Enhancing Smart Grid System Processes via Philosophy of Security - *Case Study based on Information Security Systems* -*

Amy Poh Ai Ling† and Sugihara Kokichi
Department of Mathematical Modeling Analysis, and Simulation
Graduate School of Advanced Mathematical Sciences
Meiji University
amypoh@meiji.ac.jp, kokichis@isc.meiji.ac.jp

Mukaidono Masao
Department of Computer Science
School of Science and Technology
Meiji University
masao@cs.meiji.ac.jp

Abstract

A system is characterized as a group of ideas, functions or instruments that performs a particular function when put together. In order to sustain a good system, the organization must put continuous effort not only into its technical management but also into keeping an ear to the voice of the customer (VOC) to produce its desired outcome. The outcome refers to the product or service by which an organization survives or supports itself, such as information security systems in the smart grid. This paper focuses on the variable that could enhance the system processes of an information security system for the smart grid. Questionnaire surveys were carried out, followed by detailed, descriptive analysis. The statistical data portrayed consumer readiness towards the acceptance of smart grid. It also showed the understanding of the consumer towards the criteria identified. Outcomes from the descriptive analysis observed the essential ranking of information security consumer requirements. Results showed that the concern for privacy is the most important element among the other fifteen requirements. The extent to which private data is disclosed consequently determines the way or manner in which the population will perceive this information. Privacy to some degree comes across security, made up of, for instance, the concepts of appropriate use as well as the protection of data and information. The data from VOC showed that philosophy of security determines priorities in enhancing smart grid system processes. The philosophy category has the most powerful impact on consumer trust and satisfaction because the philosophy and strategy of management with regard to information security is the perfect standard against which technology and other security mechanisms can be measured. This statistical data could be referenced by utility providers or policy makers to strengthen information security systems of the smart grid. Correlation relationship ring and cluster concluded that the items in the hardware category are highly correlated to each other. Quality assured distributed devices have a high potential for solving significant process integrity security challenges. This paper gives insight into a picture of smart grid system information security's future direction.

Keywords: System processes, security, philosophy, smart grid, privacy, trust

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 3, number: 3, pp. 94-113

*This paper is an extended version of the work originally presented at the 26th IEEE International Conference on Advanced Information Networking and Applications (AINA 2012), Fukuoka Institute of Technology (FIT), Fukuoka, Japan, March 26-29, 2012 [1].

†Corresponding author: JSPS Research Fellow, Meiji Institute for Advanced Study of Mathematical Sciences, Meiji University, 1-1-1 Higashimita, Tamaku, Kawasaki, Kanagawa 214-8571, JAPAN, Tel: +81-080-4168-3882

1 Introduction

Smart grid, by and large, has to do with the technology savvy groups, who are endeavoring to bestow high end utility electricity delivery systems into the new century, putting into service computer-based remote control and automation. In the future, by adopting smart grid systems, we will be able to track our energy usage via real-time data retrieval from the Internet, switch on our washing machines remotely through a simple, quick click, and charge our electric vehicles in our own carports. Life would be engaged to new technology and much more convenient. However, since data and control management are heavily dependent upon the grid, an attack by hackers would create a serious hazard and bring the whole system down into chaos [2]. Once the system is damaged, society would be exposed not only to an unstable power supply but also to security risks [3, 4]. In order to avoid all of the volatilities of this ideal system, we realize the importance of information security as well as the protection of individual privacy. Previous research has successfully identified a set of sixteen information security functional requirements that includes information access limitation best practices, data authenticity, data and back-up recovery, personal key exchange, trusted networks, inter-operability and security, and so on [5]. This set of requirements facilitates the increasing usage of IT-based electric power systems, which then raises cyber security vulnerabilities and, by extension, the importance of cyber security. They are important mainly for helping the government and energy utility providers to enhance their system processes by providing a comprehensive and secured information security management system. This paper focuses on the five categories identified for the above-mentioned sixteen consumer requirements, namely philosophy, human behavior, rule based social systems, strategy systems and hardware [5]. A smart grid thinks and complies with the demands of energy utility providers and consumers. Hence, it is important to identify the consumers' expectations through VOC towards information security in the smart grid system and the essentiality of the classification.

The finding of logical or causal connection of the variable identified helps determine variables that are having close relation to each other and consensus level accuracy of the respondents. Grouping strong correlated variable in a cluster creates better security strategy planning with the enhance of the correlated main variables as a cluster. From the result, cluster I gives a motivated idea of a quality assured distributed devices have a high potential for solving significant process integrity security challenges.

2 Review of Literature

2.1 Security Issue

Security issues are always mentioned in forums, blogs and conferences; people want to know if the smart grid, with electricity prices that vary according to demand, can provide a strong assurance of protection to consumers. Efforts are made to ensure privacy and shrink bills while improving grid security and resilience. Energy utility providers are increasingly using Information and Communication Technology (ICT) to increase the efficiency and reliability of the grid, as well as incorporating smaller-scale sources of intermittent wind and solar power into the electricity supply. However, developments in international security have made clear that increased reliance on ICT within the electricity sector will create new vulnerabilities that may undermine these gains [6].

