J Electr Eng Technol.2017; 12(2): 495-501
https://doi.org/10.5370/JEET.2017.12.2.495

ISSN(Print) 1975-0102
ISSN(Online) 2093-7423

Methodology of Cyber Security Assessment in the Smart Grid

Pil Sung Woo* and Balho H. Kim†

Abstract – The introduction of smart grid, which is an innovative application of digital processing and communications to the power grid, might lead to more and more cyber threats originated from IT systems. In other words, The Energy Management System (EMS) and other communication networks interact with the power system on a real time basis, so it is important to understand the interaction between two layers to protect the power system from potential cyber threats. This paper aims to identify and clarify the cyber security risks and their interaction with the power system in Smart Grid. In this study, the optimal power flow (OPF) and Power Flow Tracing are used to assess the interaction between the EMS and the power system. Through OPF and Power Flow Tracing based analysis, the physical and economic impacts from potential cyber threats are assessed, and thereby the quantitative risks are measured in a monetary unit.

Keywords: Smart grid, Cyber threat, Information security, Energy management system, Optimal power flow, Power flow tracing, Analytic hierarchy process, Power system

1. Introduction

The power industry in South Korea has recently undergone various internal and external changes. With the goal of meeting its 2020 emission reduction target and realizing a green growth economy, South Korea has envisioned building a Smart Grid, which is a new power system to address climate change and increase energy usage efficiency. However, a power system requires strongly real-time characteristic as well as a high level of availability (low fault frequency and rapid recovery). Such characteristics make cyber threats in power systems more complex and fatal than in existing information technology (IT) systems.

Although much attention has been focused on cyber security issues regarding smart grids, the scope of previous research on cyber security issues does not extend beyond existing communication networks. Previous studies on smart grid security have concentrated on the area of communication as policy studies to apply existing information technology (IT) system security policies to the smart grid field [1-3].

In this paper, issues of smart grid security where physical characteristics of power systems were taken into consideration are defined clearly, and a strategic methodology was established that can produce a cyber-risk index in the smart grid using optimal power flow (OPF) and power flow tracing.

In addition, the study summarized and quantified security vulnerabilities in smart grid operations systematically through case studies, thereby proving that more efficient security measures can be established.

2. Risk Quantification in the Smart Grid

According to SANS institute[1] definition, a security vulnerability is a concept by which an external threat is introduced to internal systems.

Vulnerability is defined as a security hole, and the presence of vulnerability determines risk level in systems. Furthermore, threats refer to cyber-attacks, and assets are defined as the level of damage when threats occur due to vulnerabilities. The concept of vulnerabilities is schematically depicted in Fig. 1.

As shown in Fig. 1, vulnerability is a security hole, which can be regarded as a parameter between threat and

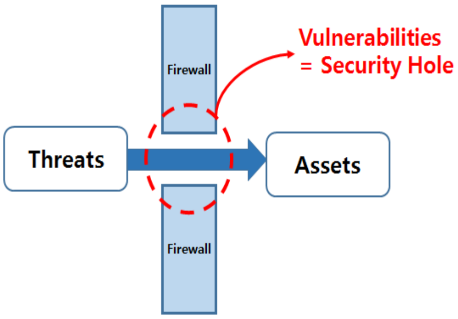

Fig. 1. Definition of Vulnerabilities

† Corresponding Author: Dept. of Electronic and Electrical Engineering, Hongik University, Seoul, Korea. (bhkim@hongik.ac.kr)
* Electrical Safety Research Institute, Korea Electric Safety CO., Korea. (woopilsung@kesco.or.kr)
Received: June 30, 2016; Accepted: October 25, 2016

[1] The SANS Institute (Officially the Escal Institute of Advances Technologies) is a private U.S. for-profit company founded in 1989 that specializes in information security and cybersecurity training. (http://www.sans.org/)

asset, and a recurring risk is defined as a combination of threat, vulnerability, to an asset [4].

