Cybersecurity Risk Assessment in Smart Grids

Thomas Hecht, Lucie Langer, Paul Smith

AIT Austrian Institute of Technology
Safety and Security Department
firstname.lastname@ait.ac.at

Abstract – Smart grids will make extensive use of information and communication technology (ICT) to enable the integration of renewable energy sources. Consequently, future power grids come with a much larger cyber-attack surface, which makes cybersecurity risk assessment a major concern. Due to their cyber-physical nature, risk assessment in smart grids is a challenging task. Moreover, the complex mix of legacy systems and new components in smart grids requires novel risk assessment methods that are able to cater for both. This paper surveys existing risk assessment methods for smart grids, addresses the key challenges, and presents ongoing research projects that aim to tackle these challenges.

1. Introduction

Future power grids will make extensive use of information and communication technology (ICT) to enable the integration of renewable energy sources and more efficient energy management. While ICT components are already part of today's power grid, they are used in a much more isolated fashion, with access restricted mainly to energy providers and grid operators. This paradigm will no longer hold in future smart grids: end-users will be connected to the grid via smart gateways, and electricity billing will be provided through smart meters, which means that every consumer (or prosumer) will have their own ICT-enabled entry point to the grid. The large number of access points introduces a much larger surface for cyber-attacks than there has been before. Possible attacks include large-scale meter tampering, spoofed measurement data leading to a misinterpretation of the current system status, or even targeted high-impact attacks on the critical infrastructure of grid operators. Moreover, recent events have shown that attacks on industrial control systems are becoming increasingly sophisticated. Consequently, assessing (and managing) the risk from cyber-attacks is of paramount importance for the security of future energy supply.

Risk assessment in smart grids is a challenging task for various reasons. First and foremost, due to the cyber-physical nature of smart grids, ICT-focused risk assessment methods are not readily applicable, and safety aspects must be considered as well. Additionally, the complex mix of legacy systems and new components in smart grids requires novel risk assessment methods that are able to cater for both. This paper summarizes existing risk assessment methods applicable to smart grids, investigates the associated challenges, and summarizes ongoing research in this area.

2. Cybersecurity Risk Assessment

The primary objective of cybersecurity risk assessment is to identify vulnerabilities and threats, and determine their impact. The outcome of the risk assessment should be used in the specification of security requirements and the selection of security controls for smart grid. Both top-down (e.g., use case analysis and smart grid functionality) and bottom-up (e.g., authentication and authorization at substations, key management, intrusion detection, etc.) approaches should be used to implement risk assessment [1]. Furthermore, existing risk assessment methods are divided into quantitative and qualitative approaches. Quantitative methods use metrics that represent the probability and impact of a threat. As this often proves to be a difficult and subjective task due to the shortage of reliable data on incidents, qualitative approaches are widely used instead, which may also be able to take advantage of other sources of information that are not readily quantifiable, such as threat graphs and game-theoretic models. The European Network and Information Security Agency (ENISA) maintains a repository of risk assessment standards, methods and tools [2].

While risk assessment has been defined to address information security in conventional ICT systems, risk assessment for smart grids is still in its infancy. For system stakeholders, utility providers, manufacturers and system developers, risk assessment for smart grid remains a huge challenge for several reasons: current risk assessment frameworks are mostly focused either on conventional ICT systems (e.g., BSI Baseline Protection [3]), or on traditional power grids (from NERC [4] or ISA standards [5]). Little consideration has been given to smart grids and their specific attributes. While risks for traditional ICT systems focus on the confidentiality, integrity and availability of information (mostly in that order), in industrial control systems and, more specifically, smart grids, operational reliability is of utmost importance, and the priority therefore is on availability, followed by integrity and confidentiality [6]. This means that cybersecurity risk assessment for smart grids must be combined with safety aspects.

