Towards Security Software Engineering the Smart Grid as a System of Systems

Vanea Chiprianov, Laurent Gallon, Khouloud Salameh, Manuel Munier, Richard Chbeir, Jamal El Hachem

Towards Security Software Engineering the Smart Grid as a System of Systems

Vanea Chiprianov*, Laurent Gallon*, Khouloud Salameh*, Manuel Munier*, Richard Chbeir*, Jamal El Hachem*
*LIUPPA, Univ Pau & Pays Adour, Mont de Marsan, France, Email: vanea.chiprianov@univ-pau.fr

***Abstract*—The Smart Grid, the next generation power grid, comes with promises of widely distributed automated energy delivery, self-monitoring, self-healing, energy efficiency, utility and cost optimization. However, as attacks on the current power grid and similar systems indicate, the Smart Grid will be vulnerable to all kinds of attacks and will even raise new security challenges, due to its complex nature. In this paper we analyze this complexity of the Smart Grid as a System of Systems, and the specific security challenges it raises. To address these challenges we propose a vision/framework based on principles of Software Engineering. This framework structures and brings together the research on Smart Grid security.**

I. Introduction

The Smart Grid (SG) is an enhancement of the 20^{th} century power grid [1]. While traditional power grids generally carry power from central generators to customers, the SG uses two-way flows of electricity and information to create an automated and distributed energy delivery network. While the information flow enables capabilites like self-monitoring, self-healing and energy efficiency, such a heavy dependence on ICT surrenders the SG to vulnerabilities associated with ICT.

This increases the risk of compromising reliable and secure power system operation, which is the ultimate objective of the SG. Therefore, cyber security is regarded as one of the biggest challenges in the SG [2]. Attacks on the current power grid and similar systems have raised a strong awareness about the possible severe consequences these may have in the SG, from customer information leakage to a cascade of failures, such as massive blackout. For example, the North American Equipment Council reported the effects of a slammer worm on the power utilities [3]; Stuxnet has shown how a stealthy attack targeting both hardware and software is possible [4].

Some of these new security challenges raise from the big number of composing elements of the SG, their interactions and the new capabilities these interactions generate. All these indicate that the SG is a System of System (SoS). In what follows, we present the main characteristics of the SG and analyze it as an SoS, in Section II. We then identify, analyze and classify security challenges and solutions in the SG, according to the specific characteristics of SoS, in Section III. To address them, we introduce a vision/framework/roadmap based on principles of Software Engineering, in Section IV.

II. The Smart Grid as an SoS

We introduce the main components of the SG, the specific characteristics of SoS and analyze how the SG is an SoS.

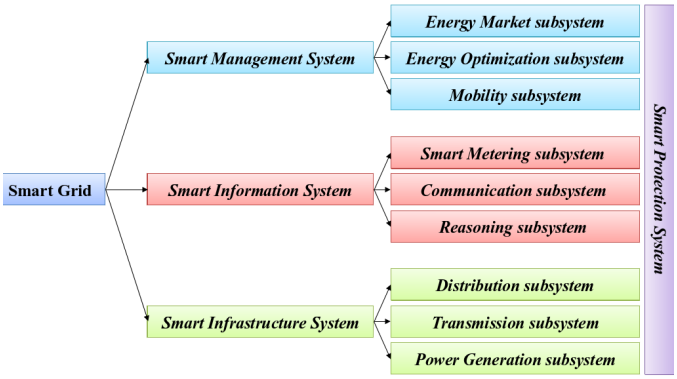

Fig. 1. Smart Grid framework.

A. The Smart Grid

An SG is a modernized electrical grid that uses ICT to gather and act on information in an automated fashion, to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity. To realize these advantages, SG architectures have been proposed, e.g. [5]. Based on the GridWise architecture [6] and the description presented in [1], we define our vision of the SG (cf. Figure 1).

