COMPUTERS & SECURITY 62 (2016) 165–176

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

From old to new: Assessing cybersecurity risks for an evolving smart grid

Lucie Langer [a], *Florian Skopik* [a,*], *Paul Smith* [a], *Markus Kammerstetter* [b]

[a] *Digital Safety and Security Department, Austrian Institute of Technology, Donau-City-Str. 1, 1220 Vienna, Austria*

[b] *Automated Systems Group, International Secure Systems Lab, Vienna University of Technology, Treitlstr. 1-3/4, 1040 Vienna, Austria*

ARTICLE INFO

Article history:
Received 11 January 2016
Received in revised form 9 June 2016
Accepted 26 July 2016
Available online 1 August 2016

Keywords:
Smart grid
Reference architecture
Risk assessment
Cybersecurity
Security testing

ABSTRACT

Future smart grids will consist of legacy systems and new ICT components, which are used to support increased monitoring and control capabilities in the low- and medium-voltage grids. In this article, we present a cybersecurity risk assessment method, which involves two interrelated streams of analyses that can be used to determine the risks associated with an architectural concept of a smart grid that includes both legacy systems and novel ICT concepts. To ensure the validity of the recommendations that stem from the risk assessment with respect to national regulatory and deployment norms, the analysis is based on a consolidated national smart grid reference architecture. We have applied the method in a national smart grid security project that includes a number of key smart grid stakeholders, resulting in security recommendations that are based on a sound understanding of cybersecurity risks.

1. Introduction

The number of businesses and communities that specialise in independent energy production is growing. Electricity consumers are evolving into *prosumers*, by operating their own solar- or wind-power stations. These trends change the traditional energy generation paradigm of one-way energy flow from producer to consumer, to one that incorporates bi-directional energy production. To enable these changes, power grids are being extended with new information and communications technology (ICT) – the power grid is being transformed into the *smart grid*.

The major drawback of a greater use of ICT power grids is new cybersecurity risks. Previously, access to the ICT components of the power grid was limited to energy producers and utilities. However, with the smart grid, ICT introduces a much larger attack surface, e.g., in the end-user domain, which brings with it an increased risk from cyber-attacks. Therefore, conducting a cybersecurity risk assessment for smart grids is important. However, this is a challenging task, because of the novelty and complexity of the smart grid, and the multi-disciplinary knowledge that is required, for example, in terms of ICT security and electrical engineering expertise. Moreover, as the evolution from the current power grid to a smart grid occurs, a risk assessment process needs to consider both legacy systems and near-term future deployment concepts.

To conduct a cybersecurity risk assessment, a clear picture of a smart grid's underlying ICT architecture must be established, and the system bounds determining the scope of the assessment have to be defined. To support the specification of such a smart grid architecture, several reference

* *Corresponding author.*
E-mail address: florian.skopik@ait.ac.at, florian.skopik@gmx.at (F. Skopik).
http://dx.doi.org/10.1016/j.cose.2016.07.008
0167-4048/

architectures and models have been proposed, such as NISTIR 7628 (National Institute of Standards and Technology (NIST), 2013) for the U.S. and the *Smart Grid Architecture Model (SGAM)* (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2012) as part of the European M/490 framework (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2014a). SGAM has proven useful for describing use cases within a given European smart grid, establishing a common view between different smart grid stakeholders. To provide the starting point for a smart grid risk assessment, the system under evaluation needs to be mapped to SGAM, including a specification of the smart grid components and technologies used. Whilst an approach to assess inherent risk of smart grid information assets is also proposed in the M/490 framework (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2014b), it does not consider deployed systems with certain security measures in place. Therefore, this approach is not sufficient to perform a comprehensive risk assessment, which requires evaluating the effect of existing controls.

We have developed a cybersecurity risk assessment method which considers the evolving nature of the smart grid. The starting point for our risk assessment is the definition of a *national reference architecture* based on SGAM. Building on this reference architecture, our risk assessment approach can be applied to both deployed systems and near-term future developments. This is accomplished by taking a twofold approach: the risks to existing systems are evaluated in an *implementation-based* stream of activity, which is complemented with a *conceptual* analysis that considers foreseeable developments and technologies that cannot be subject to implementation-based analysis, e.g., penetration testing. As a consequence, cybersecurity risks can be assessed and mitigated for the evolving power grid. Our method can support Distribution System Operators (DSOs) in conducting a risk assessment for their specific system implementation, and understanding the risks associated with different architectural choices.

In Section 2 we summarise related work on smart grid architectures and risk assessment, and embedded system security analysis. Our risk assessment method is presented in Section 3, showing the two streams of activity. In Section 4, we describe how the method was applied in a nationally-funded smart grid security project, in order to develop a technical reference architecture and risk catalogue for smart grids in Austria, and we highlight our key findings. The article concludes with a summary and an outlook on future work in Section 5.

2. Related work

Based on the three main pillars of our risk assessment method, we outline important related work in terms of *(i)* smart grid reference architectures, *(ii)* cybersecurity and risk management concepts, and *(iii)* security analysis of embedded systems.

2.1. Smart grid reference architectures

Based on an adaptation of the U.S. National Institute of Standards and Technology (NIST) Conceptual Model (National Institute of Standards and Technology (NIST), 2010) and the GridWise guidelines for smart grid interoperability (GridWise Architecture Council Interoperability Framework Team, 2007), CEN, CENELEC and ETSI have developed a reference model for smart grids in Europe, as part of their response to the EU Smart Grid Mandate M/490 (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2014a). The motivation for the *Smart Grid Architecture Model (SGAM)* (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2012) originates from a need to identify gaps in standardisation. The SGAM reference model, or simply SGAM, is defined by three dimensions: *zones*, *domains*, and *interoperability layers*. While the *zones* are derived from the typical layers of a hierarchical automation system, the *domains* reflect the different stages of power generation, transmission, distribution, and consumption. In the third dimension, SGAM features *interoperability layers*, to which the different aspects of networked smart grid systems are aligned. Today, SGAM has three main uses: *(i)* it is a means to visualise and compare different smart grid architectures; *(ii)* it allows the identification of standardisation gaps in all layers; and *(iii)* it can support model-driven architecture development. Here, SGAM is applied to establishing a national smart grid ICT reference model that provides the starting point for a smart grid cybersecurity risk assessment. By using a framework like SGAM for this task, the system bounds for the assessment can be clearly defined, and an increased confidence in the completeness of the resulting architecture can be gained.

2.2. Smart grid security and risk management

Smart grid cybersecurity and risk management have been addressed in several standards, guidelines, and recommendations. A general survey on cybersecurity for smart grids can be found in Yan et al. (2012). The Smart Grid Interoperability Panel Cyber Security Working Group (SGIP-CSWG) launched by the U.S. National Institute of Standards and Technology (NIST) has developed the *Guidelines for Smart Grid Cyber Security (NIST-IR 7628)* (National Institute of Standards and Technology (NIST), 2013), a set of high-level recommendations which can be applied to the proposed smart grid architecture for the U.S. The report identifies seven smart grid domains and a logical interface architecture used to identify and define categories of interfaces within and across those seven domains. The security requirements for these interface categories are identified through a risk assessment process, which relies on a top-down and a bottom-up approach. Whilst the top-down approach defines smart grid components and interfaces, the bottom-up approach focuses on cybersecurity issues in power grids, such as user authentication, key management for meters, and intrusion detection for power equipment.

