands chooses to be guided by what is possible (and how to do it), rather than by setting strict goals in terms of sustainability ratios.

[6] http://www.smartenergycollective.com/

So, the Netherlands is lagging behind in decentralized generation, especially compared to Germany. But the Dutch approach to decentralized generation is different, according to Tubben:, the Netherlands tries to tackle the problem according to the principle **local-for-local**, which means local generation used locally. This requires more innovations than just feeding back into the main grid. For one, it is unavoidable to *use IT*, in order to know when you have surplus, and to respond to it. Also *storage* will be crucial in this: local battery packs, or e-vehicles as batteries. Local storage is important for energy efficiency, as it saves losses from transforming electricity to feed it back into the transmission grid.

The local-for-local approach is community driven: people get satisfaction out of watching TV using their 'own' energy. It is an adequate characterization of the Texel pilot. Goorix describes as a positive characteristic of the setting of Texel, is the clear commitment of the people of Texel to build a sustainable, self-sufficient energy system together. So the prospects for pilot participation and for continuation beyond the project are extremely good. Texel is an island and a closely knit community. This also makes it easier to achieve the goal of 300 households for the pilot: 200 with solar panels already installed, and 100 possibly without. But thanks to previous activities of TexelEnergy to stimulate the placement of solar panels for households, the availability of solar is well above average for the Netherlands. The project will be based on the existing solar capacity from households, because a planned local 'Solar Pasture' (zonneweiland), is overdue for inclusion in the Proeftuin project. Apart from the solar energy, the windmill of Texel is also being connected to the DEMS-system.

Local-for-local is also a guiding principle for the Lochem pilot. The area of Lochem selected for the pilot, is a modern built neighbourhood (90s), so the grid is modern and safely (over)dimensioned for modern use. This means that introducing a significant amount of solar power there does not immediately require investments in the grid.

But these specific characteristics of those pilots where the local-for-local approach works, also point at its limits. Tubben stresses that experiences in one setting are not straightforwardly generalizable. The point is: you have to make specific decisions for the specific region. And 'smartness' (such as storage solutions) is only practically relevant in certain situations: where the capacity for the demand to absorb the surplus is not enough, and/or the grid is less resilient to fluctuations in load. For example, implementing renewables in old neighbourhoods in Amsterdam would be a totally different scenario: the old grid of those neighbourhoods would be very sensitive for overgeneration of energy. That does not mean it is impossible: there is a choice between 1) strict supply-demand balancing, 2) switching the generator off if necessary, or 3) expanding and upgrading the grid. But the latter is what we want to prevent, for economic reasons. We have to look at the characteristics of each situation to see what is necessary and what works best. In Arnhem for example, solar energy could well work without too many investments to the grid, because the solar potential over the entire inner city would be completely absorbed in the energy demand. Putting in storage facilities for surpluses would not be necessary then.

## 2.5 New actors, roles, responsibilities in smart grids

The smart grid is a multi-actor system, with new (market) roles and responsibilities in comparison to the traditional energy grid. Which are the most important ones that we can expect, or that shine through in the current pilots?

An often highlighted new role, also in the interviews, is that of the *prosumer:* a party that both consumes and produces electricity. Broekmans points out it is often overlooked that prosumers not only produce energy, but also *flexibility* (time of consumption) and *data*. These two aspects may prove to be of great value in the context of smart grids.

Broekmans highlights the truly new role of *aggregator*: representing a (large) group of households. An aggregator buys flexibility from the households, and sells this to the DSO or other parties. This could be at neighbourhood level, but it is not unimaginable for a large retailer of appliances (e.g. MediaMarkt) to become an aggregator as well, by selling Smart Grid Ready washing machines, or by offering discounts on fridges, to be able to retain a certain control on the use of the appliance in exchange. Aggregated to a certain quantity, this flexibility can be sold to DSOs etc. Similarly, Nissan could serve as aggregator for the right to sell charging flexibility on their cars.

In the Houthavens pilot, dedicated to an energy neutral built environment, aggregators also play a role. Tubben mentions that peak shaving can probably be solved for a large part by storing energy in batteries during the day, and then use the stored energy for public lighting in the evening (during the peak demand). Collectively or not, owning such batteries and selling their flexibility is an example of a realistic new business model for Houthavens. This is not automatically a role for the DSO: when thinking in such new roles, you can see local cooperations emerge for new business models (providing a guaranteed price, for example), like LochemEnergy or TexelEnergy.

Another question is how the responsibility for the energy supply is distributed within the new situation with more distributed and dynamic sources and actors involved. The Houthavens pilot, aimed at energy neutrality, does not address this responsibility question, according to Tubben. It focuses on how to make an efficient *system* for local transactions. For this the Powermatcher system is used as auctioning system, with a second control application (unique for Houthavens) to deal with the peer-to-peer agreements. But one can see that the question of responsibilities for the energy supply, will become connected to the question of who will be responsible for the coordinating system.

Tubben mentions that the SEC Heerhugowaard pilot does address more specifically what the new roles are. This pilot involves an energy service company (ESCO) for mutual energy trading, an energy producer (Essent), DSO, and the customers. The ESCO can be seen as the central point within the triangle: producer–DSO–customers. An ESCO does not necessarily need to be a cooperation –this can also be a for profit business organization.

**Non-technical complexity** Ringelstein stresses that smart grid systems have many levels of complexity, and estimates that about half of the complexity is non-technical: in policy, regulatory issues, incentives, laws etc. The problem is that no-one has the final picture: it is like putting together a jigsaw puzzle without the picture. Everybody seems to have a different vision on what the system should look like, and there are no clear guidelines. Market design is another big issue: stable incentives are necessary for business models that are economically viable. In the research projects at IWES, it was found that for a business model to be viable, it needs multiple different business cases with different goals.

Ringelstein believes that the actors are in essence the same as in the old situation: distribution and transmission system operators, eletricity providers, generators, people operating loads, end users. New players may be the metering system provider, and operators of virtual power plants, or operators more concerned with ICT grids and ICT security.

Portula adds that probably the most complex element in the smart grid is the end user, as it is the least predictable element. Compared to the traditional grid, the role of the end user totally changes. But at the same time, many users will still only be consumers, who are accustomed to getting their energy needs satisfied at any time. They will have to accept the changes that are needed. This may be feasible in small communities, especially in the setting of a pilot, but it will be hard to change expectations and behavior of large groups of diverse people, e.g. on a national scale.

IWES was involved in a pilot in Mannheim, with about 700 participants (all residential consumers). They implemented an automatic energy management system there, based on the "bidirectional energy management interface"[7] and OGEMA.[8] The results from that project indicate that if you double the price of energy at a certain hour, you can expect 10% less energy consumption during that hour. However, for specific groups among the participants, this percentage could rise to 30 or 35%. This indicates that impact of smart grid approaches for residential customers very strongly depends on the group of people involved. So, maybe psychological research is needed, or maybe behaviour is too different from one group to another to be able to make general predictions. Little is known yet in this respect.

It was reported about a pilot project in the community of Boulder, Colorado (USA),[9] that user behaviour hardly changed over the 2 or 3 years of the pilot, despite their general environmental awareness. As it turns out, the hurdle in this project was not on the user side, but in bad project management. In this case, there was a clash between the very high expectations of the users combined on the one hand, and underestimation of the technical complexity (interoperability of appliances) by the company conducting the pilot (Xcel energy) on the other. In fact, the only thing that changed was the price differentiation, which was much more a punishment for peak usage, than a reward for off peak usage. This experience indicates that the success really depends on a combination of psychology (the high motivation and expectation of the users, that turned into disappointment), technology (the failing interoperability) and market mechanisms (the flawed pricing scheme). Ringelstein comments on this case:[10]

- For a smart grid field test of that type, there were, and still are, no standardized, robust off-the-shelf components with plug&play interoperability
- The complexity of the overall system (including long-range communication) is typically underestimated, leading to cost increases during the test.
- On the other hand, the robustness of subsystems is often overestimated.
- Offering good customer services and keeping the customers happy is absolutely crucial and efforts for that are also often underestimated.

[7] `http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5255576&tag=1`

[8] `http://www.ogema.org/`

[9] `http://finance-commerce.com/2013/04/the-lessons-of-smart-grid-test-in-boulder/`

[10] Quote from e-mail dd. 13/9/2013.