A small number of frameworks address risk assessment for critical (energy) infrastructures. The *Guidelines for Smart Grid Cyber Security* developed by NIST (NIST-IR 7628) [7] provide a set of high-level recommendations applicable to the proposed smart grid architecture for the U.S. However, a general approach for assessing cybersecurity risks is not provided. NIST-IR 7628 and ISO 27002 have been the basis for a report on smart grid security by ENISA [8]. It provides a set of specific security measures for smart grid service providers, aimed at establishing a minimum level of cybersecurity. The importance of performing a comprehensive risk assessment before selecting appropriate measures is pointed out, but no specific methodology is recommended. The Reference Security Management Plan for Energy Infrastructure developed for the European Commission [9] is intended to provide guidance for operators of energy grids or components thereof, and contains recommendations on performing a risk assessment, based on the *Performance and Risk-based Integrated Security Methodology (PRISM)*. The European standardization bodies CEN, CENELEC and ETSI have issued a report on *Smart Grid Information Security (SGIS)* [10, 11] addressing cybersecurity and risk assessment in smart grids in response to the M/490 Smart Grid Mandate by the European Commission. It 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 to classify inherent risks of smart grid assets. The risk assessment proposed by SGIS takes a clean-slate approach, assuming a future smart grid with no security controls in place. Consequently, this approach does not reflect the way that smart grids are being deployed, in which the present power grid undergoes an incremental transformation into a smart grid. Thus, a practical cybersecurity risk management approach must be able to deal with a complex combination of legacy systems and new technologies, which is only one among many challenges.

3. The Challenges of Risk Assessment for Smart Grids

In this section, we summarize a number of the key challenges associated with conducting a risk assessment for the smart grid. Some of these challenges exist in others contexts for different types of system; however, implementing a risk assessment in the smart grid is particularly difficult as all of these challenges are present.

3.1 Managing Safety and Security Risks

Cyber-attacks to an electric power grid have the potential to result in safety-related incidents, i.e., those that could result in a loss of life. For example, data injection attacks may be used to change measurement values of some devices, in order to hinder the operation of the grid [12]. Further challenges include data integrity attacks [13], which have the goal of inserting, changing or deleting data in network traffic, so that a management system takes incorrect decisions. Arguably, such attacks could result in safety-related incidents if they lead to the unsafe usage of plant equipment, for example. In the safety domain, a number of analysis techniques have been applied by the community for a number of years. Examples of these include the Hazard and Operability (HAZOP) [14] and Failure Modes and Effect Analysis (FMEA) [15] techniques, which can be used to identify hazard scenarios and the failure modes and their effect on a system, respectively. Similarly, in the security domain, a number of techniques exist for threat and vulnerability analysis, including Microsoft’s STRIDE method [16] and attack trees [17]; the latter being very closely related to fault tree analysis [18], which is commonly used for safety analysis. Whilst these two classes of analysis methods are mature, their combined use to understand the safety-related incidents that could emerge from cyber-attacks is still in its infancy.

3.2 Analyzing Cyber-physical Risks

Closely related to the issue of safety in the smart grid, are the challenges associated with analyzing cyber-physical risks. The fact that the smart grid is a cyber-physical system has two major implications for risk assessment: *(i)* in addition to the cyber threats and vulnerabilities that must be considered, physical risks must also be assessed – this both increases the number of scenarios that have to be assessed and introduces the challenge of understanding the relative importance of cyber versus physical risk; and *(ii)* the physical impact of an attack must be assessed, e.g., in terms of disturbance to energy supply, which can be particularly difficult to determine for cyber-threats. For instance, it is not readily apparent what effect cyber-attacks, such as a Denial of Service attack to a part of a smart grid's ICT infrastructure, could have on the physical operation of a grid – we anticipate this to be somewhat limited currently, as ICT services play an ancillary role, but this may change in the future as it is introduced to support increasingly critical functions of a grid.

3.3 Understanding the Risks to Legacy Systems

The future smart grid will consist of existing *legacy* systems and new ones that, for example, implement novel control mechanisms. In this context, it may be beneficial to examine the security risks associated with new smart grid sub-systems when they are architectural concepts – for example, such an analysis at design-time can ensure secure architectural decisions are made. Examining this combination of legacy and new systems should be catered for when carrying out a risk assessment for the smart grid. For example, specific processes should be defined that support the architectural analysis of conceptual smart grid components that, e.g., identify topological vulnerabilities.