The European Network and Information Security Agency (ENISA) has issued a report on smart grid security, which builds on existing work like NIST-IR 7628 and ISO 27002 (International Organization for Standards, 2013), and provides a set of specific security measures for smart grid service providers, aimed at establishing a minimum level of cybersecurity (European Union Agency for Network and Information Security (ENISA), 2012). In this report, it is pointed out that it is important to perform a risk assessment before selecting appropriate measures, but no specific method is identified.

The German BSI has developed a *Common Criteria Protection Profile for the Gateway of a Smart Metering System and its Security Module* (German Federal Office for Information Security (BSI), 2013a, 2013c). Based on a threat analysis, both profiles define a set of minimum security requirements. However, the Common Criteria approach cannot provide a holistic view of cybersecurity threats in smart grids. This is because Protection Profiles focus on a specific Target of Evaluation, such as a smart metering gateway, which is only one of the many components of a smart grid.

As part of the M/490 framework (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2014a), the *Smart Grid Information Security (SGIS)* report provides a framework for assessing the criticality of smart grid components by estimating the power loss caused by potential ICT systems failures. It defines five *SGIS Security Levels* to categorise the inherent risks associated with smart grid information assets, which need to be identified through a use case analysis. The Security Level depends on impact and likelihood, where the impact is expressed in five Risk Impact Levels considering different categories (operational risks relating to availability; legal, human, reputational, and financial risk), and the likelihood is determined by considering the potential resources and intentions of different threat agents. SGIS also provides high-level guidance on appropriate Security Levels for the cells of the smart grid plane, spanned by SGAM domains and zones. As the SGIS risk assessment methodology aims at assessing the organisational value of each smart grid information asset, it considers the *inherent* risk posed to an asset with no security controls in place. Consequently, this clean-slate approach is not readily suitable for assessing cybersecurity risks to an existing infrastructure. As smart grids are being deployed in a step-by-step fashion, in which the present power grid undergoes an incremental transformation into an intelligent grid, a practical cybersecurity risk management approach must be able to deal with a complex combination of legacy systems and new technologies.

2.3. *Security analysis of embedded systems*

Fundamental to the operation of the future smart grid is a wide range of Supervisory Control and Data Acquisition (SCADA) and embedded systems. Recent studies have shown that the level of security provided by these systems is rather low (Kermani et al., 2013; Viega and Thompson, 2012). This is mainly due to the fact that the security analysis of embedded systems is very challenging. Moreover, there is a significant gap between the state-of-the-art security analysis techniques available for off-the-shelf PC systems and those applicable to embedded systems. For instance Liu et al. (2012) and Austin and Williams (2011) provide a generic overview of how software implementation security vulnerabilities can be discovered in PC systems. The available techniques range from generic dynamic analysis approaches to sophisticated tainting, and symbolic or concolic execution techniques (Cha et al., 2012; Schwartz et al., 2010). However, for embedded systems, the prevalent vulnerability discovery techniques are still based on static analysis (Brylow et al., 2001; Khare et al., 2011; Venkitaraman and Gupta, 2004). This can be due to custom proprietary hardware, undocumented peripherals, strict system limitations, or the supporting environment necessary for the embedded devices to run. These properties especially hold for today's smart grid devices.

3. A two-stream risk assessment method

Our risk assessment method provides a unified approach that covers both existing system components and near-future developments. It does so by employing two interrelated processes: a *conceptual* and an *implementation-based assessment*, which both use SGAM (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2014a) as a starting point (see Fig. 1). The focus of our conceptual approach is on near-to-mid-term developments of the smart grid; these systems typically have not been implemented yet. Therefore, an assessment that takes into consideration implementation details of systems, such as poor configurations and software implementation vulnerabilities, cannot be undertaken. On the other hand, the implementation-based approach deals with existing systems that allow for a security audit. We give an overview of both approaches in the following, and explain how they relate to each other in Sections 3.1 and 3.2.

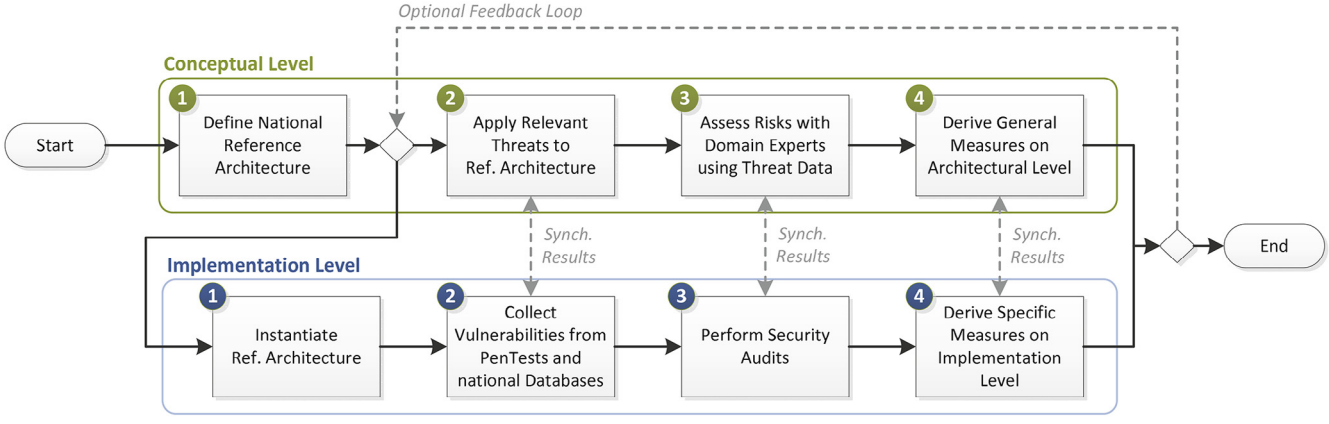

Fig. 1 – Process model: two-tier approach covering both conceptual and implementation-based risk assessment in several interrelated steps.

Outline of the Conceptual-Level Assessment:

1. Based on SGAM, a *national reference architecture* is defined that respects country-specific circumstances, such as regulatory constraints, market-specific conditions and technologies.
2. Next, relevant cybersecurity threats are identified and mapped to the reference architecture. This results in a *threat matrix*, showing threats against architecture components.
3. In a third step, the risk assessment is performed by rating probability and impact of a successful manifestation of the respective threat within the reference architecture. The outcome is a *risk matrix*, showing conceptual risks against different areas of the reference architecture.
4. The last step of the conceptual approach is to develop *mitigation strategies* that address the identified risks.

