International Journal of Smart Grid and Clean Energy

Risk assessment for the security of power information control systems

Pil Sung Woo[a], Sang Sun Hwang[b], Soon Hyun Hwang[c], Balho H. Kim[c] *

[a] *KESCO (Korea Electric Safety Corporation), 12, Ogong-ro, lseo-myeon, Wanju-gun, Jeollabuk-do, 55365, Korea*
[b] *Korea Housing management, Korea*
[c] *Hongik University, 94, Wausan-ro, Seoul, 04066, Korea*

Abstract

The modern power industry needs to deal with the rapidly increasing demand for electricity and address environmental problems regarding sustainable growth. To this end, smart grids provide a comprehensive solution for next-generation power systems. Such a power information control system collects power information in real-time and yields optimum power generation control using different types of energy management systems. Owing to such characteristics a power information control system requires strong real-time information collection and control capabilities. Information collection and control properties are necessary because of the increased vulnerability associated with cyber security as opposed to existing information and communications systems. This study introduces a theoretical standard for the establishment of secure systems by analyzing the structure of the power information control system in addition to quantifying the risk of cyber-attacks that remain poorly studied.

Keywords: Smart grid, cyber security, risk assessment, EMS (energy management system), power system, SCADA

1. Introduction

The power industry is currently experiencing internal and external environmental changes. Changes in the infrastructure of the power industry due to the establishment of the smart grid and the promotion of new and renewable sources of energy together with the advent of fuel-free applications such as electric cars have ushered the upgrading of power information control system technology. Technological sophistication has promoted the efficiency of the operation of power systems but also affected other issues regarding this industry. A typical example is the smart grid, which is threatened by cyber-attacks. Cyber-attacks on information control systems of basic industries are increasing worldwide [1],[2]. In Ukraine, in 2015, a malicious code spread within the internal network of a power plant via a cyber-attack aimed at halting the power information control system, resulting in the interruption of power supply to over 80,000 households [3]. A power system requires reliable real-time operation and a very high standard of availability. Therefore, a cyber-security problem within these systems could cause complex and extensive damage; consequently, the establishment of a security system appropriate for smart grid is essential.

Thus, herein, we investigate the vulnerability of power systems to cyber-attacks by analyzing power information control systems and propose a quantitative risk-assessment methodology for the same.

2. Operation of Power System Following the Establishment of a Smart Grid

Existing power information control systems are usually hosted in buildings and exchange minimal data for continuous power supply [4]; i.e., a power system operates as a unidirectional communication system

*Manuscript received October 12, 2018; revised May 26, 2019.
Corresponding author. Tel.: +82-02-320-1462; *E-mail address:*.bhkim0711@gmail.com.
doi: 10.12720/sgce.8.4.488-494

from the power plant to households. However, future power information control systems will perform real-time bidirectional exchange of power information between the supplier and consumer through the connection of existing power systems and Information and Communications Technologies. Table 1 summarizes the operation of a power system when an existing system is converted to a smart grid [5]. The changes in the operation of power systems encourage reasonable energy consumption and enhance the quality of energy and related services. The increased vulnerability toward cyber-attacks due to the connection with an open communication network undermines the reliability of the operation of such a power system. In the next section, we propose a methodology for the risk assessment of a smart grid's security system by analyzing power information control systems.

Table 1. Changes in operation of power systems

Parameter	2010 Power System	2030 Smart Grid
Communication	Unidirectional	Bidirectional, real-time
Operation	Manual monitoring Regular maintenance	Automatic monitoring Condition-based maintenance
Generation	Centralized	Centralized and distributed power source

3. Analysis of Power Information Control Systems

A power information control system, known as the energy management system (EMS), includes a supervisory control and data acquisition system (SCADA), a master terminal unit (MTU), a remote terminal unit (RTU), and a field device (FD), as illustrated in Fig.1; the function of each component is well documented in the literature [6].

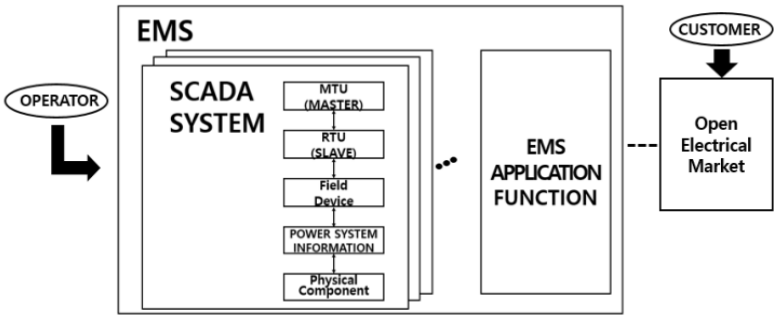

Fig. 1. Structure of the power information control system.

3.1. Energy management system

EMS performs the core functions of a power information control system including monitoring, control, analysis, and planning. It ensures optimum system operation through a combination of diverse application programs. EMS includes a SCADA system, the generation control and planning application program, and the power system analysis application program EMS controls the operation of power systems by regularly performing system stability evaluations and credible accident analyses through off-line analysis. Recent improvements enable EMS to execute various application programs with micro-grid requirements to account for the incorporation of distributed power sources into the network. The generalized functioning of EMS is illustrated in Fig. 2 [7].

