Practical Risk Assessment Using a Cumulative Smart Grid Model

Markus Kammerstetter[1], Lucie Langer[2], Florian Skopik[2], Friederich Kupzog[3] and Wolfgang Kastner[4]

[1] *Institute of Computer Aided Automation, Automation Systems Group, International Secure Systems Lab, Vienna University of Technology, Vienna, Austria*

[2] *Safety and Security Department, Austrian Institute of Technology, Vienna, Austria*

[3] *Energy Department, Austrian Institute of Technology, Vienna, Austria*

[4] *Institute of Computer Aided Automation, Automation Systems Group, Vienna University of Technology, Vienna, Austria*

mk @ iseclab.org, {lucie.langer, florian.skopik, friederich.kupzog}@ait.ac.at, k @ auto.tuwien.ac.at

Keywords: Smart Grid, Risks, Risk Assessment, Critical Infrastructures

Abstract: Due to the massive increase of green energy, today's power grids are in an ongoing transformation to smart grids. While traditionally ICT technologies were utilized to control and monitor only a limited amount of grid systems down to the station level, they will reach billions of customers in near future. One of the downsides of this development is the exposure of previously locked down communication networks to a wide range of potential attackers. To mitigate the risks involved, proper risk management needs to be in place. Together with leading manufacturers and utilities, we focused on European smart grids and analyzed existing security standards in the Smart Grid Security Guidance $(SG)^2$ project. As our study showed that these standards are of limited practical use to utilities, we developed a cumulative smart grid architecture model in a joint approach with manufacturers and utilities to represent both current and future European smart grids. Based on that model, we developed a practical, light-weight risk assessment methodology covering a wide range of potential threats that have been evaluated and refined in course of expert interviews with utility providers and manufacturers.

1 INTRODUCTION

Over the last years, the electrical power grid has undergone a tremendous change. The traditional power grid could be described as a producer-consumer model. The producers generate electricity and the electricity is transferred by utilities to the consumers. As a result, the amount of employed ICT technologies was limited. Today, there is a strong trend in the direction of sustainable green energy, energy saving and higher efficiency. Energy is no longer only produced at the top and delivered to the bottom; instead, everyone can become an energy producer. Consumers change to "prosumers" by running their own solar or wind power stations. Businesses and communities specializing on independent energy production through wind turbines, heating, or biogas plants emerge and grow. The boundaries in the traditional power grid model start to fade. On the other hand, large-scale energy producers and utilities can save energy and achieve higher energy efficiency by having the ability to influence or control devices in the user domain. To make this possible, energy grids are heavily expanded with ICT technologies – the traditional power grid is being transformed into the *smart grid*. On the downside, these technologies bear unforeseen risks for critical infrastructures. Smart grid ICT technology providers and utilities have limited experience with these new technologies and market pressure may force them to throw new products on the market before they have undergone quality assurance processes suitable for critical infrastructures. While traditionally access to smart grid ICT networks was limited to energy producers and utilities, new smart grid ICT technologies allow the massive amount of consumers to participate in these networks. Communication infrastructures in energy grids and especially in power grids are thus also exposed to a wide range of potential adversaries. To mitigate the security risks involved, there have been significant international efforts in terms of smart grid cyber security standards, risk assessment and security mechanisms (see Section 2).

However, focusing on smart grids in the European Union and especially in Austria, it quickly turned out that many architectural or technological assumptions do not hold for the smart grid systems currently being rolled out in large quantities. For instance, within the European Union, the Smart Metering Protection Profiles (BSI, 2013b; BSI, 2013c) are widely known for their security requirements and definitions. Yet, smart metering is only one of many areas within the smart grid, and today's advanced metering infrastructure (AMI) typically does not correspond to the *gateway* and *security module* design concept suggested in those Protection Profiles.

As a result, in the Smart Grid Security Guidance (SG)^2 joint project (AIT, 2013) with leading smart grid component manufacturers and utilities, we set out to create a cumulative smart grid landscape model representing both current and future European smart grids. Based on established industry security standards and in close cooperation with manufacturers and utilities, we identified a comprehensive set of threats that are applicable within our cumulative smart grid model. To foster practical usability, we clustered both identified threats and smart grid systems to form the two dimensions of a threat matrix. This threat matrix allows practical threat assessment for both current and future European smart grids, and forms the basis for an according risk assessment determined by probability and impact. In summary, the main contributions of our work are:

- A cumulative smart grid model representing both current and near-future European smart grids as a basis for sound risk assessment
- A thoroughly designed threat catalog for modern smart grid architectures
- An accompanying practical risk assessment approach evaluated and refined in course of expert interviews with utility providers and manufacturers

The remainder of this paper is organized as follows. Section 2 provides an overview of related work. In Section 3 we explain how we developed the cumulative smart grid model. In Section 4 we describe our risk assessment approach, while Section 5 covers the evaluation and our results. The conclusions and suggestions on further work can be found in Section 6.

2 RELATED WORK

Mainly focusing on U.S. smart grids and technology, NIST has developed Guidelines for Smart Grid Cybersecurity (NIST, 2013b). In Europe, the German Federal Office for Information Security (BSI) has come up with a Common Criteria Protection Profile for the Gateway of a Smart Metering System and its Security Module (BSI, 2013b; BSI, 2013c). In contrast to our approach, the NIST guidelines do not allow an integrated approach. They are based on technologies employed in U.S. smart grids and give high-level recommendations only. Similarly, the BSI protection profiles do not provide a holistic approach either. Instead, they focus on smart metering only (which is only one building block of a smart grid), and their Target of Evaluation is a very specific smart metering implementation that does not reflect deployed smart metering systems.