Based on the above definition, risk can be formalized as shown in (1) where T, V, A, and R are threat, vulnerability, asset, and risk, respectively.

$$R = T \times V \times A \qquad (1)$$

In this study, a methodology for quantifying each factor was presented based on (1). First, T and V were classified as information system factors while A was quantified based on the power systems. Finally, to organically interlink the cyber threat from the point of view of reliability in power systems, optimal power flow and power flow tracing, which are core technologies in power system operation, were employed.

2.1 Methodology of quantification in information systems

Advanced researches have proposed and analyzed various quantification methods for information system factors. In this study, similar to many advanced researches, attack graphs are used to quantify cyber threats and vulnerabilities in the Smart Grid and potential probability per threat type was applied to measure the risk [5-8].

In this study, a part of the analytic hierarchy process (AHP), which is a quantification assessment method that considers multiple attributes, was applied based on data in previous studies [9, 10].

2.1.1 Quantification of Vulnerability (*V*)

To quantify vulnerability, 15 types of cyber threats were chosen and a correlation between components in power systems and individual threats was defined as shown in Table 1 [2].

A power system is normally controlled by the EMS; therefore, components of the EMS were considered.

Table 1. EMS Components and Threats

Components / Threats	EMS	SCADA	Com. Infra		RTU
			TCP/IP	Serial	
Eavesdropping	1	1	1	1	1
Traffic Analysis	0	0	1	1	0
EM/RF Interception	0	0	0	0	1
Indiscretions by Personnel	1	1	0	0	0
Media Scavenging	1	1	0	0	0
Trojan Horse	1	1	0	0	1
Trapdoor (Backdoor)	1	1	0	0	1
Service Spoofing	1	1	0	0	1
Masquerade	0	0	0	0	1
Bypassing Controls	0	0	0	0	1
Authorization Violations	1	1	0	0	1
Physical Intrusion	1	1	1	1	1
Replay	0	0	0	0	1
Theft & Illegitimate Use	0	0	0	0	1
Denial of Service	1	1	1	0	0
Total(36)	9	9	4	3	11

The shaded part in Table 1 refers to real risks that exist between EMS components and threats, while the non-shaded part refers to no correlation between components and threats.

To quantify vulnerability, the following four assumptions were established.

1. Correlation existed between components and threat = 1
2. No correlation existed between components and threat = 0
3. Threat occurrence probability = 50%

$$\text{Vulnerability} = \frac{\sum E_k}{T} \times 0.5$$

where,

E_k = Correlation of kth component in the EMS
T = Total correlation

Based on Table 1 and four assumptions, a quantitative value of vulnerability can be established as follows:

Table 2. Calculation of vulnerability quantification

	EMS	SCADA	TCP/IP	Serial	RTU
Vulnerability	0.13	0.13	0.06	0.04	0.15

In Table 2, the higher the vulnerability value, the easier the exposure to cyber threats.

2.1.2 Quantification of Threats

The quantitative values of threats are based on Table 1 in which vulnerability was analyzed and threat quantification

Table 3. Normalized potential threats as per EMS component (horizontal axis)

Components / Threats	EMS (5)	SCADA (4)	Com. Infra		RTU (1)	Normalization
			TCP/IP (3)	Serial (2)		
Eavesdropping	0.33	0.27	0.20	0.13	0.07	1
Traffic Analysis	0.00	0.00	0.60	0.40	0.00	1
EM/RF Interception	0.00	0.00	0.00	0.00	1.00	1
Indiscretions by Personnel	0.56	0.44	0.00	0.00	0.00	1
Media Scavenging	0.56	0.44	0.00	0.00	0.00	1
Trojan Horse	0.50	0.40	0.00	0.00	0.10	1
Trapdoor (Backdoor)	0.50	0.40	0.00	0.00	0.10	1
Service Spoofing	0.50	0.40	0.00	0.00	0.10	1
Masquerade	0.00	0.00	0.00	0.00	1.00	1
Bypassing Controls	0.00	0.00	0.00	0.00	1.00	1
Authorization Violations	0.50	0.40	0.00	0.00	0.10	1
Physical Intrusion	0.33	0.27	0.20	0.13	0.07	1
Replay	0.00	0.00	0.00	0.00	1.00	1
Theft & Illegitimate Use	0.00	0.00	0.00	0.00	1.00	1
Denial of Service	0.42	0.33	0.25	0.00	0.00	1