## 2.6 Standardization efforts

Tubben stresses that Alliander wants to get out of the conceptual and ”architecture on paper” phase. So Alliander’s interest in the pilots is to really implement the technology that is currently available. Currently next steps are being made: Alliander and TNO are working together in the FAN (Flexible Alliance Network) on the Flexible Power Application Infrastructure, a framework for an application platform connecting to the Powermatcher. The FPAI framework and applications will form the demand-supply control system

Broekmans describes similar efforts involving Stedin. To enable manufacturers and retailers to take up market roles of aggregators, like the examples of MediaMarkt and Nissan given above, and to make it interesting as a business model, it is important to have certain standards. These are currently under development, for example by the Smart Energy Collective in the form of the Universal Smart Energy Framework, which is currently being developed within the collective.

Currently, many parties are experimenting with IT platforms for smart grids (IBM, Cap, Cofely, Powermatcher). By being the first to come up with something that works, and by having so many parties and their stakes involved, the SEC parties hope to set the standard. As mentioned above, the Powermatcher is used in a number of pilots, such as Lochem, but also Powermatching City (Hoogkerk) and appartment building Couperus in Ypenburg. So Powermatcher seems to emerge as a standard for the algorithm - and then it becomes just a matter of agreeing which information one exchanges as partners to connect different systems. That is: provided that the technology proves to be scalable.

For (cyber)security issues, Broekmans is member of working group Cybersecurity in Smart Grids in the context of Netbeheer Nederland. This working group looks at use cases in the light of EU Mandate/490, the “Standardization Mandate to European Standardisation Organisations (ESOs) to supportEuropean Smart Grid deployment” [6]. Netbeheer Nederland also provides input to Expert Group 2 of the European Smart Grid task force: Regulatory Recommendations for Privacy, Data Protection and cyber-security in the Smart Grid Environment.

**Smart Meter Requirements** For the privacy and security issues of the smart meters, a national sector-wide collaboration of DSOs, including Gosliga for Alliander, has done a broad stakeholder analysis, involving DSOs, power suppliers, customers and customer organizations such as the Consumentenbond (who were the instigators of the discussion around the mandatory roll out), the ministry, the regulator, etc. It has performed an integral risk analysis of the system: which values does the system represent for each of the stakeholders, and which are the actors that influence these values. This is the first time that such analysis has been done, and within the scope of an entire sector: stakeholder analysis – risk analysis – sector requirements. So, it was also a normative effort. The sector requirements (Sector eisen, current version 1.5[11]) are both requirements the system needs to satisfy *and* control measures that can be applied, in order to mitigate the identified risks. These also include the legal input, such as the Wet Bescherming Persoonsgegevens, or the E-wet (*Energie wet*).

[11] http://www.netbeheernederland.nl/themas/thema-overzicht/dossier-detail/?aId2=f9c01482-ba09-43dd-b781-f66e6f6cc0e2&attributeId=f9c01482-ba09-43dd-b781-f66e6f6cc0e2&title=Slimme%20meter, last checked: 15 Oct. 2013.

Based on the same analysis, and specifically for the smart meter, this collaboration put together the Dutch Smart Metering Requirements (DSMR), which is used to communicate the requirements to the technology suppliers. This is why this document is in English. These also include functionality.

These sets of requirements have been handed to Netbeheer Nederland, with a normative purpose. What is good about the current sets, is that the requirements are pretty concrete and checkable. On the negative side, the level of abstraction and the depth in which the items are described, varies greatly throughout the documents (from 'end-to-end security needs to be in place', to detailed descriptions of the properties of a certain port). But more important than perfection is that these requirements have been set and are supported throughout the sector. Also, the process of analysis and setting requirements is agreed to be cyclic, about once every 5 years. This is more or less in sync with the cycle for the relevant jurisdiction around privacy and the electricity sector. The next version is now being worked on.

**Control systems** So, for smart meters in the Netherlands, a lot of work has been done for regulating the security, privacy and to some extent, functionality of the smart meters. Is a similar standardization process currently going on for other components of the grids, for example for ICS (Industrial Control Systems) or SCADA (supervisory control and data aquisition) systems in the mid-voltage range?

According to Van Bekkum, this is not the case. Also, the way it has been done for the smart meters, holds only for the Netherlands. Within Europe, standardization initiatives in other countries, such as France, Spain, Germany, are quite different. So, even though some standards have been developed, the general process is fragmented. While the DSMR do lead to a relatively secure meter, where privacy is reasonably well guaranteed, they also have some issues. Some manufacturers consider them to be too restrictive (and crossing the line into the design of the technology) and too particular for the Dutch market, which is small anyway. So, this approach to standardization may also not be the best.

For other parts of the grids, such as SCADA and ICS (remote access and control), there is also quite some fragmentation, with the exception of international standards such as ISO, NIST, NERC CIP, IEC. But they only reach to a certain, quite high, abstraction level, and not to the implementation level like in the case of the DSMR.

Lack of standardization can lead to security issues. In the next chapter we move on to discussing vulnerabilities of smart grids and how they are addressed in the pilots.

# Chapter 3

# Part II: Vulnerabilities and risk management

Risk management for electricity systems has been very successful over the past century, with very high security of electricity supply as the result -at least in most European countries. The introduction of IT change may require a revision of risk management procedures. How are responsibilities for the security and safety of the IT system distributed?

## 3.1 Attention to security in the pilots

Within the pilots, many aspects of smart grids are being experimented with. How are vulnerabilities, security issues and risk management addressed?

In Houthavens (energy neutral building) and Lochem (decentralized generation), there is no concern for security of supply in the sense that situations of insufficient supply could arise. The presumption is that Houthavens will always be connected to the main grid. In Houthavens 'energy neutral' is restricted to building related energy consumption (lighting, heating, airconditioning, street lighting, etc.), and it has to be neutral only on a yearly basis: it definitely does not have to be self-sufficient. According to Tubben the question is not: whether there is energy, but how you will trade it and put it to use (e.g. first local-for-local, and then grey electricity from outside). And for this, IT is crucial.

In the customer-oriented setting of Lochem, attention has been paid to personal information security of users in the form of privacy statement for the pilot environment. Kootstra stresses that, also in the future (non-experimental) situation, users can determine their privacy settings when installing the software on their system, but they can also always revoke this. The user determines himself which data will be shared into the cloud with certain service providers. For the non-user sides of the system, it is still so much under development, that security issues have not been worked out yet completely. But the aim is to incorporate security issues immediately. The IT-department of Alliander has been involved to address the question: which security and management aspects need to be addressed when a system goes to a more formalized system level (the three steps from experimental to certified compliance with laws and regulations, cf. page 14). At the same time, we discuss these issues with TNO: if we want to put our platform on the market, how do we address security issues?

The second issue that will be addressed in Lochem, comes from ENCS: which protocols will be used for the communication of the performance data, and how are we going to protect those protocols at the OT side? Are current standards secure enough? Within a month, the entire chain for the 'sand box model Lochem' will be tested for the first time, so we can see which security aspects will arise. We already have user data from about 60 households. The real chain in Lochem will probably be finished by the end of this year.

In the Texel pilot, cybersecurity is being addressed by both CapGemini and in the IT department of Liander. IT security was not an explicitly defined point of interest in the project, but in the course of the project the care for the security of the system has been taken up. In the Houthavens and Lochem pilots, it is DSO Alliander -as neutral party- who takes up this role. In the long run, this could become a new locally facilitating role for DSOs. Commercial IT companies would do this task from a business model that does not fit the domain, such as on the basis of CPU-time used, or the number of connections. The connection of IT to OT is better placed with a DSO, as a gatekeeper, while it can at the same time stimulate commercial IT companies to develop apps and services. This would be a totally new market, and the DSO could take care of the accreditation etc.

The rejection of the Dutch law for mandatory roll out in the Netherlands by the senate on the basis of privacy concerns, has received international attention. One would expect this discussion to be very alive in Germany in particular. However Ringelstein does not report objections from the users regarding data security were recorded in the pilots IWES was involved in. But then again, the systems were small scale and specific. In the Mannheim project, every user had a smart meter, but the network was not connected to public networks. Secure protocols were used (such as SSL and HTTPS), and possibly data encryption, but nothing sophisticated, as data security was not a priority. Instead of internet, it used powerline communication, with one of the project partners responsible for operating it, including data security.

## 3.2 Smart grid specific vulnerabilities?

A number of vulnerabilities were mentioned and discussed in the interviews. Even if it is not always possible to strictly categorize vulnerabilities, we present them along the distinction between technical, human and institutional vulnerabilities.