Regarding risk assessment, Lu et al. outline security threats in the smart grid (Lu et al., 2010). In comparison, our approach is targeted on the broad range of system components in European smart grids. Ray et al. provide a more formal approach to smart grid risk management (Ray et al., 2010) while one of our goals was to develop a practical risk assessment approach usable for utilities. Varaiya et al. show various ways to manage security critical energy systems (Varaiya et al., 2011). However, they rather focus on formal methods, and their smart grid model does not reflect current European smart grids. Finally, Hou et al. outline the differences in risk modeling between traditional grids and smart grids (Hou et al., 2011), while we focus on the smart grid landscape that is currently deployed or will be deployed in the near future. In addition, existing risk assessment approaches are covered in more detail in Section 4.1.

Regarding smart grid security mechanisms, Yan et al., Mohan et al. and Vigo et al. provide an overview of security mechanisms for smart grids and smart meters (Yan et al., 2012; Mohan and Khurana, 2012; Vigo et al., 2012). While their work provides an overview of how security mechanisms should be realized, in our approach, we focus on the security mechanisms that are either implemented in current implementations or will be part of near-future implementations. Finally, Wang et al. (Yufei et al., 2011) present smart grid standards covering security, but rather target U.S. standards like those published by NIST.

3 CUMULATIVE SMART GRID MODELING USING SGAM

In our joint approach to identify technological risks in current and future European smart grids, it turned out that leading experts, utilities and even manufacturers have a very different view and definition of what *the smart grid* is. Focusing on European smart grids and the Austrian power grid in particular, on a high-level view, the smart grid domains and actors within those domains are comparable to existing standards such as the NIST Smart Grid Framework (NIST, 2013a) or the European Smart Grid Reference Architecture (Smart Grid Coordination Group, CEN-CENELEC-ETSI, 2012b). In a first task, we asked utilities to compare their deployed smart grid systems, model regions, pilot projects and concepts with existing reference models. Since, unlike the NIST framework, the European smart grid reference architecture focuses on European smart grid technologies, it was chosen as a basis for the comparison. Specifically, we used the Smart Grid Architecture Model (SGAM) (Smart Grid Coordination Group, CEN-CENELEC-ETSI, 2012b) to allow for a well-structured comparison. Overall, 45 different projects could be identified and prioritized according to project size, project relevance, and both amount and quality of available information. The study showed that, in general, the SGAM model is usable with some limitations, but the reference model is only applicable on a high level. While it sketches the general structure of European smart grids, it does not contain detailed information on the technologies implementing smart grid components in this structure. For that matter, it is not adequate for qualified risk modeling suitable for utilities. To close this gap, we combined seven national and four international projects within the SGAM model to form a cumulative architecture model allowing us to deduce threats and risks for both current and future smart grid installations in Europe. The following sections describe our approach in more detail.

3.1 The Smart Grid Architecture Model (SGAM) Framework

The SGAM model had its original motivation in identifying gaps in standardization and locating these gaps in the SGAM model space. The model is structured in zones and domains (see Fig. 1). While the *zones* are derived from the typical layers of a hierarchical automation system (from field via process, station towards operation and enterprise level (Sauter et al., 2011)), the *domains* reflect power-system specific fields of different actors such as transmission system operators, distribution system operators, and customers. In contrast to the NIST model, the European approach has a dedicated DER (Distributed Energy Resources) domain, which captures small distributed generators with their special infrastructure. Finally, in the third dimension, SGAM features *interoperability layers*. With these layers, the different aspects of networked smart grid systems are aligned. The base layer is the component layer, where physical and software components are situated. On top of that, communication links and protocols between these components can be placed. The information layer holds the data models of the information exchanged. On top of that, the function layer holds the actual functionalities, and the uppermost layer describes the business goals of the system.

Today, SGAM serves three major purposes: first of all, it is a means to visualize and compare different smart grid automation architectures. This also allows the identification of gaps in all layers. Finally, SGAM can serve as a useful model to support model-driven architecture development. In this work, SGAM was applied for the first two purposes: comparison and identification of gaps.

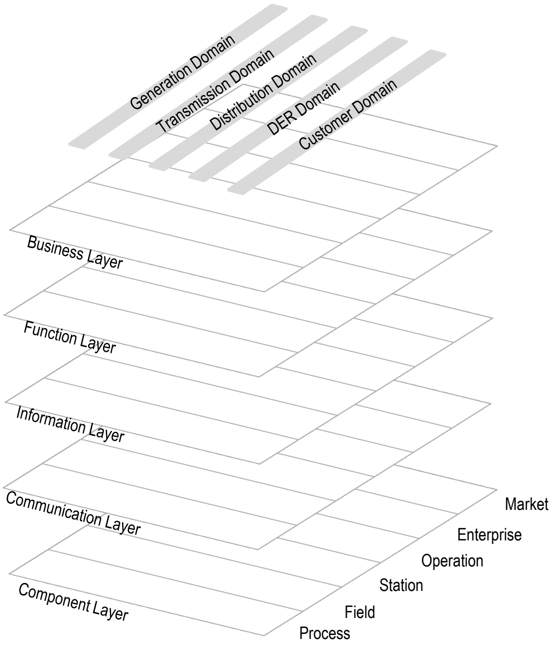

Figure 1: Smart Grid Architecture Model (SGAM) Framework

3.2 Current and Future Smart Grid Technologies within SGAM

Within the project, a holistic architecture was derived, which reflects the short- to mid-term extension of today's power grid IT technology towards future smart grid functionalities. The methodology used to achieve this architecture is based on individual SGAM modeling of national and international smart grid projects that significantly build on the use of ICT systems. From 45 project candidates, seven significant national smart grid research projects were selected for modeling:

- IEM: Intelligent Energy Management

- Smart Web Grids (Smart Grid Modellregion Salzburg, 2011)
- DG DemoNetz Smart LV Grids (Klimafonds, 2012)
- ZUQDE: Zentrale Spannungs- und Blindleistungsregelung mit dezentralen Einspeisungen in der Demoregion Salzburg (Smart Grid Modellregion Salzburg, 2010)
- EMPORA: E-Mobile Power Austria (E-Mobile Power Austria, 2010)
- AMIS Smart Metering Rollout

A similar approach was applied to international projects. The selected significant projects were:

- The European FP7 Project OpenNode (OpenNode, 2012)
- The European FP7 Project EcoGrid EU (EcoGrid, 2012)
- The US Demand Response Automation Server (DRAS) (DRAS, 2008)
- The German ICT Gateway Approach OGEMA (OGEMA, 2012)

For SGAM modeling, detailed information about the technical implementations had to be requested from the projects under analysis. The availability of information (or contacts to the projects) was an additional selection criterion for the international projects.