Alongside these forms of analysis, concrete threat and vulnerability assessment can be undertaken, e.g., via penetration testing, to understand the implementation-based risks that are related to legacy systems. However, it is widely understood that legacy industrial control systems can be fragile when subjected to active vulnerability scanning, which can result in the need for manual procedures, thus increasing the complexity of smart grid risk assessment. Similarly, the limited possibilities to perform active security tests may require expensive testing facilities that represent copies of the operational infrastructure, or limited passive tests being realized that are based on eavesdropping communication, for example.

Additionally, the impact on legacy systems from the introduction of new ones must be assessed, and vice versa. In some cases, the different technologies may not interact, e.g., because they use different protocols. When they do interact, there may be unclear security outcomes because of poorly documented legacy systems – such risks may be challenging to evaluate.

3.4 Complex Organizational Dependencies

The power grid is a complex system, which in the liberalized European energy market involves a number of different organizations, including Energy Producers, Transmission System Operators (TSOs), Distribution System Operators (DSOs), and Energy Suppliers. The smart grid has the potential to add more organizations such as telecommunications providers and cloud service providers, e.g., to support the implementation of an Advanced Metering Infrastructure (AMI). Energy customers in the smart grid have a potential role as an energy producer – operating their own equipment – potentially as part of a community of virtual energy producers. Additionally, a diverse range of equipment suppliers and solutions providers can be drawn upon to implement different sub-systems of the smart grid. This complex web of organizational dependencies and responsibilities has the potential to make risk assessment and management very challenging. For example, assessing the risks associated with third-party services and solutions is difficult, because of a lack of transparency. It is widely understood in the ICT sector that organizational boundaries are breaking down, making risk assessment problematic – the use of third-party cloud services by companies is a good example of this phenomenon. With the widespread use of ICT solutions in the smart grid, these problems become inherent. Also, determining which organization is responsible for accepting the risk burden can be difficult.

3.5 Understanding Cascading Effects

The smart grid is a combination of ICT systems that are interconnected via communication networks, which support an underlying grid infrastructure. Incidents in each of these sub-systems of a smart grid have the potential to cause cascading effects that result in problems in another. This issue is closely related to the previously discussed challenge of cyber-physical impact analysis, i.e., that a cyber-attack to an ICT sub-system could result in an effect in the power grid. However, here we describe a more general problem, in which one attempts to analyze effects across multiple subsystems that could be both cyber and physical. A particularly pathological case relates to the dependency between ICT systems and a supporting power infrastructure – a cyber-attack could result in a disturbance in its supporting power supply, such as a localized blackout, that could in return result in the ICT systems becoming unavailable when a battery-based uninterruptible power supply expires. To understand such cascading effects, appropriate models of the infrastructure must be developed, along with an understanding of how the impact of an attack could propagate through it.

4. Moving Forward: Addressing the Challenges of Smart Grid Risk Assessment

In ongoing research we will look to address the challenges of implementing a risk assessment for the smart grid via a number of related initiatives. Focusing on current and near-future distribution systems, the Austrian research project *Smart Grid Security Guidance (SG)^2* has developed a cybersecurity risk assessment method that considers the evolving nature of the smart grid, as well as the given national context in terms of prevailing systems, regulatory constraints, or legal specifications. This method is based on the definition of a national reference architecture, and can be applied to both deployed legacy systems and near-term future developments. The risks to existing systems are evaluated through practical security assessments, which are complemented with a conceptual analysis of future developments. The latter involves threat modeling based on existing collections by the BSI [3] and ENISA [19], subsequently applying those threats to the architecture model, and assessing probability and impact in a semi-quantitative manner. The semi-quantitative analysis is achieved by developing possible attack scenarios and drawing on past experience of the DSOs in the project. Going beyond the activities in the (SG)^2 project, a number of initiatives are seeking to address many of the challenges that are outlined in Section 3, although not necessarily in the context of the smart grid.

