Electricity grids are in a transition phase. With the rise of renewable energy, energy “prosumers,” and electric vehicles, traditional models of matching supply and demand are no longer adequate. Grid pilot projects can help identify ways to improve cybersecurity in future grids.

A n electricity grid’s main task is to deliver electricity from suppliers to consumers through a complex network, including high- to low-voltage transformations from the transmission grid to the distribution grid. Nowadays, electricity grids are increasingly incorporating new resources of renewable and modular energy, such as wind farms and electric vehicles. Studies have found that current grids aren’t efficient. For example, from 2005 to 2009, New York’s electricity demand was above 70 percent of the grid capacity for only 12 percent of the time, while the total capacity had to be kept available at any time to remain reliable during peak loads. In addition, in current grids, up to 8 percent of energy is lost during transmission.

To aid in the grid’s transition and incorporation of more efficient solutions, researchers have introduced different innovations under the umbrella concept of smart grid. Essential elements of this change are decentralized production and the increased flexibility required of the grid, due to the dependence on customers and the instability of renewable energy sources. Traditional models of matching supply and demand are no longer adequate.

Although there are no detailed specifications defining the grid of the future (we prefer to use the term future grid rather than smart grid), the common description implies an upgraded electricity network with two-way communication between supplier and consumer, requiring intelligent metering and supervision. Information and communication technologies (ICTs) are indispensable for controlling the required adaptive infrastructure, both for monitoring and (remote) control.

The development of future grids brings uncertainty about its effects on critical public values, in particular, security of supply and customer data privacy. The increased dependence on communication and remote operation raises concerns that cyberattacks will become a very realistic threat. Indeed, transitions from physical to digital systems—for instance, electronic voting, electronic health records, and smart metering—have gone wrong too often.

Many scholars argue for privacy and security by design to ensure such values are addressed in the early stages of technology development—not just after the technology is deployed. However, due to uncertain futures and dynamic threats, obtaining the right
information for such strategies at the right time isn’t always easy—or even possible. To tackle this challenge, responsible experimentation with emerging technologies via controlled environments, pilots, and so on, is essential. In this article, we aim to complement a “cybersecurity by design” approach to future electricity grids by providing a vision of security-aware pilots for smart grids.

**Stakeholder Perspectives on Future Grids**

The development and implementation of future electricity grids depend on different technical and organizational stakeholders. We explore the perspectives of stakeholder roles that are key influences in grid and pilot design: authoritative bodies (using available documentation), automation vendors (using available documentation and expert opinions), and grid operators (via structured interviews). The former two contextualize the environment, and the latter helps us derive our key conclusions.

**Authorities**

In Europe, systematic efforts to develop smart grids are mainly motivated by several EU Energy Efficiency Directives with guidelines for member states focusing on new technology deployment. The EU’s overarching goal is to have 80 percent smart grid coverage by 2020 and 100 percent by 2022. In the US, the 2007 Energy Independence and Security Act led to the creation of the Grid Modernization Commission and directed the National Institute of Standards and Technology to develop standards for the US energy market to be implemented under regulation by the Federal Energy Regulatory Commission.

In this context, most predictions for the next decades anticipate electric vehicles to be a major factor in the grid’s changing landscape, with estimates projecting up to 40 million electric vehicles in the US by 2030. Bulk storage technologies, on the other hand, aren’t seen to be likely to gain widespread deployment.

To make EU strategies more concrete, the directives introduce different tasks to tackle organizational complexities in the realization of future grids. Authorities envision new business roles, such as service aggregators who assist in matching energy demand to supply by offering services that encourage use when supply is high. They also envision the need for technologies that handle power injections, such as power ingress from electric vehicles, and for shared technological standards, such as the Consumer Electronics Association’s effort to establish a common communication standard for home appliances. This vision leaves future grids’ cybersecurity aspect quite open, commonly proposing the exploitation of best practices rather than advocating specific breakthrough developments.