### 3.2.1 Technical vulnerabilities

The controlled settings of the pilot projects apparently have not (yet) brought to light many concrete vulnerabilities of the system, especially not in the cybersecurity domain. This can be explained from their temporary and detached set up, but maybe also simply from the fact that many pilots are not fully operational yet (such as Texel, Houthavens, Lochem). This may be why several interviewees referred to a thought experiment rather than a pilot to illustrate expected vulnerabilities of an energy infrastructure that is connected and operated through information technology: Marc Elsberg's 2012 novel "Black Out" [5] describes a not so unrealistic chain of events that leads to disaster in the current European electricity grid.

**technical complexity as vulnerability** From a general electricity supply perspective, one could think that by the introduction of decentralized generation and ICT in the grid, complexity is added, and (thereby) vulnerabilities. In a panel discussion at TU Delft,[1], five out of six panelists agreed that introducing an extra layer indeed introduces extra vulnerabilities. But one professor claimed that by working in a decentralized way, the impact of disturbances can be contained by switching off the local area grid. In relation to this, Broekmans believes in the decentralized architecture, with autonomous agents balancing the load and finding their demand in a networked way. With respect to risk in complex systems, it is probably more effective to put the effort into reducing the impact, than into reducing the probability.

**Remote operation** Both Broekmans and Van Bekkum stress that an important source of vulnerabilities will be in the use of components (SCADA, ICS) equipped with ICT. Substations have physical protections, but once we start connecting substations for remote operation, from one substation to the other or from outside, there are more access points and less physical protection. This in combination with a possible increase of control devices, like in smart homes, creates more possibilities for mistakes and abuse. Particular vulnerabilities arise if the grid comes to rely on a number of complex devices from the same vendor with the same bugs: mistakes will be enlarged (as is part of the scenario in "Black Out"). The smaller the diversity, the bigger the effect of small bugs. We should be careful to avoid Vendor- or Technology Lock In. The developments are going very fast, variety, quality and testing procedures take time and may not necessarily be able to keep up.

Van Bekkum points out that standards for control systems are pretty fragmented and usually on a high level of abstraction. In fact, some devices are still brought to market without any security measure implemented, sometimes with the idea that this is not necessary yet. Or that it would be possible to secure the perimeter around the device (firewalls, diodes, cameras, access control, authentication). This can give an enormous amount of security, so you could defend the viewpoint that the devices within such perimeter do not need extra protection. On the other hand, perimeters can also be broken, or attacks can come from inside. So, it is always good to have some extra security measures on the devices. And apart from trying to prevent intrusion, it is also important to monitor and detect intrusion, by checking for deviant behaviour of the system, so you can mitigate the consequences as quickly as possible. Ideally, you detect and take away the intrusion before any damage has been done. Summarizing, we can distinguish three layers here: 1) securing the devices, 2) securing the perimeter and 3) detecting intrusion.

Broekmans adds that the gathering and processing of too much information can also be a source of vulnerabilities in the operation of the grid. The operational side may be affected by the delays, or components may be overloaded by information demands.

**Security of communication and information** Tubben expects that the Virtual IT-layer (cf. page 11) will mainly take place in cloud applications, which can be done through the internet with additional security measures. With respect to OT, it is a different story: because communication becomes so important for a DSO, it should be able to control the availability of the network and the data. Therefore, the CDMA (Code Division, Multiple Access) protocol is now being developed and worked with, within Alliander. Everything within the OT world, will go through CDMA to a central point, which is like a 'militarized zone' –even physically.

[1] Smart Grid Security and Privacy, 19/6/2012, organized by Layla AlAbdulkarim and Wolter Pieters: `http://cesun2012.tudelft.nl/wiki/index.php/TB4`, last checked: 16 Nov. 2013.

The virtual side of things makes the system more open and bigger, thereby introducing new risks, for example the fact that DSOs start building their own data sets. How are these connected? DSOs are held accountable for the issue of security by SODM (Staatstoezicht op de Mijnen) and DTe (Dienst uitvoering en Toezicht energie). DSOs among themselves work against the benchmark set by the best one (for the lowest cost). If you produce something that works, it becomes the norm; one could wonder if this is the best mechanism in such a small playing field.

**Information security in the smart meter** How are the desired functionalities of smart meters balanced against security and privacy risks? According to Gosliga, the developments towards more decentralized energy generation hardly depend on extended functionality of smart meters.

It is still under debate whether the smart meter should have a switch and/or remote control. A remote switch could be used to switch off the electricity for a household in case of payment issues or crisis situations from a functional grid management perspective. However, this may be accompanied with serious privacy and security issues. For example, what if a hacker gains control over that functionality? (See "Black Out" [5].)

Which data are gathered by the smart meter should be connected to the expected functionalities, and balanced against privacy and security risks. The Dutch meter provides four different types of data: 1) interval values: every 15 min for electricity and 1 hr for gas; 2) usage, billing information: per day, aggregated per 1 or 2 months; 3) technical information, necessary for the operation of the meter, like clocks 4) meteorological information, for calibration etc. The privacy risk is greater for the first than for the other categories. Therefore, information of type 1 can only be accessed with explicit permission of the user. This is implemented in the design of the meter chain: interval data are stored within the meter (number of days, intervals, specified in DSMR), and stay within the meter until it is pulled by the DSO (not: pushed to the DSO).

### 3.2.2 Human vulnerabilities: trust and privacy concerns

Agreeing with Ringelstein and Portula, Broekmans sees as the biggest risk in smart grids, that prosumers do not engage. Broekmans: From the part of the grid managers and operators, there has been too much of a "You can safely sleep" ("Gaat u gerust slapen") attitude towards the users. In the Netherlands, we have seen what happens if you don't take users seriously enough, with the smart meter discussion on privacy: it has led to consumers being suspicious on the real intentions behind the meter, as demonstrated e.g. in websites like `http://www.wijvertrouwenslimmemetersniet.nl/`.[2]

**Trust** Broekmans's view is that privacy is probably not the real problematic issue for the people - probably it lies more in the potential for remote switching. And it is healthy to be a bit distrustful towards utilities (the government, the DSOs, commercial service providers etc). The only way for them to take away such lack of trust, is to be transparent, allowing consumers to make their own decisions. A lot depends also on the privacy-value creation trade-off for consumers: "what can I earn from providing a bit of my personal data?". Research at RU

[2] Translation of the url: "*We don't trust smart meters*"; last checked: 4 Oct. 2013.

Groningen[3] shows that people are willing to have their speeding tracked, if they get reduction on their car insurance for not speeding.

In terms of solutions, Broekmans sees it as essential is to establish trust in the parties that ask the users to participate and share our information. This means those parties need to be (truly) transparent, for one in informing us immediately when things go wrong. This is more realistic than promising that everything will go as planned. Also, there should be transparency on where the limitations of the grid are, and that certain balancing and information is necessary for the grid to function. This awareness of the role of information in the new energy supply is something we need to establish as a community. It may be a difficult message to explain, but the only way to earn trust, is to be transparent.

**Security, autonomy and privacy** Broekmans remarks that the confidentiality of data discussion may also become radically different if public attitude towards data would change to see them as open data, for example for the purpose of transparency. Such development is not unrealistic, and different attitudes exist: while salary data are considered to be highly confidential in the Netherlands, they are publicly available in Norway. It creates a level playing field. (In terms of information security: data availability and -integrity issues would remain.) But **Big Data** is a real issue: increasing availability of data will lead to patterns and profiles being identified. Correlations in data are not necessarily logical or causal relations with facts. For the purposes of keeping the grid up, it is more than enough to aggregate and generalize consumption data over time and over users, so that no surveillance state emerges.

Privacy asks for security requirements and investments. In smart *grids* (rather than just meters), the question is if data on an individual level are necessary. According to the *College Bescherming Persoonsgegevens* (CBP), data should only be provided to tasks which have been defined in advance, with a clear aim, and a concrete storage term. With smart grids, we are only just starting to determine what we want from it and need for it. Personally, Gosliga believes that the data is not needed on a household level in order to be able to manage a smart grid. It should be enough to work with a certain, anonymized, aggregation level: the dimensions are not fine grained enough to necessitate that. Also, in production there is enough capacity, in transport there is enough capacity to buffer the dynamics of solar etc. Also it is doubtful whether we can really deal in a good way with the enormous amount of data that would be generated if we would collect data on that level of detail.