A closer look at the SG functioning leads us to define four basic systems, namely: i) Smart Infrastructure System, ii) Smart Information System, iii) Smart Management System, and iv) Smart Protection System. The key success of the SG lies on maintaining a seamless interaction and data exchange between its CSs. We detail each in the following.

1) Smart Infrastructure System: Its focus lies in the energy system, consisting of the following subsystems:

a) Power Generation subsystem: due to the support of two flows of electricity, new power generation paradigms are enabled. They comprise:

i) Distributed Energy Resources: include small scale power generation like solar panels, combined heat and power or cogeneration systems, wind turbines, micro turbines, back-up generators and energy storage. Storage elements can be deployed every where in the SG: power generation, transmission, distribution, and customers (e.g. electric vehicle batteries). They can be seen as a distributed storage system, which helps balance energy consumption and production. The storage system is critical for the SG, and must be highly secured.

ii) Virtual Power Plants: an aggregation of customers (e.g. residential, commercial, industrial, etc.) under one type

of Pricing, Demand Response or Distributed Energy Resource program. Their distributed generators may have a total capacity comparable to that of a conventional plant.

iii) Grid-to-Vehicle and Vehicle-to-Grid: electric vehicles with energy stored in batteries could perform a variety of services while connected to the power grid. In Grid-to-Vehicle, vehicles need to be charged after the batteries deplete. The charging operation leads to a significant new load on the existing distribution grids. In Vehicle-to-Grid, vehicles provide a new way to store and supply electric power. The two concepts are related. For example, vehicles can be used to provide power to help balance loads by "peak shaving" (sending power back to the grid when demand is high) but also "valley filling" (charging when demand is low).

b) Transmission subsystem: responsible for moving the power over long distances to substations. The generated electric power is stepped up to a higher voltage for transmission. Upon arrival at a substation, the power is stepped down from the transmission level voltage to a distribution level voltage.

c) Distribution subsystem: upon arrival at the service location, the power is stepped down again from the distribution voltage to the required service voltage(s).

2) Smart Information System: In this system, the information exchanged between the SG components can be found. This information is processed by several subsystems:

a) Smart Metering subsystem: a smart meter is usually an electrical meter that records consumption in intervals of an hour or less and sends that information at least daily back to the utility for monitoring and billing. It has also the ability to disconnect and reconnect remotely and control the user appliances and devices in order to manage loads and demands.

b) Communication subsystem: is responsible for communication connectivity and information transmission among systems, devices, and applications. It will leverage existing wireless and wired communication technologies. The Supervisory Control and Data Acquisition (SCADA) system is a power operation monitoring system across the management, transmission, and distribution domains.

c) Reasoning subsystem: after receiving the data extracted from smart meters, the role of this subsystem is essential in translating it semantically, providing a shared understanding of the information exchanged in the SG domain and allowing its CSs to reason and act autonomously.

3) Smart Management System: Uses information extracted from the Smart Information System to provide advanced management and control services and functionalities using:

a) Energy Market subsystem: negotiates the energy price between the consumers and the producers with the goal of reaching the optimal balance in energy production and consumption at any given point in time.

b) Energy Optimization subsystem: applies optimization techniques, to maximize the utility function of each SG CS.

c) Mobility subsystem: bearing in mind the mobility of SG components (e.g. electric vehicles), this subsystem handles their operations even during their displacements.

4) Smart Protection System: Transversal to the other systems, provides grid reliability analysis, failure protection, and security and privacy protection services. The Security and Privacy part will form the focus of what follows in this paper.

The SG is a complex system, with significant differences in terms of new components, new interactions and capabilities, when compared to the traditional power grid. To analyze this complexity, we use concepts related to Systems of Systems.

B. Systems of Systems

Systems of Systems (SoSs) [7] are large and complex systems, composed of several independent, concurrent and distributed Constituent Systems (CSs), although numerous definitions for SoS have been advanced (e.g. cf. [8]). SoSs have been identified [9] in defence and national security, earth observation systems, space systems, modelling and simulation, sensor network, healthcare, electric power grid, business information system, transportation system and astronomy.