has EMS components (horizontal axis) and threats (vertical axis). A relative rank of threat is assigned according to potential damage size and the sizes of threat are normalized with 1. Normalization means that an individual EMS component I assigned its own threat level.

The following pre-conditions were made to quantify threats on the basis of the horizontal axis.

1. Non-shaded part based on Table 1 = 0
2. Relative rank according to EMS components (EMS=5, SCADA=4, TCP/IP=3, Serial=2, RTU=1)
3. The size of a threat = 1 (Normalization)

Applying the above three pre-conditions, the following Table 3 can be obtained.

The following pre-conditions were established with respect to the vertical axis in a similar manner as that for the horizontal axis.

1. Non-shaded part based on Table 1 = 0
2. Classification of threats based on three elements (Confidentiality, Integrity, and Availability (CIA)) of information security and mixed elements
3. Application of security threat level to control systems (Availability (4) > Integrity (3) > Mixed (2) > Confidentiality (1))
4. The size of a threat = 1 (Normalization)

Table 4. Normalized risk as per threat type (vertical axis)

Threats	Components	EMS	SCADA	Com. Infra		RTU
				TCP/IP	Serial	
Confidentiality	Eavesdropping (1)	0.04	0.04	0.08	0.13	0.04
	Traffic Analysis (1)	0.00	0.00	0.08	0.13	0.00
	EM/RF Interception(1)	0.00	0.00	0.00	0.00	0.04
	Indiscretions by Personnel(1)	0.04	0.04	0.00	0.00	0.00
	Media Scavenging(1)	0.04	0.04	0.00	0.00	0.00
Mixed (Confidentiality + Integrity)	Trojan Horse(2)	0.08	0.08	0.00	0.00	0.08
	Trapdoor (Backdoor) (2)	0.08	0.08	0.00	0.00	0.08
	Service Spoofing (2)	0.08	0.08	0.00	0.00	0.08
Integrity	Masquerade(3)	0.00	0.00	0.00	0.00	0.12
	Bypassing Controls(3)	0.00	0.00	0.00	0.00	0.12
	Authorization Violations(3)	0.12	0.12	0.25	0.38	0.12
	Physical Intrusion(3)	0.12	0.12	0.25	0.38	0.12
	Replay(3)	0.12	0.12	0.00	0.00	0.12
	Theft & Illegitimate Use(3)	0.12	0.12	0.00	0.00	0.12
Availability	Denial of Service(4)	0.16	0.16	0.33	0.00	0.00
Normalization		1	1	1	1	1

Table 4 shows the normalized results of risk per threat type (vertical axis).

To finally quantify threats, products between matrix components in Table 3 and Table 4 were calculated. Calculation of products between matrix components means that when a single arbitrary cyber threat occurs, its risk is shared over threat types and system components. Table 5 shows the product results between matrix components.

2.2 Methodology of Quantification in Power Systems

2.2.1 Quantification of Assets

In this section, the smart grid asset is defined as the value of communication equipment, such as EMS, SCADA, communication infrastructure (TCP/IP, Serial), and RTU that control the power system.

Therefore, the lost load value of communication equipment and supply disruption cost from exposure to threats were taken into consideration to quantify the values of assets.

$$A_n = \sum_{k=1}^{P} \left(LV_n^k(P) + OC_n^k(P) \right) \approx OC_n^k(P) \qquad (2)$$

where

P : Power[MW]
k : kth Subcomponent of EMS
A_n : Value of n components in EMS [KRW]
LV : Value of communicaiton equipment [KRW]
OC : Outage cost [KRW]

Eq. (2) states that the value of outage cost is overwhelmingly larger than the value of communication equipment; hence, the total cost can be approximated to the

Table 5. Results of threat quantification

Threats / Components	EMS	SCADA	Com. Infra		RTU	Total
			TCP/IP	Serial		
Eavesdropping	0.01	0.01	0.02	0.02	0.00	0.06
Traffic Analysis	0.00	0.00	0.05	0.05	0.00	0.10
EM/RF Interception	0.00	0.00	0.00	0.00	0.04	0.04
Indiscretions by Personnel	0.02	0.02	0.00	0.00	0.00	0.04
Media Scavenging	0.02	0.02	0.00	0.00	0.00	0.04
Trojan Horse	0.04	0.03	0.00	0.00	0.00	0.08
Trapdoor (Backdoor)	0.04	0.03	0.00	0.00	0.01	0.08
Service Spoofing	0.04	0.03	0.00	0.00	0.01	0.08
Masquerade	0.00	0.00	0.00	0.00	0.12	0.12
Bypassing Controls	0.00	0.00	0.00	0.00	0.12	0.12
Authorization Violations	0.06	0.05	0.00	0.00	0.01	0.12
Physical Intrusion	0.04	0.03	0.05	0.05	0.01	0.18
Replay	0.00	0.00	0.00	0.00	0.12	0.12
Theft & Illegitimate Use	0.00	0.00	0.00	0.00	0.12	0.12
Denial of Service	0.07	0.05	0.08	0.00	0.00	0.19
Total	0.34	0.28	0.20	0.12	0.54	

outage cost.

2.2.2 Methodology of Quantification in Power Systems

2.2.2.1 Optimal Power Flow (OPF) Formulation

In general, the OPF concept refers to the economic dispatch plan under technical, physical, and environmental constraints [11]. That is, economic dispatch plan and power flow calculation are conducted simultaneously. The formulation of OPF used in this study is summarized as follows:

Objective Function

$$\text{Minimize F} = \sum_{i\in I}\sum_{m\in M_i} f_{im} \tag{3}$$

$$\forall \text{m} \in M_i$$

$$f_{im} = \alpha_{im} + \beta_{im}\cdot PG_{im} + \gamma_{im}\cdot PG_{im}^2$$

Constraints

$$\sum_{m\in M_i} PG_{im} + \sum_{j\in I} PF_{ij} = PL_i\,,\ \ \forall \text{i} \in \text{I} \tag{4}$$

$$\sum_{m\in M_i} QG_{im} + \sum_{j\in I} QF_{ij} = QL_i\,,\ \ \forall \text{i} \in \text{I} \tag{5}$$

$$PF_{ij} = V_iV_j\{-G_l\cos(\delta_i-\delta_j)+B_l\sin(\delta_i-\delta_j)\} + (V_i)^2G_l\,,\ \ \forall l \tag{6}$$

$$QF_{ij} = -V_iV_j\{G_l\sin(\delta_i-\delta_j)+B_l\cos(\delta_i-\delta_j)\} + (V_i)^2(B_l - B_{cap}/2)\,,\ \ \forall l \tag{7}$$

$$PF_{ij} \le TP_l,\ \ \forall l \tag{8}$$

$$QF_{ij} \le TQ_l,\ \ \forall l \tag{9}$$

$$PG_{im}^{min} \le \text{P}G_{im} \le PG_{im}^{max},\ \ \forall \text{m} \in M_i \tag{10}$$

$$QG_{im}^{min} \le \text{Q}G_{im} \le QG_{im}^{max},\ \ \forall \text{m} \in M_i \tag{11}$$

$$V_i^{min} \le V_i \le V_i^{max},\ \ \forall \text{i} \in \text{I} \tag{12}$$

where,

I : Set of bus
M_i : Set of generators in Bus i
i, j : Bus No.
l : Trasmission line No.
m : Generator No.
PL_i : Active power injection in Bus i
QL_i : Reactive power injection in Bus i
G_l : Conductance in Line l
B_l : Susceptance in Line l
B_{cap} : Parallel capacitance in Line l
TP_l : Capacity of active power transmission line in Line l
TQ_l : Capacity of reactive power transmission line in Line l
PG_{im} : Active power from Bus i to Generator m
QG_{im} : Reactive power from Bus i to Generator m
PF_{ij} : Active power flowing from Bus i to Bus j
QF_{ij} : Rective power flowing from Bus i to Bus j
δ_i : Phase angle of Bus i
V_i : Voltage size of Bus i
f_{im} : Generation cost function of Generator m in Bus i

Eq. (3), which is an objective function, refers to the minimization of power generation cost. In addition, (4) and (5) are active and reactive power balance constraints, respectively. Eqs. (6) and (7) are active and reactive power flow constraints, respectively. Eqs. (8) and (9) refer to active and reactive constraints, respectively, with respect to power transmission lines. Eqs. (10) and (11) refer to active and reactive constraints, respectively, with respect to power generation. Finally, (12) is a constraint with respect to voltage size.

2.2.2.2 Power flow tracing

Power flow tracing is a technique for identifying a correlation between an individual generator and load based on power flow connected between gross generation and load parts. That is, damage owing to service interruption caused by disturbance can be estimated by identifying amounts of power supply to specific loads by individual generators.

There are many ways to perform power flow tracing. A power flow tracing method devised in [12] was used in this study; this power flow tracing method is based on Kirchhoff's current law (KCL) and graph theory and is suitable to resolve issues related to system topology and has an advantage of fast calculation.

3. Case Study

The simulation power system in this study is a 13-bus system: gross six generation and seven load buses. The loads have different attributes (residential, commercial, and industrial regions) and the same 345 kV line capacity is applied. The above assumptions are schematized in Fig. 2.

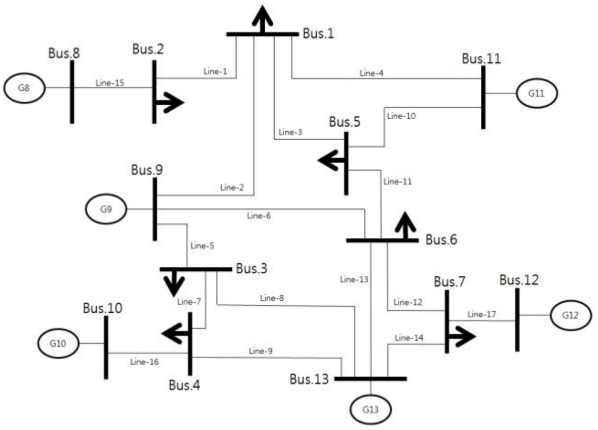

Fig. 2. 13-Bus power system

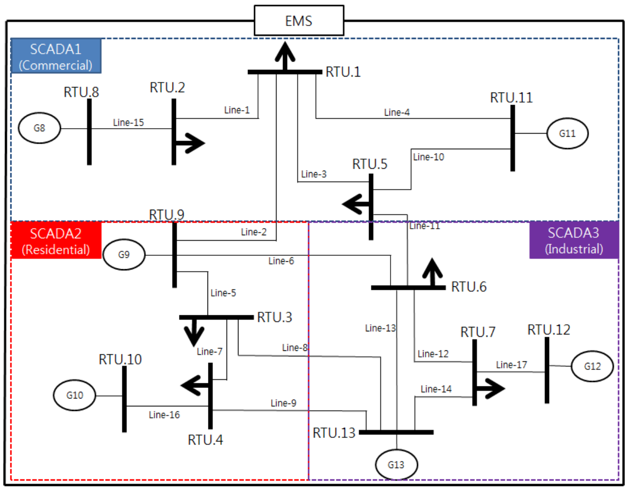

Fig. 3. Operation system of the EMS

Table 6. Generator and load data

Generator	Capacity [MW]	Load region	Load	Capacity [MW]
G8	1300	Commercial region	Bus 1	3500
G9	1300		Bus 2	700
G10	1400		Bus 5	1000
G11	2500	Residential region	Bus 3	500
G12	2500		Bus 4	600
G13	1500	Industrial region	Bus 6	700
			Bus 7	1800

Table 7. Outage cost according to load region

Load region	Outage cost [KRW/kWh]
Residential	2,800
Commercial	37,365
Industrial	127,420

According to Fig. 2, the Smart Grid was constructed based on the EMS operation system, which is shown in Fig. 3.

Information in each bus in Fig. 3 is transferred to a remote terminal unit (RTU) and controlled by supervisory control and data acquisition (SCADA) according to regional characteristics. Furthermore, the overall power system operation is managed by the EMS and all lines are constructed with communication lines as TCP/IP serial.

Table 6 shows the assumptions made for the simulation about generator capacity and loads.

For the outage cost, studies conducted by the Korea Electrotechnology Research Institute were referred [13]-[14]. The outage cost is defined in Table 7 according to load region.

4. Case Study Result and Analysis

The results of the optimal power flow using PSS/E based on the simulation power system data are as follows:

Table 8. Results of the optimal power flow(Net generation)

Generator	Net Generation [MW]
G8	1299.995
G9	200.0011
G10	800.0577
G11	2499.997
G12	2500
G13	1499.95

Table 9. Results of the optimal power flow

From	Line	To	Power Flow[MW]
Bus2	Line01	Bus1	600
Bus9	Line02	Bus1	1039.8
Bus5	Line03	Bus1	1050
Bus11	Line04	Bus1	810.2
Bus3	Line05	Bus9	608.8
Bus6	Line06	Bus9	231.1
Bus4	Line07	Bus3	400.8
Bus13	Line08	Bus3	708
Bus13	Line09	Bus4	200.7
Bus11	Line10	Bus5	1689.8
Bus6	Line11	Bus5	360.2
Bus7	Line12	Bus6	674.7

Table 10. Results of the power flow tracing

	G8	G9	G10	G11	G12	G13
Bus1	600	200	175.98	1675.61	227.53	620.86
Bus2	700	0	0	0	0	0
Bus3	0	0	144.49	0	5.83	349.68
Bus4	0	0	479.52	0	1.98	118.5
Bus5	0	0	0	824.39	0	0
Bus6	0	0	0	0	371.47	328.53
Bus7	0	0	0	0	1800	0

Power amount supplied to each regional load by individual generators can be calculated using power flow tracing based on the results of the optimal power flow in Tables 8 and 9 and the results are shown in Table 10.

A computerized model for power flow tracing in this study was implemented using C++.

An asset can be estimated by the production of outage cost according to load characteristics (Table 7) and power amount supplied to each region.

Table 11 represents results of each element in the information hierarchy after applying the quantification methodology for power systems based on Eq. 1.

The values in Tables 2 and 5 were calculated using the AHP technique in 2.1.1 and 2.1.2, which were applied to threat (T) and vulnerability (V), respectively.

Asset (A), which includes assets of EMS, SCADA, communication infrastructure (TCP/IP), and RTU, was calculated based on the EMS operation used in the power system shown in Fig. 3.

The asset of RTU was calculated by multiplying the value of lost load (Table 7) based on the load characteristics shown in Fig. 3 by the result of each region according to the power tracing method (Table 10). Furthermore, the asset of the communication line (Serial, TCP/IP) is

Table 11. Risk calculation results by EMS components

	EMS	SCADA1	SCADA2	SCADA3	RTU1	RTU2	RTU3	RTU4	RTU5
T	0.34	0.28	0.28	0.28	0.54	0.54	0.54	0.54	0.54
V	0.13	0.13	0.13	0.13	0.15	0.15	0.15	0.15	0.15
A	2,525,956	848,185	28,480	1,649,291	130,778	26,156	1,400	1,680	37,365
R	111,647	30,874	1,037	60,034	10,593	2,119	113	136	3,027
R[%]	37.69	10.42	0.35	20.27	3.58	0.72	0.04	0.05	1.02
	RTU6	RTU7	RTU8	RTU9	RTU10	RTU11	RTU12	RTU13	TCP1
T	0.54	0.54	0.54	0.54	0.54	0.54	0.54	0.54	0.16
V	0.15	0.15	0.15	0.15	0.15	0.15	0.15	0.15	0.06
A	89,194	229,356	48,575	560	8,323	93,412	288,694	69,450	22,419
R	7,225	18,578	3,935	45	674	7,566	23,384	5,625	215
R[%]	2.44	6.27	1.33	0.02	0.23	2.55	7.89	1.90	0.07
	TCP2	TCP3	TCP4	TCP5	TCP6	TCP7	TCP8	TCP9	TCP10
T	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16
V	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06
A	38,852	39,233	30,273	1,705	647	1,122	1,982	562	63,139
R	373	377	291	16	6	11	19	5	606
R[%]	0.13	0.13	0.10	0.01	0.00	0.00	0.01	0.00	0.20
	TCP11	TCP12	TCP13	TCP14	TCP15	TCP16	TCP17	Serial1	Serial2
T	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.08	0.08
V	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.04	0.04
A	13,459	85,970	78,554	3,224	48,574	2,240	318,550	22,419	38,852
R	129	825	754	31	466	22	3,058	72	124
R[%]	0.04	0.28	0.25	0.01	0.16	0.01	1.03	0.02	0.04
	Serial3	Serial4	Serial5	Serial6	Serial7	Serial8	Serial9	Serial10	Serial11
T	0.08	0.08	0.08	0.08	0.08	0.08	0.08	0.08	0.08
V	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04
A	39,233	30,273	1,705	647	1,122	1,982	562	63,139	13,459
R	126	97	5	2	4	6	2	202	43
R[%]	0.04	0.03	0.00	0.00	0.00	0.00	0.00	0.07	0.01
	Serial12	Serial13	Serial14	Serial15	Serial16	Serial17	T = Threat V = Vulnerability A = Asset[1millon KRW] R = Risk R[%] = Ratio of risk		
T	0.08	0.08	0.08	0.08	0.08	0.08			
V	0.04	0.04	0.04	0.04	0.04	0.04			
A	85,970	78,554	3,224	48,574	2,240	318,550			
R	275	251	10	155	7	1,019			
R[%]	0.09	0.08	0.00	0.05	0.00	0.34			

calculated by multiplying the value of the lost load of the region by the result of power flow (Table 9).

The asset of SCADA was controlled according to regional characteristics (commercial zone, residential zone, and industrial zone) so it was calculated as a total sum of assets of RTU and communication lines (Serial, TCP/IP) of the region.

Since the asset of EMS operated the total power system, it was calculated as the total sum of the assets of SCADA.

Finally, risk (R) was derived by applying Eq. 1 and multiplying by each of the elements (T, V, A).

So table 11 shows the risk in terms of monetary unit calculated finally based on the case study data. As shown in the table, the highest ratio of risk was found in EMS as 37.69%.

A ratio of risk according to load region also showed the following order : SCADA 3(industrial region) > SCADA 1(commercial region) > SCADA 2(residential region).

For RTUs and communication lines, the risk is different depending on power flow.

5. Conclusion

It is important to verify vulnerabilities individually and establish a countermeasure against them. However, it is also equally important to define and classify individual vulnerability in an orderly fashion, thereby assigning security resources and budgets appropriately from the viewpoint of overall system management.

In this paper, a foundation that can develop future security measures and solutions was provided by defining and classifying smart grid security elements, which had not been analyzed in detail.

In particular, the security assessment methodology where physical characteristics of power systems are taken into consideration proved that it could establish more effective security measures in the smart grid system. Moreover, this study concentrated on practicability by applying exact values.

For future study, more significant results can be derived if the smart grid security assessment algorithm is applied to real power systems.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation by the Ministry of Education (grant number. NRF-2015 R1D1A1A01057823)

References

[1] Sang Sun Hwang, Pil Sung Woo, Balho H. Kim, “Analysis of the Impact of Cyber Attacks on Energy Management Systems in Smart Grid Environment,” *International Journal of Smart Drid and Clean Energy*, Jun. 2016.

[2] Pil Sung Woo, Don Hur, Balho H. Kim, “Towards Cyber Security Risks Assessment in Electric Utility SCADA Systems,” Journal of Electrical Engineering & Technology, May. 2015.

[3] M. Negrete-Pincetic, F. Yoshida, and G. Gross, “Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environment,” in Proceedings of IEEE Power Tech Conference, Romania, July. 2009.

[4] SANS Institute InfoSec Reading Room, “Vulnerability Assessment,” July. 2001

[5] Vulnerability Assessment, Wikipedia.

[6] S. Massoud Amin, “Cyber and Critical Infrastructure Security: Toward Smarter and More Secure Power and Energy Infrastructures,” Canada-U.S. Workshop on Smart Grid Technologies at Vancouver, March. 25, 2010.

[7] S. P. Hong, “Introduction to Information Security,” Gilbut, 2004.

[8] P. Burris and C. King, “A Few Good Security Metrics,” METAGroup Inc., October. 11, 2000.

[9] Analytic Hierarchy Assessment, Wikipedia

[10] Ernest H. Forman, “Decision by Objective: Analytical Hierarchy Process,”

[11] Balho H. Kim, Ross Baldick, “Coarse-Grained Distributed Optimal Power Flow,” *IEEE Transactions on Power Systems*, May. 1997.

[12] Feliz Felix F. Wu, Yixin Ni, Ping Wei, “Power Transfer Allocation for Open Access Using Graph Theory-Fundamentals and Applications in Systems Without Loopflow,” *IEEE transactions on power systems*, vol. 15, No. 3, 2000.

[13] Korea Electrotechnology Research Institute and Incheon National University, “A Study to Investigate Industrial Customer Interruption Cost for Power System Planning,” Ministry of Commerce Industry and Energy, February. 2008.

[14] Korea Electrotechnology Research Institute and Seoul National University, “A Study to Establish the Range of Reasonable Compensation for Damages due to Power Outages by the Level of Electricity Price and Develop Strategies for Hedging Risks,” Marketing Department, Korea Electric Power Corporation, April. 2011.

Pil Sung Woo He received his B.S. degree from Pai Chai University, Korea, in 2012, and his M.S. degree in Electronic and Electrical Engineering from the Hongik University, Korea, in 2014. Currently, he is pursuing a Ph.D. degree in Electronic and Electrical Engineering at the Hongik University and has worked for research planning department in Electrical Safety Research Institute of KESCO since 2016. His research interests include optimization modeling and analysis for Smart Grid and power system operation & planning.

Balho H. Kim He received his B.S. degree from the Seoul National University, Korea, in 1984, and his M.S. and Ph.D. degrees from the University of Texas at Austin in 1992 and 1996, respectively. He was with KEPCO (Korea Electric Power Corporation) from 1984 to 1990 and joined Hongik University in 1997 where he is presently a professor of Electronic and Electrical Engineering. His research fields include optimal power flow, public utility pricing, electricity market design & operation, Smart grid, resource planning and demand management.