### 3.2.3 Institutional vulnerabilities

With complex developments that are emerging and dynamic, both technologically and societally, such as smart grids, it is not easy for institutions to keep up.

According to Van Bekkum, risk management for smart grids should include the following: Investigate which are the threats to the infrastructure. To which extent do you follow best practices? Which controls are in place? Then make a gap analysis. Best practices already contain a number of good ways of protecting yourself. The role of organizations such as ENCS in managing the risk of smart grids, is to provide knowledge advising the companies responsible for the operation of smart grids. The government has a role in stimulating the care for cybersecurity –a task they could put more effort into. Many managers –though not

[3] Bolderdijk, J. W. et al. (2012). Buying People: The Persuasive Power of Money. Retrieved May, 2012, from http://irs.ub.rug.nl/ppn/334141206

all that need to be– are very much aware that cybersecurity is a major issue, even though they will not advertise this as such.

Collaboration on cyberdefense between different companies, possibly from different sectors, can be tricky. Companies don't want to share sensitive information by sharing their security measures. That leads to reduced security, and exposes vulnerabilities (which can also lead to bad reputation). But there are international working groups, that build standards that try to incorporate the latest knowledge.

Broekmans mentions market mechanisms within this cooperative endeavour as source of institutional vulnerabilities. Market mechanisms can be a means to balance demand and response. But as long as we allow parties to earn big money from imbalance, when the market has become the goal rather than the means, it is not the right mechanism for basic public goods. And energy/electricity has become a basic public good.

Market mechanisms, parties that are in the business purely to make money, challenge the necessary trust. Consumers often don't realize that some parties are not in it for the money: for them the DSOs and the energy providers are one and the same. All profit made by DSOs is spent on innovation and improvement. The message of the *Autoriteit Consument & Markt* that switching providers saves the consumer a lot of money, does not help either: it gives the false image of energy providers making big profits from the consumers' wish for stability. Also, the discount for switching is only temporary, and has to be paid by someone - - if we would all switch all the time, it would not be cheaper.

## 3.3 Risk management strategies

Do the new vulnerabilities ask for radical changes in Risk Management procedures for the parties involved in the smart grid? Or would it suffice to simply combine the known procedures from the traditional electricity grid operators, with known procedures from the IT part? And how do cybersecurity related risks compare to the existing (physical) risks of the grid, such as cables being broken during road construction, or a helicopter hitting the high voltage cables?

In the pilot practice, the attention for risk management has mostly emerged in the course of the project. According to Tubben, risks and risk management are very different for IT and OT. Authentication for example as a typical IT-risk, on the OT side it is more about tracking and tracing the physical events. In projects such as Houthavens, these issues have not been explicitly raised, because everything is still conceptual. Lochem is a different story because the role of the DSO in these issues will be experienced in practice. The MS Live Lab in the Bommelerwaard is used to experiment with this role in grid management. In Lochem, we use experiences from LiveLab, but still new things arise. For example, the supply-demand mechanism runs on a server of Alliander. How do we organize the systems management? What is its value?

From the archictectural point of view, a risk management strategy is to keep the IT component modular, so that the system can fall back to a more traditional system in case the IT fails. Kootstra reports that this is the case in Lochem for the way the Powermatcher is implemented. Electricity and communication are strictly separated. The apps communicate over the internet with the central system, and so the central system is also connected to the internet, but there is a conscious decision not to integrate IT and OT. It is realistically possible to see, on the basis of the measurements on the user side and on the mid-voltage side, where the problems originate (that's also what the TRIANA simulation model shows).

In case of malicious attacks in the user layer of the central software, it should always be possible to switch back to traditional operation of the network. The intelligence is configured locally in the apps, which only communicate to the central system, so they do not have the capacity to influence the peers. This makes the effect of breaking into an app and sabotaging it, very local. In order to sabotage the system, one has to break into the central system, which is a lot harder.

Cyber attacks are a new threat that comes up with the integration of IT and the electricity grid. According to Portula, you have to transfer the security aspects. These are not new, and there is a lot that can be transferred: knowledge, standards, protocols for secure ICT into smart grids. However, this is new for the electrical engineers: they do not only get the benefits, they also now have to deal with the downsides of adding ICT.

Van Bekkum notes a fundamental issue for technologies and systems: how to detect the vulnerabilities (without waiting for things to go wrong)? Technology suppliers should continuously provides fixes for vulnerabilities as soon as they have been discovered. This works for example when Siemens develops a device with Siemens software that is also maintained by Siemens: you then have to remain in close contact with the supplier, and make sure you always run the latest version of the software. Just like we are used to with operating systems such as Windows. But there is also the issue that as soon as the vulnerabilities become known, they become known world-wide, so if you don't patch in time, your vulnerability increases. So it remains important to shield your perimeter, and to monitor.

The shielding of the perimeter is also done in the pilots, as described above: the electricity net itself does not change that much, the complexity is shielded off in the IT-layers on the user side. This is called zoning: to create a zone for users, a zone for the technical system and a zone for the electricity infrastructure. The separations between those zones can be made quite strict. The electricity net then changes at the level of information gathering and remote control. Remote control is a real development: TenneT does it, and so do the bigger DSOs.

According to Van Bekkum, two types of information are essential in securing smart grid operation and in the mitigation of certain risks. First, information on status of components, to reduce the amount of unserved energy. "Minutes down time" is the main performance indicator for the DSO, so this status information is very important. Second, the tariff information, to enable peak shaving through pricing incentives: people are price sensitive. A very big risk is introduced with the remote operation. If an insider can do it, someone who hacks the communication can do the same thing. So you need strong protection. At this moment, we may be lucky that the technology we use is too old and specific to be easily hackable. On the other hand, this technology has not been designed for security in the light of the ultra-connectedness of the internet. Think of search engines like Shodan, that allow you to find devices and read out the protocols they use. Similar risks arise by providing network access to service providers or technology suppliers. Or your own employees, for that matter. Some countries decide to hermetically close off all their component, both physically and virtually (Israel for example). They implement a strict division, a (physical, not just a fire-) wall, between the Industrial Control Systems and the rest. The Dutch attitude towards extreme internet accessibility can be seen as taking the opposite direction. But this does not mean that all Dutch companies neglect security. Some take it quite seriously.

**Information protection in the smart meter** For the privacy risks associated with the smart meter, non-technical measures are applied, as Gosliga explains. Whether it is possible to collect certain information, depends on the legal grounding. For example, the E-wet gives DSOs legal grounds to collect daily intervals and technical data. But there is no ground for finer interval (e.g. 15 minute) values: for this, a specific customer mandate is necessary. Giving such mandates is not implemented in the technology, because it would give rise to too much risk of accidental failures (customers forgetting to put their switch on or off etc). Therefore, it is arranged through procedures on the governance level. Monitoring of the way the procedural implementation is realized, is done by an auditor by random checks ex post. This is actually causing quite some debate, because the ACM (*Autoriteit Consument en Markt*, regulator) might conclude this course of affairs is not strict enough. However, in a stricter scenario, energy supply to a household might come to a stop if an energy supplier has made a mess of its billing administration - at the expense of the customers. The current modus operandi (accepted by ACM and CBP) is a balancing between protecting privacy and having workable checks. We should note that while it works now for the small number of smart meter connections (a few hundred thousand meters), we should re-evaluate if it still works when 80% of households are connected.

Gosliga expects that necessary changes will be implemented in the procedural framework and in the control system of the smart meter chain, rather than in the smart meters themselves. On the other hand, some changes have been included in the DSMR4 over the DSMR2, for example, light indicators as information element to show the user when the meter is being read. The party (a supplier, or service provider) requesting information, must have a contract with the customer, about the aim for which the data is gathered. The responsibility to comply with the Wet Bescherming Persoonsgegevens (WBP) also belongs to that party. The debate is, who will be policing this? DSOs see they have a societal role, but not a referee task: it remains the requesting party's responsibility, so this leads to the current modus operandi. If the DSOs would get this referee task, this would also require quite some investments.