Several characteristics that differentiate SoSs from monolithic systems have been identified. For example, it is well accepted that SoSs are characterised by the fact that the CSs are *independent from an operational and managerial* point of view, that the SoS does not appear fully formed, but rather its *development is evolutionary*, with functions and purposes added, removed, and modified with experience, by the fact that the functions and purposes of the SoS do not reside in the CSs, but rather *emerge* from the entire SoS, and finally by the large *geographic extent* of the CSs [10]. Other sets of characteristics of SoS, partially overlapping, have been identified, e.g. [11]: autonomy, belonging, connectivity, diversity, emergence.

Using the management criterion, SoS have been categorized into [10]: (1) Directed: CSs operate subordinated to the central managed purpose; (2) Collaborative: CSs voluntarily collaborate to fulfill the agreed central purposes; (3) Acknowledge: there are recognized objectives, a designated manager, and resources for the SoS; (4) Virtual: lack of a central management authority and a centrally agreed purpose for the SoS.

C. The Smart Grid as an SoS

A study [12] analyses the SG according to the five criteria that differentiate SoSs from monolithic systems: (i) Operational and managerial independence: the SG is constituted from systems such as solar, wind plants, swarms of electric vehicles, which operate on their own and have different owners and managers. (ii) Evolutionary development: different energy generating systems can be dynamically aggregated/removed to/from the power grid. (iii) Emergent behaviour: producers, providers and consumers coordinate in order to balance supply and demand. (iv) Geographic distribution: the energy generation, storage, and consumption should be realized as near as possible to the physical location of consumption/generation in order to achieve greater efficiency of the system. This requires a shift from current centralized energy infrastructures towards more distributed ones. The study concludes that the SG is a Collaborative/Acknowledge SoS that integrates other SoSs, which have operational and managerial independence.

III. Security Challenges to the SG as an SoS

Traditionally, security deals with confidentiality, integrity and availability [13]. Related to these, the high-level SG security objectives identified by [14] are: i) *Availability*: ensuring timely and reliable access to information. Its loss means the disruption of access to information, which may further undermine power delivery. ii) *Integrity*: guarding against improper information modification or destruction. It is essential to ensure non-repudiation and authenticity. Its loss may induce incorrect decisions regarding power management. iii) *Confidentiality*: preserving autorisations on information access. It is necessary for the protection of proprietary information and personal privacy. In the SG, availability is more important than integrity, which is more important than confidentiality [15], [16]. In what follows we analyse challenges to assuring these security objectives, challenges raised by the characteristics that differentiate the SG SoS from monolithic systems.

A. Operational independence challenges

a) Identification, authentication and access control: The SG infrastructure incorporates millions of electronic devices and users. Identification and authentication is the key process of verifying the identity of a device or user as a prerequisite for granting access to resources in the SG information system. To meet these requirements, *every* node (cf. Availability objective) in the SG must have at least basic cryptographic functions, such as symmetric and asymmetric cryptographic primitives, to perform data encryption and authentication [16]. A review on how encryption, authentication, and access control can be added to current communications is presented in [17].

b) Device security issues: Each of the key components of the SG may have its specific vulnerabilities [14]. For the *smart meter*: customer tariff varies on individuals, and thus, breaches of the metering database may lead to alternate bills; functions like remote (dis)connect and outage reporting may be used by unwarranted third parties. Possible solutions may include: ensuring the integrity of meter data; detecting unauthorized changes on meter; authorizing all accesses to/from smart meter networks. *Electric vehicles* can be charged at different locations, thus inaccurate billing or unwarranted service will disrupt operations of the market. Possible solutions include establishing electric vehicle standards. For *SCADA* [15]: intercepting, tampering, or forging distribution control commands or access logs; synchronizing time-tagged data in wide areas; improper models for decision making; inconsistent agreement on load control; false forecasts. Possible solutions may include: ensuring commands and log files are accurate and secure; using a common time reference (GPS time-stamped) for time synchronization; using multi-layer intrusion detection.