Outline of the Implementation-Level Assessment:

1. First, the national reference architecture from the conceptual approach is instantiated by determining a real-world implementation of the individual architecture components and communication protocols. The scope of a security audit is set by determining the *System Under Test (SUT)*.
2. Second, potential *vulnerabilities and attack vectors* for the SUT are identified by applying the conceptual threat matrix and known vulnerabilities of the specific SUT parts.
3. Next, *security audits* are performed to assess the security of the SUT with respect to the potential attack vectors and vulnerabilities, resulting in a set of possible exploits.
4. Finally, specific *security measures* are developed to address the implementation-based risks. These may be a specific instantiation of the generic measures developed in the conceptual approach.

3.1. Conceptual-level assessment

3.1.1. Step 1: Define a national smart grid reference architecture

As a first step, a national reference architecture is developed, based on SGAM (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2014a). This is done by analysing the architectures of smart grid systems that are currently deployed by major utilities, or that will be deployed in the near future, and mapping them to SGAM. By considering the different SGAM dimensions for the smart grid systems under analysis, the bounds for that system are determined, and the completeness of the resulting national reference architecture can be ensured. The resulting architecture reflects the specific technology and market situation within the country under consideration, including the regulatory constraints that apply.

The architecture modelling in this step focuses on the lower SGAM interoperability layers; more specifically on the component and communication layers. The upper SGAM layers deal with information structures, message formats and business functions. Considering these higher layers is useful when developing new systems from scratch. However, in our approach, SGAM is used to depict the architecture of near-term smart grid scenarios, which are given by a specific set of devices and protocols. Therefore, the cybersecurity risk assessment must also focus on the lower SGAM layers. To realise this step, we recommend using a model-driven approach, as advocated by Dänekas et al. (2014), with support from the SGAM Toolbox, an extension to the Sparx Systems Enterprise Architect tool[1].

3.1.2. Step 2: Compile a technology-focused threat matrix

Next, a technology-focused threat catalogue for smart grids is developed. To this end, existing threat collections such as the European Union Agency for Network and Information Security (ENISA, 2013) and the German Federal Office for Information Security (BSI, 2013a, 2013b, 2013c) can be used. The resulting *threat catalogue* will in general not be country-specific and can therefore be reused. Its soundness and completeness should be verified by domain experts, including utility providers, device manufacturers, and research institutions. The threat catalogue is then applied to the component and communication layer of the reference architecture that is defined in Step 1, i.e., an evaluation is performed as to the extent to which each threat applies to each architecture component. This evaluation can be implemented using expert knowledge and supported with threat analysis techniques, such as attack trees (Schneier, 1999). This results in a *threat matrix*, displaying the individual threats against different areas of the reference architecture.

3.1.3. Step 3: Assess risk

As a next step, the potential risk for each element of the threat matrix needs to be assessed. This is done by rating the *probability of occurrence* and the *impact of a successful attack*. Since a purely quantitative approach would require determining accurate values for both probability and impact, which is problematic due to the lack of past experience in this area, we recommend the use of a semi-quantitative approach. To obtain realistic values, experts need to perform the proposed rating independently using the Delphi method (Linstone and Turoff, 1975). These experts should include different stakeholders from industry, including national utility providers, and academia. Additionally, to calibrate the assessment of operational impacts, such as power outages, analytical (Teixeira et al., June 2014) and simulation models (Lin et al., 2011) can be used. The major drawback of these approaches is a significant overhead in developing the models for a specific scenario that is being considered. The outcome of this step is a *risk matrix* that shows the risk of a specific area within the reference architecture being successfully attacked; the risk is obtained by multiplying probability and impact values.

3.1.4. Step 4: Define security measures

The last step is to define mitigation strategies for the risks determined in Step 3. The goal of these strategies is to either decrease the probability of a successful attack, alleviate its impact, or both. For each of the identified conceptual risks, generic countermeasures are defined – these should take into account previous work, such as that undertaken by ENISA (European Union Agency for Network and Information Security (ENISA), 2013). The focus is on mitigation actions that are suitable for establishing a basic level of protection in order to ensure a broad application among the utilities. Additionally, ad-

[1] The SGAM Toolbox: http://www.en-trust.at/downloads/sgam-toolbox/.

vanced controls for a higher security level are defined, which can be implemented by utilities with more mature security management processes in place.

3.2. Implementation-level assessment

3.2.1. Step 1: Instantiate the national smart grid reference architecture

Initially, the national reference architecture is instantiated with implementation details, and where possible populated with specific protocols and components. The scope of the implementation-based analysis is determined at this point by identifying which parts of this architecture should be subject to the practical risk assessment. In an ideal case, security audits would be performed on all smart grid systems in a given setting. However, this is neither possible nor advisable in practice, as the scope of the audits is a question of resources and testability[2]. Therefore, it is necessary to focus on high-risk systems, in which potential attack vectors or vulnerabilities could be easily exploited, and security breaches would have a high impact. To this end, the conceptual risk assessment results are considered when determining the *System-Under-Test (SUT)*, focusing on high-risk areas. The outcome of this step is an instantiation of the national reference architecture, showing implementation details, and the SUT as its subset.

3.2.2. Step 2: Identify potential attack vectors and vulnerabilities

After the architecture model has been instantiated with specific hardware and software systems in Step 1, it includes specific technical information, such as the physical communication media and protocols employed, the protection mechanisms in place (i.e., firewalls, VPN tunnels or physical separation), and the specific purpose of each device (for instance, some generic systems may be used for different purposes such as control and measurement applications in different smart grid domains). Considering these settings, and taking into account the conceptual threat matrix and known vulnerabilities, relevant attack vectors for each of the devices and technologies that are part of the SUT are determined.

3.2.3. Step 3: Perform security audit

In this step, the type of security audit to be performed on each device is determined, and the audit is carried out. The type of audit depends on the vulnerabilities that are to be exploited (see Step 2), and should be chosen carefully based on the results of the conceptual risk assessment. While a full-scale in-depth security audit can expose a wide range of hardware and software vulnerabilities, it will also take a considerable amount of time. On the other hand, with a more limited security audit, all devices may be covered, but possibly severe vulnerabilities and implementation flaws may not be found.

In our approach, all devices undergo a limited security audit, whilst the most critical devices in the SUT are additionally subjected to an in-depth security audit. The risk matrix resulting from the conceptual risk assessment allows the analyst to focus on areas of high risk when carrying out intensive implementation-based assessment, such as reverse engineering software. This approach ensures that high-risk devices also receive the highest security auditing level. We describe the auditing approaches that we have used as part of our research in Section 4. Having performed the security audit, its findings can be related back to the risk matrix. For example, threat probability values can be affirmed or adjusted based on the outcomes of the audit, which reflect a concrete understanding of the nature and severity of the vulnerabilities that have been identified.