2.2 Grid Technology

Grid technology provides opportunities for simple and transparent access to different information sources. This idea was proven when the data grid could be interpreted as the consolidation of different data man-

aging systems furnishing the user with data, information and knowledge [7]. With the adoption of grid technology, business practices regarding personal data appear to be primarily responsible for people's privacy concerns. Opinion surveys show that consumers do not trust businesses' assurances of privacy [8]. This leads to security concerns and the need for proper access control policies. The call for security protection seems to be more attractive because the government or the energy utility providers need to gain consumer trust along with the development of the smart grid system with viable solutions for individual privacy protection introduced. The need to protect the privacy and security of priceless data over the grid is fueling an even greater need for common security evaluation criteria. In brief, information security professionals need to be aware that the workings of the most basic IT resource of electricity supply is changing in a manner that introduces a far larger and remotely addressable attack surface combined with the tempting opportunity for mischief and monetary gain [9, 10]. Such a vision facilitates our goal to identify the requirements for creating a strong hold for smart grid information security and privacy preservation.

2.3 Smart Grid and Security

Observing the increase awareness about the modern electric grid's vulnerability to cyber attack, utility providers and suppliers are concerned on the preventive action on the security of the smart grid. At this moment, the utilities employ grid monitoring and control system in the process of smart grid development. In the process, these grids and systems are linked to the internet which at the same time, exposed to unlimited risks. Consumer are the main role of play in a smart grid development, fearing of cyber attacks could create negative force towards smart grid adoption. Countries started to aware of the security issues and venture into security enforcement investment. There are many type of security models, one of the security requirements model were developed base on focused group and interview [11].

3 Significance of the Study

The importance of information security criteria is the main aspect perceived to impact customer trust towards the entire smart grid system [12]. While a number of smart grid information security requirements and regulations are available online, and although those guidelines are a significant step in securing the smart grid, they do not fully address potential vulnerabilities that can emerge [13, 14]. In these cases, security is generally described in terms of availability, integrity, and confidentiality while cyber systems are observed to be vulnerable to worms, viruses, denial-of-service attacks, malware, phishing, and user errors that compromise integrity and availability [15, 16].

In smart grid, there is such a broad spectrum of security issues, it is important to narrow down the areas of security categories so that the security of the smart grid system can be incredibly strong to protect against any possibility of vulnerabilities. Furthermore, we want to know how important the sixteen identified consumer requirements are, as perceived by the consumers. In addition, the degree of essentialness of the category would help to create a picture of the future direction of smart grid's system information security and provide deeper insight into information security enhancement solutions.

4 Research Methodology

4.1 Questionnaire Construction

A preferences questionnaire was adopted with questions that measured separate variables, which was used to generate the bounded questionnaire in which the respondent was presented with a continuous likert scale.

A non-comparative likert scaling techniques was used. The level of measurement of a variable in mathematics and statistics is a classification that was proposed in order to describe the nature of information contained within numbers assigned to objects and, therefore, within the variable.

The questionnaire was divided into 2 sections:
(1) Consumer perception of Consumer Requirements Model
(2) Demography

The respondent was asked to indicate his or her degree of agreement with the statement, or any kind of subjective or objective evaluation of the statement. In Section 1, a five-point scale was used. The questions comprised sixteen requirements: confidentiality, integrity, availability, privacy concerns, tactical oversight monitoring systems, facilities misuse prevention, networking issues, quality assurance, mature or proprietary protocols, cryptography and key management, reliable system levels, strategy support, security in wireless media reliable device levels, high bandwidth of communication channels, and microprocessor performance memory and compute capabilities. The demography variables measured at a nominal level in Section 2 include information on area of research interest and country.

4.2 Data collection

50 sets of questionnaires were distributed via international workshop, email and peer groups. Respondents were carefully selected based upon their varying degrees of knowledge on the subject of smart grid and its information security. 7 questionnaires were unreturned; 38 usable questionnaires were returned; 5 returned questionnaire were unusable. Each of the transaction numbers were recorded for back-up reference. The returned 38 sets of usable questionnaires were used to generate the analysis. Figure 1 shows the distribution of the country from where the respondents participated in the questionnaire survey.