B. Managerial independence challenges

c) Accountability: It means that the system is recordable and traceable. Even if a security issue appears, the accountability mechanism determines who is responsible for it, be it a user or an organisation managing a part of the SG. This is especially important because the SG involves different organizations, each with its own business objectives and regulatory requirements depending on the country in which it is based and in which it operates. This part of security concerns both the energy and the information. All records can be used as evidence in future judgment. Under such a circumstance, no one can deny their actions, not even the administrators or other users with high privileges. Together with some suitable punishments or laws, this will prevent many attacks [15]. Additionnaly, it can be used to determine the cause or extent of damage from an attack or failure, in digital forensics.

C. Evolutionary development challenges

d) Backwards compatibility: Compatibility problems could emerge while integrating legacy devices (of the traditional power network) into the SG, which may cause the system to fail or malfunction [14].

e) Secure and efficient communication protocols: Differing from conventional networks (e.g. Internet), message delivery requires both time-criticality (from legacy power grid) and security in the SG, in particular in Distribution and Transmission Grids. Tradeoffs are required to balance communication efficiency and information security in the design of communications protocols and architectures for the SG [16]. Therefore, the impacts of security protections need to be minimized and their timing made predictable [15].

f) Co-design of control and security: Industrial control normally does not do too much about security. Recently, some attention has been dedicated to it. Co-design of control and security in the SG will be interesting in the future [15].

D. Emergent behaviour challenges

g) Hidden vulnerabilities due to interdependencies: Ensuring the management objectives of the Smart Management System (e.g. energy efficiency) involves interactions between several CSs of the SG SoS. This makes these objectives exposed to chains which include vulnerabilities specific to each CS, and which could be exploited when the CSs interact to realize a management objective. Possible solutions include continuous (real-time) monitoring to identify them [18]. In this way, attacks can be detected in time and appropriate actions can be taken quickly through a rapid restoration plan.

E. Geographic distribution challenges

h) Attack detection: The SG features a relatively open communication network over large geographical areas. Accordingly, it is almost impossible to ensure every part or node in the SG to be invulnerable to network attacks. Therefore, the communication network needs to consistently perform profiling, testing and comparison to monitor network traffic status such as to detect and identify abnormal incidents due to attacks [16]. Types of attacks targeting:

1) *Availability*: The most important type of attack is *Denial of Service (DoS)* - the attempt to delay, block or corrupt the communication in the SG. It can appear at all layers: physical - channel jamming, MAC - ARP spoofing, network

and transport - traffic and buffer flooding and application; for a literature review of these attacks in the SG, consult e.g. [16]. In the SG, a DoS attacker does not need to completely shut down network access by using some extreme means (e.g. all-time jamming) but instead it may launch weaker versions of attacks to intentionally delay the transmission of a time-critical message to violate its timing requirements. Therefore, the goals of DoS attacks in the SG include not only disrupting the resource access but also violating the timing requirements of critical message exchange. To model the impact of DoS attacks in Distribution and Transmission Grids, message-oriented metrics, which not only characterize the end-to-end message delay but also reflect the delay constraints, should be properly defined. Assessing the risk of large DoS attacks is reviewed in [16], which concludes that it is quite difficult for Probabilistic Risk Assessment to estimate the probability of potential large-scale DoS attacks against the Smart Grid, as there is no historic data for profiling; also graph and security metric assessments are not able to demonstrate to what extent a DoS attack would undermine the power system with respect to time-critical messages; therefore accurate risk assessment of such attacks remains a challenging issue.

2) *Integrity*: Attacks aim at deliberately and illegally modifying or disrupting data exchange in the SG. They occur generally at the application layer. The target can be customers' information (e.g. pricing information and account balance) or status values of power systems (e.g. voltage readings and device running status). The *false data injection* attacks against power grids, discovered and designed in [19], have drawn increasing attention. Research on false data injection attacks has become an active and challenging field in SG security. This research is classified e.g. in [16] into attacks against: DC SCADA and AC SCADA, impacting the state estimation, and against the electric market, with potential financial loses.

3) *Confidentiality*: Attacks intend to acquire unauthorized information from network resources in the SG. The attackers *eavesdrop* on communication channels to acquire information such as a customer's account number, personal profiles of customers which can be used to detect whether people use specific facilities. Such abuses may allow a malicious person to know whether or not you are at home, know your working hours, or if you are away on vacation. The thief could then visit your home without fear of being caught! These attacks have low impact on the functionality of the SG, but very high on customer privacy [1], and social concerns have received more and more attention in recent years. Examples include wiretappers and traffic analyzers [16]. These issues may be addressed [15] by anonymous communication technologies. However, to effectively implement these anonymisation mechanisms, it is first necessary to have clearly identified the information to be protected, the inferences to be avoided, and computations to perform on such anonymised data. Moreover, these technologies may cause overhead or delay issues. In addition, network traffic camouflage techniques could be considered to hide critical entities (e.g. database, control center) in the grid.

IV. Roadmap/Vision/Framework for Security Software Engineering the Smart Grid as an SoS

Having identified and analysed security challenges specific to the SoS nature of the SG, we have also seen that addressing them involves a multitude of solutions. How could these solutions be integrated into a more complete framework? One such vision could be similar to the one described in [1] for management applications and services. This proposes the "Smart Grid Store", an integrated platform in which many management applications and services are available online. Users can choose their expected services and download them. Of course, verifications of interoperability and compatibility are necessary as well. A similar integrated platform can be envisioned for security solutions. To build such a platform, principles of Software Engineering could be used.

Software Engineering deals with systematic methods, life-cycle processes and tools for defining software. As the SG is a cyber-physical system [17], Software Engineering is useful at addressing especially the cyber/software security challenges, and the impacts of physical security challenges on the cyber part, but it will be limited when addressing challenges specific to the physical nature of the SG.

A. Life-cycle Management

The main challenge for managing the life-cycle of the SG is taking into account the legacy system of the traditional power grid. If we consider the traditional power grid as the first iteration, and the SG as the second iteration, we may consider that an iterative, spiral development process describes the life-cycle of the SG SoS. Such a spiral process begins with considering the requirements of the new iteration, developing an architecture to fulfill them, implementing it in code, verifying the code and releasing the new iteration.

B. Requirements

The requirements of the second iteration in developing the SG need to both integrate the characteristics of the legacy power grid, and fulfill the expectations for the new SG. Examples of legacy characteristics that influence security include high restrictions on transmission delay and failures; e.g. delay constraints for messages for substantion communication in IEC 61850, range from 3 ms to 500 ms. This is directly related to the *backwards compatibility* and *co-design* challenges.

In the requirements phase, risk management is usually performed. Security-related risks are part of SG risk identification and mitigation. In this work we focus not on the management of risks inherent to the industrial activity itself, but on risks regarding the security of information. These include new security risks resulting from new capabilities composed from interacting CSs, as well as any residual security risk of CSs [20]. How to identify and mitigate risks associated with end-to-end flow of information and control in the SG, without, if possible, focusing on risks internal to individual systems? While there are standards for risk management of standalone systems [21], there are not for SoS. To what extent do they apply to the SG SoS? In the same way it is necessary to take

into account the operational independence of CSs in the design of the security of the SG SoS - the framework should enable the cooperation of various Information Security Management Systems for overall risk management.

For example, [22] applied SQUARE to identify security requirements for the SG. They concluded that, from an SoS perspective, it is necessary to increase the method's support for dealing with and resolution of conflicts between requirements. These conflicts could be caused by the fact that requirements come from different stakeholders, or by impacts between security and functional and other non-functional requirements.