Portula mentions Germany's technical directive on securing privacy and information security specifically for smart metering. It gives technical rules that you have to comply with in your smart metering system, and these are currently taken as sufficient for data security issues.[4]

Gosliga stresses that a smart meter is still OT. Within Alliander, a project has started under the name of IT-OT integration. Features of OT require different security measures than the IT components, but it is good to integrate them even though the technical features are different. The basic IT is, and will be, developed within Alliander. If you see the security of the IT infrastructure as a societal responsibility, you should not outsource it. However, it

[4] The ministerial draft of the European Metering System directive (Messsystem-Verordnung) is available in English: http://ec.europa.eu/enterprise/tris/pisa/app/search/index.cfm?fuseaction=pisa_notif_overview&iYear=2013&inum=164&lang=DE&sNLang=DE&CFID=6279894&CFTOKEN=bc6e32b810f46c1b-0C28D28B-FDAD-A30B-5E3BD73F9A859996, last checked: 13 Sept. 2013. This directive refers to a technical directive (TR-03109) developed by Federal Office of Information Security (BSI) and two Common Criteria Protection Profiles. The technical directive ("Technische Richtlinie") and the Protection Profiles ("Schutzprofile") are available here (Protection Profiles in English): https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html, last checked: 13 Sept. 2013.

can be paid for from the transport tariffs, so if these are reduced, as seems to be the plan, cost issues may force a violation of that principle.

**Ex post risk management** Broekmans believes that a pro-active risk management should no longer be the primary strategy. With the speed of development and updates of IT, it is not possible to avoid zero day attacks, for example. Data streams are so predictable, that one should be able to signal errors or attacks easily from data monitoring (**intrusion detection**) – despite the fact that there is the issue with malicious software sending out misleading regular performance data, like Stuxnet did. There are limits to what risk a DSO can carry responsibility for: protection against script kiddies and cyber criminals, but not against terrorists or countries. Just as we don't take measures against bombing our head quarters.

What is important to create is a certain **awareness** throughout the company about cybersecurity issues. Integrate zoning, and strive for situational awareness on the ICT level: the ability of switching off the ICT if strange data streams occur. Another example, smart charging of e-vehicles: there is also communication necessary to synchronize several charging stations (for example if all cars want to fast charge at once, this has to be balanced and spread over time). If such communication fails, there should be the possibility to revert to failsafe mode ('dumb' charging).

### Vulnerabilities and attacks in "Black Out"

The fictional scenario described in Marc Elsberg's novel "Black Out" [5] turns out to be a fruitful though experiment when trying to get a feeling for (cyber)vulnerabilities and their impact in a smart grid system: it was mentioned several times in the interviews. The novel describes the vast effect of an attack on the European power system. Attackers make use of vulnerabilitirs in the modern European net, including the following (spoiler alert!):

- The remote switch and peer-to-peer communication facility of smart meters installed in early adopting countries, had been disabled upon installation. However, this hidden functionality is restored through some social engineering and hacking. Then these features are used to suddenly switch off electricity in a number of households, creating imbalance on a few locations, with cascading effects.
- The interconnectivity of the European transmission grid: blackouts in one or two countries lead to serious problems and cascading effects throughout Europe.
- The control *data* in power plants are tempered with (not with the operational components), violating the integrity of the data shown on the monitors. This fools the operatore in initiatiating emergency measures that cause and worsen problems.
- In the emergency situation, it turns out that some control systems by one Vendor are used in a vast number of plants. They all contain the same back door (insider threat) and the same bug preventing the fallback systems from working properly.

There is also the issue of timing. Because the underlying source of the problems (the hacked smart meters switching off) was only discovered in a later stage (the messenger who figured it out was not believed), partly due to the fact that misleading information was sent to monitoring systems, the effects were able to cascade quickly.

# Chapter 4

# Part III: Vision on (near) future smart grid developments

The pilot projects give a first impression of what parts of the smart grid development are realizable, and which parts will be hard. We asked the interviewees to speculate, informed by their experiences, on how they expect smart grids to function in 5 to 10 years. Which goals will be realized, and which obstacles need to be taken?

## 4.1 Realizable goals

Goorix sees that the smart grid contributes to the sustainability of the energy supply, not so much to the security of it (as security of supply can hardly be improved upon compared to the current situation). It supports the transition to sustainable energy sources, and the desire to be involved in local energy systems. The "smartness", the IT component of it, contributes to dealing with the increased complexity of the combination of centralized with decentralized energy generation, and it enables individual citizens to organize their own decentralized generation. ICT will also be important in exploiting the capacity of the current grid, which is quite over-dimensioned to guarantee the security we currently have. It may help us save on infrastructure investments while maintaining the security level under the growing complexity.

Also, Gosliga sees the main contribution of smart grids in integrating the variety that comes with the energy transition, which requires investments in a new energy management, as it becomes a branched two-way highway. A question is where the necessary investment should come from.

Tubben believes that the main driver for smart grids will be 'local-for-local'. Lochem may be a bit ahead of the Netherlands in that respect, and have different circumstances than e.g. a neighborhood in Rotterdam, but he also sees a general movement towards local initiatives and community. The supply-demand developments in the smart grid will a bit higher up than just the household level (programming washing machines etc), more on the aggregation level of streets or neighbourhoods: batteries for storage, e-vehicle charging. There will be smarter ways of scheduling appliances (in the sense of more efficient and cheaper), but this will not be from the perspective of balancing the grid. The latter would require an enormous amount of standardization over an enormous amount of appliances.

For Kootstra the smart grid is also about participation. Lochem has good chances of continuation in the future, because of its user focus: the pilot listens to determine what is necessary, and don't try to force choices upon the users. This approach should also benefit the scalability, from 25.000 households, to a city or even bigger. It is important to look at the demographics of the pilot population, which is quite homogeneous in the pilots. In Lochem, they are 50-70 year olds, who have some money to spare, are idealistic towards the environment and have time to spare to inform themselves about smart grids and to participate. Similar homogenity appears to be replicated in other pilots.

## 4.2 What is needed to get there?

Tubben believes that the central question is, what the necessary measures are to make it work as efficiently as possible in a particular local setting. What measures are effective will be very diverse over different settings: human behaviour, and what is needed to change it where necessary; technical measures like batteries for storage; smart combinations of energy sources that are locally available (e.g. using gas for transport; combining wind and biogas). With respect to acceptance, a lot will be gained by local ownership of energy sources: having shares in a wind park.

Kootstra has brought the aspect of the demography of pilot participants under the attention of Netbeheer NL and Agentschap NL: how do we get other generations to participate? There are some initiatives running, such as the school project for primary schools about the energy transition, supported by Netbeheer NL: "The Missing Chapter", led by Princess Laurentien van Oranje.[1] This should lead to young parents getting involved as a side effect. But it is not just about awareness, the aspects of money and time can be real constraints for people. For younger people, their life dynamics (changing jobs, commuting, startup investment costs) may be a hurdle to participate. So it is important to make concrete what is in it (in economic terms) for the people. It has to become tangible for the users. Also, more research should highlight the needs of those groups. Currently there are a lot of dependencies and administration involved in order to get private solar panels connected, for a very small prospective financial advantage. Offering the possibility of renting or lease contracts for solar panels etc.: just relieving people of the hassle, could help a lot. If the administrative burden is reduced, and the payoff increases to –let's say– the cost of a ski vacation, it will become a lot more attractive...

Goorix sees politics and the complexity in the energy world as a major obstacle for the further development of smart grids. If you see the amount of organizational complexity involved in starting a cooperative party such as Texel Energy (established 2006), this makes it very hard for new parties to enter. It may not be necessary for the further development of smart grids that new parties enter, but people will increasingly feel the need for *local* initiatives, when more people drive electric vehicles, own solar panels etc. While some regulatory freedom is allowed in the current experimental practice, it is important that in the end, DSOs and other parties involved gets clarity on their legal roles, freedoms and responsibilities.

Germany serves as an example how NOT to do it, according to Kootstra. Subsidies are quite well arranged there (in principle, the consumers pay the subsidies themselves), however, the technical solution is not smart at all: there is enormous overcapacity (from which we in NL profit through low prices). One has to have industry with matching energy profiles that can help balance the load: matching energy consumption, heat production profiles, etc. We have the information for those profiles.

[1] The Missing Chapter: `http://www.missingchapter.org/`, last checked: 21 Nov. 2013.

**Privacy** Giving another perspective to the privacy discussion, Gosliga believes that privacy is for a large part emotion, which is also generation connected. We have grown up in a generation that has to deal with the change of leaving digital traces everywhere - but our children grow up getting used to it, they will not oppose to that. If only, because almost everybody tends to choose the gadget over the (partly unknown) risks. For example, everybody uses digital television, without thinking about what information the providers may track - but with the smart meter, suddenly everybody seems to be concerned about indirectly derivable data. The data security component (and data integrity) will remain important, however the balance between functionality for the system and what data may be gathered, will shift.

