2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing

Smart Grid Wireless Network Security Requirements Analysis

Khaja Altaf Ahmed, Zeyar Aung, and Davor Svetinovic
Computing and Information Science
Masdar Institute of Science and Technology
Abu Dhabi, UAE
Email: {kahmed,zaung,dsvetinovic}@masdar.ac.ae

***Abstract*—Power grids are being enhanced by integrating the Information and Communication Technology (ICT) to make them more reliable, economic, efficient, and environmentally friendly. The integration of power grids with ICT to build Smart Grids (SGs) has reduced costs and improved their performances. But, on the other hand, this has also brought the cyber security threats as well. In traditional ICT systems, the end devices are the powerful systems which have high computation power and memory capacity to perform the intense computations to avoid cyber security threats, whereas most of the end devices in SG lack these capabilities. Incorporating the security in the early stages of SG development through systems security requirements engineering can reduce the potential cyber security threats. This paper presents the results of applying Security Requirements Engineering Process (SREP) on the SG wireless network, and proposes the potential solutions that can be implemented such as using Global System for Mobile Communication (GSM)-enabled Intelligent Electronic Devices (IEDs) with Global Positioning System (GPS) support.**

I. Introduction

The success of any system relies on effectively capturing the stakeholders' needs in requirements specification [1], [2], [3]. Some studies show that the cost of adding the requirements in later stages of the system development could be 10 to 200 times higher [4], [5]. Jones et al. [6] propose that, in most of the system development projects, fixing the requirements, design and code defects cost 40% to 50% of the total system development efforts. In addition, more than 50% of the defects originate during the systems requirements engineering; if not done properly it can seriously impact the system. Flaws in requirements typically cost 25% to 40% of the total project costs [7]. This highlights the importance of the requirements specifications as the vital step in the systems development lifecycle. Similarly, security requirements also have greater impact on the fault-free functioning of any system.

Security is a quality attribute of a system. Most of the times, the functional requirements are clearly defined, but non-functional or quality requirements are ignored or added later on. Reliability, availability and robustness of the system depend on how secure a system is. Like functional requirements, security requirements too should be incorporated from the early stages of the systems development lifecycle. It is strongly advised by security experts, e.g, [8], [9], to add security requirements in the initial phases of system development, yet, it is not the common practice in industry up till now. In recent times, we have seen many security breaches even in the presence of the robust and reliable ICT systems. For example, Sony Inc. had to shut down the Playstation network for more than a week. The breach compromised 77 million customers personal information records, including 12.5 million credit cards records [10]. To incorporate security requirements engineering in early stages of the system development, various methods and techniques are available such as [11], [12], [13], [14].

Smart Grid (SG) is capable of converting the present power grid to an intelligent and complete autonomous structure. Almost all aspect of the power grid, most of which are currently manually carried out, can be automated in SG. These include automatic demand response, power storage, distributed power generation and integration, grid control and electricity pricing, etc. ICT control systems take care of the complete control of SG. They require a constant information feedback from all the sources in SG in order to take automatic control actions. The information needs of the control system can only be achieved by a centralized and integrated communication system. Because of their cost and performance benefits, wireless networks form the core of SG communication systems. Some of the places where they are widely deployed include house-to-grid communications and intra-grid communications (for generation, transmission, distribution). Unfortunately, the wide deployment of wireless networks within SG poses significant cyber security threats. The nature of the threats requires a detailed and systematic analysis of security vulnerabilities through systems security requirements engineering methods.

To elicit systems security requirements, we use a security requirements engineering method called SREP (Security Requirements Engineering Process) [15]. These requirements could be used to deter potential security threats or vulnerabilities in SG and to reduce their impact on the overall system. Typically, any security solution should answer three basic questions: what to protect, against whom, and to what extent. SREP takes into consideration these security questions in nine steps. SREP 1) defines the system context; 2) identifies the critical and vulnerable assets which should be protected from attacks; 3) identifies the security objectives and dependencies; 4) identifies threats and vulnerabilities to the assets; 5) assesses risks and analyzes the impact and likelihood of the threats

978-0-7695-5046-6/13 $26.00 © 2013 IEEE
DOI 10.1109/GreenCom-iThings-CPSCom.2013.153

and vulnerabilities; 6) elicits and categorizes the security requirements; 7) prioritizes the requirements based on the risk assessment; 8) inspects the requirements, and 9) improves the repository, if applicable.

The major contribution of this paper is the systematic application of the SREP to specify SG wireless network systems security requirements. It provides a step-by-step guide to apply SREP in SG domain. In order to evaluate the elicited systems security requirements, this paper proposes the systems integration of SG with the GSM and GPS networks. Integrating the GSM and GPS networks with SG wireless networks is a novel combination of already evolved and matured wireless communication systems. It is also a new direction for the SG system security solutions.