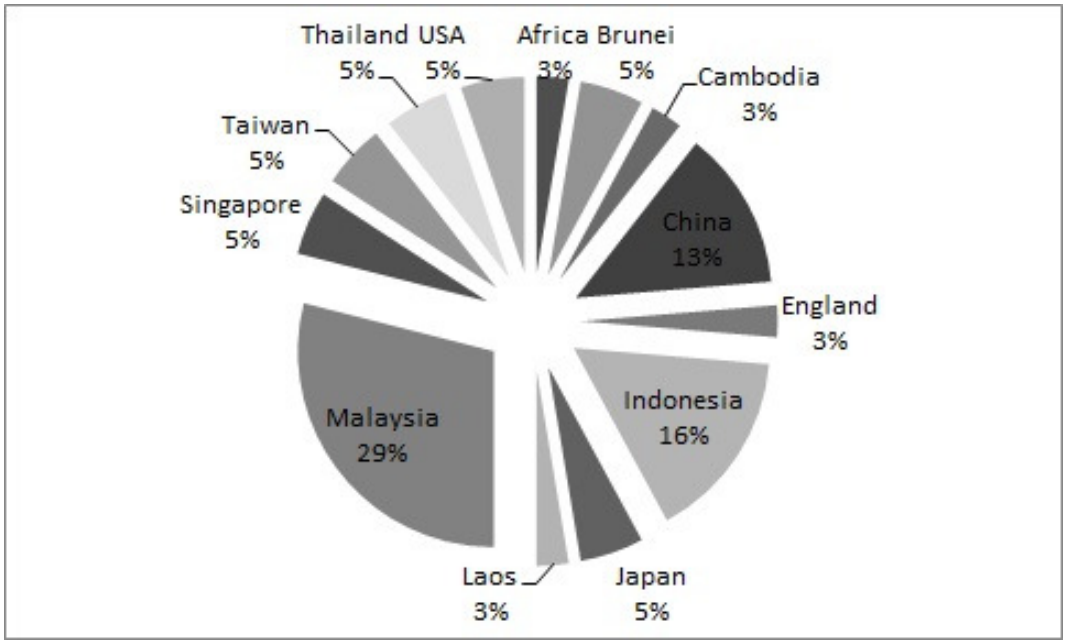

Figure 1: Country Distribution

4.3 Data Analysis: Descriptive analysis

Descriptive analysis was employed to examine the level of agreement of the respondents towards the identified sixteen information security consumer requirements in a smart grid system.

An attempt was made to develop a module that could be used to help the user to understand the plot of raw data, distribution pattern, and to generate descriptive analysis [17]. Minitab was employed to enhance the mathematical calculation to validate the effects of the importance of the consumer towards the information security in a smart grid system.

4.4 Observation via Means

This method enabled us to answer an important question in raw data management in our observations configuration to correctly capture the important feature in our expected model. In this paper, a systematic approach was developed of observation and ranking via mean to evaluate the importance of information security consumer requirements.

4.5 Lattice ordering

Lattice ordering was employed to examine the ranking of the importance of the five categories mentioned. The aim of the analysis was to concentrate on the category that the consumer perceived was the important element that contributed towards a strong foundation for a smart grid system.

A partially ordered set was developed in which any two elements had a unique supremum which referred to the elements least upper bound, called their join, and an infimum which referred to the greatest lower bound; called their meet [18]. This simpler lattice order model was developed to examine the rank of five categories perceived by the consumer.

4.6 Correlation Relationship (Ring and Cluster)

To determine the variables which are correlated to each other. If they are correlated, we could prove that the information security consumer requirements are mutually related by having corresponding characteristics.

5 Results

5.1 Plot Graph of 16 Consumer Requirements

Plot graph was employed to highlight clusters and gaps. In Figure 2, each dot represented up to 8 observations, and the number of dots in each column represented the frequency of respondents who selected the value associated with that column for the outlined sixteen consumer requirements. For example, 5 was the most popular rate, followed by 4. Value 1 was the least popular rate, having only 1 dot.

Out of the identified sixteen consumer requirements, respondents most strongly agreed “5”, followed by agreed “4” and then neutral “3”. There were only a few who expressed their disagreement to “1” and “2” on the identified requirements.

A cluster was observed. Variables 4, 5, 6 and 12 showed that there was no dot on the values of 1 and 2, which stand for disagree and disagree strongly, respectively. This proved that no respondent disagreed with the consumer requirements identified. Results concluded that the below variables are totally acceptable to the consumer.

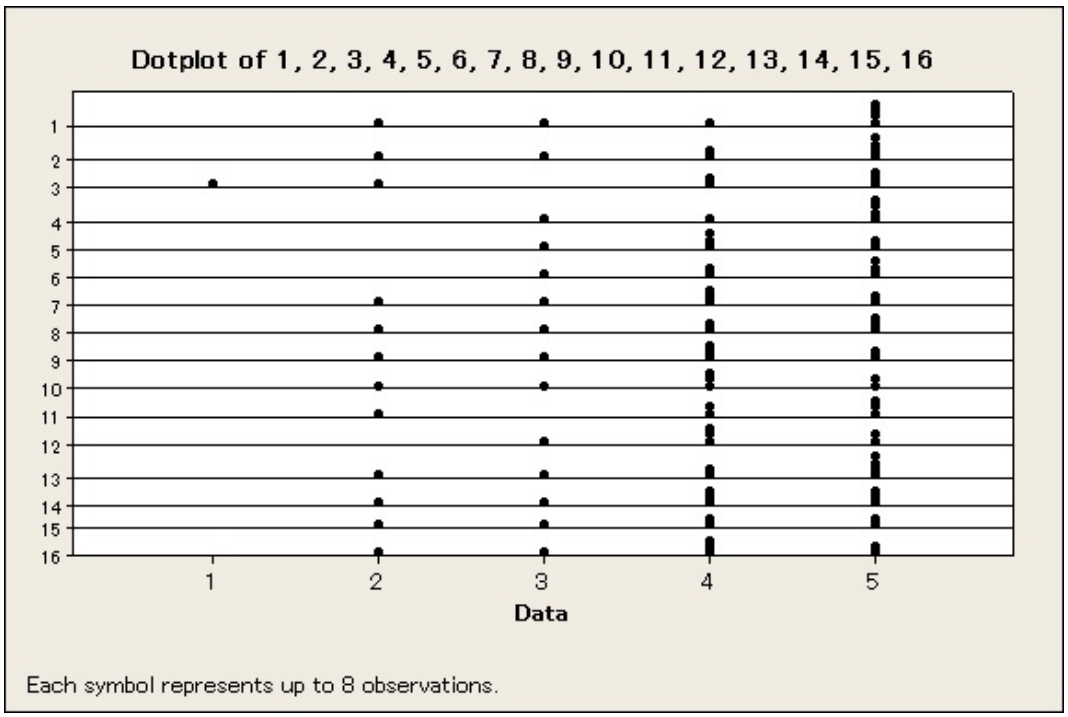

Figure 2: Plot Graph

(1) Variable 4: Privacy concerns

(2) Variable 5: Tactical oversight monitoring systems

(3) Variable 6: Facilities misuse prevention

(4) Variable 12: Strategic support

We could conclude that privacy concern, tactical oversight monitoring system, facilities misuse prevention and strategic support were among the undeniable important requirements that the consumer would expect the energy utility providers or government to keep an eye on.