This will erode, partly because of the generation effect, and partly because the advantages will become clear. With the increasing reliance on data, quality of software becomes more important (this could also be called a security issue, because malicious software usually relies on backdoors). So testing is important, and a very structured approach is necessary. Smart meters that follow the DSMR are actually quite dumb: they only contain very basic software. They may be too simple even for a hacker to be interesting. The type of vulnerabilities associated with bad programming would probably only occur in the control system of the grid, not in the meter itself.

The keys of the smart meter are configured at installation of the SIM-card and its GPRS-communication protocols are encrypted. A hacker cannot access other meters from accessing one meter. So the chance that hackers focus on breaking into a smart meter is considered to be relatively small. In the risk analysis, we have defined different groups of hackers, and those we would expect to break into the smart meter are journalists and a script kiddy (hobby hacker). Or the academic, for a proof of concept. A terrorist will not be interested, at least: not in our architecture. This is different in the devices used in the USA and elsewhere, where it is possible to get into the grid from a meter (as also [5]).

For Broekmans, cybersecurity issues should not be hyped, and communication about it should be honest and transparent. In a sense, the Dutch privacy discussion around the smart meters is in contrast with the practice of people giving away the same data in another context. Not being home can also be monitored through your mobile. The channel you are watching is also visible to your provider of digital TV.

Also: no one is saying that abusers should get away with it: it is still a criminal offence to break into a house. Although some things are different: if your identity gets stolen, it is hard to notice. And Big Data has a different scope than gossip. But this information can be used both for the good and for the bad. We should balance the risk with the benefit. Over time, acceptance of these phenomena will develop and norms will evolve.

With respect to securing the physical networks: a good strategy for risk management for DSOs, is to divide the network into zones (domains). We will need a more granular approach to controlling the data flows in the grid. No interconnection between stations, only direct communications between a station and central control. Desktops in my BVC (Bedrijfsvoeringscentrum) should only be able to communicate with the systems in the data center, not directly with the stations (through DMZs).

## 4.3 New institutions, unpredictability and risks

According to Gosliga, it is a necessary precondition for the smart grid that we learn more about business and organizational issues. DSOs are technology driven, and tend to get ahead with the technology on those aspects. We should try to learn from other sectors, for example cable companies, or telecommunication-operators, who also take major similar decisions and investments with similar risks.

For example, it is important to realize that the entire market will produce a lot more data. From the EU, the telcos are promoted as data brokers, but it is not right to control critical infrastructure using commercial infrastructure. Broekmans sees the DSO as still the best candidate data broker, being neutral, equal for everyone, regulated and not for profit. Especially for data collection for basic needs, such as energy. Which does not mean that commercial cannot play a facilitating role. Also the electricity providers will play a more important role, when there will be new types of subscriptions to energy.

With respect to security of supply, things may change for the worse with the development of smart grids. Where it is currently quite difficult to produce a blackout, the IT component and increased interconnectivity of components (with remote operation) in smart grids add new ways of producing blackouts. On the other hand, Portula points out that securing against cyber attacks is not new from an IT perspective, and that a lot of these issues can be addressed as in IT security.

Ringelstein has a slightly different view on the controllability of security issues. In Ringelstein's view, smart grids can turn into something rather chaotic because they add so much complexity. At the same time, IT security technologies have proven to be far from perfect (e.g. banking cards, e-bay transfers, the new German health information system etc). If you look at the things that come up, data being sold, transmitted over internet, users becoming more and more transparent, it sheds doubt on the claim that classic IT security can protect critical infrastructure, such as the smart grid. On the other hand, the smart grid vision should be driven by our ultimate goal, the 100% renewable energy system, and make that secure. The focus should be on *simple* solutions, such as small villages being able to build an autonomous energy system (there are some in Germany). Data security issues do not come up that much there. That success is not scalable to bigger cities with their greater complexity.

Ringelstein's hope is that we might introduce best practices, such as technologies, and implement them in our grid first. For example, there are already technical guidelines specifying requirements for PV inverters derating active power or giving reactive power depending on local frequency or voltage measurements and these do not need any data transmission at all. So, solutions that don't really rely on secure data transmission, or just safe by design, are to be preferred. Some of them we already know. It might not be enough to reach that goal of 100% renewable energy, we will still be needing some elements. In research we have to put together all the pieces to build a system that is both secure, providing the means to reaching the goal AND scalable to German or European level. Scalability is needed unless you go to completely decentralized level, but it seems that that is not really possible. For example: offshore wind cannot be decentralized.

According to Broekmans smart grid developments will be very unpredictable, as you can see with other technology developments. To illustrate the unpredictability, think of ”the rise and fall” of SMS: from test protocol, to business model for telecommunication companies, to superfluous because of mobile internet. A realistic scenario would be a development towards capacity tariffs with a flat rate for used electricity. There could be new market parties, like the telco's, IKEA (who may sell energy with their appliances), and an entirely different way of billing. For example, everyone could have a chipcard for different energy subscriptions (green, cheapest, on the basis of participation in a wind park...).

It is really not clear yet what the future energy systems will look like, unlike the past 50 years in which only relatively small changes took place. If only 30% of the electricity is from consumer electronics, consumer smart grids will not be enough to provide the necessary flexibility. At the same time, the flexibility of the heavy users (industry) is already utilized, they already have contracts. Broekmans suggests an important future role for postponed load, by smart use of storage. And for DC replacing AC, because it will be guaranteeing 50Hz is very hard once all our coal plants are turned off and we only have renewables.

Ringelstein agrees that the vision question is the most difficult one, because it involves all complexity and we don't see the big picture yet. For now we can do small steps and work on it....

# Chapter 5

# Conclusions

This chapter describes the impression of the current smart grid practice, insights and expectations, with respect to vulnerabilities and security, as it emerges from the interviews.

## 5.1 Integration of technologies in a dynamic context

The traditional electricity grid has been built over a long period and for the long term. Components were, and still are, installed to be operational for at least a few decades. Risk management procedures and architecture for the traditional grid have developed over the course of a century and resulted in an extremely reliable system.

ICT developments happen in a different time scale, and in general, the grades of security and reliability are of a totally different order than those of the electricity grid (in any case in Europe). Also, whereas the electricity grid has always been a top-down controlled system, ICT is characterized by broad connectivity and less hierarchy - a completely different structure.

With the incorporation of sustainable energy sources, resulting in dynamic generation patterns, ICT has become essential for the operation of the electricity grid as it develops. This means that electricity- and ICT experts have to collaborate, not only to integrate technology, but also the cultures related to the different characteristics of their backgrounds.[1]The difficulty of integrating the cultures may be a hurdle to a smooth integration of the technologies, and security may (temporarily) be impacted by it. However, this is probably only a matter of time, pushed by the technological developments.

A major hurdle in assessing risks and developing risk management procedures is not only the fact that "*the* smart grid" as such does not exist yet, or, taking a liberal interpretation of the term, already exist for a number of years. More importantly, it is hard (if not impossible) to define exactly which functionalities and goals of the smart grid will be realized in 5, 10, 20 years (and in which order). It has to become clear in practice how current small scale solutions (like the pilots) can be scaled up to 80 or 100 % of households. How the balance between the goals, costs, physical hurdles and societal acceptance plays out, is not a 'simple' matter of design, but the result of an interplay between different technology

[1] This remark was also made by research director Klaus Kursawe of ENCS in his address at the "EU-US Open Workshop on Cyber Security of ICS and Smart Grids", Oct. 15, 2012 in Amsterdam, `http://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/eu-us-open-workshop`, last checked: 21 Nov. 2013.. In this respect it may be relevant to note that the perspective on smart grids sketched in the interviews, comes mostly from experts with an IT background.

developments (within the electricity sector, car sector, building technology, ICT), societal developments (politics, economics, electricity demand and dependency, cultural attitudes) and environmental developments (climate change, demography, availability of renewable energy sources).

## 5.2 Main issues highlighted in the interviews

But this does not mean that nothing can be said about vulnerabilities that need to be prepared for, dealt with, and possibly solved. The most concrete current practice, at least in the Netherlands, is within smart grid pilots. In the interviews, we tried to highlight the views of experts, based on this current practice, on the issue of security and risk management for smart grids, from as broad a perspective as possible.

In this section, we review what we consider to be the main points regarding security in smart grid developments as highlighted in the interviews, more or less along the three main parts of the interview (cf. page 7).

### 5.2.1 Operational definition of smart grids

Among the interviewees there was wide consent that *the smart grid* as such is hard to define. However, there was also consent about the purposes for which a new electricity grid, with higher integration level of ICT, is being developed:

- Integrating renewable energy sources (in the long run replacing traditional sources), while keeping a reasonable level of security of supply;
- Exploiting ICT for more efficient use of the current infrastructure (thereby postponing investments);
- Helping consumers to save energy by more insight into and more control over their consumption (through feedback systems and smart homes);
- Creating local energy efficient ecosystems that are less dependent on the main grid (local-for-local);
- Enabling new technology developments such as e-vehicles

These goals are not entirely disjoint, and some of them can be aligned. The development of smart grids will probably be a complex interplay of fulfilling each of these goals. For which goals the solutions are available and realistic, depends on many external factors, and some solutions may introduce threats to other goals. Which objectives are within reach, depends on many eternal factors, making the exact development of smart grids unpredictable.

### 5.2.2 Technical, human and institutional vulnerabilities

What becomes clear from the interviews, that in smart grid practice, technical, human and institutional issues are deeply intertwined. It turns out that most vulnerabilities of the system have aspects in in all three categories. We highlight four general issues that reoccurred throughout the interviews. User participation (non-technical complexity) and Scalability are arguably mostly institutional and human issues, Privacy and Big Data mostly human, and Control Systems and Cybersecurity mostly technical.

**Non-technical complexity and user role** DSOs, energy providers, traditional electricity companies (historically) tend to approach smart grids, and security issues, from a technical perspective. However, user participation, in providing energy (prosumers), flexibility (essential for load balancing) and data (for grid management), is the key factor for the successful operation of a smart grid system. The new and central role of the user and user behavior, is considered to be the main source of complexity and unpredictability. At the same time, many initiatives are being taken to make the involvement of the (future) users smoother on different levels (economic, education, regulatory etc.). A new role is expected to emerge around the new commodity of flexibility, essential for streamlining the dynamics of the technical and behavioral parts. Business models for such role require robust market mechanisms with stable incentives.

A remarkable feature of the pilots is the relative homogeneity of the participating population: mostly middle-aged or older, which seems to indicate that a certain amount of time, money, education and outlook on life strongly contributes to participation. Social research is needed to inquire why other generations are less represented, in order to develop the smart grid as an inclusive system and achieve the necessary participation level.

**Scalability** The pilot projects are conducted to experiment on a small scale with what is envisaged to be the general model for the electricity grid in the next decades. However, as far as the pilots are successful, it is not directly clear whether the successes are generalizable. The local-for-local approach works well, given that the specific characteristics of the local environment are leading in the set-up of the system: in terms of energy sources, geography (e.g. Texel as an island), social coherence of the population (the island structure of Texel also seems to stimulate organization into cooperations). But this also means that extending the smart grid to a national level, local differentiation will require a lot of attention, so it will be costly.

The local-for-local approach seems to be highly complex by its decentralized locally-specific structure, but some think this may actually be a form of complexity that contributes to a more secure grid. With local-for-local, local systems would be less interdependent, so less vulnerable for cascading effects.

**Privacy and Big Data** The blocking of the Dutch law for mandatory smart meter roll out has awoken the regulator and the companies about the necessity to consider privacy and security issues in the technology design AND in governance design. This was convincingly described by Gosliga. It works now for smart meters because they are relatively concrete, and related to similar information intensive infrastructures that raised societal discussions.

As a consequence however, it seems that functionality is decided to be limited and pushed to outside the smart meter for example in the virtual layer. Privacy issues are resolved to a certain extent by giving users autonomy over the amount of data they are willing to share, for example in exchange for services. In a virtual IT layer, users can choose to use apps to help them control their own usage and costs (as described by Kootstra). Such apps usually come with privacy statements, specifying which data will be collected for which purpose, for the user to agree with (according to the principle of *informed consent*, which is also an important pillar of the EU Privacy and Data Protection Directives). However, in the practice of mobile phone apps for example, we can see three problems with this solution: 1) the privacy statements are usually too long and not concrete enough to make users truly understand what they consent to, 2) practice shows repeatedly[2] that companies violate these agreements, and 3) users themselves have little realistic means to detect infringements.

But the development of Big Data, i.e. massive data gathering, will definitely have an impact in the smart grid. Data mining can be benificial for the operational management of the grid, but profiling users on the basis of energy usage data (per household, or aggregated on street or neighbourhood level) can lead restriction of the freedom to choose. This issue fits in the general discussion on Big Data.[3]

According to the CBP, data should only be provided to tasks which have been defined in advance, with a clear aim, and a concrete storage term. With smart grids, we are only just starting to determine what we want from it and need for it. Certification and regulation are then no simple solution. Something similar holds here as holds for software in general, as phrased by Prof. Bart Jacobs:[4] "It is hard, if not impossible, to delimit the precise functionality of software. And additionally, for each time information is gathered, it has to be established that (only) the certified software was applied, and this is a problem in itself." This remark relates to the conclusions of [12] on privacy and the smart meter, who say that it is necessary to first determine functionalities, derive minimal information for the functioning of the smart grid in order to avoid involving unnecessary personal data. This clear determination of functionalities is not done by the European Commission, according to them. The problem however is that nobody wants to delimit the functionalities yet, because nobody knows how exactly the smart grid will operate.

**Control systems and cybersecurity** Apart from privacy, and with a greater impact on security of the energy *supply*, the vulnerability of SCADA systems and ICS to cyberattacks was mentioned as an ICT-related weakness of smart grids. Often, the robustness of subsystems, such as control- or communication systems is overestimated. It is dubious whether cybersecurity issues in the smart grid can be solved by current IT standard solutions, but which will be the exact new threats, will depend on the implementation and functionalities. Issues that are to be expected are backdoors, and technology- and vendor-lock in. On the other hand, a technology supplier that provides the devices, the software and their maintenance, can also be expected to be the most efficient in detecting bugs and security holes, and providing fixes for them.

### 5.2.3 Risk management strategies for smart grids

The (cyber)security issues in smart grids highlighted above, ask for measures. As it turns out, risk management is in none of the pilots addressed from the start (no *security-by-design* approach).

It seems that with the dynamics of technical and organizational developments (more and more diverse actors), **timing** is an issue in managing the system and its risks. In general,

[2] Recently, small telecommunication companies in the Netherlands were fined for unauthorized use of customer data: `http://www.volkskrant.nl/vk/nl/2686/Binnenland/article/detail/3527583/2013/10/15/Flinke-boetes-voor-schenden-privacy-door-providers.dhtml`, last checked: 21 Nov. 2013.

[3] An excellent discussion of societal and moral impacts that counterbalance the promises of Big Data recently appeared in the Stanford Law Review: *Three paradoxes of Big Data* [8].

[4] In radioprogram Argos, 13-10-2013 on the admissibility of police methods against cybercrime, such as "hacking back", explaining why the situation is different from physical surveillance technology such as cameras.

one could expect that coordination between the higher number of actors creates bigger delays between discovery of vulnerabilities and implementing measures (with zero-day attacks, for example). Vulnerabilities also arise in the time gaps needed for communicating and coordinating between actors and subsystems. On top of that, (current) dynamics make standardization procedures more complex and time consuming.

The following risk management strategies, are adapted for such dynamic envrionment:

- Not all vulnerabilities can be prevented or even known in advance, so a fundamental task in risk management is to detect them (through *situational awareness*), and have procedures in place to deal with them once detected. Putting too much effort into reducing the probability is less effective than putting effort into reducing the impact.
- Zoning is an architectural principle to put prevent impact on the core system through vulnerabilities of the outer (more open) layers. Similarly, one can strive for a modular combination of the IT and OT layers, such that in case of cybersecurity issues, the system could always revert to traditional operation.
- With respect to human vulnerabilities, such as privacy and trust: be transparent on the purposes for which data is gathered, and be open when things go wrong.

With respect to the latter point, a Value Sensitive Design (VSD)[5] [7] (or more specifically: a 'privacy by design') approach to the development of smart grids could be recommended for the further development of smart grid systems. However, such approach involves the balancing of the functional requirements of the system against non-functional effects. It is a severe obstacle to such design approach if functionality is not (yet) specified, (as was argued for reconfigurable sensor technology in [4]), and this is the case for smart grids and their components.

Broekmans stressed that it is important that companies (and other organizations) are transparent on where the limitations of the grid are, and that certain balancing and information is necessary for the grid to function. It is up to society to determine which balance is acceptable.