As part of the Artemis-funded *EMC^2* project (http://www.emc2-project.eu/), Schmittner *et al*. have developed an extension to the FMEA safety analysis technique, which can be used to analyze the likelihood and impact of cyber-attacks [20]. The EMC^2 project is applying this technique to embedded multi-core systems, such as those found in the automotive industry. This represents early work; further investigation is required, for example, to allow the direct comparison of security and safety-related incidents, and support analysts determining the measures that are associated with threat actors, such as their incentive and capability. Whilst the EMC^2 project focuses on analyzing safety and security aspects for embedded systems, the techniques can be tailored to the analysis of specific smart grid components and sub-systems.

The EU-funded *HyRiM* project (*Hybrid Risk Management for Utility Providers*, https://www.hyrim.net/) is developing novel risk analysis techniques that can be applied to utility networks, e.g., gas, electricity and transport networks. An aspect they are investigating in the project relates to analyzing cascading effects, whereby incidents in the electricity grid result in effects in a transportation system, for example. In order to approach this problem, the project will seek to combine analysis methods that are based on game theory [21] with those related to network theory [22]. As mentioned earlier, parallels can be drawn with the investigations being undertaken in HyRiM and those needed for smart grids, which is comprised of multiple interconnected power and ICT networks and sub-systems.

The EU-funded *SECCRIT* project (*Secure Cloud computing for Critical Infrastructure IT*, https://www.seccrit.eu) is investigating how to support the implementation of high-assurance ICT services, such as those that underpin critical infrastructure services, in the Cloud. In this regard, they have developed a cloud-specific threat and vulnerability catalogue that can be applied when understanding the risks associated with migrating services to the Cloud [23]. The catalogue is organized into categories that relate to the usage of Cloud, such as the use of virtualization technology. Additionally, they have created an extension to an existing risk assessment process that supports the modeling of ICT services in the Cloud and the analysis of risk scenarios, based on the aforementioned catalogue. Assessing the risks associated with Cloud usage has similar challenges as those for the smart grid: there are a number of organizations involved with potentially complex responsibilities with respect to risk, for example. Our future work will seek to leverage the results from the SECCRIT project, especially with respect to the use of the Cloud to implement smart grid ICT services – a deployment model that could be applied.

Finally, the EU-funded *SPARKS (Smart Grid Protection Against Cyber Attacks)* project is investigating cybersecurity and resilience for the smart grid (https://project-sparks.eu). As part of the project's research activity, it will investigate suitable risk assessment methods. As a starting point to achieve this it will draw upon the findings from the projects that have been previously discussed. A specific contribution the project will make relates to the simulation and modelling of attack scenarios, which can be used to understand the potential physical impact of a cyber-attack on the smart grid. At the time of writing, the project is investigating existing tools that can be used to simulate communication networks, e.g., OMNeT++ (http://www.omnetpp.org), and power systems, e.g., GridLAB-D (http://www.gridlabd.org/). The goal is to combine these tools and develop suitable models that simulate attack behaviour, for example. Furthermore, the project will seek to develop models that can be used to analyze the impact that tampering with measurement signals have on the control algorithms that will be realized for the smart grid. This activity will build on previous research carried out in the EU-funded Viking project, which investigated this issue for transmission systems [24]; an initial study is seeking to learn what will be the important control algorithms for the smart grid.

An overview of how these projects address the different challenges that are outlined in Section 3 is presented in Table 1. A further aim of the SPARKS project is to develop an overarching risk assessment framework that can be used to address these challenges, drawing on results from the aforementioned initiatives. A starting point for reaching this objective will to examine the SGIS toolbox – a risk-driven approach to incorporating security into a use case analysis framework – which is described in the CEN-CENELEC-ETSI Smart Grid Coordination Group's *Smart Grid Information Security* documentation [11].

Table 1 Overview of the major contribution of the different initiatives with respect to the challenges outlined in Section 3. SS – Managing Safety and Security Risks, CP – Analyzing Cyber-physical Risks, LS – Understanding the Risks to Legacy Systems, CO – Complex Organizational Dependencies, CE – Understanding Cascading Effects.