3.2.4. Step 4: Define specific security measures on the implementation level

The security audit will likely expose security vulnerabilities and highlight practical attack vectors. On the one hand, the results of the security audit can be directly passed on to utilities and device manufacturers, in order to harden their systems. On the other hand, the security audit can also expose whole attack classes and vectors that might not have been previously considered. In both cases, specific security measures can be implemented at the utilities, the manufacturers and, of course, also in the actual device implementations. However, as any system changes can introduce new security vulnerabilities, the continuous auditing of all relevant components is necessary.

4. Applying the method: an Austrian case

The method defined in Section 3 has been applied and evaluated in the course of the Austrian research project *Smart Grid Security Guidance – (SG)*[2], focusing on secure energy distribution systems. The project consortium is composed of different types of smart grid stakeholders, including equipment manufacturers and DSOs, and experts with ICT security and energy systems knowledge. In the following, we describe the application of our method and the outcomes from its use.

4.1. Conceptual-level assessment findings

4.1.1. Step 1

In order to define a national reference architecture, we surveyed the ICT architectures of past and ongoing national smart grid pilot projects and model regions in Austria. Overall, 45 different national projects were identified and prioritised according to size and relevance, out of which seven were selected for a closer review and mapped to SGAM. In addition, the utilities participating in the (SG)[2] project were asked to map their local smart grid systems and foreseeable developments to SGAM. The resulting architecture sketches were combined into a holistic reference architecture for Austrian smart grids, which reflects the current power grid ICT technology, as well as its near-to-mid-term extension towards future smart grid functionalities (see Fig. 2).

The architecture shows the different SGAM zones and domains, as well as the component and communication layer of SGAM. The transmission and generation domains were not covered for this mapping exercise because in the Austrian or,

[2] Systems with requirements that cannot be met in a lab testing environment, e.g., because of large acquisition and/or setup costs, or unsafe working conditions for security analysts, cannot be tested.

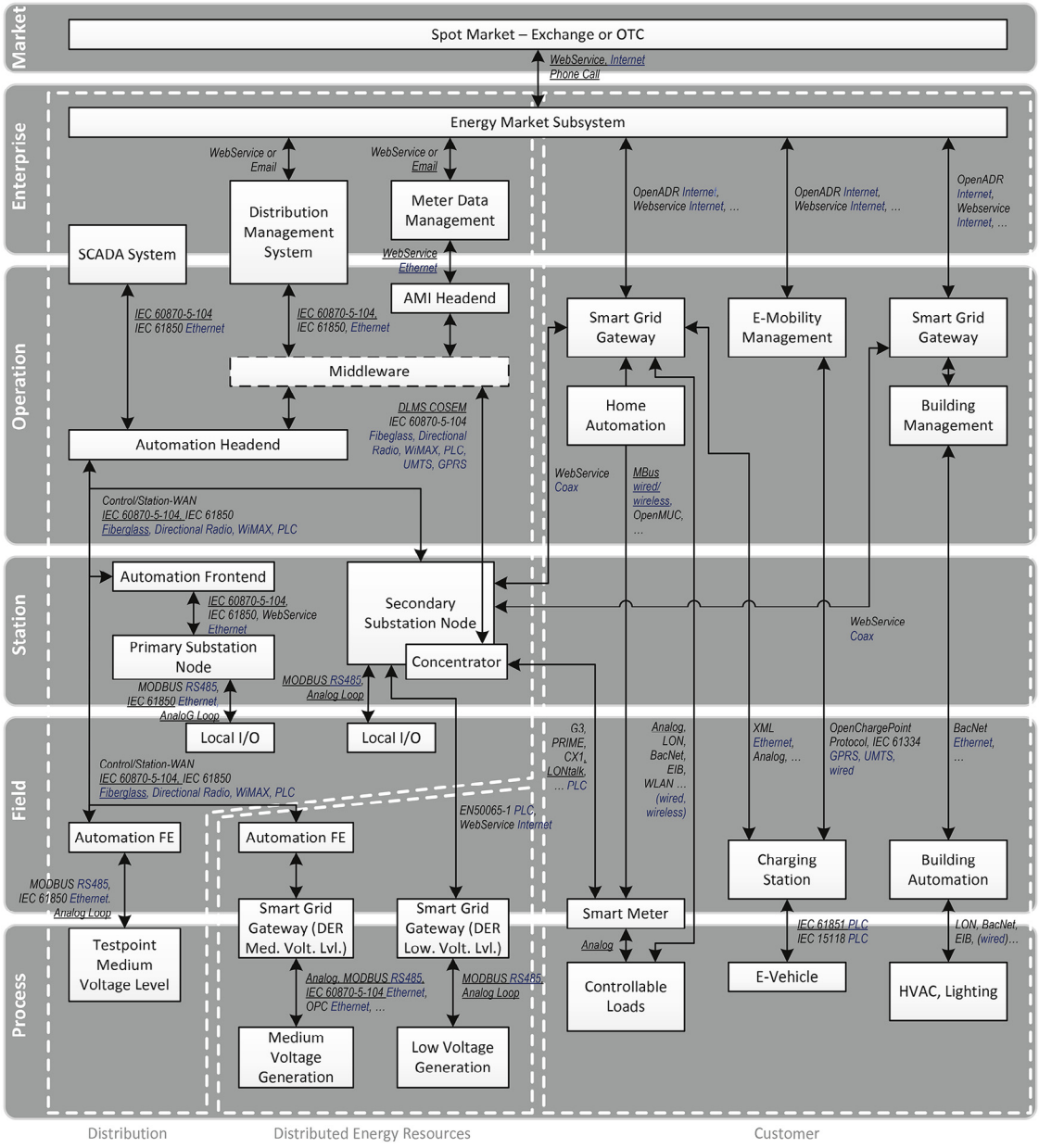

Fig. 2 – The Austrian Smart Grid Architecture, structured according to SGAM: blocks represent entities on the component layer, while arrows are annotated with the communication layer.

respectively, European view, the smart grid is primarily related to distribution systems. The reference architecture draft was subjected to a number of feedback rounds with utilities, manufacturers, and research organisations, until a consolidated result was reached.

4.1.2. *Step 2*

The *IT Baseline Protection Catalogues* (German Federal Office for Information Security (BSI), 2013b) were chosen as the main source of input for the threat catalogue, and were screened for the ICT-based threats that are applicable to smart grids, such as undetected software vulnerabilities, or use of insecure protocols. Additionally, the smart grid threat landscape introduced by ENISA (European Union Agency for Network and Information Security (ENISA), 2013), and the BSI Protection Profiles (German Federal Office for Information Security (BSI), 2013a, 2013c) were taken into account. Non-technical threats, i.e., threats that are related to organisational issues or force majeure, were not considered due to the scope and focus of the $(SG)^2$ project. This resulted in a list of 31 threats (see Kammerstetter et al., 2014) that were applied to the reference architecture defined in Step 1. Since certain components in the architecture model (usually located in identical or at least adjacent SGAM areas) are tightly coupled and strongly interact with each other, we considered *clusters* rather than individual components or communication links when applying the threat catalogue (see Fig. 3). For each element of the threat matrix, the relevance of the threat to the cluster of architecture components was assessed by de-