3.3 European Smart Grid View according to the Cumulative SG Model

The derived architecture (Fig. 2) includes a harmonized cumulative view of the components found in all analyzed projects. The SGAM domains transmission and bulk generation were not covered by the selected projects since in the Austrian or, respectively, European view, the smart grid is primarily related to distribution systems. The architecture shows the component and communication layer of the SGAM model. On the bottom, the field devices can be found (such as smart meters or dedicated sensors and actuators). On the station level, both primary and secondary substation are situated with their current and prospective automation components. On the customer side, mainly residential customers, commercial buildings, and electric mobility can be found. On the top of the architecture, the enterprise level and market components are located.

However, one of the main differences to existing models is the addition of detailed communication technology descriptions allowing a more in-depth risk assessment approach. The communication protocols and technologies underlined are the ones that are predominantly used in the projects we analyzed. For instance, in future smart grids the broad use of Web Services is anticipated for communicating with the energy market. Nevertheless, as depicted in our architecture, the predominant way to achieve this in current smart grids is to use personal communication via email or phone calls. From a risk assessment perspective, this results in a significant difference as Web Services can potentially be more easily compromised than a phone call made between a group of persons who probably know each other well from their daily work routine.

3.4 Evaluation of the Model

After a first draft of the architecture model had been developed, it was subject to a number of feedback rounds with members of the consortium (utilities and manufacturers). Improvements and additional information were integrated into the architecture. The $(SG)^2$ architecture model serves as an anchor point for further analysis and as a common document of energy, IT and security experts. The main benefit of the model is that questions between the different expert domains can clearly be formulated and therefore easily be answered by referring to individual elements of the architecture.

4 SMART GRID RISK ASSESSMENT

4.1 Existing Approaches

Smart grid cyber security and risk assessment in particular has been addressed in several standards, guidelines and recommendations. The U.S. National Institute of Standards and Technology (NIST) has developed a three-volume report on “Guidelines for Smart Grid Cyber Security (NIST-IR 7628)” (NIST, 2013b): Volume two focuses on risks related to customer privacy in the smart grid, and gives high-level recommendations on how to mitigate these risks. However, no general approach for assessing security risks in the smart grid is provided. The European Network and Information Security Agency (ENISA) has issued a report on smart grid security. It builds on existing work like NIST-IR 7628 or ISO 27002 and provides

