A Framework for Risk Analysis in Smart Grid

Perspective Based Approach

Rani Yesudas and Roger Clarke

College of Engineering and Computer Science, The Australian National University, Canberra, Australia
{rani.yesudas,roger.clarke}@anu.edu.au

Abstract. Smart Grids have great potential for the management of energy consumption. However, moving from a traditional grid to a smart grid introduces significant new risk to the energy sector that were not present in the power grids that operated in isolation. The data that is generated in the smart metering systems can possibly harm its stakeholders. Hence it is important to protect all the stakeholders by providing effective controls to the vulnerable elements in the smart metering system. This highlights the necessity to conduct a risk analysis to evaluate the harms, threats and vulnerabilities that are introduced into this critical infrastructure by modernization. Currently there are numerous risk analysis methodologies available; there are many differences among them, and hence selecting an appropriate one is challenging. Risk that technical experts perceive to be minor often elicits strong public concerns. Consequently during risk analysis, different perspectives need to be considered. This article reports on an extensive analysis of risk management frameworks, which resulted in a framework specifically targeted at smart grid and smart metering systems. Perspective of risk analysis is a key element in this framework.

Keywords: smart meter, smart grid, security, risk assessment, risk analysis, framework.

1 Introduction

Smart grids, including smart meters, offer great promise for the efficient management of energy. However, concerns remain about the security of smart meter designs, and the potential negative impacts on householder privacy. These could slow adoption of the technologies, and threaten return on the considerable investments involved.

Like any infrastructure, smart grid is also prone to attacks. Moving systems from a manual process to an automated process creates new vulnerabilities. As systems are added, complexities and functionalities increase making it more difficult to address security. Increasing connection to previously isolated systems and networks expands the threat surface. Connection points between different networks become access points for interception and for the infiltration of malware. The dependence on networking technologies introduces new threats to service reliability [1].

Confidentiality, integrity and availability are the commonly used terms in security. In the electrical power system, availability of electricity is considered as the most

E. Luiijf and P. Hartel (Eds.): CRITIS 2013, LNCS 8328, pp. 84–95, 2013.

critical element and a disruption in communications can cause a blackout to a vast region. So a secure power grid should have the best control measure to ensure that availability of electricity is protected. Secondly, a smart grid uses data collected by various sensors and agents and this data is used for number of functionalities which include automated billing, peak usage determination, power outage tracking etc. The integrity of this data is very important. Unauthorized modification of the data or insertion of data from unknown sources can cause loss and damage to the system. Next is confidentiality. Customer information, general corporation information, and electric market information are some of the areas that need to be confidential. In smart grid, detailed information of electricity usage is recorded in the smart meter and this information is transmitted at certain intervals to the remote system via different communication methods [2].

Having identified availability as the top priority in a power system, does not deem integrity and confidentiality as elements of less importance. The system should ensure that the customer privacy is not violated and that the consumer is well informed of what could happen to their utility usage and personal data. Ultimately it will be the consumer who will have to bear the cost of running such a system and if the system can't guarantee safety and security they can backlash the system with the help of consumer advocacy groups. Risk that technical experts perceive to be minor, and even non-existent, often elicit strong public concerns and have even resulted in systems being discarded after huge investments have been made [3].

In various countries, after the initial roll out of smart metering systems there have been protests and demonstrations against them. The main reasons for their protests have been media reports regarding health hazards and privacy breaches that smart meters cause to its consumers. The smart meter has been described as a spy in the home [4]. This was based on a report that found that detailed smart meter data at one-minute intervals could provide insights into a household's living patterns to the extent that it could reveal the appliances used and activities conducted by the household [5]. It was completely misleading, as mostly the smart meters were read on half-hourly basis and it was almost impossible to deduce such information. Even if the meter was read at one minute intervals, detailed knowledge of the appliances present in the home and the habits of the consumer would be required to deduce living patterns [4]. Nonetheless, the perceptions of health and privacy threats persist.

If erroneous information sources find ready access to the mass media without effective remedies, then large social impacts, even for minor events, becomes possible [3]. This demonstrates the need to take security and privacy more seriously. In order to avoid any public resistance towards the Smart Grid especially from poorly drawn evidence, risk from the system should not only be analysed and managed but also effectively communicated.

Though over years, experts have stressed the need to have risk analysis embedded into design, it seldom happens. Even if risk analysis is done during design or after deployment; it requires distinct steps or processes that can be followed effectively. A good framework should make its processes transparent and understandable to all its stakeholders. It should also be adaptable and extensible as the system grows or modifies. A great many frameworks are available. They have a lot of commonality, but also differences, some of which are significant in the context of smart meters.

This paper reports on an extensive study of frameworks for the assessment and management of risk, whose purpose was to produce a framework specifically targeted at smart grid and smart metering systems. Following a brief introductory section on smart grids, a summary and comparison of existing smart grid models are presented, followed by a presentation of a method that is proposed as an effective but efficient approach to risk assessments for smart grid projects generally, and is illustrated by means of application to smart meter projects.

2 Background

2.1 Current Smart Grid Scenario

All around the globe, utilities and government have identified that the traditional energy grids needs to be replaced by Smart Grids. It emerged as a need to effectively manage the electricity requirements from the needs of an increasingly large world population. Though the initial interests were limited to accurately measuring the power usage, the focus has shifted to environmental gains through the reduction of peak demand and hence lower production cost and lower carbon emissions [6, 7].

As smart meters were identified as a primary requirement in a smart grid, many countries have started the smart meter roll-out for residential customers, in some cases mandated.

During and after roll-out, many schemes have been subjected to considerable criticism in relation to security and privacy aspects of the design. In many cases, public concerns have been exacerbated by the discovery that the risk assessments had been performed solely from the perspective of the utility provider [8, 9, 10]. Also by narrowing down the context, most of the documents have failed to consider vulnerabilities of the new system to different kinds of threats.

2.2 Models for Smart Grids

As a part of the realignment of the utility industry to support a smart grid, various countries and organisations have developed architectural and conceptual models to plan, evaluate and monitor the success of transformation from the traditional to a modern grid. Two popular models are Smart Grid Conceptual Model (SGCM) established by the National Institute of Standards and Technology (NIST) and Smart Grid Architecture Model (SGAM) established by the Working Group Reference Architecture (SG-CG/RA).

SGCM provides a visualized diagram explaining how different components of smart grid can be integrated and organised into seven Domains: Bulk Generation, Transmission, Distribution, Customers, Markets, Service Providers and Operations [11].

SGAM has a Smart Grid Plane. Zones are present in additions to the Domains to form a matrix, distinguishing between electrical process and information management viewpoints. The Domains encompass the complete electrical energy conversion chain (Bulk Generation, Transmission, Distribution, Distributed Electrical Resources (DER)

and Customers Premises) and the Zones represent the hierarchical levels of power system management (Process, Station, Operation, Enterprise and Market) [12].

SGAM provides a better basis for risk assessment, because it provides more comprehensive coverage of parties than SGCM, and its structuring of the area into Domain/Zone cells assists the analyst in identifying the relevant scenarios.

3 Preparation for the Risk Analysis Framework

3.1 Chaos in Risk Terms

Before entering a discussion on risk analysis it is important to have the terminologies correct. Over years different entities have developed many standards and methods for risk analysis, and the terms and definitions used for risk elements and processes vary.

Most commonly used risk process terms are 'Risk Analysis', 'Risk Assessment' and 'Risk Management'. Some of the descriptions given by few standards and organizations are as follows:

- In ISO/IEC 27005, 'Risk Assessment' consists of 'Risk Analysis' and 'Risk Evaluation'. 'Risk Analysis' is then further divided into 'Risk Identification' and 'Risk Estimation' [13].
- In SP 800-30 by NIST, 'Risk Management' is said to encompass three processes, namely 'Risk Assessment', 'Risk Mitigation', and 'Risk Evaluation' [14].
- According to a Working Group (WG) established by European Network and Information Security Agency (ENISA), 'Risk Management' consists of 'Definition of Scope', 'Risk Assessment', 'Risk Treatment', 'Monitoring' and 'Communication' [15].
- Society of Risk Analysis (SRA) defines 'Risk Analysis' to broadly include 'Risk Assessment', 'Risk Characterization', 'Risk Management', 'Risk Communication', and policies [16].

In one definition, 'Risk Assessment' encompasses 'Risk Analysis' and in another one it is the reverse. Similarly 'Risk Management' in one interpretation includes all activities from scope definition to monitoring whereas in another it refers only to the planning and implementation phases.

Reference [17] drew attention to the problems inherent in defining the key term 'risk'. This article adopts a similar approach to the other key terms in the area; rather than attempting a universal definition, each term needs to be defined within the risk assessment document and used consistently within that document.

It is also important not to confuse one risk element with others. The Expert Group of the European Commission's Smart Grid Task Force prepared a Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') in 2012. The main flaw that was highlighted by the Working Party against the DPIA template was that it often confused risk and threats [18].

3.2 Defining Elements of Risk

In this section the key elements of risk are defined. They variously adopt and adapt definitions found in the most relevant sources found during the conduct of the research [13, 14, 19, 20, 21, 22]. The terms used for each risk element by different entities have been tabulated in Table 1.

Table 1. Terminologies used for Risk Elements

Risk Elements	Different Terminologies Used
Stakeholder	User, Party
Asset	Resource, Property
Threat	Hazard
Vulnerability	Weakness, Susceptibility
Harm	Impact, Consequence, Damage, Effects of Unwanted Incident
Control	Safeguard, Treatment , Countermeasure
Risk	Probability, Chance

1. **Stakeholder:** Any entity that has interests in the target of evaluation, and whose interests are taken into account during the process.
2. **Asset:** Anything to which a stakeholder assigns value and which therefore requires protection. An asset can be physical or intangible. Assets include people, property, information and reputation.
3. **Threat:** Any circumstance that can potentially cause an event (sometimes referred to as an 'unwanted incident') that can result in harm or damage to an asset. A threat can be intentional (in which case it is referred to as an attack) or unintentional (an accident).
4. **Vulnerability:** A feature of a system that represents a susceptibility to a threat. A vulnerability may be a weakness, flaw or deficiency, or it may be an intentional aspect of the system.
5. **Harm:** The impact or damage to an asset arising from a threatening event.
6. **Controls:** A Countermeasure or safeguard against a threat or a vulnerability. Four types of control are commonly distinguished:
   - Preventative controls to protect vulnerabilities.
   - Corrective controls to reduce the effect of harm.
   - Deterrent controls to reduce the likelihood of unwanted incident.
   - Detective controls to discover threats and trigger preventative or corrective controls.
7. **Risk:** A risk is the probability of the occurrence of a harmful event. It can be considered as a function of threats exploiting vulnerabilities to create unwanted incidents to harm assets.

4 Proposed Framework

4.1 Purpose

The quality of security and privacy risk assessments conducted on smart meter projects has generally not been sufficient to satisfy the public [9, 23]. A framework is needed that enables efficient conduct of risk assessment, and that produces understandable results that convince all stakeholders, including consumers who are suspicious about the compulsory installation of a smart device on their premises.

4.2 Framework Description

Standards like ISO/IEC 2700x, NIST SP 800-30, BSI 100-x and methods like CORAS and OCTAVE have been exhaustively analysed, with the specific needs of smart meter projects in mind, in order to develop this framework [13, 14, 19, 20, 21]. We choose to use the terminology 'Risk Analysis' for this entire decision-making and management process and hence the framework is termed 'Risk Analysis Framework'. The proposed framework has a set of optimal steps that can be used to identify, evaluate and control risk to mitigate potential negative effects in Smart Grid. Fig. 1 provides a visual presentation of the framework.

Definition of Scope
The risk analysis process starts with the definition of scope. To define the scope, the target of evaluations should be identified. Each target will have involvement with one or many stakeholders. To identify the target of evaluation in a smart grid, the Smart Grid Architecture Model (SGAM) is used. There are few ways in which the target can be chosen:

- Each Domain/Zone cell can become a target. For example in the Customer Premises/Process cell the target will be a smart meter. For a smart meter there are multiple stakeholders like customer, utility provider, etc. Choosing a stakeholder helps to narrow down the analysis to how the meter hardware and the data that exist within the meter affect that particular stakeholder.
- Zone to Zone for a particular domain helps to target data in transmission from one zone to another. So if we consider the zones Process and Field we can target the data transmitted from the smart meter to the concentrators/collectors and vice versa.
- Domain to Domain for a particular zone helps to identify the target of interaction between each domain.

We can identify a number of targets and the stakeholders involved. Then the next step is to choose the target for assessment. We have found that each target may have more than one stakeholder, hence a stakeholder must also be chosen from those identified for the target. Narrowing down the target and stakeholder enables to easily identify the assets involved. At the end of this step we can identify targets, their stakeholders and assets involved.

Risk Identification
In this step for each asset identified, all possible threats will be listed. Using the threats identified, all possible vulnerabilities and unwanted incidents can be identified. Using the unwanted incidents list, the harms on the assets can be extracted. Activities should be conducted to ensure stakeholder participation in this phase of risk analysis in particular.

Risk Characterization
This is vital step in risk analysis. The results from this step will vary based on the perspective of analysis. We have mentioned earlier how risk factors that have been assessed as minor by technical experts had elicited strong public concerns. For example, an unauthorized party gaining access to the meter data may occur as a minor risk to a utility provider if the access is read-only but from the perspective of the consumer it is still a major risk. So in this step, the perspective of analysis is vital. Based on the perspective, severity levels and likelihood levels need to be identified and tabulated. A risk matrix can be generated using this information.

Risk Evaluation
In this step the unwanted incidents and the harmful impacts that were identified are evaluated using the established levels for severity and likelihood. A likelihood level is assigned to the unwanted incident listed and a severity level assigned to the harms listed. Based on the values of likelihood and severity given, a risk value can be assigned to each case. This risk value can be used to prioritise the risks identified.

Risk Mitigation Plan
This section specifies the treatment that needs to be provided to the identified risks. It begins with the identification of existing controls. The suitability of the control for the target of evaluation is then evaluated. Common factors affecting suitability are cost and resource limitations. For example, there are strong and complex encryption techniques available to protect data, but it may not be feasible to apply them on a smart meter with a limited processor. Based on the evaluation, a list of applicable controls can be specified, and the residual risk determined. Apart from countermeasure, contingency response also needs to be identified so that those actions can be taken should the risk event actually occur.

Risk Management
With all the risks and countermeasures identified, the next step is to plan and implement the safeguards. The implementation needs be tested to ensure that the risk have been mitigated as expected during the analysis.

Risk Communication
A planned communication process is very important to improve the awareness of risk to all its stakeholders. In addition, education of the media is needed, in order to avoid negative impacts caused by erroneous information sources.

Monitoring and Review
All identified unwanted incidents, harm and their controls need to be documented and then to be reviewed regularly in order to adapt to new threats and vulnerabilities and to improve control measures and find better ways of implementing and maintaining them.

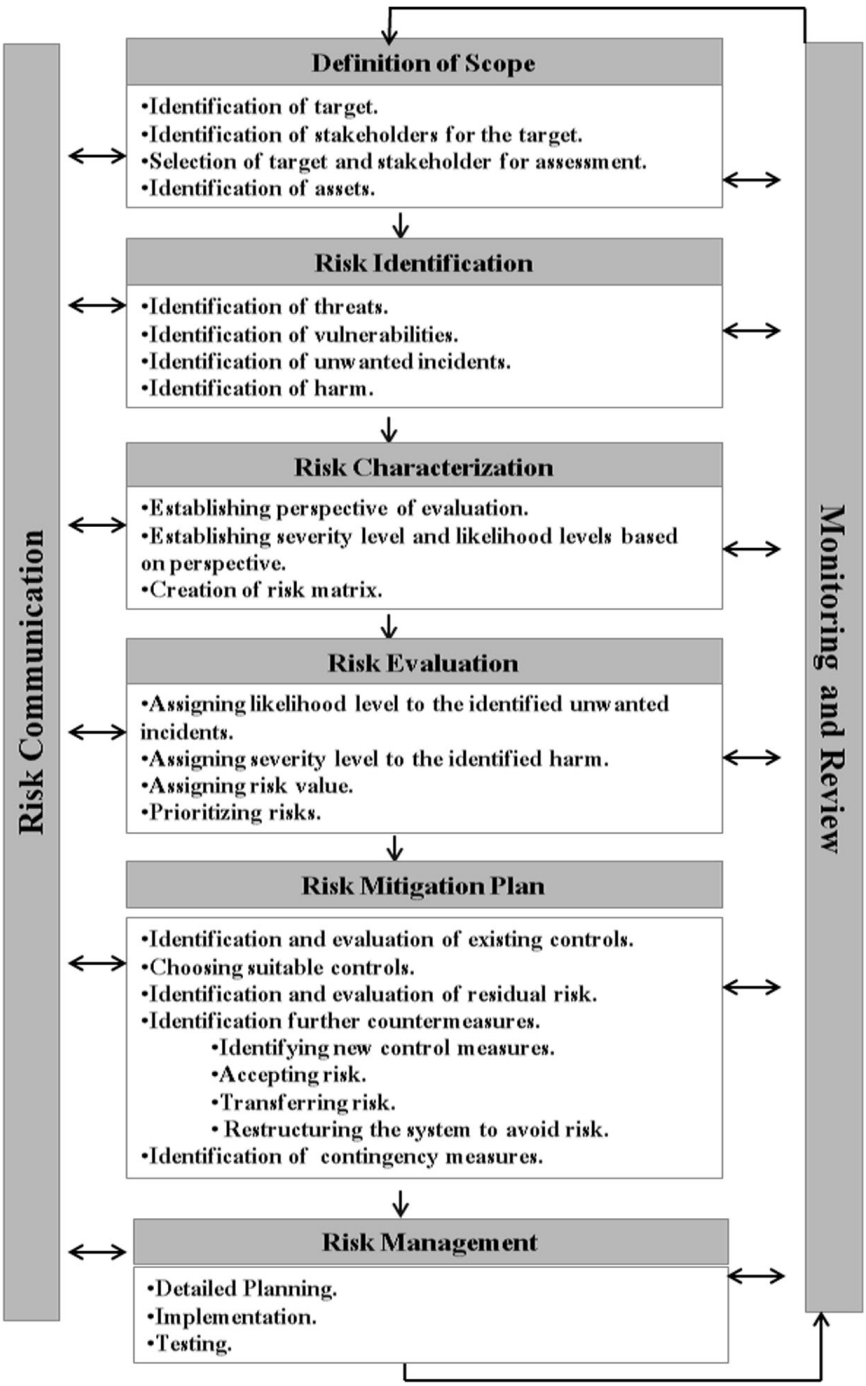

Fig. 1. Proposed Risk Analysis framework and its steps

5 Indicative Application of the Framework

5.1 Testing the Framework

In this section we analyse a scenario using the proposed framework. Customer Premises/ Process cell is chosen for analysis from the SGAM model. Smart Meter is chosen as the target of evaluation and consumer as the stakeholder. Then the assets have to be identified. The identified assets can be classified as direct and indirect assets. For the consumer, the direct assets involved with a smart meter are the hardware, firmware and the information stored. Some of the indirect assets are availability of electricity; integrity of billing and other functionalities; confidentiality of personal information and safety of human and non-human elements involved.

The assets can further be classified as physical, functional and informational. The physical assets comprise of the meter hardware and communication module. The functional assets entail measuring, conversion, communication and supply-switching functions. The informational assets consist of measurement, configuration, monitoring and consumer's personal information data.

The next step is to identify threats, vulnerabilities and harms. For this analysis we consider the meter hardware. There have been few reports that power surges have caused the smart meters to overheat and start a fire [24]. Power surge is a non-human threat. The vulnerabilities are poor quality components and improper assembly of the meter. Overheating of the meter is the unwanted incident and fire is the harm caused by the threat. This risk can be analyzed from different perspectives. For a utility provider, as there were only few incidents reported, the risk value will be low. But from a consumer perspective it is very high as there is always a chance of fire that could damage their property and even cause death.

As a control measure to overheating, some smart meters have temperature alert functionality. When the temperature rises above a set threshold, it shuts down the supply and alerts the utility management to take further actions. For a utility provider this control is sufficient as it prevents a fire and there is no harm to their reputation. But from the perspective of a consumer there is still residual risk. It provides safety by preventing the fire, but the power supply is disrupted. If it is a consumer on life-support machine, it could even cause death. This scenario clearly shows how the perspective of analysis changes the requirements in control measures for each stakeholder. Diagrammatic representations of some of the elements of the scenario are shown in the following figures (Fig. 2, Fig. 3 and Fig. 4).

5.2 How to Use the Framework

In the previous section we have seen how a scenario has been analysed using the framework. Similarly for each target of evaluation, its key risk elements can be identified. A repository can be created for assets, harms, risk and controls. Both quantitative and qualitative risk analysis can be carried out using this framework. A risk register or risk log can be created using the criteria mentioned in the framework. For qualitative risk register descriptive terms are used where as in a quantitative risk register numerical quantities will be used.

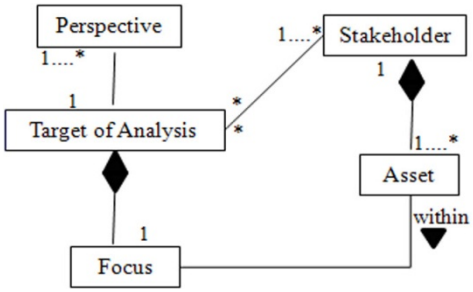

Fig. 2. Defining Scope for Analysis

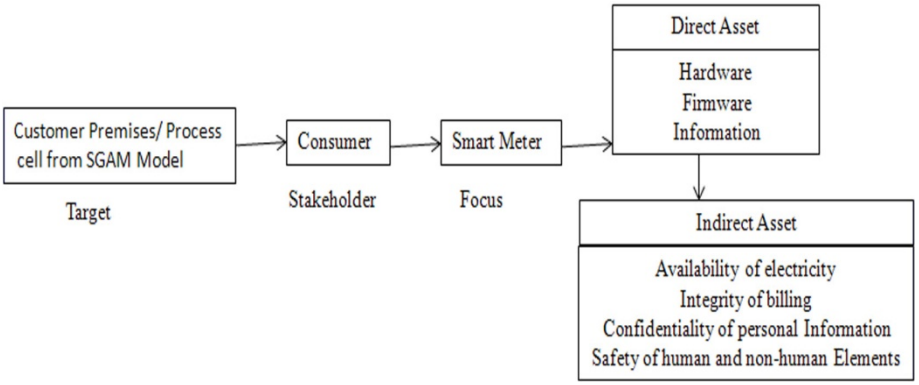

Fig. 3. Choosing Focus of Analysis

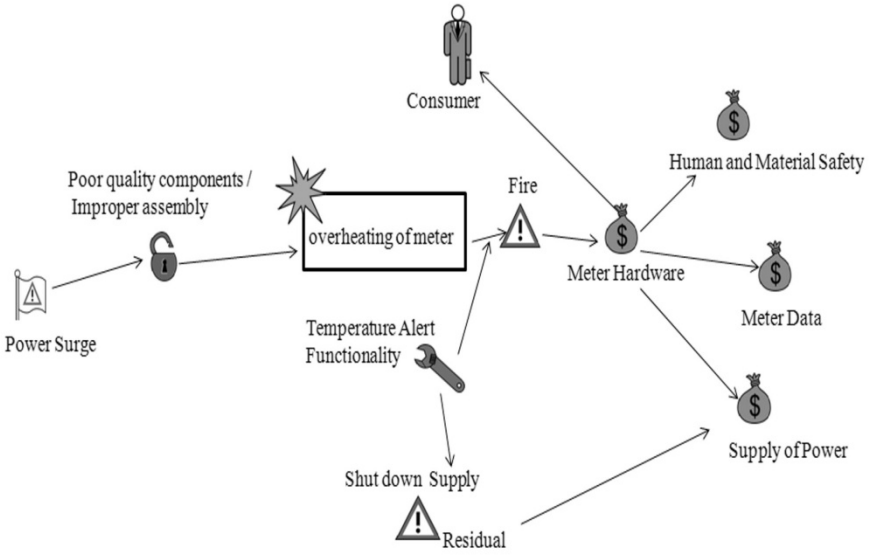

Fig. 4. Scenario Analysis

Alternately, tools like CORAS can be modified to satisfy the framework and then used for conducting security analyses. This model-based approach, improves communication and interaction between parties involved in the analysis. It will help in easily identifying the missing links and errors [19].

6 Conclusion and Discussion

Smart grids, and their critical sub-element smart meters, have great potential, but harbour risk to various stakeholders. The perception by householders that they are subject to significant security and privacy risk has proven to be a significant impediment to progress.

The field of risk assessment suffers from an excess of frameworks and a great deal of terminological ambiguity. The risk evaluation framework proposed in this paper reflects the substantial accumulated literature on risk assessment, and is sculpted to the needs of smart grid projects. It is now being applied to existing AMI systems and will then be applied to other categories of project within the smart grid arena. Experience gained from its use will result in clarifications and improvements to the framework.

Also there are some of the directions in which we can expand this work. We have mentioned in the definition of scope that the stakeholder needs to be identified. It has been conventional to identify consumers or customers as a large number of homogeneous entities. But can all the consumers be considered the same? Even if residential purpose alone is considered, a free-standing house requirement will vary from those of residential apartments and those of holiday apartments. Hence there will be value for all parties from deepening risk evaluation from a consumer perspective and comparing the results with the current, provider-focused system.

Though this proposed framework is intended for the smart grid, it may have implications for other critical infrastructures as well. The ‘definition of scope’ changes based on the choice of infrastructure and except for that one process all the other processes remains the same. The SGAM model is only used as a plug-in to define the targets in the Smart Grid. So even if the model changes or a new model is used the framework will not be affected.

References

1. Danahy, J., Bochman, A.: Smart Grid for the CSO (2009)
2. Baumeister, T.: Literature Review on Smart Grid Cyber Security, Department of Information and Computer Sciences. University of Hawaii, Hawaii (2010)
3. Kasperson, R.E., Renn, O., Slovic, P., et al.: The Social Amplification of Risk - a Conceptual-Framework. Risk Analysis 8, 177–187 (1988)
4. Roberts, S., Redgrove, Z.: The smart metering programme: a consumer review. The Centre for Sustainable Energy, Bristol (2011)
5. Quinn, E.L.: Privacy and the new energy infrastructure. SSRN eLibrary (2009)

6. Fang, Y.D.: Smart Grid – The New and Improved Power Grid. IEEE Communications Surveys Tutorials PP, pp. 1–37 (2011)
7. Farhangi, H.: The path of the smart grid. IEEE Power and Energy Magazine 8(1), 18–28 (2010)
8. Deloitte, Department of Treasury and Finance- Advanced metering infrastructure cost benefit analysis- Final Report, Victoria (2011)
9. Lockstep Consulting, Privacy Impact Assessment Report - Advanced Metering Infrastructure (AMI), Victoria, Australia (2011)
10. Rambi, J.: Lessons learned from the new Smart Meter Risk Analysis Methodology in the Netherlands, Chairman Policy Committee Privacy & Security Netbeheer Nederland (January 16, 2013)
11. NIST, National Institute of Standard and Technology, NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0, Office of the National Coordinator for Smart Grid Interoperability (2010)
12. CEN-CENELEC-ETSI, Smart Grid Coordination Group Smart Grid Information Security (2012)
13. ISO/IEC 27005, ISO/lEC 27005 Information technology - Security techniques - Information security risk management, ISO/IEC 2008 (2008)
14. Stoneburner, G., Goguen, A., Fering, A.: Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30, VA 22042 (2002)
15. ENISA, Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, http://www.enisa.europa.eu/activities/risk-management (2005-2013)
16. SRA, Society for Risk Analysis (SRA) (2013), http://www.sra.org/
17. Kaplan, S.: The words of risk analysis. Risk Analysis 17(4), 407–441 (1997)
18. WP 29, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force, Article 29 Data Protection Working Party (2013)
19. Dimitrakos, T., Raptis, D., Ritchie, B., Stølen, K.: Model based Security Risk Analysis for Web Applications: The CORAS approach (2002)
20. Marek, P., Paulina, J.: The OCTAVE methodology as a risk analysis tool for business resources. In: International Multi-Conference on Computer Science and Information Technology (2006)
21. BSI, BSI-Standard 100-3: Risk analysis based on IT-Grundschutz (2008)
22. Security Risk Analysis Group, Introduction to Risk Analysis (2003), http://www.security-risk-analysis.com/introduction.htm
23. NRECA, Guide to Developing a Cyber Security and Risk Mitigation Plan, National Rural Electric Cooperative Association/Cooperative Research Network, Arlington, VA (2011)
24. EMF Safety Network, Smart Meter Fires and Explosions (2012), http://emfsafetynetwork.org/?page_id=1280