**Vendors**

On a high level, vendors producing automation equipment envision future grids as adaptive, predictive, and proactive systems that rely less on human operators, can perform distributed power generation, and are capable of self-healing. On a practical level, the realization of these objectives is envisioned in phases, based on priorities:

- Implement end-to-end distribution grid management to maintain reliable grid balance.
- Establish asset health management, developing mechanisms to monitor aging infrastructure.
- Incorporate microgrids and distributed energy resources, such as adding support for electric vehicle charging.

Although requirements for future grids are emerging, there’s no generally accepted specification of grid layout and devices. Because automation devices are traditionally required to have a long lifetime—up to 30 years—and vendors are in a continuous run for market share, a secure and long-lasting grid component design for a competitive price seems hard to achieve.

Vendors are developing security features in newly designed grid components, incorporating key management and performing software security testing. However, current security paradigms aren’t necessarily the best solutions for future grids; outdated encryption schemes are still in use, and key management schemes aren’t scalable. To overcome the complexity of the transition period from aging devices to devices with security features, vendors are deploying intermediate devices to provide a security shield for aging grid components.

**Operators**

Our third perspective comes from grid operators. In the context of the Dutch research project Vulnerability and Security for Intelligent Distribution Grids, we performed in-depth, structured interviews with eight individuals involved in smart grid pilots in the Dutch IPIN (Innovation Platform Intelligent Networks) program. Our interviews targeted experts involved in pilot design and monitoring, risk management, and ICT integration into the electricity infrastructure. Five experts were distribution system operators (DSOs), and three were in applied research.

We structured our open-ended interview questions along the following dimensions:

- an operational definition of smart grids as it transpires from the current (experimental) practice and an inventory of actors in the smart grid pilots;
- an inventory of technical, human, and institutional
vulnerabilities and current risk management approaches; and
• visions of directions of smart grid development and necessary policy with respect to vulnerabilities and security.

Each interview lasted between 60 and 90 minutes. The interviews were transcribed and presented to the interviewee for comments and corrections. All interviewees expressed their personal experiences and opinions; they don’t represent official company or organization policies. The opinions we sought were limited to the Netherlands and the organizations involved in the aforementioned pilots. More details on the study, including the list of interviewees and interview questions, can be found in our report “(Cyber) Security in Smart Grid Pilots.”

We coded and grouped the responses that were relevant to security and extracted seven key concerns. These concerns aren’t a complete overview of the results, as the study’s aim was broader. In this article, we use the study as a background for outlining security concerns.

Definition of smart grid. Although the term smart grid is used frequently, practitioners agree that there’s no commonly accepted definition. General properties are more or less agreed on, but detailed properties aren’t specified; thus, various future grid implementation solutions will likely differ. The pilot projects’ smart grid implementations differ in setup: implementation in new building developments versus existing neighborhoods, focus on technical control and feasibility versus user participation, self-sufficiency versus integration in the existing grid, and so forth.

Cyber-physical risk. Grid infrastructures integrate operational and IT infrastructure. Experts raise concerns that the existing best practices in IT don’t sufficiently address future grid security risks. Integrating the cyber and physical domains leads to novel vulnerabilities. DSOs believe increased remote operation is an important threat, making it possible for adversaries to access and control operational technology without physical barriers.

Implementation complexity. Operators point out that future grid implementation choices are highly context-dependent and thus not necessarily scalable or transferrable. This is mainly due to large infrastructure differences among cities and neighborhoods. In particular, there’s an essential practical difference between building a new neighborhood from scratch—using current insights and energy generation technology and attracting inhabitants on the basis of their willingness to participate—and implementing a smart grid in an existing neighborhood, with its potentially outdated electricity infrastructure, lack of space, and mix of inhabitants.

Architecture. Operators note that the impact of two-way electricity flow will depend on the grid architecture. The Dutch pilots take a local-for-local approach as key principle—use up and store locally as much locally generated energy as possible—because feeding it back into the high-voltage transmission grid requires more complex technology and is less efficient. For example, in contrast to the German situation, energy generated by rooftop solar panels isn’t expected to be fed back into the transmission grid. Rather, there will be local storage solutions, suggesting that the bi-directional feature’s effect on the grid will mainly play a peripheral role.