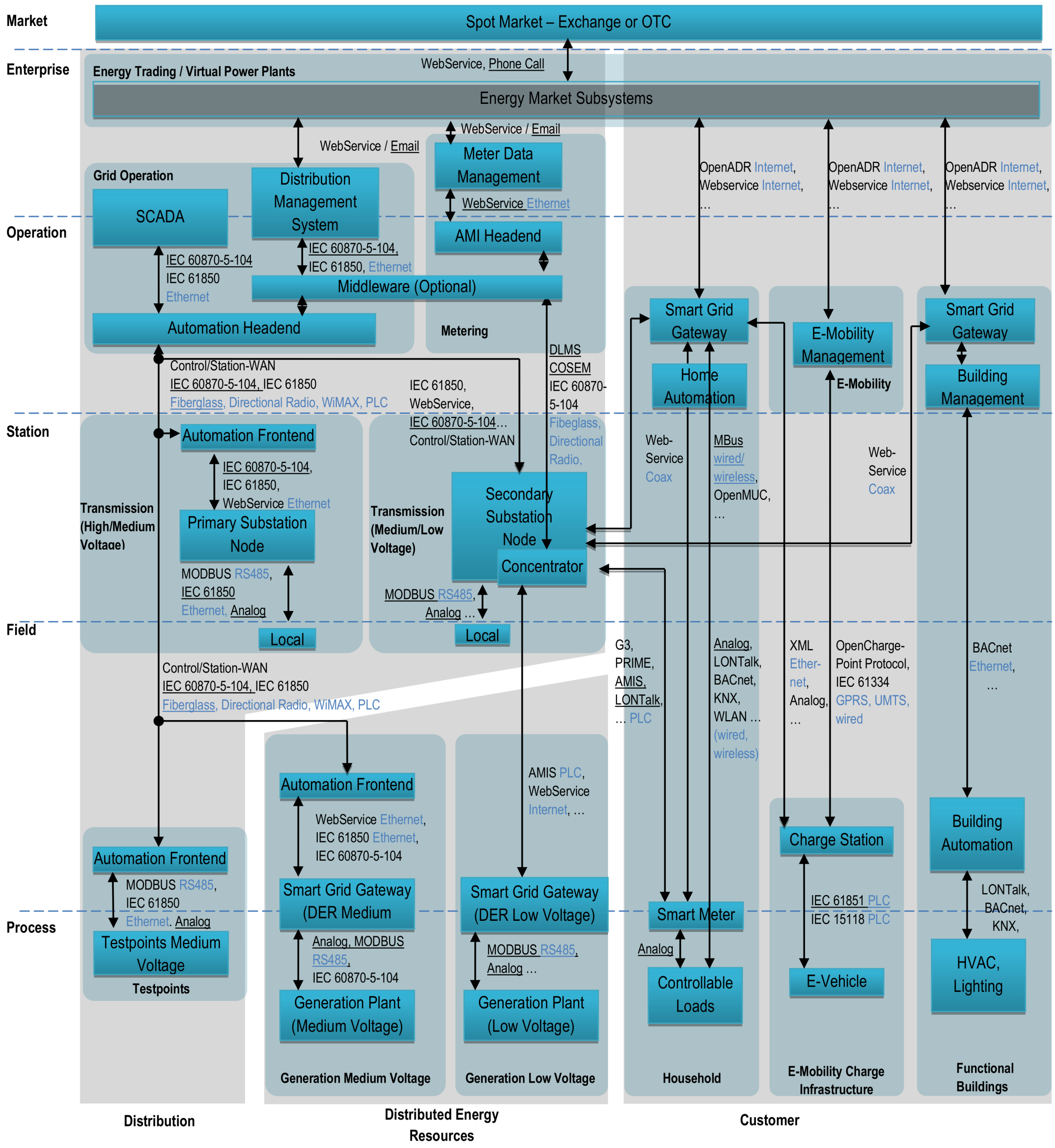

Figure 2: Cumulative Smart Grid Model

a set of specific security measures for smart grid service providers, aimed at establishing a minimum level of cyber security (ENISA, 2012). Each security measure can be implemented at three different “sophistication levels”, ranging from early-stage to advanced. The importance of a risk assessment to be performed before deciding the required sophistication levels is pointed out, but no specific risk assessment methodology is identified within the report.

The German Federal Office for Information Security has come up with a Common Criteria Protection Profile for the Gateway of a Smart Metering System and its Security Module (BSI, 2013b; BSI, 2013c). Both define minimum security requirements for the corresponding smart grid components based on a threat analysis. However, the Common Criteria approach, which focuses on a specific, well-defined Target of Evaluation, cannot provide a holistic view on cyber security threats in future smart grids. Another drawback is that the implementation of many smart metering systems currently being rolled out does not correspond to the defined gateway and security module design concept.

The CEN-CENELEC-ETSI Smart Grid Coordination Group has provided a comprehensive framework on smart grids in response to the EU Smart Grid Mandate M/490 (Smart Grid Coordination Group, CEN-CENELEC-ETSI, 2012a). As part of that framework, the "Smart Grid Information Security (SGIS)" report defines five SGIS Security Levels to assess the criticality of smart grid components by focusing on power loss caused by ICT systems failures. Moreover, five SGIS Risk Impact Levels are defined that can be used to classify inherent risks in order to assess the importance of every asset of the smart grid provider. This means that the assessment is carried out under the assumption that no security controls whatsoever are in place. While this is a valuable approach, it is not suitable for a more practical scenario that focuses on actual, currently deployed or foreseeable implementations.

Risk assessment methodologies have also been addressed by the FP7 project EURACOM, which considered protection and resilience of energy supply in Europe and aimed at identifying a common and holistic approach for risk assessment in the energy sector. As part of a project deliverable[1], existing risk assessment methodologies and good practices have been analyzed in order to identify a generic risk assessment method which could be customized to suit the specific needs of the energy sector.

While most of the existing risk assessment methods are asset-driven, the $(SG)^2$ project required an architecture-driven approach for developing a risk catalog. This approach is described more closely in the following.

4.2 Our Approach: Threat Matrix and Risk Catalog

The risk assessment approach taken in $(SG)^2$ focused on the ICT architecture model initially developed within the project (see Section 3). The goal was to come up with a comprehensive catalog of ICT-related risks for smart grids in Europe from a Distribution System Operator's perspective. The following steps were taken to achieve that goal:

1. Compile a *threat catalog* for smart grids focusing on ICT-related threats and vulnerabilities
2. Develop a *threat matrix* by applying the threat catalog to the ICT architecture model, i.e., identify which threats apply to which components of the model
3. Assess the potential risk for each element within the threat matrix by estimating the probability and the impact of an according attack, thus eventually producing a *risk catalog*

These steps are explained in more detail in the following paragraphs.

4.2.1 Compiling the Threat Catalog

The $(SG)^2$ threat catalog was not to be developed from scratch, but should build upon a well-established source of ICT-related security threats. To that end, the IT Baseline Protection Catalogs developed by the Federal Office for Information Security (BSI, 2013a) were chosen to form the main source of input as they provide a comprehensive list of security threats that could possibly apply to an ICT-supported system. Additionally, the threats specified in the smart-grid-specific Protection Profiles (BSI, 2013b; BSI, 2013c) were taken into account. Non-technical threats, i.e., threats related to organizational issues or force majeure, were not considered due to the scope and focus of the $(SG)^2$ project. Thus, out of a list of initially 500 threats accumulated from the identified sources, the ones without any relevance to smart grids or without any relation to ICT were eliminated at first, yielding roughly half of the initial threats for further consideration. While certain threats listed in the BSI Catalogs are very generic, others apply to very specific settings only; therefore, it was necessary to merge some of the threats that remained in our list after the "weeding" step. This resulted in a list of 31 threats, which were grouped into the following clusters:

- Authentification / Authorization
- Cryptography / Confidentiality
- Integrity / Availability
- Missing / Inadequate Security Controls
- Internal / External Interfaces
- Maintenance / System Status

Since the BSI Baseline Protection Catalogs are not tailored for any specific use case, the relevant threats had to be adapted to the smart grid scenario, i.e., they were interpreted in the smart grid context.

[1] The EURACOM project deliverables can be downloaded at `http://www.eos-eu.com/?Page=euracom`.