C. Architecture

Any architecture of the SG will have to first describe the legacy power grid and then allow for modelling the mechanisms that implement the expectations of the new SG. The same applies for the security architecture. Features of the SG, such as heterogeneous devices and network architecture and delay constraints on different time scales, make it impractical to uniformly deploy strong security approaches all over the SG. Consequently, the SG requires fine-grained security solutions designed for distinct network applications [16]. How to choose between them, how to use them together? Tradeoff analysis of security mechanisms is necessary.

A key architectural tool in this respect may be the use of predictive modelling and simulation to compare architectural alternatives, "what-if" scenarios [23]. Alternative architectures would need to be carefully considered and modelled to ensure the SG is not compromised or undesirable emergent behaviours result, or the security requirements are not met. A review of simulation challenges, techniques, and future trends in the SG is performed in [24]. Among simulation techniques, event-based has been considered as particularly well suited due to its enabling loose couplings [25].

D. Implementation

If the architecture is described using Model-driven languages and tools, this will enable readily code generation. However, specific issues will persist. One such issue is related to information management (in the Smart Information Subsystem of the Smart Infrastructure System).Information analysis, integration, and optimization in the SG will need Big Data approaches, as exemplified by [26].

E. Verification

As CSs of the SG will be defined by different organisations, this implies that certification and quality processes will be different. Still, common standards need to be agreed upon. Additionally, using simulation for creating descriptive architectures is useful for verifying them as well.

F. Release

The SG release process is triggered every time some aspect of the SG (including individual CSs) evolves. *Operational and managerial independence* properties mean that synchronisation between the CSs and their managing organisations may not be possible when updates are deployed. Special care needs to be taken, therefore, at each release to detect undesired *emergent behaviour*, so monitoring becomes essential. In some cases, evolution may impact the conformance to requirements. At runtime, it is important to ensure that the required levels of requirements (security, but also performance, etc.) are achieved. If not, re-engineering is required.

V. Related work

To identify works related to security challenges to the SG as an SoS, we performed a Systematic Literature Review (SLR) [27] For this, we searched the databases of Scopus, ACM Digital Library, IEEE Xplore Digital Library and SpringerLink, in title, abstract and keywords, using the search string: (challenge OR issue) AND security AND ("smart electrical grid" OR "smart power grid" OR "intelligent grid" OR intelligrid OR futuregrid OR intergrid OR intragrid) AND ("system of system" OR "system-of-system" OR "system of systems" OR "system-of-systems"). We included only papers in English, from the Computer Science domain, published all years. We excluded conference reviews. From the results, we excluded papers after reading their titles and abstracts, and deciding they are not sufficiently related to the research question. After reading these papers, we found among their references new studies pertinent for our research which were therefore added. The papers we finally retained are presented next in this section.

A clear disscussion and review of security issues in the SG and possible solutions to them, well structured around the three high-level objectives of availability, integrity and confidentialy, is presented in [16]. Another catalogue of challenges and possible solutions is furnished in [15]. A review of attacks and risks in the SG, analyzing the coupling between the power control applications and the cyber system is presented in [17]. Some security challenges in the SG and approaches to address them are presented in [18]. While these reviews consider the SG as a complex system, and even mention SoS, they do not analyse the security challenges for the SG by considering the specific characteristics that differentiate the SG as an SoS from monolithic systems, as we do.

[22] applies SQUARE to identify security requirements of the SG and analyses them from an SoS perspective. [28] applies Model Based Engineering to capturing security requirements of the SG analyzed from an SoS perspective. A risk analysis of the SG as an SoS [29] focuses on the increased dependence on GPS and the spoofing threaths this engenders for the SG. All these works focus on security requirements of the SG, while we address al phases of the life-cycle.

Some works focus on the security architecture of the SG. Challenges with respect to authentication and authorization of SG applications are discussed in [30], which proposes a reference architecture based on Service Oriented Architecture (SOA). However, this is limited to authentication and autorisation, and the SG is analyzed as an SoS just to identify loosely conected interfaces which supports the use of SOA. An SG simulation of a wireless ecosystem architecture, using OMNeT++, studied DoS attacks [31]. However, specific

challenges due to the SoS nature are not highlighted. Another simulation prototype, based on a testbed using customisable hardware and available software, is used in [32] to investigate mitigations to a blackout attack targetting the SG as an integrated system, an interconnected SoS.

A mathematical modelling of the SG as two complex interdependent networks: power and communication, interconnected by edges, enables analysis of random and selective attacks, which shows that the SG disintegrates faster for targeted attacks compared to random attacks [33].

The results of the SLR we performed show the number of works addressing the security of the SG as an SoS is quite reduced, but has increased recently, especially in 2014. However, most of them focus only on one phase of the development life-cycle of a security solution. Moreover, they focus on requirements and architecture phases, using (mathematical) modeling and simulation, but they do not address implementation, verification or release phases. This may be explained at least partially by the physical nature of the SG, which is costly to emulate, especially in an academic context, and suggests collaborations with industry would be highly desirable to have access to more realistic conditions.

VI. Conclusion

In this paper we discussed how specific characteristics of the SG SoS (operational and managerial independence; evolutionary development; emergent behaviour; and geographic distribution) raise challenges for security engineering. To address these vulnerabilities, we proposed a framework based on Software Engineering principles. This framework indicates directions which could be taken, based especially on modelling, simulation and code generation techniques.

References

[1] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid - the new and improved power grid: A survey," *Communications Surveys Tutorials, IEEE*, vol. 14, no. 4, pp. 944–980, Fourth 2012.

[2] "Nist framework and roadmap for smart grid interoperability standards, release 2.0," National Institute of Standards and Technology, Tech. Rep., 2012.

[3] "Sql slammer worm lessons learned for consideration by the electricity sector," North American Electric Reliability Council, Tech. Rep., 2003.

[4] D. Kushner, "The real story of stuxnet," *IEEE Spectrum*, 2013.

[5] E. Ancillotti, R. Bruno, and M. Conti, "The role of communication systems in smart grids: Architectures, technical solutions and research challenges," *Computer Communications*, vol. 36, no. 1718, pp. 1665–1697, 2013.

[6] D. P. Chassin and L. Kiesling, "Decentralized coordination through digital technology, dynamic pricing, and customer-driven control: The gridwise testbed demonstration project," *The Electricity Journal*, vol. 21, no. 8, pp. 51 – 59, 2008.

[7] M. Jamshidi, "System of systems engineering - new challenges for the 21st century," *Aerospace and Electronic Systems Magazine, IEEE*, vol. 23, no. 5, pp. 4–19, 2008.

[8] A. Gorod, R. Gove, B. Sauser, and J. Boardman, "System of Systems Management: A Network Management Approach," in *System of Systems Engineering. IEEE International Conference on*, April 2007, pp. 1–5.

[9] J. Klein and H. van Vliet, "A Systematic Review of System-of-systems Architecture Research," in *Proc. of the 9th Intl ACM Sigsoft Conf. on Quality of Software Architectures*, 2013, pp. 13–22.

[10] M. W. Maier, "Architecting principles for systems-of-systems," *Systems Engineering*, vol. 1, no. 4, pp. 267–284, 1998.

[11] J. Boardman and B. Sauser, "System of systems - the meaning of OF," in *System of Systems Engineering, IEEE/SMC Intl Conf. on*, 2006.

[12] J. Pérez, J. Díaz, J. Garbajosa, A. Yagüe, E. Gonzalez, and M. Lopez-Perea, "Large-scale smart grids as system of systems," in *Proc. 1st Intl Wksh on Software Engineering for Systems-of-Systems*, 2013, pp. 38–42.