User participation. The interviewed operators perceive user participation as the most difficult, uncontrollable source of threats to future smart grids. Basically, this is due to the radical change from top-down control to decentralized components involving user behavior and actions. The concern here is that it seems impossible to anticipate all effects of the interaction between the highly automated system and the less predictable, and possibly malicious, human behavior.

Data granularity and privacy. After the mandatory smart meter rollout was cancelled due to privacy concerns, the Dutch operators were forced to involve consumer organizations,3 leading to limitations on data collection. For example, real-time usage data is accessible only to users for their personal insight. DSOs can collect daily data on a meter’s operational status, and energy providers get yearly data for billing purposes and are only allowed to use weekly or monthly data to support their customers in usage monitoring.

No security focus. The practitioners report that attention to cybersecurity in the pilots is marginal. None of the 12 Dutch IPIN pilots explicitly targets understanding and solving cybersecurity issues. Instead, the main focus is finding an optimal technical and organizational architecture.
Core Security Concerns in Future Grids

Authorities have a high-level view of future grid security issues, whereas vendors focus on implementation challenges in the transition phase. Thus far, pilot projects have yielded operators only limited, implicit insights into future grid security problems. However, we can use the patterns in the stakeholders’ perspectives to distill overarching security concerns. We found common stakeholder concerns and derived three core security challenges and associated threats.

Future Grids as Emerging Technology

Several security challenges arise from the emergent character of future grid development. Our findings show that future grids don’t have a defined set of functionalities. Because each stakeholder has a different vision, different stakes in the current grid, and uncertainties about its role in future grids, it’s impossible to define precisely what characteristics make a grid smart and whether current grids qualify as smart grids.

Rather than being a well-defined type of grid architecture, future grids appear to have only “family resemblances,” in that they share certain characteristics but no single property is shared by all of them. From a security perspective, this raises the issue of how security by design can be implemented effectively without specification of what functionalities the system should have or when the design can change on the fly.9,10

The emerging character also manifests itself in aging devices with poor or no security features. Infrastructure design often depends on these devices, which sometimes operate in the same setup for decades but were never built with security in mind. Thus, new, more connected architectures are prone to previously isolated devices’ existing vulnerabilities (for example, see Project Basecamp by DigitalBond; www.digitalbond.com/tools/basecamp).

Increased Organizational Complexity

Commonly implied characteristics of future grids are power production and consumption flexibility, preventing excessive production and energy loss through adaptive usage.11 Practitioners at DSO systems emphasize that future grids are highly interconnected infrastructures in which initial deviations can produce cascading effects on different elements, related to both infrastructure and market.

The practitioners anticipate a new role: aggregators as intermediaries between utilities and consumers. One type of aggregator could be store chains selling home appliances with preconfigured electricity packages, for instance, offering lower prices on washing machines that schedule operation based on grid conditions. From a security perspective, aggregators are an example of the broadened spectrum of emerging and adaptive threats, both malicious and negligent. For example, by tampering with appliances in the supply chain, attackers can affect electricity consumption in many households. Also, control over a series of appliances can produce a botnet attack on the infrastructure.11

Organizational complexity also increases as communication becomes the backbone of future grids. A prominent change is the upward flow of energy from decentralized energy sources. Although the reverse flow feeds the grid and ensures efficient consumption, practitioners raise concerns that the current infrastructure is incapable of handling this reverse flow and that the added electricity could become an attacker’s means to destabilize the system. For example, hundreds of attacker-controlled cars could connect to the grid simultaneously and push back accumulated energy.1 Similarly, allowing suppliers to remotely disconnect potentially harmful or nonpaying customers enables attacks in which an adversary obtains access to a DSO system to remotely disconnect target households, potentially in large numbers.