4.2.2 Developing the Threat Matrix

The next step on the path to the (SG)^2 risk catalog was to apply the threats identified in the first step to the components of the (SG)^2 architecture model (see Section 3), i.e., to state which threats are relevant for which of the components and why. To answer that question, the functionality and the characteristics of the individual architecture components had to be assessed first. For feasibility reasons, the granularity of the components to be considered was set to the level of the boxes depicted in dark grey in Fig. 2:

- Functional Buildings
- E-Mobility & Charge Infrastructure
- Household
- Generation Low Voltage
- Generation Medium Voltage
- Testpoints
- Transmission (High/Medium Voltage)
- Transmission (Medium/Low Voltage)
- Grid Operation
- Metering

The Energy Markets domain was not considered due to lack of current ICT utilization and lack of information on future functionalities.

For each element of the threat matrix, it was first decided whether the threat could be relevant to that particular component or not. If potential relevance was assessed, the reason for that decision was noted, and possible attack scenarios were developed. Since the architecture model considered also smart grid developments for the near future, reasonable assumptions regarding the implementation had to be made in certain cases. These assumptions were discussed and verified by the involved manufacturers and utilities.

4.2.3 Assessing the Risk Potential

The final step of the (SG)^2 risk assessment involved estimating the risk potential for each element of the threat matrix, thus providing a comprehensive risk catalog. To that end, the probability and the impact of each of the threats occuring was rated for each of the components of the architecture model. A semi-quantitative approach was chosen for the risk assessment, which had previously been applied and practically assessed by one of the member organizations of the project consortium: both probability and impact were measured on a five-level scale ranging from very low (level 1) to very high (level 5). The probability level was determined by the number of successful attacks per year, ranging from less than 0.1 incidents (level 1) to multiple incidents (level 5) per year. The impact of a successful attack was determined by monetary loss, customer impact, and geographic range of the effects (e.g., local, regional, global). The outcome of this step is a comprehensive catalog of cyber security risks on smart grids in Europe. The steps taken to evaluate the catalog as well as the main findings are described in the following section.

5 EVALUATION AND RESULTS

A good threat and risk assessment model delivers useful results, i.e., captures specific threats appropriately, is easy to use, and well applicable in reality. With these targets in mind, we evaluated and revised the model in a series of workshops, where domain experts from both areas of information technology and energy rated the proposed risk assessment approach.

5.1 Evaluation Methodology

The evaluation, partly integrated in the overall creation of our cumulative smart grid model for risk assessment, included in the following three steps:

- *Step 1: Evaluation of Threat Catalog.* In order to evaluate our threat catalog, we set up end user workshops with experts from utility providers, device manufacturers, and academic institutions to evaluate both the relevance and completeness of the identified threats. During that evaluation, additional threats were added that are unique to the smart grid domain.
- *Step 2: Threat Relevance.* Experts surveyed the applicability of identified threats to the various domains in the SGAM model. This step enabled the identification of the most important threats per domain as well as their interdependencies, and further allowed to focus on most relevant threats. The result was again discussed and refined with major utility providers in Austria in end user centric workshops.
- *Step 3: Probability and Impact Assessment.* In a last step, we had experts independently rate the probability of occurrence of identified threats and the impact from their point of view. These experts represent the opinions of different utility providers, ranging from small and locally operating organizations, to larger ones. In a joint workshop, the individual results were again discussed and consolidated to ensure the broad use of the resulting threat and risk catalog.

5.2 Main Findings

Dealing with proper risk assessment in the smart grid domain is indeed challenging, mainly because of the novelty, complexity, and multidisciplinarity of this topic. Here, we present some of the main findings, derived from the application of our approach in a real user context. We foresee these qualitative statements as a major contribution for future improvements of our smart grid risk assessment approach.

5.2.1 Unbalanced Risk Distribution

Essentially, the probability of a security breach is comparatively low on the upper levels of the cumulative smart grid model, because components are small in numbers and easy to protect. An attacker typically has no physical access to components, and well-trained experts acting under rigid policies maintain the grid's backend. Furthermore, protection mechanisms on the upper levels do not suffer from cost pressure on this level; for instance, redundant systems and hot stand-by sites are state-of-the-art here. However, once an attacker manages to get access to critical systems, the negative impact will eventually be high; for instance, shutting down a primary substation node could affect whole city districts. This makes the security of higher level smart grid components a first priority for utility providers. On the other hand, the probability of a security incident on the bottom level of the cumulative smart grid model is much higher. The reason is that attackers can easily get hold of components (e.g., a concentrator or a secondary substation node) or have them installed on their own premises (e.g., a smart meter). The impact of an attack towards these components is expected to be (geographically) limited at a first glance. The situation may however change tremendously if someone publishes a successful smart meter mass attack on the Internet. This could lead to unanticipated cascading effects in the power grid. Hence, smart grid security on the lower levels of the smart grid is of major importance for utility providers as well.

5.2.2 Evolution of the Grid

Security challenges arise from the fact that the current power grid architecture is just step-wise transformed to a smart grid. While neither a pure legacy system nor a completely new system designed from scratch is too hard to be properly secured, while a mixture of both *is*. We identified that during the transmission of the current power grid into a smart grid, we are facing many security challenges: (i) the mix of legacy protocols and new protocols; (ii) the usage of wrappers, data converters, and gateways to make devices interoperable; (iii) short innovation cycles and rapid pace with which technologies advance clash with the traditional views of grid investments, where components have been designed to last for decades.

5.2.3 Technological Diversity

Not only the transformation phase, but also the final smart grid architecture foresees the application of a wide variety of different technologies (Skopik and Langer, 2013). Many security specialists argue that this diversity leads to a large attack surface, meaning that in hundreds of different protocols and implementations, a security relevant flaw is much more likely compared to only a small set of well-tested standardized technologies. This technological diversity and the need for seamless interoperability mostly avoids rigid designs and the setup of a uniform and secure architecture. On the other side, systems may be designed with different goals in mind so that the intermediary interfaces between them may lead to security vulnerabilities. Although standardization bodies, such as the NIST and BSI, have published (vendor-independent) viable technology recommendations and guidelines, there are no obligations for device vendors and utility providers to stick to them. However, we must not negate the positive aspects of technological diversity. Combining different technologies and products can help to prevent cascading effects caused by a specific vulnerability prevalent in a single technology or series of devices. As a consequence, an attack that has been successful at one utility provider is not necessarily successful at another one, if different technologies are deployed.