The remainder of this paper is organized as follows. Section II presents background and related work[1]. Section III presents the results of the study. Section IV presents evaluation and proposed solutions. Finally, Section V presents the conclusions.

II. Background and Related Work

Integration of the power grid with ICT systems to form a SG has brought a number of security challenges to power grids [16]. Through this integration, the power grid has inherent security risks due to the fact that the power grid and applications were not designed for the general ICT environment. To counter the impact of security issues that would arise in the power grid, the security should be incorporated from the requirements gathering phase during SG development. Currently, academic research focuses on either highlighting the possible threats [17], vulnerabilities [18], security issues [19], [20], [21], [22], and challenges [23], or recommending certain frameworks [24] and technologies to be used [22], [16], [25].

Wireless networks are a fast growing trend in ICT and they offer a lot of cost and performance benefits. Our analysis shows that the wireless communication can result in significant savings (see Figure 1). Wireless networks are widely deployed in SGs because of their advantages in cost, performance and ease of installation given the fact that SGs cover large land areas, difficult terrains and various geographic locations.

However, wireless networks add more challenges to the security issues faced by SG, as it can potentially expose the entire power grid to various cyber security threats because of the very nature of wireless communication, which is vulnerable to interception.

III. Results

SREP (Security Requirements Engineering Process) consists of nine steps. SREP itself acts as a research framework according to which SG wireless network security requirements specification was performed. Following are the results of applying SREP on SG wireless networks.

Step 1: Agree on Definitions. The best practice to conduct a study is to follow certain basic standards, definitions

[1]Background and related work section is shortened due to the page limit restrictions.

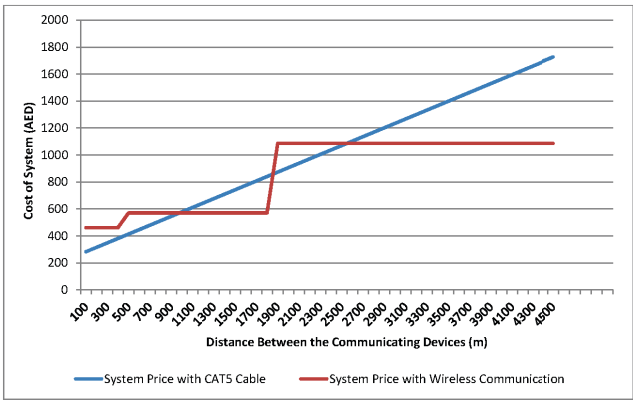

Fig. 1. Wired vs. Wireless Cost Analysis for Non-Line of Sight Link for a Micro-Hydro Project. (Note: AED means United Arab Emirates Dirhams. USD 1 = AED 3.67 as of April 2013.)

and terminology for the purpose of the consistency. Security requirements engineering and SG technology definitions in this research are extracted from international standards such as International Standards Organization (ISO), International Electrotechnical Commission (IEC) and Institute of Electrical and Electronic Engineers (IEEE). Some of the definitions used in this research are: ***Confidentiality*** is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes (source ISO 13335-1:2004). ***Integrity*** is the property of safeguarding the accuracy and completeness of assets (source ISO 15489:2001 and ISO 13335-1:2004). ***Availability*** is the property of being accessible and useable upon demand by an authorized entity (source ISO 13335-1:2004). *Supervisory Control and Data Acquisition* (SCADA) software can be considered as part of the Energy Management System (EMS) application. The monitoring and control functions of the EMS application are performed by SCADA while the optimization functions are performed by remaining EMS [26]. *Home Area Network* (HAN) is a residential local network whose purpose is to communicate with the digital devices installed within a household [27].

Step 2: Identify Vulnerable and/or Critical Assets. The SG is controlled by an interoperated communication network and a distributed control system. The communication systems are thus considered to be the critical assets of the whole SG [28]. Similarly, the network operations are critical assets of SG because they handle all the aspects of grid information and control instructions. Every aspect of SG where wireless network exists is now a vulnerable asset. These two networks are prone to data theft or cyber attacks. Some vulnerable assets of SG are:

1) House-to-gird wireless data and control network
2) Intra-grid wireless data and control network (encompassing power generation, transmission, and distribution facilities)

The wireless network between a household and the grid refers to the connectivity between the Advanced Metering Infrastructure (AMI) and SG's control center, where the power

flow is monitored and recorded for various purposes as required by the stakeholders. Table I shows the vulnerable data that is communicated in this segment of SG network. This data is available within AMI at each household, and can be breached if the household to SG network is vulnerable to security threats.

V1	Number of appliances in a household
V2	Power and wattage nature of the appliances
V3	Ideal parameters and loading status of the appliances
V4	Threshold power values for the appliances
V5	Present load received at the household
V6	Present activeness of the appliances
V7	Secondary power (as distributed energy resources) storage information

TABLE I
DATA-RELATED VULNERABILITIES IN HOUSE-TO-GRID NETWORK.

The intra-grid network covers the communications among the various facilities of SG such as power generation, transmission, and distribution centers. It has two independent tasks to be addressed, namely, grid control and consumer data handling. Grid control involves certain parameters about the generator, transmission, and distribution power management systems. Among all this, system failure information (available to a number people responsible for grid control) and reliability and accuracy of the grid communication devices are the most vulnerable subjects.

Table II presents the network-related vulnerabilities in SG (both for house-to-grid and intra-grid networks). If SG's wireless network is breached through one or more of those vulnerabilities, this can in turn trigger the data-related vulnerabilities mentioned in Table I. In other words, the data-related vulnerabilities are dependent on the network-related ones.

V8	Network monitoring and interception vulnerabilities
V9	Network discovery and access control vulnerabilities
V10	MAC Address Access Control List (ACL) provides minimal access control to limited people with authorized wireless cards
V11	SSID - Any wireless consumer, malicious or not, can be able to listen to this beacon to get the SSID and bypass this low level access control
V12	Authentication mechanism vulnerabilities
V13	Shared key authentication flaw
V14	802.1X/EAP vulnerabilities
V15	WEP vulnerabilities
V16	WPA/WPA2 Vulnerabilities
V17	Way handshake and weak pass-phrase vulnerability

TABLE II
NETWORK-RELATED VULNERABILITIES.

Figure 2 presents a simplified SG and the wireless communication. A dotted line represents wireless communication and solid line represents electricity connection. The home network is extended and shown in detail along with data-related vulnerabilities. The left side of the diagram depicts the various devices that are part of SG along with the communication links. The vulnerabilities associated with the wireless network are also presented.

The network-related vulnerabilities are a challenge for any wireless network irrespective of the system (whether it is house-to-gird or intra-grid). Hence, these network-related vulnerabilities are the major concern for security requirements engineering process for SG. Since the data-related vulnerabilities are dependent on the network-related ones, in order to address the vulnerabilities in Table I it is critical to first address those presented in Table II. Further steps of the SREP derive several precautionary steps and security requirements that should be implemented in SG's development.

Step 3: Identify Security Objectives and Dependencies. The security objectives for a system should be determined based on safeguarding the assets or the system from vulnerabilities and their associated threats, also considering the scope of any future threats.

In order to mitigate the vulnerabilities identified in Step 2, the basic objective should be to prevent SG's various wireless network components such as Access Points (APs), Routers & Switches, Power Amplifiers, Transceivers, Intelligent Electronic Devices (IEDs), Remote Terminal Units (RTUs) from potential attackers. The types of attacks are determined in later steps of the SREP.

Confidentiality, Integrity and Availability (CIA) are the basic security goals to be achieved in order to secure SG's wireless networks. These CIA goals as used in SG wireless networks are discussed below:

Confidentiality of information or controls that exist on SG's wireless network are safeguarded by protecting the network components that are vulnerable to frequent attacks. It means preserving the privacy of information by protecting invalid access to it.

Integrity prevents unauthorized modification or alteration of information and ensures the originality of information. Integrity is attained by proper and restricted authorization of those who can access the data on SG network.

Availability means the system is available continuously to every authorized user without any disruption. This can be achieved by avoiding threats of attacks on SG wireless network. SG's wireless network should be designed to resist any attacks that might lead to service disruption.

The ultimate goal is to secure wireless transmissions in SG. Building a wireless network that responds effectively to a particular attack will ensure the security of a particular piece of information. For example, to protect the consumer data from being breached, SG's wireless network should be made robust against the Access Point (AP) attack via several possibilities discussed earlier, and the Wired Equivalent Privacy (WEP) should also be designed to resist and detect any potential attack. In essence, for each single task of SG to be effectively performed, the wireless network should be made to resist any attacks that are likely to happen.

Step 4: Identify Threats and Develop Artifacts. The major threats to SG are the network-based attacks. Attacks on networks have several intended characteristics ranging from data breach through system disruption. Besides network attacks which originate outside SG, certain threats also evolve

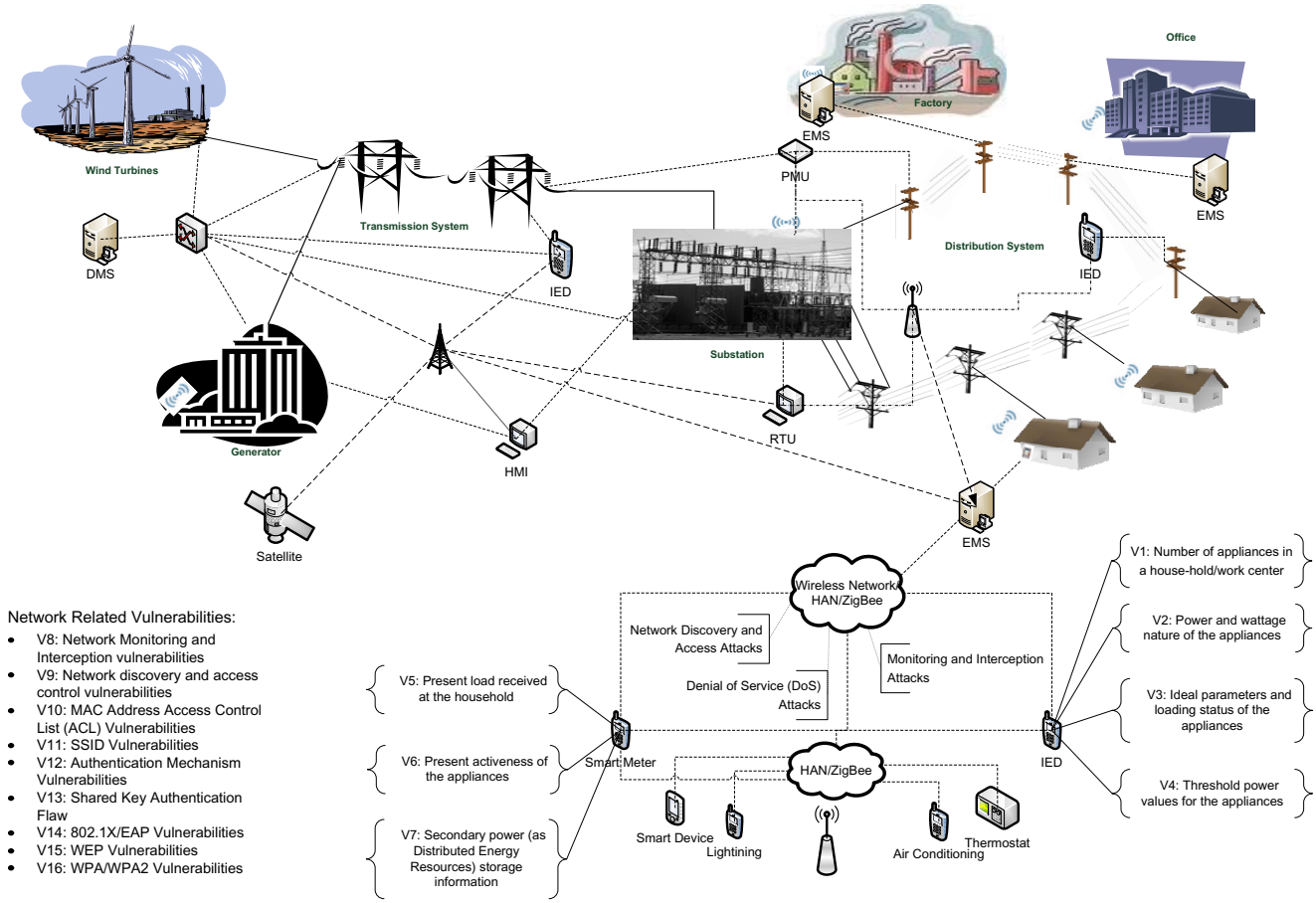

Fig. 2. SG Block Diagram with Communication Network and Devices.

from within SG. To prevent such inside threats, SG control parameters which are to be delivered to the central control unit should go along with the constraints such as less latency and criteria for reliable delivery, etc. [29], [30].

The wireless networks are vulnerable to a set of predefined attack models such as integrity attacks, confidentiality attacks, availability attacks, and access control attacks. Various aspects of the Wireless Local Area Network (WLAN) for house-grid communications discussed in Step 2 represent the weakest points of the system that can be targeted for attack. Several threat cases are developed, along with a few attack trees. Threats are analyzed using the threat cases, such as the examples in Tables III and IV.

Figure 3 shows an example attack tree that was developed as part of the artifacts development.

Step 5: Risk Assessment. Risk assessment for a system can be done in several steps. The National Institute of Standards and Technology (NIST) [31] suggested a simplified approach to risk assessment for a system. The steps include identifying the systems characteristics, possible threats, vulnerable aspects of the system, determining likelihood of occurrence of threats, analysis of risks and impact estimation, determine the potential of risks and propose solutions to solve or avoid those in advance [31], [32], [15], [33], [34]. In Step 4, most of the possible threats are identified for SG's wireless network. In this step, the task is to determine the likelihood of these threats or risks, and analyze and specify the preventative steps to be taken.

Among the threats that are identified, following three are the ones which exhibit considerable impacts on SG's wireless network when active:

1) Network Discovery and Access Attacks
2) DoS Attacks
3) Monitoring and Interception Attacks

However, not all the threats may occur frequently. The frequency depends on the importance of the targets, their vulnerability levels, and the prevention measures that are in place. If successful, even a small and simple attack on SG communication system can be very advantageous to the attackers. They can control power flows, breach confidential information, or even sabotage the grid.

The next step in the assessment of threats is to identify the part of SG that hosts vulnerable spots for these threats to target. We considered a set of vulnerable data shown in the

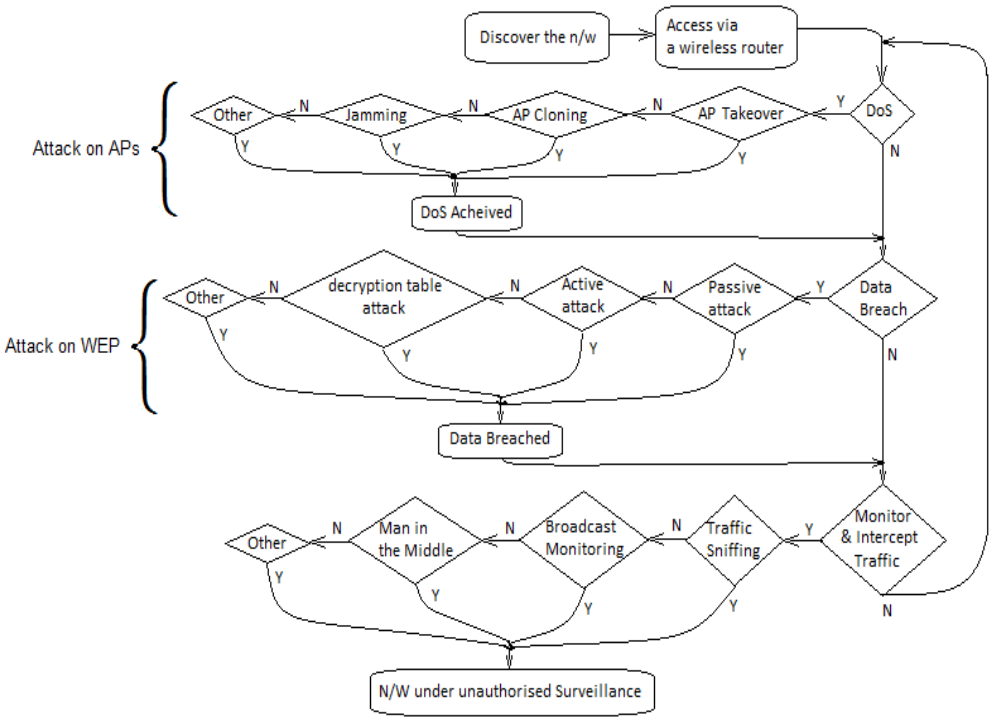

Fig. 3. Wireless Network Attack Tree.

Case	Description
Source	APs with an in-built wireless router and Dynamic Host Configuration Protocol (DHCP) services enabled
Stimulus	Network Access via Wireless Router
Artifact	Network Access
Assumptions	• DHCP enabled wireless routers are significantly susceptible to bandwidth hijacking attacks • Attacker is used to Internet Protocol (IP) requests via DHCP server
Action	• Attacker first discovers the target network and originating router, and then requests IP of the router via DHCP server • The attacker restarts his network affiliation and has an IP automatically assigned
Consequence	• Attacker hijacks the target network's bandwidth • If safety features are not enabled, the attacker can have complete access to the target network • The attacker can re-route the traffic, manipulate the data packets and reject the traffic or requests as well

TABLE III
NETWORK ACCESS - THREAT CASE.

Case	Description
Source	WLAN security safeguards and operating frequencies
Stimulus	Overwhelm the medium used for transmission
Artifact	Jamming the Radio Frequency (RF) channel
Assumptions	• Network uses 802.11b/g/n standards and 2.4GHz radio frequency band • Attacker has simple tools which can flood the communication channel used in SG
Action	• Rather than making spurious information to overwhelm the processing capability of network devices in RF jamming, attacker overwhelms the medium used for transmission, during this case - radio waves • With easily available open source tools attacker will simply flood the medium for the network with noise
Consequence	• RF jamming is incredibly effective as a result of it works against all WLAN security safeguards • When noise is injected at the WLAN operating frequency, signal-to-noise ratio drops below acceptable level and therefore the network merely ceases to operate

TABLE IV
JAMMING THE RF CHANNEL - THREAT CASE.

first column of Table V, which is related to a household part of SG. The second column of Table V describes the location of this vulnerable data.

Vulnerable Data	Availability Spot in SG
Customer ID, authentication and passwords	APs falling in the Home Arean Network (HAN) & SG Wide Area Network (WAN)
Appliance information	APs falling in the HAN
Appliance activity	APs falling in the HAN & SG WAN
Ideal power parameters of appliances	APs falling in the HAN
Power readings and consumer information	APs falling in the HAN & SG WAN

TABLE V
VULNERABLE DATA IN SG AND THE AVAILABILITY SPOTS.