Increased Demand for Stakeholder Cooperation

Cooperation of customers and other stakeholders is important, as visions of future grids rely on active user involvement, potentially mediated by aggregators. The main smart features—balanced power production and consumption—rely heavily on user behavior, such as adopting grid-desirable energy consumption patterns to contribute to the overall efficiency.

Non-cooperation of users can affect the system in various ways. Operators acknowledge that synchronized misbehavior might bring a system to an unstable state. Such misbehavior could be due to user collusion or malware on smart meters. Other types of user participation, such as the issuing of campaigns against smart grid technology, can destabilize the energy market.11 In addition, data granularity and data handling are important aspects of consumer privacy; a breach would significantly influence consumers’ trust in the system. Although privacy breaches have already occurred in other domains, the misuse of energy consumption data—for example, by
burglars who get to know when a resident is away—is an important new threat. Technical developments and new business models might push to make finer-grained information accessible to more actors.

**Security Concerns as Incentive Problems**

Future grids raise different technological, institutional, and human-related concerns. The question is whether it’s possible to identify an overarching framework to make these issues understandable to those who design the systems and run the pilots, and to ensure they can identify concerns to the best possible extent using the available resources and knowledge.

We believe incentive-centered piloting and design can help in this regard. This approach makes it possible to express the reasons for attackers to attack and for defenders to defend in the same terms. When trying to secure future systems, we want to ensure that there’s not too much utility for a diverse set of stakeholders to mess with the system. Tampering doesn’t need to be impossible, but the expected utility for adversaries should be relatively low, or preferably negative. In addition, there should be positive incentives for stakeholders to provide defensive measures against misuse. Although future technological developments and environments are uncertain, we believe that common values and incentives can be translated to similar technological contexts in future grids.

To make the incentives perspective more concrete, we use the crime science approach, which defines five categories to design an environment to reduce incentives for crime: increase effort, increase risk, reduce rewards, reduce provocations, and remove excuses. Both technical and organizational core security concerns about future grids can be explained from this perspective.

First, incentives play a role in dealing with the challenges of emerging technologies. As we pointed out, future grids will contain a larger range of components, with different ages, life cycles, and development cycles. For cyberterrorists, attacking outdated devices will require less effort, as the devices are more likely to carry known vulnerabilities. The reward in terms of damage caused could be high because the complex architecture might have many identical components. Remote access reduces the effort and the risk for attackers trying to disrupt critical infrastructures. For defenders, costs of upgrading or updating the equipment are typically significant, and there are risks involved, such as accidental failures caused by updates, resulting in various excuses for not updating systems.

Second, incentives are key to understanding security problems associated with roles in increased organizational complexity. Business innovations, such as the new aggregator role, increase the complexity of attributing responsibility for security issues and might attract malicious parties to the system. For example, aggregators’ malicious activity might include distributing devices with back doors or malware, which can then be controlled remotely to cause blackouts or market disruptions with low effort. The lack of security assessment in the supply chain causes aggregators to perceive less risk of being detected when performing such malicious activity. Other potential malicious actors might include grid users and terrorists.

Finally, incentives can shed light on the problems associated with stakeholder cooperation. Users have several incentives to resort to undesirable behavior, such as tampering with smart meters. They might be provoked by problems in supply, such as frequent blackouts, or by a sense of infringement of the personal sphere, for instance, if operators can remotely disconnect their smart meters. Users might also use malfunction or unworkable user interfaces as an excuse. Lack of fines and enforcement might reward such behavior and keep the risk low. Whether such behavior will occur also depends on design: How much effort does it take to tamper with a meter?

**Experimenting with Incentives**

From this perspective, we discuss how future grid pilots can use incentives. Based on our concerns, we analyze the application of incentives in life-cycle security (to tackle the emerging character of future grids), in governing dependency (to tackle system complexity), and for anti-stakeholders (to understand stakeholders’ involvement). Aligning incentives in a changing environment is hard. However, while a qualitative analysis of incentives can’t predict stakeholder behavior, it does provide opportunities to identify realistic yet undesirable scenarios created by misaligned incentives and thereby provides opportunities to prevent such scenarios.