5.2.4 Risk Assessment Complexity

The complexity of risk assessment in the energy domain increases rapidly with the introduction of ICT components. This situation will become even worse, once smart grid technology is rolled out on a large scale, because systems become more and more coupled, even across geographical borders, resulting in strong interdependencies among components. The utility providers' concerns are therefore mainly centered around the understanding, detection, and mitigation of complex attack scenarios, where similarly to highly distributed computer systems, a multitude of vulnerabilities may be exploited in course of a complex attack. Estimating risks for such cases is extremely difficult, since numerous mostly unknown variables need to be considered. An example for such a complex attack case is the potential intrusion of malicious users into the metering backend through an exploitation of the smart meter communication network. Here, we argue that our architecture model, which clearly documents existing communication links as well as utilized protocols, is of significant help.

6 CONCLUSION AND FUTURE WORK

In this work we analyzed existing smart grid standards with respect to smart grid security and risk assessment together with leading manufacturers and utilities. Our study indicated that standards like NISTIR 7628 (NIST, 2013b) or the Protection Profiles published by the The German Federal Office for Information Security (BSI, 2013b; BSI, 2013c) are only of limited practical use to utilities. As a consequence, in a joint approach with leading manufacturers and utilities, we analyzed seven national and four international smart grid projects to form a cumulative smart grid model representing both current and future European smart grids. In comparison to existing models like the U.S. NIST Smart Grid Framework (NIST, 2013a) or the European Smart Grid Reference Architecture (Smart Grid Coordination Group, CEN-CENELEC-ETSI, 2012b), our model is technically more detailed and includes a description of predominant communication technologies. In the second part of our work, we developed an extensive methodology to assess the risks involved within our cumulative smart grid model. While our threat catalog initially comprised a list of more than 500 threats, we were able to create a clustered catalog of no more than 31 threats that can be practically handled on top of the smart grid areas in our model. Due to the close cooperation with leading manufacturers and utilities, we believe that our work has a high practical impact on European utilities, as it can support them to conduct a risk analysis of their specific infrastructure.

In near future, we also plan to extend our risk catalog with respect to risk mitigation approaches and security controls, so that utilities can effectively mitigate identified risks with the help of our framework.

ACKNOWLEDGEMENTS

This work has been made possible through the joint SG^2 KIRAS project under national FFG grant number 836276.

REFERENCES

AIT (2013). SmartGrid Security Guidance. http://www.ait.ac.at/research-services/research-services-safety-security/ict-security/reference-projects/sg2-smart-grid-security-guidance/. [Online; accessed 14-October-2013].

BSI (2013a). IT Baseline Protection Catalogs. http://www.bsi.bund.de/gshb.

BSI (2013b). Protection Profile for the Gateway of a Smart Metering System. BSI-CC-PP-0073.

BSI (2013c). Protection Profile for the Security Module of a Smart Metering System (Security Module PP). BSI-CC-PP-0077.

DRAS (2008). The US Demand Response Automation Server. http://drrc.lbl.gov/projects/draserver. [Online; accessed 16-October-2013].

E-Mobile Power Austria (2010). Empora. http://www.empora.eu/. [Online; accessed 16-October-2013].

EcoGrid (2012). European FP7 Project. http://www.opennode.eu. [Online; accessed 16-October-2013].

ENISA (2012). Appropriate security measures for smart grids. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/appropriate-security-measures-for-smart-grids.

Hou, H., Zhou, J., Zhang, Y., and He, X. (2011). A brief analysis on differences of risk assessment between smart grid and traditional power grid. In *Knowledge Acquisition and Modeling (KAM), 2011 Fourth International Symposium on*, pages 188–191.

Klimafonds (2012). DG DemoNet - Smart LV Grid. http://www.ait.ac.at/departments/energy/research-areas/electric-energy-infrastructure/smart-grids/dg-demonet-smart-lv-grid/. [Online; accessed 16-October-2013].

Lu, Z., Lu, X., Wang, W., and Wang, C. (2010). Review and evaluation of security threats on the communication networks in the smart grid. In *MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010*, pages 1830–1835.

Mohan, A. and Khurana, H. (2012). Towards addressing common security issues in smart grid specifications. In *Resilient Control Systems (ISRCS), 2012 5th International Symposium on*, pages 174–180.

NIST (2013a). NIST Special Publication 1108R2 - NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0.

NIST (2013b). NISTIR 7628 - Guidelines for Smart Grid Cybersecurity.

OGEMA (2012). The German ICT Gateway Approach. http://www.ogema.org. [Online; accessed 16-October-2013].

OpenNode (2012). European FP7 Project. http://www.opennode.eu. [Online; accessed 16-October-2013].

Ray, P., Harnoor, R., and Hentea, M. (2010). Smart power grid security: A unified risk management approach.

In *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on*, pages 276–285.

Sauter, T., Soucek, S., Kastner, W., and Dietrich, D. (2011). The evolution of factory and building automation. In *IEEE Magazine on Industrial Electronics*, pages 35–48.

Skopik, F. and Langer, L. (2013). Cyber security challenges in heterogeneous ict infrastructures of smart grids. *Journal of Communications*, 8(8):463–472.

Smart Grid Coordination Group, CEN-CENELEC-ETSI (2012a). Reports in response to smart grid mandate m/490. `http://www.cencenelec.eu/standards/sectors/SmartGrids/Pages/default.aspx`. [Online; accessed 16-October-2013].

Smart Grid Coordination Group, CEN-CENELEC-ETSI (2012b). Smart grid reference architecture. `http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_reference_architecture.pdf`. [Online; accessed 15-October-2013].

Smart Grid Modellregion Salzburg (2010). ZUQDE. `http://www.smartgridssalzburg.at/forschungsfelder/stromnetze/zuqde/`. [Online; accessed 16-October-2013].

Smart Grid Modellregion Salzburg (2011). Smart Web Grid. `http://www.smartgridssalzburg.at/forschungsfelder/ikt/smart-web-grid/`. [Online; accessed 16-October-2013].

Varaiya, P., Wu, F., and Bialek, J. (2011). Smart operation of smart grid: Risk-limiting dispatch. *Proceedings of the IEEE*, 99(1):40–57.

Vigo, R., Yuksel, E., and Ramli, C. (2012). Smart grid security a smart meter-centric perspective. In *Telecommunications Forum (TELFOR), 2012 20th*, pages 127–130.

Yan, Y., Qian, Y., Sharif, H., and Tipper, D. (2012). A survey on cyber security for smart grid communications. *Communications Surveys Tutorials, IEEE*, 14(4):998–1010.

Yufei, W., Bo, Z., WeiMin, L., and Tao, Z. (2011). Smart grid information security - a research on standards. In *Advanced Power System Automation and Protection (APAP), 2011 International Conference on*, volume 2, pages 1188–1194.

APPENDIX

Threat Category	**Threat**	**Functional Buildings**	**E-Mobility incl. Infrastruct.**	**Household**	**Generation (Low Volt.)**	**Generation (High Volt.)**
Authentication / Authorisation	*Defective or missing authentication or inappropriate handling of authentication data*	Relevant for all interfaces to the Smart Grid Gateway (Building Automation, Market/Internet und Secondary Substation) (P: 2; I: 2)	An attacker could impersonate the EMS and take control over all charge stations in an affected area (e.g., a street), which could lead to instabilities in the grid (P: 2; I: 3)	Relevant for Smart Grid Gateway and Smart Meter and all interfaces (configuration interface, Market, PLC to data concentrator and Secondary Substation) (P: 2; I: 2)	Exact scope and functionality of Smart Grid Gateway is not clear to date - how will the authentication towards the Automation Front-end and the Smart Grid Gateway be handled? (P: 1-3; I: 2-3)	Exact scope and functionality of Smart Grid Gateway is not clear to date - how will the authentication towards the Automation Front-end and the Smart Grid Gateway be handled? (P: 1-3; I: 3-4)
Cryptography / Confidentiality	*Disclosure of sensitive data*	Building automation data are sensitive since they may give away information about productivity or working hours (P: 2; I: 2)	Confidential load data could be eavesdropped on through the connection to the E-Mobility Management System or Smart Grid Gateway (P: 2-3; I: 2)	Metering data is confidential since it affects privacy and habits of the customers; impact of accidental disclosure depends on the scope of data and the number of households affected (P: 2; I: 3)	Output data of small producers is confidential since they may allow conclusions to be drawn on consumer behavior; high probability since no protection measures currently in place (P: 4; I: 3)	Hardly relevant since outout data are not confidential; low motivation (P: 1; I: 1)
Integrity / Availability	*Tampering with devices*	Hardly relevant due to physical access control; Smart Grid Gateway could be physically part of the Building Automation system; building operator has no motivation to compromise his own load management (P: 1; I: 1)	Tampering with EV, charge station or E-Mobility Management System; a malicious user can easily access relevant components; impact depends on whether private or public charge station is targeted (P: 3; I: 2-3)	Customers have direct access to the components; main motivation is fraud, but more severe attacks might as well be possible (e.g. issuing control commands) (P: 4; I: 3)	Relatively exposed (in a household); the amount of energy supplied may be a subject to fraud; depends on the use of anomaly detection techniques and plausibility checks (P: 4; I: 2)	Basic level of physical protection; low probability due to professional operator (P: 1; I: 4)
Missing / Inadequate Security Controls	*Defective or missing security controls in networks*	Communication via the network in the building; Smart Grid Gateway communicates via insecure networks (Internet), which opens up the possibility of distributed attacks on the Smart Grid Gateway (P: 1; I: 4)	Use of protocols that lack security features (e.g. IEC 61334 via PLC)could lead to eavesdropping on confidential load data; negative consequences for manufacturer / operator of the charge station, although the utility may also be affected (P: 2; I: 2)	Communication over insecure networks (Internet, PLC) (P: 3; I: 3)	Especially relevant for Internet connection to Secondary Substation Node (P: 2; I: 2)	Especially relevant for communication over the telecontrol WAN, currently IEC 60870-5-104 without encryption (P: 2; I: 3)
Internal / External Interfaces	*Illegal logical interfaces*	Illegal communication channels between the Gateway and interfaces (Market/Internet, Secondary Substation, Building Automation) could be established and exploited in an attack (P: 2; I: 3)	Illegal communicating with EV, charge station or E-Mobility Management System could lead to disclosure of confidential load data (P: 2; I: 3)	Illegal communication channels between the Smart Grid Gateway and ist interfaces (Market/Internet, Secondary Substation, Smart Meter) could be establish and exploited in an attack (P: 2; I: 3)	Due to physical exponation an attacker could interact with the system directly, thus revealing new interfaces that could be exploited (P: 3; I: 2)	Basic level of physical protection; access to telecontrol WAN may be feasible through faulty operation or targeted attacks (P: 2; I: 3)
Maintenance / System Status	*Operation of unregistered or insecure components or components with overly broad range of functions*	The Gateway could have a wide range of capabilities and functions, thus increasing the attack surface via the interfaces (Building Automation, Market/Internet, Secondary Substation) (P: 2; I: 2)	Possible disruption of the E-Mobility Management System or Smart Grid Gateway if connected to a non-standard or manipulated charge station ; local impact only (P: 1; I: 1)	Smart Grid Gateway or Smart Meter could have a too wide range of capabilities and functions, thus increasing the attack surface via the interfaces (Smart Metering, Market, Secondary Substation) (P: 2; I: 2)	Rather low probability since the components are dedicated to a very specific use; however, backdoors constitute a realistic threat scenario especially in replicated devices (P: 3; I: 2)	Rather low probability since the components are dedicated to a very specific use; however, backdoors constitute a realistic threat scenario (P: 2; I: 3)

Table 1: Threat Assessment (Part 1). Notice, the threat category and an exemplary threat are given in the first two columns. Subsequent columns contain the quantitative and qualitative assessments results for (P)robability and (I)mpact on a scale from 1 to 5 for each threat and per domain.