[13] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," in *Dependable and Secure Computing, IEEE Trans, vol.1, no.1, pp.11-33*, 2004.

[14] "Guidelines for smart grid cyber security," NISTIR 7628, Tech. Rep., 2010.

[15] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *Communications Surveys Tutorials, IEEE*, vol. 14, no. 4, pp. 981–997, Fourth 2012.

[16] W. Wang and Z. Lu, "Survey cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, 2013.

[17] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber physical system security for the electric power grid," *Proc. of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[18] A. Bari, J. Jiang, W. Saad, and A. Jaekel, "Challenges in the smart grid applications: An overview," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.

[19] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. of the 16th ACM Conf. on Computer and Communications Security*, 2009, pp. 21–32.

[20] J. Dahmann, G. Rebovich, M. McEvilley, and G. Turner, "Security engineering in a system of systems environment," in *Systems Conference (SysCon), 2013 IEEE Intl*, 2013, pp. 364–369.

[21] ISO/IEC, "ISO/IEC 27005:2011: Information security risk management," International Organization for Standardization (ISO), Geneva, Switzerland, Tech. Rep., 2011.

[22] N. Zafar, E. Arnautovic, A. Diabat, and D. Svetinovic, "System security requirements analysis:a smart grid case study," *Systems Engineering*, vol. 17, no. 1, pp. 77–88, 2014.

[23] I. Eusgeld, C. Nan, and S. Dietz, "System-of-systems approach for interdependent critical infrastructures ," *Reliability Engineering & System Safety*, vol. 96, no. 6, pp. 679 – 686, 2011.

[24] W. Li and X. Zhang, "Simulation of the smart grid communications: Challenges, techniques, and future trends," *Computers & Electrical Engineering*, vol. 40, no. 1, pp. 270 – 288, 2014.

[25] V. Chiprianov, K. Falkner, L. Gallon, and M. Munier, "Towards modelling and analysing non-functional properties of systems of systems," in *System of Systems Engineering, 9th Int. Conf. on*, 2014, pp. 289–294.

[26] B. K. Tannahill and M. Jamshidi, "System of systems and big data analytics bridging the gap," *Computers & Electrical Engineering*, vol. 40, no. 1, pp. 2 – 15, 2014.

[27] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering a systematic literature review," *Information and Software Technology*, vol. 51, no. 1, pp. 7 – 15, 2009.

[28] S. Lakshminarayanan and M. Souvannarnarth, "Applying model based systems engineering approach to smart grid software systems security requirements," *INCOSE Int. Symposium*, vol. 22, no. 1, pp. 13–20, 2012.

[29] K. Chen, C. Heckel-Jones, N. Maupin, S. Rubin, J. Bogdanor, Z. Guo, and Y. Haimes, "Risk analysis of gps-dependent critical infrastructure system of systems," in *Systems and Information Engineering Design Symposium (SIEDS), 2014*, April 2014, pp. 316–321.

[30] S. Lakshminarayanan, "Authentication and authorization for smart grid application interfaces," in *Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES*, March 2011, pp. 1–5.

[31] C. N. Pitas, C. E. Tsirakis, E. T. Zotou, and A. D. Panagopoulos, "Emerging communication technologies and security challenges in a smart grid wireless ecosystem," *Int. J. Wire. Mob. Comput.*, vol. 7, no. 3, pp. 231–245, 2014.

[32] B. Min and V. Varadharajan, "Design and analysis of security attacks against critical smart grid infrastructures," in *Engineering of Complex Computer Systems (ICECCS), 19th Intl. Conf. on*, 2014, pp. 59–68.

[33] S. Ruj and A. Pal, "Analyzing cascading failures in smart grids under random and targeted attacks," in *Advanced Information Networking and Applications (AINA), IEEE 28th Intl. Conf. on*, 2014, pp. 226–233.