**Life-Cycle Security**

The existing grid design can’t sufficiently manage cybersecurity, being in a gradual development toward future grids while the lifespan of devices is still 30 years. How can we ensure that devices will meet the security requirements we’ll have at the end of their lifetime? Emerging vulnerabilities reduce effort—for example, the knowledge needed to exploit a legacy system’s vulnerability—even for opportunistic attackers.

The concept of modular designs seems like a viable strategy for future devices. To understand incentives related to this idea, it’s important to analyze how the exchange of components works in practice (for instance, does it provoke users to disassemble the devices, and does it decrease vendor effort for device maintenance?) and affects attackers (for instance, does the design
The impact of specific vulnerabilities). For this, we can set up environments in which one user periodically changes the deployment at home—for instance, using different modularity levels—and observe whether the specific design and its characteristics cause different user behavior. In addition, serious gaming can be used as an environment to explore how potential attackers choose targets in relation to device specification.

Pilots must also consider the tradeoff between standardization and diversity in relation to adversary effort and reward. For example, increasing smart meter diversity will likely decrease the impact of a specific vulnerability or denial-of-service attack. However, this strategy could easily lead to increased technical and organizational complexity, thereby introducing new vulnerabilities. Diversity also shares features with "security by obscurity." Vendors might use diversity as an excuse to neglect security features—a negative incentive—so careful implementation is necessary.

We summarize the suggestions for pilots in two recommendations:

- Use device and system architectures with different modularity levels to investigate the incentives created for different stakeholders in the pilots.
- Consider the tradeoff between standardization and diversity in relation to adversary effort and reward. Make conscious choices about deploying single or multiple versions of, say, a smart meter and about whether a single design should be selected as the best, and thus used in the future.

**Governing Dependency**

We outlined how organizational complexity increases in future grids. The central issue here concerns designers’ assumptions about different stakeholders’ honesty, government stability, and so on. Michael Assante drew a parallel with Roman aqueducts to show how governing dependency can go wrong: the aqueducts gradually introduced a dependency on vulnerable infrastructures, which were an easy target for enemies when the threat context changed (that is, during war). High dependencies create high rewards for enemies when they think they have excuses to attack. For future grids, mutual dependencies of electricity, ICT, and human resources could provoke increased adversary activity while inhibiting opportunities for adequate defense and response.

Investigating increasing dependencies can be part of responsible experimentation. For example, focus groups including both social and technical experts and pilot users can be used to analyze potential needs that arise in various situations—for example, understanding how lack of electricity impacts smart homes, telecommunication, and transportation and the alternative measures users take to bypass the situation, and investigating alternative energy sources.

Two recommendations summarize these points:

- Use threat scenario analysis, with scenarios representing possible future threat contexts, to identify emerging dependencies. What if the country is at war, under cyberterrorist threat, or a target of industrial espionage? What do the pilot results tell us about the implications of dependencies in such contexts?
- Use focus groups to identify the incentives the piloted technology might create in different scenarios. Are there opportunities for local operation? Do stakeholders have incentives to attempt local operation under different threat scenarios?

**Anti-stakeholders**

With the increased dependence on stakeholders, there’s a need for a holistic risk management approach that includes analysis of criminal business cases for different adversary types. How do we prevent stakeholders, both directly involved and external, from having clear incentives for noncooperation (for example, in grid usage), parasitic behavior (for example, electricity theft), or manipulation to advance their own interests (for example, tampering with smart meters)? Pilots should identify criminal business cases in which reward exceeds effort and risk for malicious stakeholders as well as incentives for noncooperation, perhaps related to provocations and excuses. Different campaigns with open and closed device design—for example, campaigns in pilots describing device functionalities and possible communication channels versus black box deployment—can be used to investigate how system presentation influences user interest and active tampering in undesirable situations such as a blackout.