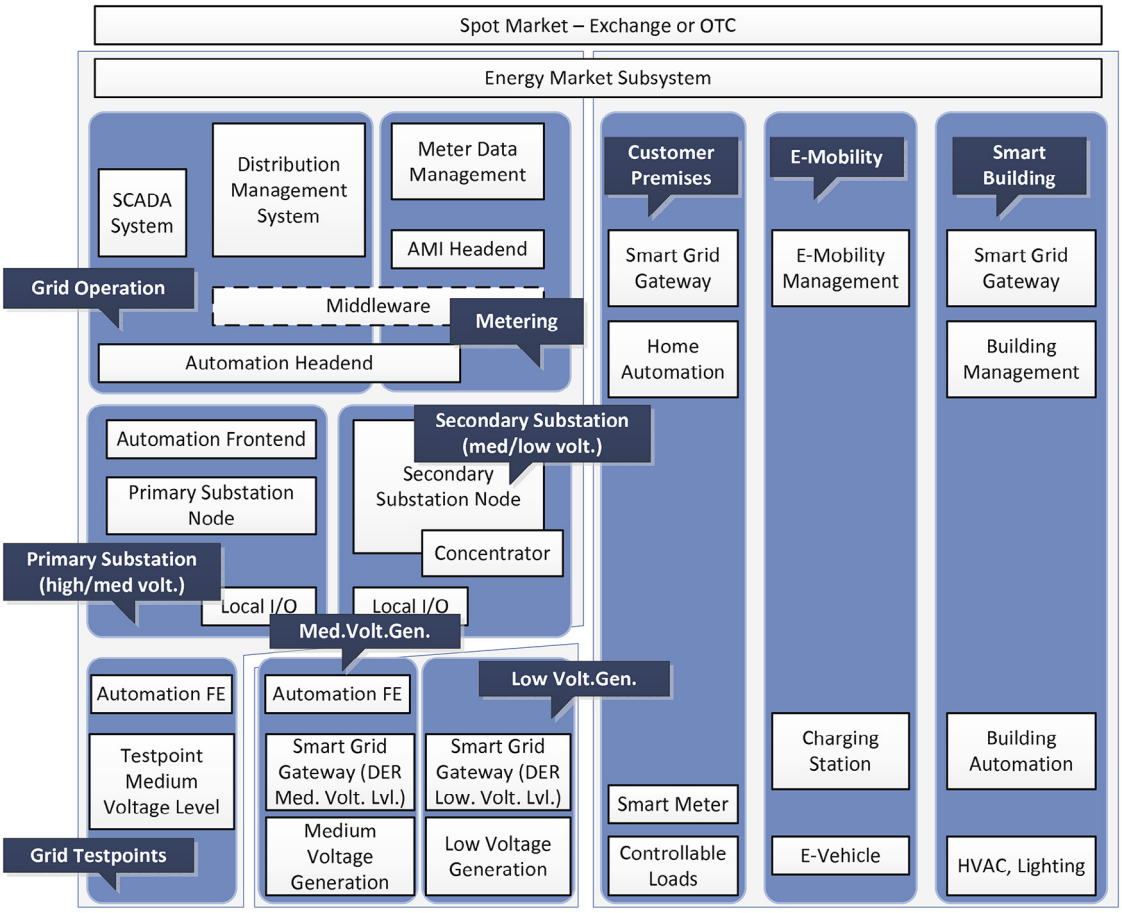

Fig. 3 – The ten clusters of related architectural components that were used for the risk assessment in (SG)².

veloping possible attack scenarios, similar to the approach taken in the National Institute of Standards and Technology (NIST, 2013).

4.1.3. *Step 3*

The third step involved estimating the risk for each element of the threat matrix, thus providing a *risk matrix*. To this end, the probability and impact of each of the threats occurring was rated for each of the clusters of the architecture model. Following a semi-quantitative approach, 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 time span, ranging from less than one incident in ten years (level 1) to multiple incidents per year (level 5). 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 experts from the project consortium independently rated the probability of occurrence of the identified threats and the impact. In a series of workshops, in which we applied the Delphi method (Linstone and Turoff, 1975), the individual results were discussed and consolidated to ensure the validity (or correctness) of the resulting risk matrix. Fig. 4 shows a heat map of the identified risks, where the individual risks are clustered into six categories from *Authentication & Authorisation* to *Maintenance & System Monitoring*. The key findings from this heat map are explained in Section 4.3.

4.1.4. *Step 4*

The final step was to define suitable mitigation strategies that can be used to address the risks identified in Step 3. For each of the identified risks (i.e., rows of the risk matrix), generic countermeasures were defined. Example countermeasures include secure authentication methods and integrity checks, adding redundancy for critical (network) components, and introducing adequate anomaly detection techniques. Additionally, specific countermeasures for the clusters of the reference architecture were also defined where appropriate. For example, these included encryption of sensitive information, such as smart meter readings or consumer data. In order to identify the most important security controls across all risks, an evaluation was carried out by adding weights to the controls depending on the severity of the risk, i.e., the calculated risk level (see Fig. 3). This exercise showed that the top-three most significant security controls are *(i)* ensure integrity and authenticity of all communication, *(ii)* conduct security audits, interoperability and penetration tests, and *(iii)* implement effective change, patch, and configuration management practices. Details on the key findings can be found in Section 4.3.

4.2. *Implementation-level assessment findings*

4.2.1. *Step 1*

First we instantiated the national smart grid reference architecture that was established in the conceptual approach. The

Threat to... / Cluster	Authentication & Authorisation	Applied Security Mechanisms	Integrity & Availability	Internal & external Interfaces	Confidentiality & Data Protection	Maintenance & System Monitoring	*Component Cluster Avg.*
Smart Buildings	3,5	4,0	2,7	2,7	5,7	4,4	3,8
E-Mobility	4,0	4,2	4,5	3,5	4,7	3,5	4,0
Customer Premises	3,0	7,5	4,7	6,3	4,7	4,6	5,1
Low Volt. Gen.	6,0	6,4	4,0	6,7	8,7	3,8	5,9
Med. Volt. Gen.	6,0	4,6	3,1	4,0	4,3	4,2	4,4
Grid Testpoints	6,3	4,7	3,1	3,3	4,0	3,3	4,1
Primary Substation	5,3	5,1	3,6	5,0	3,7	3,9	4,4
Secondary Substation	8,3	5,9	4,7	4,0	5,6	5,3	5,6
Grid Operation	7,0	7,1	4,0	5,8	7,5	5,8	6,2
Metering	5,0	3,0	4,5	2,3	3,8	3,6	3,7
Threat Category Avg.	5,4	5,2	3,9	4,4	5,3	4,2	

Fig. 4 – Simplified risk matrix showing the individual risk levels per threat category per component cluster (cf. Fig. 3).

architecture instantiation includes specific smart grid devices and protocols that are typically deployed in Austria. This exercise is done to ensure that the resulting architecture (including specific technologies like communication protocols and media, system configurations, or protection mechanisms) resembles the national power grid, as closely as possible.