The following system information has to be thoroughly analyzed and monitored regularly to check the occurrence of any such threat:

1) Check hardware and software malfunctioning
2) Monitor interface systems working in between any two points in the system
3) Monitor the data and information flow between any two points (in fact, this concern is covered elaborately in the research. A perfect scrutiny of the loopholes of information flow system is demanded.)
4) Monitor the people who support the IT system, and who look after a particular system function
5) Be up to date on security and protection levels of data and its sensitivity
6) Monitor system users
7) Check the security policies implemented in the system
8) Check the security architecture of the system
9) Continuously check and observe the control points, both managerial and technical in the system that continuously take care of the system functions

Final stage is the estimation of impact. In this step of risk assessment, we identify threats which have the greatest impact on the system. For example, in DoS attack, the intruder can disturb the normal services of SG by an effective wastage of the system communication resources. System resources like the communication bandwidth and the various control signals regarding source availability, power distribution, power usage, and electricity pricing, etc. can be made unavailable by this attack. These resources are very important for the smooth functioning of SG and the reduction or unavailability of these resources can have negative impacts on SG. The DoS attack during peak power demand period can seriously affect the economic stability.

Step 6: Elicit and categorize security requirements. SREP does not provide or indicate anything about the requirements elicitation, categorization and prioritization techniques or methods to follow. However, SREP suggest to retrieve associated clusters of security requirements from the repository (SRR), if they are not found in SRR then SREP suggest to get them by other means but does not indicate or suggest any such means.

Each security goal and objective is to be analyzed along with its threats and risks in order to elicit a suitable set of security requirements. Security requirements when implemented should be able to mitigate all the security threats and vulnerabilities identified. Moreover, requirements should also have some countermeasures to the security issues that are hindrance in achieving the security goals.

Table VI presents an example subset of 4 out of the total of 43 elicited requirements along with the category and the preventive measures for several specific security objectives for SG wireless network.

Step 7: Requirements Prioritization. SREP does not specify any requirements prioritization technique or method. In our case of SG, we have used NIST prioritization technique [31], [30] and assigned priority according to the significance of a requirement. Prioritization is done based on the levels of *low*, *medium* and *high*.

A requirement is assigned *low* priority if its absence may have low-to-moderate effect on SG, *medium* priority if its absence may have moderate-to-high effect on SG, and *high* priority if its absence may have high-to-severe security impact on SG [31], [30].

Based on these criteria, all the requirements specified in the previous step are evaluated. Table VI also includes the requirements priorities of the four examples.

Step 8: Requirements Inspection. This step is performed to guarantee that all the artifacts that are generated are valid and cover most of the system vulnerabilities, threats and risks to the defined assets. It ensures that all the documents, requirements, use cases, and attack trees are consistent, and complete. This step also verifies if the requirements are ranked according to their importance or not, as discussed in Step 7.

Apart from the process specific details, this step also runs a sanity check against the standards that are incorporated in SREP such as IEEE 830-1998, SSE-CMM (ISO:IEC 21827), CC SS-CMM and CC assurance requirements, and organization policies.

We did not have any organization's involvement or any already available documents such as SRR with security specific details such as requirements, use cases, security threats, vulnerabilities and risk. Hence, we did not consider all these standards in this research; however, we have performed several iterations of security requirements inspection in order to ensure the completeness.

Step 9: Repository Improvement. As we do not have any repository in this research, this step is out of the scope of this research. However, we strongly believe that having any such document while applying SREP would be very useful, time-saving, and efficient way to elicit, specify, categorize and prioritize security requirements. In addition, incorporating such a repository would also enable requirements or data reuse.

Requirement No.	Description	Category or Preventive measure	Priority
R1	Wireless networks access points should be made secure by preventing unauthorized traffic into the network.	Confidentiality and integrity of wireless transmission	High
R2	Anti-sniffing and spoofing tools and technologies should be at the access points as well within the wireless network domain. This will prevent malicious attackers from monitoring the network traffic.	Sniffing and spoofing	High
R3	Secure sessions should be implemented in case of highly sensitive wireless transmission. This includes generating a new security token each time a user request is made to the server.	Confidentiality and integrity of wireless transmission	Low
R4	RAPs (Rogue Access Points) should be eliminated in order to secure the wireless access points. The best technique to cope with the threat of RAPs is to use 802.1x on the wired network to authenticate all devices that are plugged into the network	Access control	Medium

TABLE VI
ELICITED, CATEGORIZED AND PRIORITIZED SECURITY REQUIREMENTS (PARTIAL).

IV. EVALUATION AND PROPOSED SOLUTIONS

After applying SREP on SG's wireless networks, we elicited, categorized, and prioritized 43 security requirements. We found 21 of them to be of high priority, 16 of medium priority and 6 of low priority. We found 7 data-related vulnerabilities in house-to-grid communication and 10 network-related vulnerabilities in intra-grid communications. We found a total of 13 threats. We identified 3 types of threats to be more harmful to SG when active.