Similarly, serious gaming can provide insights into attacker decision making. Games might have a mixed setting between the real world and a virtual environment. For example, tampering with smart meters might be part of a real-life game, but, for ethical reasons, blackouts must be simulated virtually.

Although these strategies are unlikely to produce quantitative inputs or complete information about uncertain futures, they can be used for qualitative discussions. Again, we have two recommendations:

- Identify attacker profiles for the pilot, in terms of knowledge, resources, and network role (insider or outsider). On the basis of the pilot observations, identify potential criminal business cases for each attacker profile.
- Investigate incentives for both external and internal attackers by letting stakeholders and specialized
Methods of governing emerging technology suffer from limited knowledge about the technology and its changing environment. However, when more knowledge becomes available, the technology has often become so fixed in economic and societal constraints that controlling its development becomes difficult. This is known as a Collingridge dilemma, and it certainly applies to future grids and their security. Thus, the question is how to make knowledge available in early design stages. 

The recommendations we provided can form a basis for distilling security-relevant information from emerging technology pilots to enable continuous security assessment in combination with adaptive and resilient technologies. 

We believe that the Dutch pilots involving smart meters should have included an investigation of the different incentives for both direct and indirect stakeholders—including users, criminals, and market parties—to cooperate, defect, or violate security and privacy in different scenarios. A responsible approach could have resulted in fewer privacy issues in the first generation of smart meters through early identification of consumer requirements as well as more awareness of actual and potential security problems with grid operators.

Our proposed pilot extensions are in-depth, qualitative studies aiming to identify potential issues of problematic incentives. Still, leveraging quantitative experimental social science knowledge—for example, how people respond to opportunity structures and incentives—would be beneficial. Such knowledge could be used to set up the pilots—ensuring that known problematic structures are covered in monitoring the pilots and defining adversarial roles—and to evaluate the results, linking stakeholder comments to known issues. However, the complex interactions among different incentives make it far from trivial to apply data from laboratory experiments to the real world.

Regarding economic aspects, studies of the market’s role in such experiments would be a valuable addition, as the market plays a key role in defining incentives. In addition, experiments might be costly, and such costs need to be compared to the benefits of reduced risk and uncertainty. Although the systems’ complexity makes this a hard task, simply extending already planned pilots with security aspects can be cost-effective.

Whether it should be direct stakeholders or professional penetration testers who perform the pilot experimentation is an open ethical issue. Security professionals’ answer to this question might be biased, as they clearly have their own incentives.

Acknowledgments

This research received funding from the European Union’s Seventh Framework Programme (FP7/2007-2013) under grant agreements SEC-261696 (SESAME) and ICT-318003 (TREPASS). This publication reflects only the authors’ views; the Union is not liable for any use that may be made of the information contained herein. The research also received funding from the Dutch Next Generation Infrastructures Foundation under project 09.08.KID and from the Centre for Safety and Security of the Leiden, Delft, and Erasmus universities.

References


Francien Dechesne was a researcher at Delft University of Technology and Leiden University (at the time this article was written). Her research interests include ethical and societal aspects of information and communications technology as well as the specification and verification of nonfunctional requirements. Dechesne received a PhD in logic from the Universiteit van Tilburg. She recently moved to the Eindhoven University of Technology. Contact her at f.dechesne@tue.nl.

Dina Hadžiosmanović is a researcher at the Delft University of Technology. Her research interests include different aspects of cybersecurity in critical infrastructures, such as smart grids and flood barriers. Hadžiosmanović received a PhD in system security from University of Twente. Contact her at d.hadziosmanovic@tudelft.nl.

Wolter Pieters is the technical leader of the TREPASS project at the University of Twente and an assistant professor of cyberrisk at the Delft University of Technology. His research interests include electronic voting, verification of security properties, and philosophy and ethics of cybersecurity. Pieters received a PhD in information security from Radboud University Nijmegen, The Netherlands. Contact him at w.pieters@tudelft.nl.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.

Expert Online Courses — Just $49.00

Topics: