Architecture-Driven Smart Grid Security Management

Markus Kammerstetter
Institute of Computer Aided Automation
Automation Systems Group
International Secure Systems Lab
Vienna University of Technology
mk @ iseclab.org

Lucie Langer
Safety and Security Department
Austrian Institute of Technology
lucie.langer @ ait.ac.at

Florian Skopik
Safety and Security Department
Austrian Institute of Technology
florian.skopik @ ait.ac.at

Wolfgang Kastner
Institute of Computer Aided Automation
Automation Systems Group
Vienna University of Technology
k @ auto.tuwien.ac.at

ABSTRACT

The introduction of smart grids goes along with an extensive use of ICT technologies in order to support the integration of renewable energy sources. However, the use of ICT technologies bears risks in terms of cyber security attacks which could negatively affect the electrical power grid. These risks need to be assessed, mitigated and managed in a proper way to ensure the security of both current and future energy networks. Existing approaches have been either restricted to very specific components of the smart grid (e.g., smart meters), or provide a high-level view only. We therefore propose an architecture-driven security management approach for smart grids which goes beyond a mere abstract view without focusing too much on technical details. Our approach covers architecture modeling, risk identification and assessment as well as risk mitigation and compliance checking. We have proven the practical usability of this process together with leading manufacturers and utilities.

Categories and Subject Descriptors

C.2 [**Computer-Communication Networks**]: General—*Security and protection*; H.4 [**Information Systems Applications**]: Miscellaneous; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

IH&MMSec'14, June 11–13, 2014, Salzburg, Austria.

http://dx.doi.org/10.1145/2600918.2600937.

Keywords

Smart Grid, Security, Security Management, Risks

1. INTRODUCTION

While traditionally electrical power grids adhered to the producer-consumer model, in modern smart grids everyone can become an energy producer – by leveraging green energy produced through solar panels, wind turbines or heating and biogas plants, consumers turn into "prosumers". For traditional large-scale utilities and energy producers, this has introduced a massive drawback: due to decentralized energy production, energy networks can no longer be centrally controlled. The solution is to upgrade existing power grids to smart grids by establishing an ICT network in parallel to the electrical power grid. While this brings advantages with respect to energy efficiency, green energy harvesting and consumer freedom, it also introduces ICT security risks in critical infrastructures that may cause disastrous effects.

As manufacturers of smart grid components move from pure electrical systems to the development of complex ICT systems, and though security may be an important target for them, market pressure and a lack of security experience may force them to roll out insecure products. Utilities, on the other hand, need to rely on manufacturers that their smart grid devices are secure in order to run this critical infrastructure. To lower the risks involved, proper risk management needs to be put in place. However, existing ICT-related risk management processes are not directly applicable to the smart grid domain as the technology and the security requirements are significantly different. On the other hand, readily available smart grid security guidelines such as the Protection Profiles [3, 4] developed by the German Federal Office for Information Security (BSI) merely focus on smart metering and thus do not map to the entire smart grid architectures deployed.

We decided to take a different approach. Instead of focusing on a single technological component, we model European smart grid architectures by using the Smart Grid Architec-

ture Model (SGAM) [17]. Based on well-established sources of ICT-related security threats, we created a catalog for ICT security threats to the smart grid, which can be applied to components in the SGAM model. In this work, we show how our approach can be practically used for smart grid risk management, including risk assessment, mitigation and compliance checking. As our approach has been developed in conjunction with leading smart grid manufacturers and utilities, we believe that it has a strong practical impact.

In summary, the main contributions of our work are:

- an SGAM-based smart grid model representing both current and near-future European smart grid architectures,
- a comprehensive catalog of cyber security threats for smart grids, and
- a practical risk assessment approach able to bridge the gap between a high-level architectural view and specific technical security measures.

The remainder of this paper is organized as follows. Section 2 outlines existing work on smart grid security and risk assessment. Section 3 describes the five steps of our smart grid risk management approach, which is subsequently evaluated in Section 4. Section 5 concludes the paper and identifies potential areas for future work.

2. RELATED WORK

Smart grid technologies have received major attention in both academia and industry in recent years. Various works discuss the basics of the smart grid, such as its structure, application, and potential impact [1, 18]. Others cover established and recently developed technical standards [5]. The European Union plans to replace traditional electricity meters with smart meters to a large extent until 2020, which draws major attention to various security and privacy aspects of this technology [8, 15]. Therefore, the U.S. NIST and European ENISA have released numerous guidelines on how to secure smart grid architectures [12, 6]. Although these documents build a solid basis, they do not show the complete picture. NIST, for instance, focuses on technologies employed in U.S. smart grids, and both guidelines give quite high-level recommendations only. Similarly, the BSI Protection Profiles [3, 4] 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.

The electric grid is perhaps the most critical infrastructure today, and thus safety, i.e., reliability and availability, is a top priority. Potential vulnerabilities of smart metering systems – and the grid in general – are widely discussed topics [9, 8, 22]. As a consequence, many research works focus on quite small (technical) parts of the overall smart grid architecture. For instance, data communication security controls (e.g., cryptographic functions such as encryption, message authentication codes, and digital signatures) provide standard security services in terms of confidentiality, integrity, and accountability of messages and their origin [5]. Others deal with effective key distribution [21] and management for devices with very limited computational power [9] to enable efficient encryption of meter readings and access control (similar to Pay-TV access control systems [21]). Yan et al., Mohan et al. and Vigo et al. provide an overview of security mechanisms for smart grids and smart meters [23, 10, 20]. 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 currently or will be part of near-future implementations.

The Smart Grid Coordination Group formed by the European standards organizations CEN, CENELEC and ETSI has provided a comprehensive framework on smart grids in response to the EU Smart Grid Mandate M/490 [16]. 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. Additionally, 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. The assessment is carried out under the assumption that no security controls whatsoever are in place. Compared to the work carried out by the SGIS group within M/490, our main goal was to develop a practical risk assessment approach for smart grid systems that are currently deployed or will be deployed in the near future. Our approach should be readily applicable by utilities in contrast to more formal approaches as suggested for example in [13, 19].

3. SMART GRID RISK MANAGEMENT APPROACH

Most efforts on smart grid security either deal with threats and vulnerabilities on an abstract, high architectural level, or focus on very specific technical aspects, e.g., encryption or authentication, without considering the overall picture.

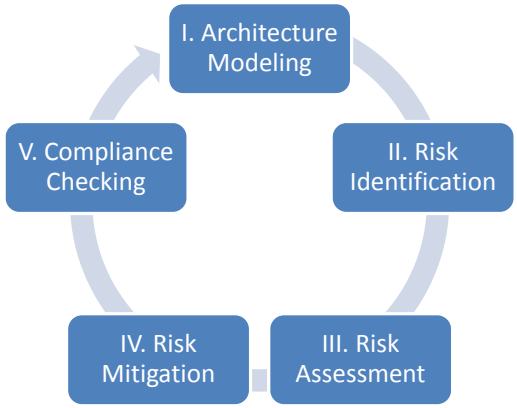

Figure 1: Architecture-driven Smart Grid Risk Management Approach

Our proposed smart grid risk management approach therefore aims at bridging the gap between a high-level architectural view and specific technical security measures. For that purpose, it employs a five-step cyclic process model depicted in Fig. 1, which consists of the following phases:

I. Architecture Modeling
II. Risk Identification
III. Risk Assessment
IV. Risk Mitigation
V. Compliance Checking

First, it allows DSOs (distribution systems operators) to map their deployed components to the standard architecture model SGAM. This phase is crucial to get a holistic view on the deployed components and their underlying technologies

in a standardized and structured manner. The second phase subsequently enables a sophisticated risk identification and a later risk assessment. Based on the concrete technologies employed, specific technical controls (in addition to organizational measures) can be applied to mitigate the identified risk. If, for instance, the architectural model reveals insufficiently secured communication lines, potential technical mitigation measures are to use stronger authentication and encryption methods. Eventually, in the fifth phase, compliance to technological guidelines, regulations and corporate strategy needs to be ensured in order to avoid undesired secondary effects of mitigation measures. The whole model, from phase I to V, is cyclic since every mitigation action will eventually cause adaptations of the architecture, which need to be reflected in the model maintained in phase I. Following these phases, our approach is able to provide concrete technical solutions without losing a connection to the overall picture. In the following paragraphs, we explain each phase more closely.

3.1 Architecture Modeling using SGAM

In order to model smart grid architectures, we employ the Smart Grid Architecture Model (SGAM) [17]. The SGAM model was originally intended to identify standardization gaps in smart grid standardization processes. The model is structured in zones and domains. The *zones* are derived from hierarchical automation system models that classify systems into Field, Process and Station towards Operation, Enterprise and Market level [14]. The *domains* reflect power-grid-specific domains ranging from the Customer, Distributed Energy Resources (DER), Distribution and Transmission to the Generation domain. In contrast to the NIST Smart Grid Framework [11], SGAM features a dedicated DER domain, in which small distributed generators with their special infrastructure find their place. Finally, in the third dimension, SGAM has *interoperability layers* that highlight different aspects of networked smart grid systems from hard- and software components over communication links and protocols up to functional and business layers. We used SGAM as a means for visualizing and comparing different smart grid automation architectures and depicting existing and near-future smart grid architectures (see Fig. 2). A more detailed description of our architecture model can be found in [7].

3.2 Risk Identification

In order to identify risks that can occur within smart grid environments, we compiled a threat catalog focusing on technical threats. Since the threat catalog should build upon a well-established source of ICT-related security threats, we used the IT Baseline Protection Catalogs [2] as our main source. Threats quoted in the smart-grid-specific Protection Profiles [3, 4] were also taken into account. We focused on technical threats and thus omitted organizational threats or force majeure. All remaining threats were checked for their generic applicability in smart grid environments and filtered accordingly. As some of the threats in the BSI Catalogs are very specific while others are more generic, we adapted the threats to the smart grid scenario and merged them into a practically usable threat catalog comprising 31 threats (see Table 1). These threats were subsequently interpreted in the smart grid context and grouped into the following clusters:

- Authentication / Authorization

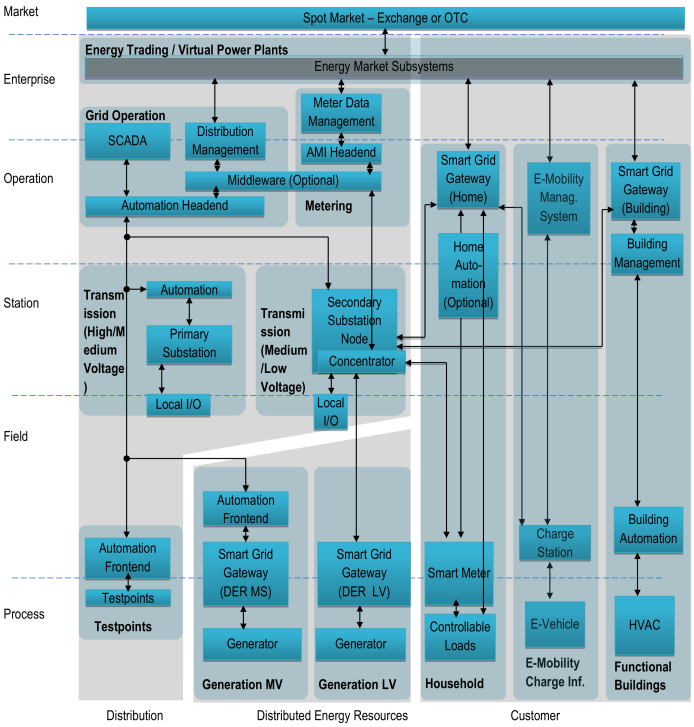

Figure 2: Proposed Architecture Model

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

Since the threats in the threat catalog are kept in a generic form, there is no need to adapt the threat catalog in case the smart grid architecture model (see Section 3.1) changes.

3.3 Risk Assessment

In the next phase, the threats identified in phase II are applied to the architecture components which have been defined in phase I. For each component and threat, we evaluated both the likelihood as well as the impact of a threat to occur. Both probability and impact were measured on a five-level scale ranging from very low (level 1) to very high (level 5), depending on the frequency and range of successful attacks. However, while this could be exercised on all smart grid components in the SGAM model, it would quickly become impractical due to the high number of elements in the threat matrix. For this reason, we decided to cluster smart grid components into the following building blocks (cf. Figure 2:

- Functional Buildings
- E-Mobility & Charge Infrastructure
- Customer Premises
- Generation Low Voltage
- Generation Medium Voltage
- Test Points
- Transmission (High/Medium Voltage)
- Transmission (Medium/Low Voltage)
- Grid Operation

Threat Category	Threat
Authentication / Authorization	Defective or missing authentication or inappropriate handling of authentication data Defective authorization
Confidentiality	Defective key management Disclosure of sensitive data Insecure encryption methods or parameters
Integrity / Availability	Outage or disruption of IT systems Outage or disruption of networks or network components Outage or disruption of supply networks Tampering with devices Tampering with data Loss or corruption of data due to physical factors Loss or corruption of data due to misuse or negligence Fee fraud
Internal / External Interfaces	Illegal physical interfaces Illegal logical interfaces Incompatibilities between systems or (network) components
Maintenance / System Status	Operation of unregistered or insecure components or components which provide unnecessary services Missing or inadequate maintenance Insufficient anomaly detection Insufficient dimensioning Security issues during software migration Insufficient monitoring and controlling capabilities Faulty use or administration of IT systems Faulty time synchronization Faulty data synchronization Uncontrolled cascading effects
Missing / Inadequate Security Controls	Defective or missing security controls in networks Defective or missing security controls in software products Software vulnerabilities or bugs Use of insecure protocols Failure or disruption of safety controls

Table 1: Threat Catalog

- Metering

In case of considerably different smart grid architectures and models, these building blocks might differ and would need to be adapted accordingly. However, in the common case there is no need for adaptation due to the generic form of the threats and building blocks.

Severity

Probability \ Severity	1	1,5	2	2,5	3	3,5	4	4,5	5
1	1	1,5	2	2,5	3	3,5	4	4,5	5
1,5	1,5	2,25	3	3,75	4,5	5,25	6	6,75	7,5
2	2	3	4	5	6	7	8	9	10
2,5	2,5	3,75	5	6,25	7,5	8,75	10	11,25	12,5
3	3	4,5	6	7,5	9	10,5	12	13,5	15
3,5	3,5	5,25	7	8,75	10,5	12,25	14	15,75	17,5
4	4	6	8	10	12	14	16	18	20
4,5	4,5	6,75	9	11,25	13,5	15,75	18	20,25	22,5
5	5	7,5	10	12,5	15	17,5	20	22,5	25

Figure 3: Assessing the Risk Potential

The result is a risk matrix showing the risk potential for all building blocks in the modeled smart grid environment. Depending on its value (i.e., probability level multiplied by impact level), the risk potential has been defined as low (green), medium (yellow) and high (red), see Fig. 3. This approach allowed us to identify potentially high risks in European smart grids. For high-risk domains it is advisable to identify the individual smart grid components causing the high risk potential, therefore, we are currently performing technical security audits (see Section 4).

3.4 Risk Mitigation

Based on the risks identified in phase II and assessed in phase III of our smart grid risk management approach, mitigation strategies are subsequently developed in phase IV. The goal of the mitigation strategies is to either decrease the probability of a successful attack, or to alleviate its impact, possibly also both at the same time. We are currently identifying suitable mitigation actions for the individual risks by addressing each of the 31 threats individually. For each threat, generic measures are first defined (such as introducing a Public Key Infrastructure to counter risks that emerge from insecure handling of cryptographic keys). Subsequently, specific measures for the individual architecture building blocks (see Section 3.3) are identified. We are focusing on mitigation actions suitable for establishing a basic level of protection in order to ensure a broad application among the utilities. Additionally, advanced controls for a higher security level are defined, which can be implemented by utilities with more mature security management processes.

3.5 Compliance Check

In order to maintain a high level of the overall smart grid system security, it is important to include automated security compliance checks. These checks should be run against all infrastructure components. Depending on the component type, the tool should check whether the device configuration (such as the firmware version or the currently deployed configuration file) adheres to the latest protection and mitigation strategies. If not, the tool can identify specific components that need to be updated accordingly. Since a single vulnerable component in the smart grid can compromise overall system security, it is highly important that all deployed system components are known to the automated checking tool. We thus advise utilities to include the tool setup into the regular deployment processes.

4. EVALUATION AND DISCUSSION

The following section describes the findings we came up with when applying our five-step risk management approach together with distribution systems operators, and comments on the necessity of complementing the theoretical approach with practical security audits.

Risk Landscape. The risk management approach outined in Section 3 allowed us to identify areas (i.e. architecture components) in European smart grids which show high risk potential in terms of cyber attacks. Specifically, our analysis showed that there are significant risks in the Functional Buildings, Customer Premises and Grid Operation domains. Regarding centralized components such as the Grid Operation and SCADA system, the probability of a security breach is relatively low as an outside attacker typically has no physical access to these components. Moreover, protection mechanisms are not prone to cost pressure on this level. However, once an attacker manages to get access to these systems, the negative impact will eventually be high; for instance, shutting down a primary substation node could affect whole city districts.

In contrast, security breaches targeted on decentralized components, which are deployed typically in the Functional Buildings and Customer Premises domain, are much more likely as attackers can easily get hold of these components. Attacks on these components are facilitated by the fact that the Smart Grid Gateways are accessible via Internet, and a lack of software security or a misconfiguration may be easily exploited. While the probability of an attack is high, the impact is expected to be limited at first. This may however turn out wrong as soon as a successful smart meter mass attack is published on the Internet, potentially leading to unanticipated cascading effects in the power grid. Thus, not only the probability, but also the impact of a successful attack occurring within the so-called "last mile" are possibly high, which explains the high risk potential.

Our analysis showed that a general risk affecting most of the architecture domains is a lack of secure authentication methods. A potential consequence is that system components accept malicious data or control commands from unauthorized sources, which could have strong negative impacts on grid stability. We therefore recommend broad use of standardized authentication mechanisms such as digital certificates, role-based access control, and two-way authentication for remote maintenance access points.

Security Audits. For high risk domains, it is advisable to identify the individual smart grid components causing the high risk potential. For these components, individual technical security audits should be performed by independent auditors in order to assess the technical risks and their reasons. According to the risk potential, we suggest two types of security audits.

The first type of security audit is a typical network and lightweight software security audit. For the chosen smart grid component (i.e. a smart meter), it focuses on network and communication security. Similarly, the lightweight software security audit analyzes how the component's software implementation reacts on security test inputs such as maliciously modified network communication or test input generated through fuzz testing. However, the monitoring of the component's software is limited to the communication with the device. For instance, if a test case leads to an unexpected device response or a crash, a potential vulnerability is identified, but it is not further investigated due to the limited technical access on the device hard- and software internals. The audit is thus feasible with limited resources such as limited time or device access.

The second type of security audit is an in-depth hard- and software security audit starting at the point where the first audit type ends. The audit includes a low level hard- and software security analysis including hardware disassembly, physical port accesses as well as both static and dynamic software analysis. In comparison to the lightweight audit, this type of analysis is extremely powerful and can uncover a wide range of vulnerabilities. Besides, it is also possible to demonstrate proof-of-concept attacks and estimate the severity of these attacks on a larger scale. The drawback of the analysis type is the high effort with respect to analysis time and costs as well as the requirement of a dedicated test system that can be physically dissembled and possibly damaged in course of the analysis.

For instance, our analysis showed that smart meters have a high risk potential, mainly due to the easy physical accessibility by attackers as well as the severity of potential large-scale attacks. Due to the requirement of a testbed, we set out to create a security test system comprising a smart meter, a PLC Data Concentrator as well as a Headend system. On this test system, we are currently performing lightweight analyses on the components. Due to the high risk potential, the smart meter is also subject to an in-depth hardware and software security audit. This allows us to get a spot sample of how secure these systems are currently, and to develop tailored mitigation strategies.

5. CONCLUSION AND FUTURE WORK

We have presented an architecture-driven approach for smart grid risk management capable of bridging the gap between a high-level architectural view and specific technical security measures. Our approach cannot replace a risk analysis per se, as technical smart grid implementations and employed products differ significantly between users such as utilities or energy providers. It is, however, the first step in a utility-centric smart grid risk analysis that needs to include low-level technical implementation specifics as well, and may help users to identify areas with high risk potential, and to focus the mitigation actions on them.

Future smart grids will integrate a wide variety of different technologies. Therefore, the crucial challenges are to

make sure that cybersecurity and interoperability requirements are satisfied. We argue that these issues can only be solved by a national smart grid reference architecture. Such a reference architecture would specify the minimum security requirements for the individual components and make sure that devices are carefully designed in accordance with them. At the same time, seamless interoperability would be ensured by defining appropriate interfaces. Individual implementations could still be derived from the reference architecture by instantiating specific domains.

Currently, there are no obligations for device vendors and utility providers to stick to the recommendations and guidelines published by existing standardization bodies. Therefore, a corresponding legal and regulatory framework should ensure that the minimum requirements defined by the reference architecture are followed. On the other hand, it must be ensured that the reference architecture is not only followed due to legal obligation, but rather broadly accepted by the different stakeholders. Therefore, all relevant stakeholders must be adequately involved in the process of establishing the reference architecture from the very beginning.

6. ACKNOWLEDGEMENT

This work has been partly funded by the project $(SG)^2$ under national FFG grant number 836276 through the KIRAS security research program run by FFG and BMVIT.

7. REFERENCES

[1] S. M. Amin and B. F. Wollenberg. Toward a smart grid: power delivery for the 21st century. *IEEE Power and Energy Magazine*, 3(5):34–41, Sept. 2005.

[2] BSI. IT Baseline Protection Catalogs. `http://www.bsi.bund.de/gshb`, 2013.

[3] BSI. Protection Profile for the Gateway of a Smart Metering System. BSI-CC-PP-0073, 2013.

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

[5] R. DeBlasio and C. Tom. Standards for the smart grid. In *IEEE Energy 2030 Conference*, pages 1–7, 2008.

[6] 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`, December 2012.

[7] M. Kammerstetter, L. Langer, F. Skopik, F. Kupzog, and W. Kastner. Practical risk assessment using a cumulative smart grid model. In *3rd International Conference on Smart Grids and Green IT Systems (SMARTGREENS), April 3-4 2014, Barcelona, Spain*, 2014. To appear.

[8] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke. Smart-grid security issues. *IEEE Security & Privacy*, 8(1):81–85, 2010.

[9] A. R. Metke and R. L. Ekl. Security technology for smart grid networks. *IEEE Transactions on Smart Grid*, 1(1):99–107, 2010.

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

[11] NIST. NIST Special Publication 1108R2 - NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0, 2013.

[12] NIST. NISTIR 7628 - Guidelines for Smart Grid Cybersecurity, 2013.

[13] P. Ray, R. Harnoor, and M. Hentea. Smart power grid security: A unified risk management approach. In *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on*, pages 276–285, 2010.

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

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

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

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

[18] L. H. Tsoukalas and R. Gao. From smart grids to an energy internet: Assumptions, architectures and requirements. In *DRPT*, pages 94–98, 2008.

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

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

[21] S.-Y. Wang and C.-S. Laih. Efficient key distribution for access control in pay-tv systems. *IEEE Transactions on Multimedia*, 10(3):480–492, 2008.

[22] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde. An integrated security system of protecting smart grid against cyber attacks. In *Innovative Smart Grid Tech.*, pages 1–7, Jan. 2010.

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