5.2 Descriptive Statistics

This part of the analysis quantitatively described the main features of the data collected and provided a snap shot of the situation under this study.

Referring to the mean shown in Figure 3, variable 4 has the highest mean of 4.7632, which means most of the respondents favored and perceived that variable 4 is an essential requirement for a sustainable information security system. Tracing variable 15, it has the lowest mean of 4.079.

The results of this descriptive analysis were then employed to carry out the ranking of variables in next session.

Variable	N	N*	Percent	CumPct	Mean	SE Mean	StDev	Sum	Minimum
1	38	0	100	100	4.737	0.105	0.644	180.000	2.000
2	38	0	100	100	4.605	0.110	0.679	175.000	2.000
3	38	0	100	100	4.500	0.140	0.862	171.000	1.000
4	38	0	100	100	4.7632	0.0794	0.4896	181.0000	3.0000
5	38	0	100	100	4.132	0.108	0.665	157.000	3.000
6	38	0	100	100	4.526	0.111	0.687	172.000	3.000
7	38	0	100	100	4.289	0.113	0.694	163.000	2.000
8	38	0	100	100	4.474	0.118	0.725	170.000	2.000
9	38	0	100	100	4.079	0.127	0.784	155.000	2.000
10	38	0	100	100	4.132	0.126	0.777	157.000	2.000
11	38	0	100	100	4.474	0.124	0.762	170.000	2.000
12	38	0	100	100	4.184	0.112	0.692	159.000	3.000
13	38	0	100	100	4.526	0.124	0.762	172.000	2.000
14	38	0	100	100	4.368	0.109	0.675	166.000	2.000
15	38	0	100	100	4.079	0.157	0.969	155.000	2.000
16	38	0	100	100	4.132	0.137	0.844	157.000	2.000

Figure 3: Descriptive Statistic Table

5.3 Ranking of Variables: Information Security Consumer Requirement

The essentiality of information security consumer requirements were numbered after the variables' were ranked according to the results of the descriptive statistics analysis. For example, variable 4 had the highest mean value of 4.7632, thus variable 4 ranked number 1, as shown with a single line, followed by variable 1 (4.737), variable 2 (4.605) and so on. Variable 15 had the lowest mean value of 4.079, as showed with double line.

When two variables had the same mean value, for example variable 8 and variable 11 with a mean value of 4.474, the standard deviation value was referenced. The lower value of standard deviation was ranked higher for the reason that it had a lesser variation or dispersion from the average value.

All the requirements were rearranged according to their ranked number, resulting in the ranking of the consumer s' requirements being clearly displayed in a column. Privacy concerns became the most important element out of the sixteen requirements in terms of information security in a smart grid system. It is interesting to see that availability was ranked only sixth while privacy concern was ranked first.

Essentiality Ranking of Information Security Consumer Requirement:

- Privacy Concerns
- Confidentiality
- Integrity
- Facilities misuse prevention
- Security in wireless media
- Availability
- Quality assurance
- Reliable systems levels
- Reliable device levels
- Networking issues
- Strategic support
- Tactical oversight monitoring system
- Cryptography and key management
- Microprocessor perform memory and compute capabilities
- Mature or proprietary protocols
- High bandwidth of communications channels

Comparing this with the results of the Plot graph, privacy concern obviously prevailed in its importance. Whereas tactical oversight monitoring system, facilities misuse prevention and strategic support did not rank high, it did show that while they were not unimportant, there were other requirements that carried a heavier weight of significance.

5.4 Observation by Category of Essentiality Ranking of Consumer Requirements via Means Observation

Comparisons were made between the table of category and the table of ranking of information security consumer requirements via means observation.

Observation of Category and Essentiality Ranking of Consumer Requirements:

1- Privacy Concern —— Philosophy
2- Confidentiality —— Philosophy
3- Integrity —— Philosophy
4- Facilities misuse prevention —— Human Behavior
5- Security in wireless media —— Strategic System
6- Availability —— Philosophy

7- Quality assurance —————————————————————— Philosophy
8- Reliable systems level —————————————————————— Strategic System
9- Reliable device level —————————————————————— Hardware
10- Networking issues —————————————————————— Rule base Social System
11- Strategic support ——————————————————————Strategic System
12- Tactical oversight monitoring system ———————————————— Human Behavior
13- Cryptography and key management ————————————————- Strategic System
14- Microprocessor perform memory and compute capabilities ———————— Hardware
15- Mature or proprietary protocols ———————————————————— Rule base Social System
16- High bandwidth of communications channels ———————————— Hardware

Results showed that the rankings came from a mixture of the five categories of philosophy, human behavior, rule based social systems, strategic systems and hardware. Hence, the simpler lattice ordering was carried out to measure how the category would contribute towards consumer impact in a smart grid system.