This seems to be a way to deal with this issue, as was demonstrated in the procedure around the smart meter in the Netherlands. The CBP requires that data can be collected only for tasks that are defined in advance, and for a clear purpose. Developers could be required to keep track of the goals and values implemented in the system: how are they balanced against each other? which data are used for which purpose? which level of detail is required for which purpose? The system should be transparent in that respect in every stage of the development. The balance between goals and values may shift, society should be able to at least discuss about the balance – and be able to verify which information is gathered for which purpose.

To 'build a culture of cybersecurity' is the first of five strategies in the "Roadmap to Achieve Energy Delivery Systems Cybersecurity" of the American Department of Energy [9]. After the interviews, the question: is there a *culture of cybersecurity* [10] in the pilot projects? A short answer is no, or at least: not yet. Within Alliander, for example, a movement in this direction is being made with their three step model of compliance 'maturity', which will be used as guideline before the Lochem pilot is brought to real operation.

[5] Value Sensitive Design is a "theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process." [7]

Smart grids probably have to move out of the experimental and tightly controlled pilot phase, into the more open real practice, to make (cyber)threats also more realistic. Which is not to say that education in 'thinking like a hacker' is not useful in the system development phase. ENCS is therefore offering this as part of their *Advanced Cyber Security Course*.[6]

## 5.3 Concluding remarks

In this report, we have recorded the outcomes of a number of expert interviews on the topic of (cyber)secuirty for smart grids, related to the current pilot projects within the Netherlands, including an international perspective. These outcomes show that smart grid developments have many unpredictable elements, as they incorporate institutional and human dynamics. But also technological developments, in sustainable energy generation and in ICT, proceed rapidly and erratically. Smart grids are a prime example of socio-technical systems, where the interaction between the societal/human and the technological are deeply intertwined for the successful operation of the system.

The complex dynamics of the smart grid development, and the fact that exact functionalities of components are determined (and changed) on the go, make it hard to assess and prepare for the vulnerabilities in advance (*by design*), and to rely on traditional risk management methods. For example, with the increased incorporation of ICT, cybersecurity issues are introduced. These may or may not be simply resolved by standard IT-security measures – if only because reliability thresholds in the electricity grid (hundreds or thousands of a percent) are of a different order from those generally sufficient in ICT.

Within the pilot projects and the practice as it transpired in the interviews, attention for (cyber)security does not seem to be a primary and explicit goal in any of the reviewed experimental settings. Most attention in those pilots goes to exploring the best architecture for smart grid systems, how to involve the consumers, experimenting with new roles and load balancing mechanisms (in the operational technology and/or demand side management).

Attention to security issues emerges in case of problematic experiences, with a very prominent example in the attention to privacy in Dutch smart meters, as recounted by Gosliga, after the rejection of the mandatory roll out law. It might be just a matter of moving from the experimental to a more operational phase before specific (cyber)security issues get attention and are addressed. This is not to say that in general there is no attention to (cyber)security issues, but most of it seems to be done on a more general than on the implementation level, in collaborative efforts such as the ENCS, the Smart Energy Collective, and EU Expert Groups.

### Acknowledgments

This report aims to provide a source of information and research questions for practice oriented research into (cyber)security for smart grids, approached not only from a technical perspective, but also from a human and institutional perspective. We thank the interviewees for their cooperation, time and insightful contributions. The work of the authors is supported by the joint programme *Empowering Networks* of the Next Generation Infrastructures (NGI) foundation and Dutch DSO Alliander (project 09.08.KID).

[6] `https://www.encs.eu/education-training/`, last checked 24 Nov. 2013.

# Bibliography

[1] L. AlAbdulkarim and Z. Lukszo. Impact of privacy concerns on consumers' acceptance of smart metering in the netherlands. In *ICNSC*, pages 287–292. IEEE, 2011. 6

[2] V. Bakker, A. Molderink, M. G. C. Bosman, J. Hurink, and G. J. M. Smit. On simulating the effect on the energy efficiency of smart grid technologies. In *Winter Simulation Conference*, pages 393–404. WSC, 2010. 13

[3] C. Cuijpers and B.-J. Koops. Smart metering and privacy in europe: Lessons from the dutch case. In S. Gutwirth, R. Leenes, P. de Hert, and Y. Poullet, editors, *European Data Protection: Coming of Age*, pages 269–293. Springer Netherlands, 2013. 12

[4] F. Dechesne, M. Warnier, and J. van den Hoven. Ethical requirements for reconfigurable sensor technology – a challenge for value sensitive design. *Ethics and Information Technology*, 15(3):173–181, 2013. Special issue dedicated to the HCI-workshop Values in Design, Lisbon, September 6, 2011. 38

[5] M. Elsberg. *Black Out - Morgen ist es zo spät.* Blanvalet Verlag, 2012. 21, 23, 28, 31

[6] EU working group Smart Grid Information Security. Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment (M/490). `http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf`, March 2011. 18

[7] B. Friedman, P. H. Kahn, and A. Borning. Value sensitive design and information systems. In *Human-Computer Interaction and Management Information Systems: Foundations. M.E. Sharpe*, pages 348–372, 2006. 38

[8] N. M. Richards and J. H. King. Three paradoxes of big data. Stanford Law Review Online, Vol. 66: `http://www.stanfordlawreview.org/online/privacy-and-big-data/three-paradoxes-big-data`, September 2013. 37

[9] U.S. Department of Energy. Roadmap to Achieve Energy Delivery Systems Cybersecurity. `http://www.smartgrid.gov/sites/default/files/doc/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf`, September 2011. 38

[10] U.S. Department of Energy. 2012 DOE Smart Grid Cybersecurity Information Exchange. `http://www.smartgrid.gov/document/2012_doe_smart_grid_cybersecurity_information_exchange`, July 2013. 38

[11] M. Weijnen, Z. Lukszo, and G. Deconinck. Introduction. In Z. Lukszo, G. Deconinck, and M. Weijnen, editors, *Securing Electricity Supply in the Cyber Age: Exploring the Risks of Information and Communication Technology in Tomorrow's Electricity Infrastructure.*, pages 1–12. Springer, 2010. 5

[12] T. Wisman and A. Lodder. Het slimme elektriciteitsnetwerk en de noodzaak tot het uitwisselen van persoonsgegevens. *Tijdschrift voor Internetrecht*, 6(4):94–100, 2013. 37

# Appendix A

# The interview plan

Each interview lasted 60 to 90 minutes. For the Dutch experts, the interview was on location, for the international experts, the interview was done through Skype. The recording of the interview was then written into an English transcript, which was presented to the interviewee for comments and corrections. The recording was subsequently deleted. Texts attributed to the interviewees are slightly paraphrased versions of the literal transcript. All interviewees and participants in the project *Kwetsbaarheid en veiligheid van Intelligente Distributienetten (KID)* receive this report. Findings of this report will be combined with literature research into a scientific publication on (cyber)security for smart grids.

## A.1 Interview structure

The interview is divided into three themes, which are described below.

### Inventory of current smart grid setting

- How exactly is the smart of smart grid implemented in this setting?
- In general: what does the notion "smart grid" mean, according to you, in your current practice?
- To what extent, and how, are ICT- and (electricity) networks integrated, both technically and organizationally?
- Which actors play a role in your smart grid setting? What are their roles and stakes? How are they organized? Can this be generalized to smart grids in general, or is it specific to your smart grid setting?

### How do you deal with Risk Management in the smart environment?

- How are the responsibilities for security of supply distributed in the current setting?
- Which procedures regarding vulnerability and security are maintained, with which actors? How does the smart aspect show in these?
- Which types of vulnerabilities have been mapped for this smart grid setting, or come out in practice?
- How about administrative, legal, societal threats?

- What is the role of ICT in the management of the security of the network?
- Which vulnerabilities are directly or indirectly related to the smart aspect? What kind of relation?

**Vision on the development of smart grids**

- Does the ongoing transition to smart grids introduce new vulnerabilities, and if so, which are the most important ones, according to you?
- Does the transition to smart grids necessitate a different approach to vulnerabilities, threats and security of energy networks? If so, which are the most essential changes?
- What is your vision on the development of smart grids in the (near) future?
- What is the most important contribution in the short term of the smart aspect to security of supply?
- What is the most important threat to the further development of smart grids?
- Which policy and law (by national and/or European governing bodies) is necessary to stimulate security of electricity supply for smart grids?

# Index