The SUT was selected based on the testability of devices and the outcomes of the conceptual risk assessment (i.e., the risk matrix): considering the average risk for the individual architecture clusters (see Fig. 4), the highest values apply to *Customer Premises*, *Secondary Substation*, and *Low Voltage Generation* clusters. Whilst the first two were selected to become part of the SUT, the third cluster was not testable in our setting. Therefore, we considered the *Grid Operation* cluster instead, which had the fourth highest risk value attached, but is nevertheless of paramount importance for highly reliable energy supply. Thus, we determined the following two subsets of the instantiated smart grid architecture for the SUT: *Secure Substation Automation (SSA)* and *Advanced Metering Infrastructure (AMI)*.

The SSA test system comprises a SCADA system, including engineering tools, and an Automation Headend system as part of the Grid Operation cluster (see Fig. 5). In the Primary and Secondary Substation cluster, the SUT includes an Automation Frontend system and multiple substation systems, such as bay controllers, protection switches or local I/O controllers. The AMI test system comprises an AMI headend system in the Metering cluster, an AMI concentrator on the Secondary Substation cluster, and as a smart grid gateway, a smart meter and controllable loads in the Customer Premises cluster. All the test systems have been equipped with sensors and actors (buttons/switches and LEDs in the simplest case), in order to simulate the surrounding energy grid in a laboratory test setup.

4.2.2. *Step 2*

Considering specific technical information of the devices and technologies that are part of the SUT, such as implementation and configuration details and specific functionalities, we evaluated the potential attack vectors and vulnerabilities on a per-device basis. Again, the results of the conceptual risk assessment were considered in this step: as the risk categories with the highest values refer to the *applied security mechanisms* and *authentication and authorisation* (i.e., data protection) issues, the audits focused on vulnerabilities in these areas. Example vulnerabilities include a lack of authentication mechanisms, interception of user credentials, and insecure or misconfigured communication protocols. The results of this step were used to determine the type of the planned security audits.

4.2.3. *Step 3*

We started the security evaluation by performing security audits on all devices in the SUT, focusing on network communication and communication protocols, and involving both passive and active tests, the latter to the extent possible for the given

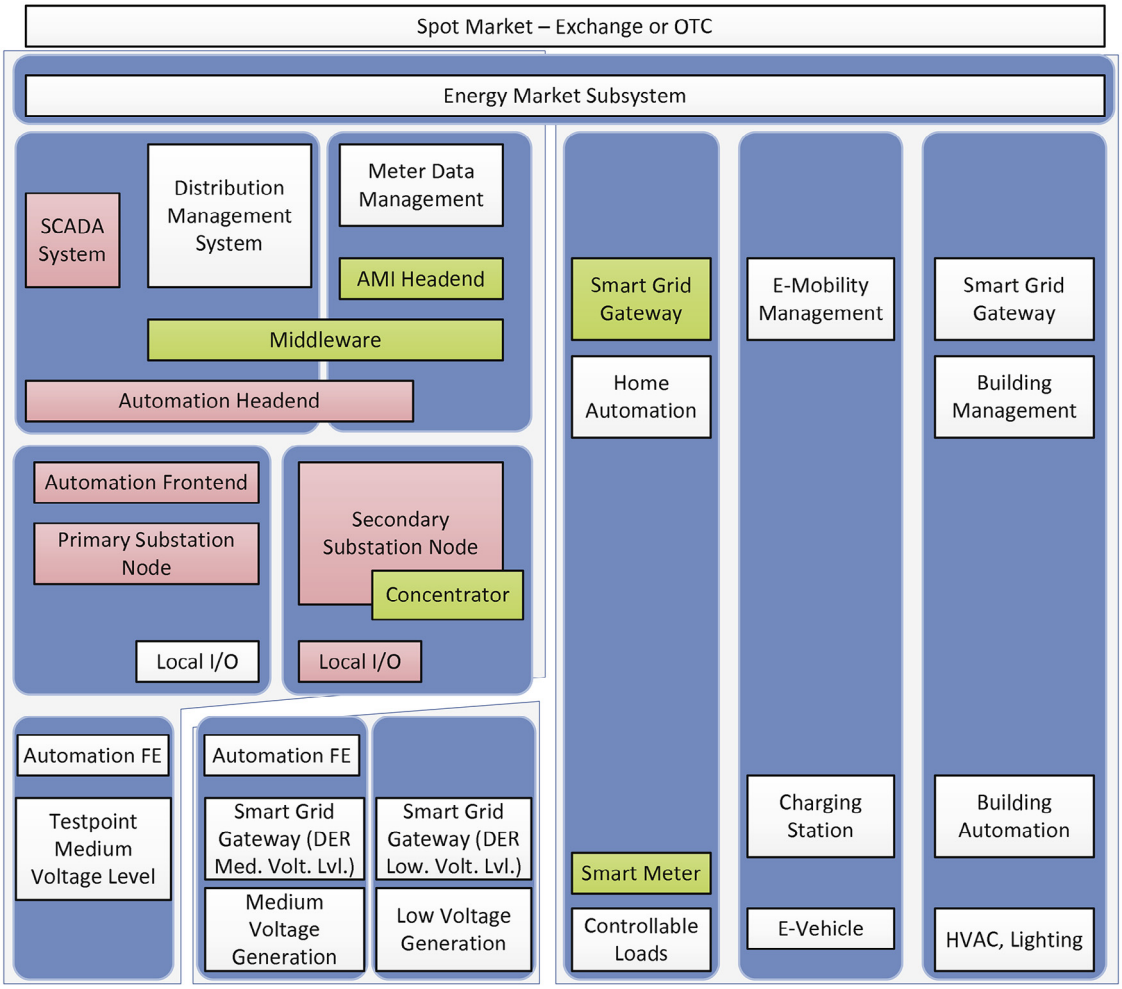

Fig. 5 – System-Under-Test (SUT) mapped to the overall architecture: SSA (red) and AMI (green).

SUT devices. In the first step of the lightweight security audit, we created network stimuli by manually triggering as many device functionalities as possible and, at the same time, passively intercepting the network traffic. For instance, in the case of the SSA, this involved the use of the SCADA system and the engineering tool to communicate, via the Automation Headend and Automation Frontend systems, with the Primary Substation Node systems like the bay controller or the protection switch. We analysed the intercepted communication with a network protocol analyser whenever the protocol was implemented. Otherwise, we implemented our own protocol analysis tools from scratch, by utilising information that we gained from standards or otherwise publicly available sources, such as manufacturer websites.

For proprietary protocols (i.e., engineering tools), we partially analysed and reverse engineered the software tools' implementation in a state-of-the-art debugger (Ida Pro[3]). The protocol analysis allowed us to gain information on the messages exchanged between the devices. For instance, we could see whether sensitive data such as user credentials are transferred in clear text or encrypted. In the next step, we proceeded with active tests by implementing custom analysis tools, allowing us to replay previously captured messages (without or with modification) to the devices (replay attack). Those devices undergoing an in-depth security audit were subject to deep firmware analysis, involving the disassembly of the devices under test followed by deep firmware code analysis techniques, like dynamic instrumentation in a debugging environment.