5.5 Simpler Lattice Ordering to Measure the Impact of Information Security

Considering the means by categories, we measure

$$\frac{\sum_{i=n_1}^{n_2} a_i}{n_2 - n_1 + 1}$$

where n refers to the variable number, $[a_i : a_1, a_2 ... a_n]$ are the mean values of the variables.

We obtained:

(1) Philosophy: 4.6513

(2) Human Behavior: 4.329

(3) Rule Based Social Systems: 4.2807

(4) Strategic Systems: 4.329

(5) Hardware: 4.193

We observed that the output result has a pattern. Obviously, it could be classed into three groups:

(1) The first group: 4.6513
(Philosophy)

(2) The second group: 4.329, 4.2807, 4329
(Human Behavior, Rule Based Social Systems, Strategic Systems)

(3) The third group: 4.193
(Hardware)

A lattice order model was developed, as shown in the Lattice Order below.

Philosophy had the highest ranking among all categories. Human behavior, rule based social systems and strategic systems were in the middle layer, and hardware ranked last.

```
                    Variable 1 (4.6513)                                  Highly Important
-------------------------------------------------------------------------------------------
Variable 2 (4.329)  Variable 2 (4.2937)     Variable 2 (4.329)       Important
-------------------------------------------------------------------------------------------
                    Variable 2 (4.193)                                   Little Important
```

Figure 4: Lattice Order

Results showed that the philosophy category has the most powerful impact on consumer trust and satisfaction, because the philosophy and strategy of management with regard to information security is the perfect standard against which technology and other security mechanisms can be measured [19, 20].

5.6 Correlation Relationship Ring

We study the dynamics of correlation between the variables with different value of threshold. For many such situations, it was found that the correlations between individual variables are better indicators than the value of attributes. Figure 5 shows the correlation with the threshold α value of 4. All variable are shown correlated to each other. When the threshold was increased gradually, the correlation pattern changed, the correlation lines reduced, as showed in Figure 6 and 7. We could see that V1, V5, V7, V9, V10 and V13 are no longer linked to each other because they have weak correlation relationship to other variables.

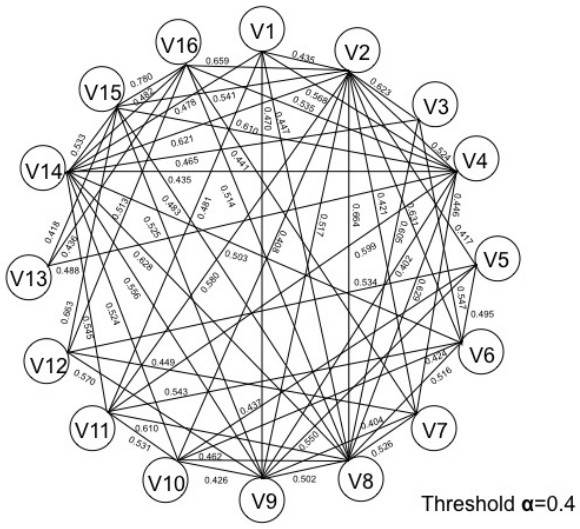

Figure 5: Correlation Relationship Ring, Threshold $\alpha = 0.4$.

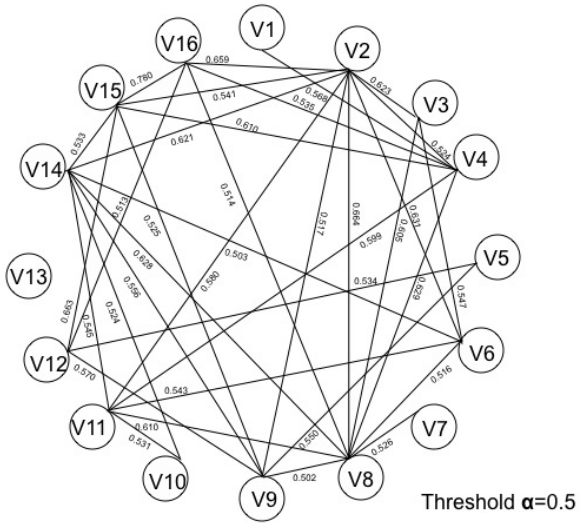

Figure 6: Correlation Relationship Ring, Threshold $\alpha = 0.5$.

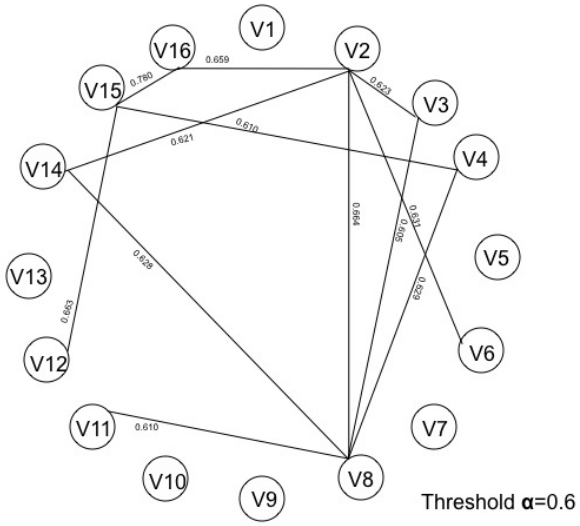

Figure 7: Correlation Relationship Ring, Threshold $\alpha = 0.6$.

5.7 Correlation Relationship Cluster

We cleaned the correlation matrix by setting the threshold value to $\alpha = 0.6$ and $\alpha = 0.66$ in order to create a correlation relationship cluster. In this cluster, we could see that they are group into two strong correlation clusters, as per below Figure 8.

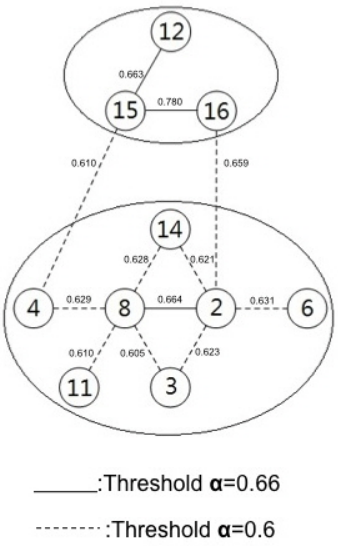

Figure 8: Correlation Relationship Cluster, Threshold $\alpha = 0.6$, $\alpha = 0.66$.

We cleaned again the correlation matrix by setting the threshold value to $\alpha = 0.66$ in order to create independent correlation relationship clusters.

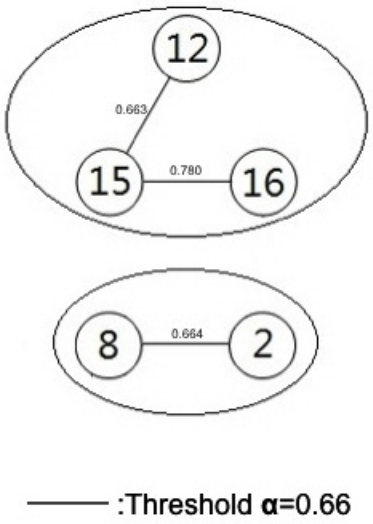

Figure 9: Correlation Relationship Cluster, Threshold $\alpha = 0.6$.

When the threshold value is $\alpha = 0.66$, we could clearly determine two clusters: Cluster I and Cluster II, as below:

- Cluster I
  (8) Quality assurance (Philosophy)
  (2) Integrity (Philosophy)

- Cluster II
  (12) Strategic support (Strategic System)
  (15) High bandwidth of communications channels (Hardware)
  (16) Microprocessor perform memory and compute capabilities (Hardware)

Strategic support belongs to the category of strategic system, while high bandwidth of communications channels, and microprocessor perform memory and compute capabilities belongs to the hardware category, so we could conclude that strategic system and hardware are closely correlated.

From Figure 9, variable 2 and 8 are integrity and quality assurance. Whereas variable 12, 15 and 16 are strategic support, high bandwidth of communications channels, and microprocessor perform memory and compute capabilities. Because integrity belongs to the category of philosophy, while quality assurance belongs to rule based social system, it supports to the statement that the elements of category philosophy and rule based social system are closely correlated.

Many discussed about security but only few talked about quality assurance. Smart grid is about providing power quality for twenty-one century needs, where quality assurance is referred to protecting customers and promoting the high quality infrastructure needed for the delivery of electricity. In another word, cyber security issues should be found during quality assurance or pre-production release testing. When quality assurance is important for security assessment, it always comes with integrity. Cluster I gives a motivated idea of a quality assured distributed devices has a high potential for solving significant process integrity security challenges.

6 Conclusion

According to the dot-plot analysis, the agreement with the identified sixteen consumer requirements was mostly strongly agreed “5” by the respondents, followed by agreed “4” and then neutral “3”. Only a few respondents responded their disagreement “4 and 5” on the identified requirements. There was no disagreement vote among the respondents on four requirements: privacy concerns, tactical oversight monitoring systems, facilities misuse prevention and strategic support. We could conclude that these four requirements were among the undeniably important requirements that the consumer would expect the energy utility providers or government to keep an eye on in order to strengthen a system process. Descriptive analysis successfully ranked the information security consumer requirements with the compass of mean and standard deviations. Privacy concerns became the most important element among the sixteen requirements in terms of information security in a smart grid system. The pattern obtained through the simpler lattice ordering analysis ranked philosophy number one, followed by human behavior, rule based social systems, strategic systems and hardware. The lattice ordering managed to narrow down the area of security category to philosophy.

Correlation relationship ring, cluster and tree concluded that the items in the hardware category are highly correlated to each other, when a consumer perceived on the hardware supporting the information security system, they perceived them as a package, for they carries the same weight.

For almost a century, utility providers have had to work on their privacy protection functions when they gather much of the data needed to provide electricity. This means that energy utility providers and the government should make philosophy their priority when enhancing their strategy and system processes so that the security of the smart grid system can be incredibly strong to protect against any possibility of vulnerabilities. The major finding of this paper exhibits agreement with the respondents on the criticality of the sixteen consumer requirements, the ranking of those requirements, and the importance of the category of philosophy in impacting consumer choice. This paper provides insight into the fact that information security enhancement strategy by identified philosophy category has the most

powerful impact on consumers' trust and satisfaction. Clearly, this would facilitate a coordinated effort to increase the energy utility providers' awareness.

As the publicity of the smart grid with its friendly function and benefits has been well presented to the consumer by NGOs, involved government parties, utility providers and suppliers, the acceptance of smart grid is no doubt at a positive level, although that level of acceptance might differ by region and country. According to the outcome of this case study, the consumer is prone to accept the smart grid with its strong information security systems specifically focused on the criteria of privacy concerns, confidentiality and integrity that belongs to the category of philosophy.

7 Acknowledgement

The authors wish to thank Professor Masayasu Mimura for mentoring. This study was supported by the Meiji University Global COE Program "Formation and Development of Mathematical Sciences Based on Modeling and Analysis", Meiji Institute for Advanced Study of Mathematical Sciences (MIMS), and the Japanese government's Ministry of Education, Culture, Sports, Science, and Technology (MEXT) scholarship.

References

[1] A. P. A. Ling, S. Kokichi, and M. Masao, "Security philosophy important for a sustainable smart grid system," in *Proc. of the 26th IEEE International Conference on Advanced Information Networking and Applications (AINA'12), Fukuoka Institute of Technology (FIT), Fukuoka, Japan*. IEEE, March 2012, pp. 29–34.

[2] C. Weber and A. Perrels, "Modelling lifestyle effects on energy demand and related emissions," *Energy Policy*, vol. 28, no. 8, pp. 549–566, July 2000.

[3] I. Rpøk, "New technology in everyday life-social processes and environmental impact," *Ecological Economics*, vol. 38, no. 3, pp. 403–422, September 2001.

[4] A. P. A. Ling and M. Mukaidono, "Smart Grid Information Security (IS) Functional Requirement," *Journal of Emerging Sciences*, vol. 1, no. 3, pp. 371–386, September 2011.

[5] Amy Poh Ai Ling and Masao Mukaidono, "Selection of Model in Developing Information Security Criteria on Smart Grid Security System," in *Proc. of the 9th International Symposium on Parallel and Distributed Processing with Applications Workshops (ISPAW'11), Busan, Korea*. IEEE, May 2011, pp. 91–98.

[6] I. L. Pearson, "Smart grid cyber security for Europe," *Energy Policy*, vol. 39, no. 9, pp. 5211–5218, September 2011.

[7] R. Stark, H. Hayka, and D. Langenberg, "New potentials for virtual product creation by utilizing grid technology," *CIRP Annals - Manufacturing Technology*, vol. 58, no. 1, pp. 143–146, 2009.

[8] A. Robbin, "The loss of personal privacy and its consequences for social research," *Journal of Government Information*, vol. 28, no. 5, pp. 493–527, September-October 2001.

[9] G. Laccetti and G. Schmid, "A framework model for grid security," *Future Generation Computer Systems*, vol. 23, no. 5, pp. 702–713, June 2007.

[10] S. Perry, "Watt matters - smart grid security," *Infosecurity*, vol. 6, no. 5, pp. 38–40, July-August 2009.

[11] A. P. A. Ling and M. Masao, "Grid Information Security Functional Requirement Fulfilling Information Security of a Smart Grid System," *International Journal of Grid Computing and Applications*, vol. 2, no. 2, pp. 1–19, June 2011.

[12] P.Herrmann, V. Issarny, and S. Shiu, "Trust Management," in *Proc. of the 3rd International Conference on Trust Management (iTRUST'05), Paris, France, LNCS*, vol. 3477. Springer-Verlag, May 2005, pp. 93–107.

[13] J.-P. Vasseur and A. Dunkels, *Smart Grid*. Morgan Kaufmann, 2010, pp. 305–324.

[14] L. Meeus and M. Saguan, "Innovating grid regulation to regulate grid innovation: From the Orkney Isles to Kriegers Flak via Italy," *Renewable Energy*, vol. 36, no. 6, pp. 1761–1765, June 2011.

[15] R. Akella, H. Tang, and B. M. McMillin, "Analysis of information flow security in cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 3, no. 3/4, pp. 157–173, December 2010.

[16] T. Flick and J. Morehouse, *Smart Grid: What Is It?* Syngress, 2001, pp. 1–18.

[17] R. Akella, H. Tang, and B. M. McMillin, "Minitab introduces advanced features for industrial statistics," *Computational Statistics and Data Analysis*, vol. 9, no. 1, pp. 165–166, January 1990.

[18] P. Jipsen and H. Rose, *Varieties of Lattices, Lecture Notes in Mathematics, Volume 1533*. Springer Verlag, 1992.

[19] S. Scott, *Cognitive Science and Philosophy of Language*. Elsvier, 2006, vol. 11, pp. 552–562.

[20] C. van der Walt, "Introduction to Security Policies, Part One: An Overview of Policies," http://www.symantec.com/connect/articles/introduction-security-policies-part-one-overview-policies, November 2010.

Amy Poh Ai Ling received her BBA and MSc from National University of Malaysia (UKM). She received her PhD in Mathematical Sciences from Meiji University. She was awarded Role Model Student Award (2003) and Excellent Service Award (2010) from UKM, and Excellent Student Award (2012) from Meiji University. She worked at Sony EMCS and Erapoly Sdn. Bhd. She is currently a postdoctoral affiliate with Meiji Institute for Advanced Study of Mathematical Sciences as JSPS Research Fellow. She has an enthusiasm for statistical calculation, smart grid and safety studies.

Sugihara Kokichi received his Master's and Dr. Eng. degrees from University of Tokyo. He worked at Electrotechnical Laboratory of the Japanese Ministry of International Trade and Industry, Nagoya University and University of Tokyo before joining Meiji University. His research area is mathematical engineering, including computational geometry, computer vision, computer graphics and robust computation. He is currently the leader of CREST research project of Japan Science and Technology Agency on "Computational Illusion".