During the analysis we found that the major security threats to SG can arise from a large number of low processing power field devices. Typically, adoption of standards guarantees certain degree of in-built security and the reliability of the devices and the technologies. However, in case of SG, many standards are still under development, and there are already millions of Intelligent Electronic Devices (IEDs) deployed in the world to control, monitor, record, report, diagnose and communicate the valuable grid related information without a set of agreed protocols or standards. These devices expose SG to many cyber threats such as the recent attack on the U.S. Water Utility SCADA (Supervisory Control and Data Acquisition) system [35].

Systems security solution of any system should not only consider the technological aspects, but also the end users and the environment (physical and logical) that a system is exposed to. In the case of SG, the system consists of the power grid, ICT systems, and smart devices. However, people usually tend to emphasize only on the system itself, often neglect the valuable contribution an end user and the environment may have on the functioning of the system. To avoid this pitfall, we must not only generate the system security requirements but also consider end user and the environment related requirements such as user training, updating manuals and network auditing and monitoring.

Some of the solutions for implementing the elicited security requirements from the systems perspective are presented here. For securing the low processing power field devices some countermeasures could be making them GSM (Global System for Mobile Communications)-enabled so that each device in the field would have its own unique identifier which is only available to the nearest hub/switch or the router on which a firewall/VPN could be installed to enhance security. GSM networks are highly reliable and secure, and hence the information exchange can be secured. Even if someone is able to duplicate a GSM, SIM (Subscriber Identity Module) based device, then another layer of security could be provided by having a small battery support to these IEDs and attaching a small and low cost GPS (Global Positioning System) chip which would capture the geo-location of the devices and any new, fake or duplicate devices can be identified. The benefit of having the GSM SIM enabled IEDs is that this mode of communication is low cost and the GSM technologies and the network is highly reliable, robust, secure and available at almost all locations. Similarly, we believe that for the information security and the physical device's security credit card and e-commerce fraud detection and prevention techniques, strategies and polices could be of greater help. As they also deal with similar kind of sensitive data and ever increasing cyber threats.

For the security within household and house-to-grid communication, we recommend to use the low signal power antennas, reduce the signal propagation or use the directional antenna if there is a potential threat from the neighborhood. In addition, the communication device in household should have high processing capabilities where the proprietary security solutions could be implemented to secure in-house and house-to-grid communication. This device can have advance encryption techniques, firewall, and intrusion detection system for sending household data to the control center so that the in-house devices could be of low processing power. It would be more cost effective to have one powerful machine in each home rather than investing money and effort to improve performance and security of each device in a household.

Another way of bringing down the risks to the acceptable level is assigning the risk score to each control command and accordingly the preventive mechanism to be activated. To add another level of security for control commands with high risk score or high impact, a validation mechanism should be developed as well.

For SG security, there is no single solution but there has to be a combination of different solutions which could be derived

from the existing evolved and matured systems such as GSM, GPS, and e-commerce, and credit card fraud detection. All such solutions and countermeasures would be beneficial only if they are incorporated at the early stages of SG development, as there is little or no margin for error in SG.

V. Conclusion

This paper presents the step-by-step systematic application of the systems security requirements engineering method to elicit, categorize and prioritize security requirements for SG wireless networks. We elicited, categorized, and prioritized 43 security requirements. We found 21 of them to be of high priority, 16 of medium priority and 6 of low priority. We found 7 data-related vulnerabilities in house-to-grid communication and 10 network-related vulnerabilities in intra-grid communications. We found a total of 13 threats. We identified 3 types of threats to be more harmful to SG when active.

During this process several high importance assets were identified along with the potential security threats to them. The identified threats, vulnerabilities, and associated security requirements can be used as a reference during SG's wireless network security development. An evaluation of SREP was also conducted. Based on the systems security analysis, we proposed a systems integration of GSM and GPS networks with SG. GSM and GPS were selected because they both have wide deployment of wireless networks. The potential integration of SG with GSM and GPS is a new direction for the future SG security research in both academia and industry. Finally, we also defined the use of risk score for all control commands in SG, and the monitoring activities to identify the occurrences of threats.

References

[1] J. S. Reel, "Critical success factors in software projects," *IEEE Software*, vol. 16, no. 3, pp. 18–23, 1999.

[2] A. Hamidovic and S. Krajnovic, "An example of a novel approach to measuring projects success within ICT industry," in *Proc. 8th IEEE International Conference on Telecommunications (ConTEL)*, vol. 2, 2005, pp. 677–682.

[3] S. C. Misra, V. Kumar, and U. Kumar, "Success factors of agile software development," in *Proc. 2006 International Conference on Software Engineering Research and Practice (SERP)*, 2006, pp. 1–7.

[4] B. W. Boehm and P. N. Papaccio, "Understanding and controlling software costs," *IEEE Transactions on Software Engineering*, vol. 14, no. 10, pp. 1462–1477, 1988.

[5] S. McConnell, "An ounce of prevention," *IEEE Software*, vol. 18, no. 3, pp. 5–7, 2001.

[6] C. Jones, *Tutorial Programming Productivity: Issues for the Eighties*, 2nd ed. IEEE Computer Society Press, 1986.

[7] K. E. Wiegers, *Software Requirements: Practical Techniques for Gathering and Managing Requirements Throughout the Product Development Cycle*, ser. Pro-Best Practices. Microsoft Press, 2003.

[8] R. Araujo, "Software security: going beyond the devlopment phase," Foundstone Professional Services," White Paper, accessed on April 15, 2013. [Online]. Available: http://goo.gl/ezQQU

[9] N. R. Mead and J. H. Allen, "Identifying software security requirements early, not after the fact (audio)," 2008, informIT.com podcasts. [Online]. Available: http://goo.gl/FXg3P

[10] N. Bilton, "Sony explains Playstation attack to Congress," *The New York Times*, May 2011, accessed on April 15, 2013. [Online]. Available: http://goo.gl/4C4aB

[11] D. Graham, "Introduction to the CLASP process," 2006, accessed on April 15, 2013. [Online]. Available: http://goo.gl/P16Cl

[12] N. R. Mead, V. Viswanathan, and J. Zhan, "Incorporating security requirements engineering into standard lifecycle processes," *International Journal of Security and Its Applications*, vol. 2, no. 4, pp. 67–79, 2008.

[13] N. R. Mead and E. D. Hough, "Security requirements engineering for software systems: case studies in support of software engineering education," in *Proc. 19th Conference on Software Engineering Education and Training (CSEET)*, 2006, pp. 149 –158.

[14] D. Firesmith, "Engineering security requirements," *Journal of Object Technology*, vol. 2, no. 1, pp. 53–68, 2003.

[15] D. Mellado, E. Fernández-Medina, and M. Piattini, "A common criteria based security requirements engineering process for the development of secure information systems," *Computer Standards and Interfaces*, vol. 29, no. 2, pp. 244–253, 2007.

[16] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in *Proc. 2010 IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, 2010, pp. 1–7.

[17] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *Proc. 2010 Military Communications Conference (MILCOM)*, 2010, pp. 1830–1835.

[18] J. Clemente, "The security vulnerabilities of smart grid," *IAGS Journal of Energy Security*, June 2009.

[19] F. M. Cleveland, "Cyber security issues for Advanced Metering Infrastructure (AMI)," in *Proc. 2008 IEEE Power and Energy Society General Meeting*, 2008, pp. 1–5.

[20] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security and Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[21] R. Schainker, J. Douglas, and T. Kropp, "Electric utility responses to grid security issues," *IEEE Power and Energy Magazine*, vol. 4, no. 2, pp. 30–37, 2006.

[22] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke, "A security architecture for computational grids," in *Proc. 5th ACM Conference on Computer and Communications Security (CCS)*, 1998, pp. 83–92.

[23] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security and Privacy*, vol. 7, no. 3, pp. 75–77, 2009.

[24] H. Cheung, A. Hamlyn, T. Mander, C. Yang, and R. Cheung, "Role-based model security access control for smart power-grids computer networks," in *Proc. 2008 IEEE Power and Energy Society General Meeting*, 2008, pp. 1–7.

[25] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, 2010.

[26] "Guidelines for smart grid cyber security: Privacy and smart grid," NIST, Interagency Report 7628, 2010, accessed on April 15, 2013. [Online]. Available: http://goo.gl/qJ4S

[27] G. A. McNaughton and R. Saint, "Enterprise integration implications for home-area network technologies," in *Proc. 2010 IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, 2010, pp. 1–5.

[28] G. N. Ericsson, "Cyber security and power system communication — essential parts of a smart grid infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501–1507, 2010.

[29] D. Von Dollen, "Report to NIST on the smart grid interoperability standards roadmap," Electric Power Research Institute," Report, 2009.

[30] A. Lee and T. Brewer, "Smart grid cyber security strategy and requirements," Draft Interagency Report 7628, 2010.

[31] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," NIST, Special Publication 800:30, 2002.

[32] D. Mellado, E. Fernández-Medina, and M. Piattini, "Applying a security requirements engineering process," in *Proc. 2006 European Symposium on Research in Computer Security (ESORICS)*, 2006, pp. 192–206.

[33] Z. Yazar, "A qualitative risk analysis and management tool — CRAMM," SANS Institute," White Paper, 2002.

[34] S. Rocha, Z. Abdelouahab, and E. Freire, "Requirement elicitation based on goals with security and privacy policies in electronic commerce," in *Proc. 2005 Workshop on Requirements Engineering (WER)*, 2005, pp. 63–74.

[35] J. Finkel, "U.S. probes cyber attack on water system," November 2011, accessed on April 15, 2013. [Online]. Available: http://goo.gl/glx2p