For dynamic analysis, we were able to run analyses on some of the devices themselves (i.e., in the case of a well-known embedded operating system), while for other devices, our analysis approaches were limited to partial executions in emulation environments. During dynamic analysis runs, we created test inputs from previously recorded network packets and observed their processing in the firmware of the device. However, this was only possible to a limited extent, due to the persisting challenges in embedded code analysis. Finally, the last step of our security evaluation involved feeding the results back to the risk matrix by adjusting the probability and impact values where required and creating Proof-of-Concept (PoC) exploits that were presented to the manufacturers and utilities.

[3] https://www.hex-rays.com/products/ida/index.shtml.

4.2.4. *Step 4*

As a last step, a report on the results of the security audits was provided to the utilities and device manufacturers involved, presenting the practical security vulnerabilities that had been exposed through the audits. Appropriate methods and activities were suggested to harden the system configurations and fix security-relevant bugs in the implementation. However, as these overall system changes might themselves introduce new security vulnerabilities, continuous auditing of all relevant components needs to be in place, in order to ensure a continuous security life cycle. For example, this includes secure configuration baselines, intrusion detection system (IDS) or intrusion prevention System (IPS) solutions at the utilities, secure design and development guidelines, or training courses for designated personnel. In addition, technical security solutions such as encryption, authentication and integrity protection, as well as control flow integrity and buffer overflow prevention mechanisms within the device implementations should be realised.

4.3. *Key findings*

Using our conceptual risk assessment, we were able to assess the security of current and near-term future smart grids in Austria in a structured fashion, resulting in a coherent set of risks and mitigation strategies. Through the implementation-based security audit, we gained deep insight into the security features provided by the devices that were part of the SUT. A summary of our key findings can be described, as follows.

4.3.1. *Importance of effective encryption and authentication mechanisms*

Through our conceptual approach we identified a large number of generic security measures for the Austrian smart grid, most of which also apply to other countries. The conceptual risk assessment revealed that the most critical risk classes are related to authentication and encryption issues (see Fig. 4). The architecture clusters that are most affected by confidentiality issues are *Low Voltage Generation* and *Grid Operation*: decentralised energy supply by small-scale prosumers is challenging in terms of privacy, as not only the consumption, but also the production of energy introduces privacy issues. For the Grid Operation cluster, confidential material such as grid plans and control data requires a high level of protection. A medium to high risk from lack of authentication applies to most architecture clusters related to energy generation and distribution, while this risk is relatively low only for clusters in the customer domain (see Fig. 4). The criticality of effective authentication and encryption was confirmed in our implementation-based risk assessment. During our network protocol analysis, we discovered the use of both standardised open and proprietary engineering protocols. Open protocols, such as IEC 60870-5-104, are in general use for device operation, and engineering tools allow engineers to perform firmware updates or device configuration changes.

Primary mitigation strategies are to apply effective authentication mechanisms to the devices and communication channels within the grid, and to secure the communication with suitable encryption protocols. To this end, the IEC 62351series of standards (International Electrotechnical Commission, 2007) have been defined and should be applied for securing the communication protocols defined by IEC TC57, specifically the IEC 60870-5, the IEC 60870-6, the IEC 61850, the IEC 61970, and the IEC 61968 protocols. The specific properties and requirements of smart grids should also be considered in other areas such as anomaly detection, which should be tailored to fit the particular context in order to provide an effective means to detect smart-grid-specific attacks.

4.3.2. *Minimise the attack surface*

Our implementation-based assessment showed that some of the devices that are part of the SUT, whilst in their default configuration, provide unnecessary or unused services. These services unnecessarily increase the attack surface of the overall system. An example of such a service are web interfaces that can be accessed without authentication, and provide developer options, including security-critical functionalities like register or memory dumping. We believe that a reduction of the attack surface of individual components is vital for achieving strong security in critical infrastructures like power grids. Therefore, any ancillary services that are not required, and might expose additional security vulnerabilities, should be disabled.

4.3.3. *Improve embedded system security analysis*

Embedded systems in critical infrastructures have very demanding security requirements. However, state-of-the-art embedded security and firmware analysis techniques are much less mature than those available for commodity PC systems. Even with the embedded analysis tools and techniques that we developed prior to this work, many of the audits that we would have wanted to perform on the smart grid devices in the SUT were not possible. This was particularly the case for dynamic firmware analysis, wherein we encountered many of the challenges that have been identified by Costin et al. (2015). We strongly believe that without adequate testing tools and techniques, performing security audits on smart grid devices will remain challenging in the future.

5. Conclusion and future work

In this article, we have presented a practical risk assessment method that involves two interrelated streams of activity: *(i)* an *implementation-level* analysis that focuses on existing legacy and prototype systems, and their role in a candidate smart grid architecture; and *(ii)* a *conceptual-level* analysis that aims to understand the risks to aspects of a smart grid for which there is no available implementation. By taking this two-stream approach, we are able to analyse the risks to near- to medium-term future architectural concepts of the smart grid – this is important to ensure smart grids are developed in a secure manner, based on a clear understanding of cybersecurity risks. The basis of our risk assessment is a *national reference architecture*, which is aligned with the European *Smart Grid Architecture Model (SGAM)*, which reflects a proposed deployment within a given national context.

We have applied our risk assessment method in a national smart grid security project that includes participants from

many smart grid stakeholder groups, including DSOs and equipment manufacturers. As a consequence, we were able to make a number of recommendations regarding how to improve the cybersecurity of smart grids within Austria, including where to apply authentication methods and introduce redundancy into the architecture, and how anomaly detection systems can be best applied. We foresee the national reference architecture that was developed in the project having significant impact as a means of ensuring a consistent view of a secure smart grid in Austria, which stakeholders can draw on.

Moving forward, future work will investigate how risks from emerging multi-stage attacks, such as advanced persistent threats (APTs), can be assessed using the national reference architecture, which includes implementation details, as a basis. Furthermore, we will investigate new embedded system security analysis techniques that, e.g., enable dynamic firmware analysis, in order to improve our understanding of the vulnerabilities associated with such systems.

Acknowledgments

The research leading to these results was funded by the Austrian FFG research program KIRAS (project (SG)^2, No. 836276) and the European Union Seventh Framework Programme (project SPARKS, grant agreement No. 608224).

REFERENCES

Austin A, Williams L. One technique is not enough: a comparison of vulnerability discovery techniques. In Internat. Symp. on Empirical Software Engineering and Measurement (ESEM), pages 97–106, 2011.

Brylow D, Damgaard N, Palsberg J. Static checking of interrupt-driven software. In Proceedings of the 23rd International Conference on Software Engineering, ICSE '01, pages 47–56, Washington, DC, USA, 2001. IEEE Computer Society.

CEN-CENELEC-ETSI Smart Grid Coordination Group. Smart Grid reference architecture, <http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx>; 2012 [accessed 05.01.16].

CEN-CENELEC-ETSI Smart Grid Coordination Group. Reports in response to Smart Grid Mandate M/490, <http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx>; 2014a [accessed 05.01.16].

CEN-CENELEC-ETSI Smart Grid Coordination Group. Smart Grid information security, <http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx>; 2014b [accessed 05.01.16].

Cha SK, Avgerinos T, Rebert A, Brumley D. Unleashing mayhem on binary code. In 2012 IEEE Symposium on Security and Privacy (SP), pages 380–394, 2012.

Costin A, Zarras A, Francillon A. Automated dynamic firmware analysis at scale: a case study on embedded web interfaces. CoRR, abs/1511.03609, 2015.

Dänekas C, Neureiter C, Rohjans S, Uslar M, Engel D. Towards a model-driven-architecture process for smart grid projects. In: Benghozi P-J, Krob D, Lonjon A, Panetto H, editors. Digital enterprise design & management. Advances in Intelligent Systems and Computing, vol. 261. Springer International Publishing; 2014. p. 47–58.

European Union Agency for Network and Information Security (ENISA). 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>; 2012 [accessed 05.01.16].

European Union Agency for Network and Information Security (ENISA). Smart grid threat landscape and good practice guide. <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/sgtl/smart-grid-threat-landscape-and-good-practice-guide>; 2013 [accessed 05.01.16].

German Federal Office for Information Security (BSI). Protection profile for the security module of a Smart Metering System (Security Module PP). BSI-CC-PP-0077, 2013a.

German Federal Office for Information Security (BSI). IT baseline protection catalogs, <http://www.bsi.bund.de/gshb>; 2013b [accessed 05.01.16].

German Federal Office for Information Security (BSI). Protection profile for the gateway of a Smart Metering System. BSI-CC-PP-0073, 2013c.

GridWise Architecture Council Interoperability Framework Team. Interoperability context-setting framework, <http://www.caba.org/resources/Documents/IS-2008-30.pdf>; 2007 [accessed 05.01.16].

International Electrotechnical Commission. Part 1: communication network and system security – introduction to security issues, IEC 62351-1. <https://webstore.iec.ch/publication/6903>; 2007 [accessed 05.01.16].

International Organization for Standards. Introduction to ISO 27002 (ISO27002). <http://www.27000.org/iso-27002.htm>; 2013 [accessed 05.01.16].

Kammerstetter M, Langer L, Skopik F, Kupzog F, Kastner W. Practical Risk Assessment Using a Cumulative Smart Grid Model. In the 3rd International Conference on Smart Grids and Green IT Systems (SMARTGREENS), pages 31–42, 2014.

Kermani MM, Zhang M, Raghunathan A, Jha NK. Emerging frontiers in embedded security. In VLSI Design and 2013 12th International Conference on Embedded Systems (VLSID), 2013 26th International Conference on, pages 203–208, 2013.

Khare S, Saraswat S, Kumar S. Static program analysis of large embedded code base: an experience. In Proceedings of the 4th India Software Engineering Conference, ISEC '11, pages 99–102, New York, NY, USA, 2011. ACM.

Lin H, Sambamoorthy S, Shukla S, Thorp J, Mili L. Power system and communication network co-simulation for smart grid applications. In Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES, pages 1–6, Jan 2011.

Linstone HA, Turoff M, editors. Delphi method: techniques and applications. Addison-Wesley; 1975.

Liu B, Shi L, Cai Z, Li M. Software vulnerability discovery techniques: a survey. In 4th International Conference on Multimedia Information Networking and Security (MINES), pages 152–156, 2012.

National Institute of Standards and Technology (NIST). Framework and roadmap for Smart Grid interoperability standards, Release 1.0, 2010.

National Institute of Standards and Technology (NIST). NISTIR 7628 – guidelines for Smart Grid cybersecurity, 2013.

Schneier B. Attack Trees. Dr. Dobb's Journal 1999;24(12):21–9.

Schwartz EJ, Avgerinos T, Brumley D. All you ever wanted to know about dynamic taint analysis and forward symbolic execution (but might have been afraid to ask). In 2010 IEEE Symposium on Security and Privacy (SP), pages 317–331, 2010.

Teixeira A, Dán G, Sandberg H, Berthier R, Bobba R, Valdes A. Security of smart distribution grids: data integrity attacks on integrated volt/VAR control and countermeasures. In American Control Conference (ACC), pages 4372–4378, June 2014.

Venkitaraman R, Gupta G. Static program analysis of embedded executable assembly code. In Proceedings of CASES 2004, pages 157–166, New York, NY, USA, 2004. ACM.
Viega J, Thompson H. The state of embedded-device security (spoiler alert: it's bad). IEEE Secur Priv, 2012;10(5):68–70.
Yan Y, Qian Y, Sharif H, Tipper D. A survey on cyber security for smart grid communications. IEEE Commun Surv Tut 2012;14(4):998–1010.

Lucie Langer has been with the Digital Safety & Security Department of AIT Austrian Institute of Technology since 2012. She is currently responsible for several applied research projects on IT security aspects of critical infrastructures and smart grids. She was the coordinator of the nationally-funded SG2 project that developed a security architecture for Austrian smart grids, focusing on distribution system networks. Previously, she was a member of the Cryptography & Computer Algebra Group at Technische Universitaet Darmstadt, receiving her PhD in 2010. Her research interests include secure reference architectures for smart grids and cyber-physical impact assessment for critical infrastructures.

Florian Skopik joined AIT in 2011 and is currently working in AIT's ICT Security Research Team as a Senior Scientist, where he is responsible for national and international (EU FP7) research projects. The main topics of these projects are centred on smart grid security, the security of critical infrastructures and national cyber security. He has published approximately 75 scientific conference papers and journal articles, and is member of various conference program committees and editorial boards. He is the co-editor, along with Dr Paul Smith, of a new book on smart grid security published by Elsevier in 2015. Florian is an IEEE Senior Member.

Paul Smith is a Senior Scientist in the Safety and Security Department of AIT, Austrian Institute of Technology. Previous to this appointment he was a Senior Research Associate at Lancaster University, UK, where he received his PhD in September 2003. Paul has been working in the area of network resilience for several years, publishing numerous conference and journal articles. Currently, he is coordinating the EU-funded SPARKS project, which is investigating the security and resilience of the smart grid – his research focus in the project is on cybersecurity risk assessment.

Markus Kammerstetter is currently working as a senior PhD candidate at the Secure Systems Lab Vienna located at the Automation Systems Group at Vienna University of Technology. His research interests include most aspects of computer and embedded-system security, with emphasis on hardware security as well as low-level binary analysis, forensics and reverse engineering. However, due to the long lasting experience in the Smart Grid and hardware security domains, his current research focus is more in that area today. In 2012 he founded and currently leads the Hardware Security Lab, a group that supports applied hardware and semiconductor security research. The lab leverages and develops dedicated equipment to support the extraction and security analysis of embedded firmware by means of fault injection, side channel attacks and IC reverse engineering.