Mukaidono Masao served as a full-time lecturer at Faculty of Engineering, Department of Electrical Engineering in Meiji University from 1970. Even since then, he was promoted to Assistant Professor on 1973 and as a Professor on 1978. He contributed as a researcher in an Electronic Technical Laboratory of the Ministry of International Trade and Industry (1974), Institute of Mathematical Analysis of Kyoto University (1975) and as a visiting researcher at University of California in Berkeley (1979). He then became the Director of Computer Center (1986) and Director of Information Center (1988) in Meiji University. At present, he is a Professor and Dean of the School of Science & Technology, Meiji University. He is also the honourable Councillor of Meiji University.

A Appendix: Exploratory Data Analysis (EDA) Stem-and-Leaf Display

The EDA Stem-and-Leaf Display analysis computed the basic statistics of data sets in a visual format, as showed below.

Result showed that there were two apparent scenarios: Rating one, two and three have lesser leaves than four and five. The result demonstrated most respondents agreed with the identified information security consumer requirement as how they perceived and was devoted to its importance towards the adoption of smart grid system.

```
Stem-and-leaf of 1  N  = 38
Leaf Unit = 0.10

 1    2  0
 2    3  0
 7    4  00000
(31)  5  0000000000000000000000000000000
```

Figure 10: EDA : Stem-and-Leaf Display for Variable 1

```
Stem-and-leaf of 2  N  = 38
Leaf Unit = 0.10

 1    2  0
 2    3  0
 12   4  0000000000
(26)  5  00000000000000000000000000
```

Figure 11: EDA : Stem-and-Leaf Display for Variable 2

```
Stem-and-leaf of 3  N  = 38
Leaf Unit = 1.0

 1    1  0
 2    2  0
 2    3
 14   4  000000000000
(24)  5  000000000000000000000000
```

Figure 12: EDA : Stem-and-Leaf Display for Variable 3

```
Stem-and-leaf of 4  N  = 38
Leaf Unit = 1.0

 1    3  0
 8    4  0000000
(30)  5  000000000000000000000000000000
```

Figure 13: EDA : Stem-and-Leaf Display for Variable 4

```
Stem-and-leaf of 5  N  = 38
Leaf Unit = 0.10

 6    3  000000
(21)  4  000000000000000000000
 11   5  00000000000
```

Figure 14: EDA : Stem-and-Leaf Display for Variable 5

```
Stem-and-leaf of 6  N  = 38
Leaf Unit = 0.10

 4    3  0000
 14   4  0000000000
(24)  5  000000000000000000000000
```

Figure 15: EDA : Stem-and-Leaf Display for Variable 6

```
Stem-and-leaf of 7  N  = 38
Leaf Unit = 0.10

 1    2  0
 3    3  00
(20)  4  00000000000000000000
 15   5  000000000000000
```

Figure 16: EDA : Stem-and-Leaf Display for Variable 7

```
Stem-and-leaf of 8  N  = 38
Leaf Unit = 0.10

 1    2  0
 3    3  00
 16   4  0000000000000
(22)  5  0000000000000000000000
```

Figure 17: EDA : Stem-and-Leaf Display for Variable 8

```
Stem-and-leaf of 9  N  =38
Leaf Unit = 0.10

 1    2  0
 8    3  0000000
(18)  4  000000000000000000
 12   5  000000000000
```

Figure 18: EDA : Stem-and-Leaf Display for Variable 9

```
Stem-and-leaf of 10  N  = 38
Leaf Unit = 0.10

 1    2  0
 7    3  000000
(18)  4  000000000000000000
 13   5  0000000000000
```

Figure 19: EDA : Stem-and-Leaf Display for Variable 10

```
Stem-and-leaf of 11  N  = 38
Leaf Unit = 0.010

 2    2  00
 2    3
 16   4  00000000000000
(22)  5  0000000000000000000000
```

Figure 20: EDA : Stem-and-Leaf Display for Variable 11

```
Stem-and-leaf of 12  N  = 38
Leaf Unit = 0.10

 6    3  000000
(19)  4  0000000000000000000
 13   5  0000000000000
```

Figure 21: EDA : Stem-and-Leaf Display for Variable 12

```
Stem-and-leaf of 13  N  = 38
Leaf Unit = 0.10

 1    2  0
 4    3  000
 13   4  000000000
(25)  5  0000000000000000000000000
```

Figure 22: EDA : Stem-and-Leaf Display for Variable 13

```
Stem-and-leaf of 14  N  = 38
Leaf Unit = 0.10

 1    2  0
 2    3  0
(19)  4  0000000000000000000
 17   5  00000000000000000
```

Figure 23: EDA : Stem-and-Leaf Display for Variable 14

```
Stem-and-leaf of 15  N  = 38
Leaf Unit = 0.10

 3    2  000
 10   3  0000000
(12)  4  000000000000
 16   5  00000000000000000
```

Figure 24: EDA : Stem-and-Leaf Display for Variable 15

```
Stem-and-leaf of 16  N  = 38
Leaf Unit = 0.10

 2    2  00
 7    3  00000
(17)  4  00000000000000000
 14   5  00000000000000
```

Figure 25: EDA : Stem-and-Leaf Display for Variable 16