Project Name	**SS**	**CP**	**LS**	**CO**	**CE**
Smart Grid Security Guidance (SG)^2			✓		
EMC^2	✓				
HyRiM					✓
SECCRIT				✓	
SPARKS		✓			

5. Conclusion

Future power grids will have to cater for many new requirements that can only be met through the support of a comprehensive ICT infrastructure. This changes the significance of cybersecurity issues: while safety and reliability aspects have been in the focus of security considerations for power grids so far, risks emerging from cybersecurity attacks must be considered in the future as well. However, cybersecurity risk management in smart grids is not a straightforward matter. ICT-focused risk frameworks cannot be readily applied to smart grids, due to their cyber-physical nature. While smart-grid-specific security recommendations do exist, they often fail to understand the particular challenges related to cybersecurity risk assessment in smart grids, such as the interrelation of safety and security risks, the mix of legacy and novel systems, or the potential of cascading effects. These challenges are currently being addressed in various research projects. The common goal of these efforts is to support smart grid stakeholders in understanding and assessing vulnerabilities and cybersecurity threats in smart grids, and to provide guidance on effective risk management by integrating cybersecurity and power systems security assessment approaches.

References

[1] NIST, Smart grid cyber security strategy and requirements, NISTIR 7628.

[2] ENISA, Inventory of risk management/risk assessment methods and tools http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory.

[3] Federal Office for Information Security (BSI), IT Baseline Protection Catalogs, http://www.bsi.bund.de/gshb, 2013.

[4] NERC, Security guidelines for the Electricity sectors: vulnerability and risk assessment.

[5] ISA, Security for industrial automation and control systems: concepts, terminology and models.

[6] IEC62443-2-1, Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program.

[7] NIST, NISTIR 7628 – Guidelines for Smart Grid Cybersecurity, 2013.

[8] ENISA, Appropriate security measures for smart grids, Dec 2012.

[9] A Reference Security Management Plan for Energy Infrastructure. Prepared by the Harnser Group for the European Commission under Contract TREN/C1/185/200. 2010. Available at http://ec.europa.eu/energy/infrastructure/studies/doc/2010_rsmp.pdf.

[10] CEN-CENELEC-ETSI Smart Grid Coordination Group, Reports in response to Smart Grid Mandate M/490, 2012.

[11] CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Information Security, December 2013.

[12] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen: Smart attacks in smart grid communication networks, Communications Magazine, IEEE, vol. 50, no. 8, pp. 24–29, August 2012.

[13] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu: Securing smart grid: cyber attacks, countermeasures, and challenges, IEEE Communications Magazine, vol. 50, no. 8, pp. 38–45, August 2012.

[14] Tyler, Brian, Crawley, Frank & Preston, Malcolm (2008). HAZOP: Guide to Best Practice (2nd Edition ed.). IChemE, Rugby. ISBN 978-0-85295-525-3.

[15] Department of Defense: MIL STD 1629A, Procedures for Performing a Failure Mode, Effect and Criticality Analysis, November,1980.

[16] Shawn Hernan, Scott Lambert, Tomasz Ostwald, Adam Shostack, Uncover Security Design Flaws Using The STRIDE Approach, MSDN Magazine, November, 2006.

[17] Bruce Schneier, Attack Trees, Dr. Dobb’s Journal, December, 1999.

[18] David J. Mahar and James W. Wilbur, Fault Tree Analysis Application Guide, Reliability Analysis Center, 1990.

[19] ENISA, Smart grid threat landscape and good practice guide, Dec 2013.

[20] Christoph Schmittner, Thomas Gruber, P.P., Schoitsch, E.: Security Application of Failure Mode and Effect Analysis (FMEA). 33rd International Conference on Computer Safety, Reliability and Security (SafeComp) 2014 (September 2014), (in press).

[21] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Bacşar, and Jean-Pierre Hubaux. Game theory meets network security and privacy. ACM Computing Surveys. 45(3), July 2013).

[22] Saray Shai and Simon Dobson. Coupled adaptive complex networks. Physical Review E 87(4). April 2013.

[23] Jerry Busby, Lucie Langer, Marcus Schöller, Noor Shirazi, Paul Smith .Deliverable: 3.1 Methodology for Risk Assessment and Management. December 2013. Available online at: https://www.seccrit.eu.

[24] György Dán, Henrik Sandberg. Stealth attacks and protection schemes for state estimators in power systems. 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm). Gaithersburg, Maryland, USA, October 2010, pp. 214 – 219.