Threat Category	**Threat**	**Testpoints**	**Transmission (High/Med. Voltage)**	**Transmission (Med./Low Voltage)**	**Grid Operation**	**Metering**
Authentication / authorisation	*Defective or missing authentication or inappropriate handling of authentication data*	No authentication between Automation Front-end and Testpoint, although the Front-end authenticates towards the Primary Subst. Node (PSN); a spoofing attack could lead to false data being sent to the PSN; low impact (suboptimal supply) (P: 2-3, I: 1)	Due to the relatively low number of Primary Substation Nodes accounts or parameters can be configured and tested manually, therefore the probability is lower than in lower parts of the architecture model (P: 1-2, I: 4)	Especially relevant for remote maintenance access points; Secondary Substation Node and Concentrator can be easily accessed mostly, which gives a high probability; possibly regional impacts in case of unauthorized access (P: 4; I: 3)	Access rights management on SCADA systems implemented on an individual basis at utilities, standard IT technologies are employed; ”identity spoofing” of calls to EMS; main threat is exploitation of insecure remote access solutions (P: 2, I: 4)	The connection between AMI headend and Smart Meters is encrypted by utilizing strong cryptographic primitives (ECDSA, AES); authentication and authorization is realized through certificates; thus, a high security standard is expected (P: 1, I: 2)
Cryptography / Confidentiality	*Disclosure of sensitive data*	Does not apply since test data (voltage, frequency) is not confidential	Current supply data and control commands are probably not confidential; consumption data are aggregated, therefore low impact (P: 2, I: 1)	Processing of confidential supply/consumpt. data in Concentrator and Secondary Substation Node; medium probability due to little (physical) protection (P: 3, I: 3)	For load estimation, consumption and energy production data is anonymized; power grid plans and control data is required to be protected accordingly (P: 1-2, I: 4)	Relevant since confidential power consumption data is processed and stored (P: 1, I: 3)
Integrity / Availability	*Tampering with devices*	Hardly relevant due to physical access control mechanisms in place; manipulation via the communication interface could be feasible (e.g. changing the configuration on SD card); low impact (P: 2, I: 1)	Tampering hardly relevant due to high voltage, but this may not hold for malicious insiders; currently strong impact (outage), but timely mitigation can be expected (P: 2, I:3)	Tampering possible especially with Concentrator; rather high probability due to little (physical) protection measures; regional impact (P: 3-4, I: 3)	Relevant if direct manipulation by insiders; remote manipulation over telecontrol WAN possible; forged process data may cause malfunction of DMS and subsequently lead to grid instability (P: 2, I: 4)	Low relevance due to physical protection measures (P: 1, I: 3)
Missing / Inadequate Security Controls	*Defective or missing security controls in networks*	Connected to Primary Substation Node via telecontrol WAN with IEC 60870-5-104 (unencrypted); low impact (suboptimal supply) (P: 2-3, I: 1)	Especially relevant for the communication via the telecontrol WAN; probability is low since security controls in place are more efficient than for the components in the lower parts of the architecture model (P: 1, I: 1-2)	Especially relevant for Internet/PLC connection to Middleware and Smart Grid Gateway (P: 2-3, I: 3)	Relevant for some interfaces (telecontrol WAN, EMS link); link to PSN secured with IPSec; telecontrol WAN link to Secondary Subst. Node could include forged data causing grid instability; (P: 2, I: 4)	Especially relevant for the interfaces to the outside world (i.e. connection to concentrators) (P: 1, I: 2)
Internal / External Interfaces	*Illegal logical interfaces*	Relevant for unauthorized access via telecontrol WAN; a DoS-attack on the Primary Substation Node could lead to generation plants going offline, resulting in voltage drops (P: 2, I: 2-3)	Relevant for access via telecontrol WAN (P: 2, I: 4)	Relevant for access via telecontrol WAN (P: 2, I: 4)	Relevant due to unauthorized access over external interfaces: telecontrol-WAN (Automation Headend), Webservice (EMS), Remote Access (SCADA) depending on deployed technologies (P: 2, I: 4)	Due to illicit logical interface (e.g. due to a successful attack) a connection from the metering system over the middleware to the grid operation system is feasible (P: 1, I: 3)
Maintenance / System Status	*Operation of unregistered or insecure components or components with overly broad range of functions*	Unregistered components hardly relevant (physical access control); an overly broad range of functions possible despite on-site maintenance (mostly no remote maintenance); low impact (P: 1-2, I: 1)	Unregistered components hardly relevant due to physical access control; an overly broad range of functions possible; low probability due to highly specialized components (compared to home area) (P: 1, I: 2-3)	Due to easy accessibility of the substations unregistered components could be installed; regional impacts (P: 3-4, I: 3-4)	Unregistered components are of low relevance due to physical access protection; unused but active system functionalities are relevant, especially considering remote access or support interfaces for manufacturers (P: 2-3, I: 4)	Unused but active system functionalities in the AMI headend lead to an increased attack surface (P: 2, I: 2)

Table 2: Threat Assessment (Part 2). Notice, the threat category and an exemplary threat are given in the first two columns. Subsequent columns contain the quantitative and qualitative assessments results for (P)robability and (I)mpact on a scale from 1 to 5 for each threat and per domain.