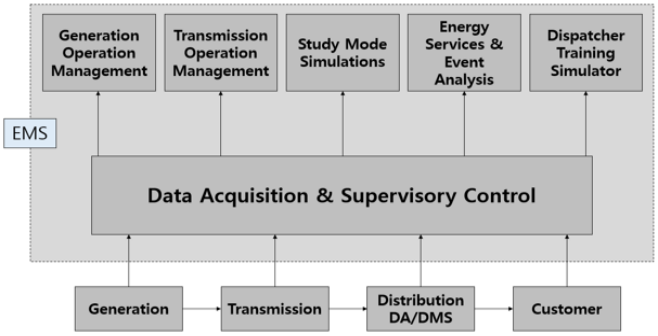

Fig. 2. Schematic showing the main components and their relations in EMS functioning.

3.2. Supervisory control and data acquisition

A SCADA system represents a sub-routine of EMS comprising the MTU and RTU for controlling the power plant and a substation of the power system. The functions of SCADA in a power system are classified as shown in Fig. 2 [8]. The basic function of SCADA is to collect general generation, transmission, and distribution data from the RTU. The collected data enables the control of power plants and substations connected to the EMS. The SCADA system usually contains one or more MTUs, with subordinate MTUs and RTUs under the main MTU.

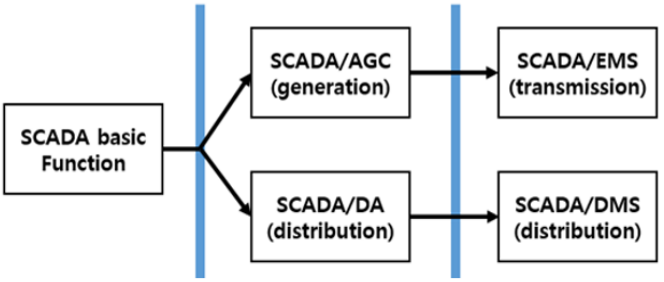

Fig. 3. Illustration of the basic functions of SCADA including generation, distribution, and transmission of data.

3.3. Master terminal unit

The MTU is a control system equivalent to the "brain" of the SCADA system. It contains an active input and output system that enables real-time monitoring and control of the power system through the connected RTU. MTU collects information transmitted from the RTU for delivery to the operator in the control room, and simultaneously enables the RTU to fulfill the operator's command.

3.4. Remote terminal unit

The RTU is a passive control system that controls on-site equipment at the command of the main MTU. It processes analog power information detected from the on-site equipment into a condition ready for digital communication through digital signal processing. In most cases, RTUs are located in physically separated areas. To collect the power information for all areas from all on-site equipment, RTUs are installed in a dispersed manner over a wide area.

3.5. Field device

FD connects the physical layer and power information control layer of a power system. It is the equipment that collects essential information of the power system and is controlled by the main MTU. The essential information includes the status values (circuit breaker, disconnector, ground switch, and

open/shut state of valves), control values (on/off condition of different power equipment and IT equipment), and measurement values (pressure, fluid pressure, voltage, current, phase angle, and frequency).

4. Methodology to Quantify Risks in Power Information Control Systems

According to the SANS Institute's definition of risks in cyber security [9], the scale of a risk is determined based on the combination of the threat, vulnerability, and asset. The relationship between the risk components are shown in Fig. 4.

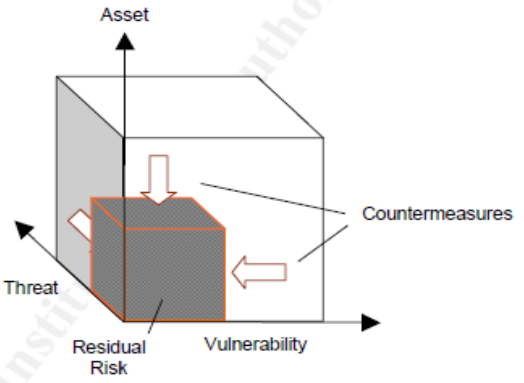

Fig. 4. Relationship between risk components.

In this study, the threat (T) was formulated using Eq. (1):

$$R = T \times V \times A \tag{1}$$

The threat indicates a cyber-attack on the power information control system and is the same as an independent variable used for calculating the system risk. Therefore, it can be defined by the number of occurrences of individual cyber-attacks that effectively damage a power information control system together with the degree of the impact from each-attack on the power information control system, as shown in Eq. (2):

$$T = \sum_{i=1}^{n} \sum_{i=1}^{n} (N_i^j \cdot I_i^j) \tag{2}$$

where, T is the total threat for a system; N is the number of cyber-attacks; I is the impact of a cyber-attack; I is the type of cyber threat; and j is a component of the power information control system.

Vulnerability represents the scale of the impact from an occurrence of a threat to the system, imposed on an individual system asset. It is calculated based on the components of the power information control system described in Section 3:

$$V = \sum_{i}^{n} (\alpha X_i^n + \beta X_i^n + \gamma X_i^n + \delta X_i^n) \tag{3}$$

where V is the total system vulnerability; α is the amplification factor of the risk for web-based open communication; β is the amplification factor of the risk for digital parallel communication; γ is amplification factor of the risk for analog parallel communication; δ is the amplification factor of the risk for analog serial communication; X is the unit control volume; and i is the type of power information.

In Eq. (3), the vulnerability estimate considers the importance of security based on the characteristics

of the control equipment and the scale of the control volume (X) of the control equipment.

In a smart grid, the assets must consider the economic value of consumer privacy. The calculated scale must consider all factors associated with damage caused by an attack. In this study, assets are classified as physical, intellectual, and human assets.

The supply interruption cost, which is a typical physical asset, represents large-scale economic damage caused by a blackout from a cyber-attack. Physical assets also include the cost of repair or replacement when electricity equipment or communication resources are damaged or broken.

Intellectual assets include the electric power technology of a power company or confidential information of the government. Information leakage of such assets incurs an enormous cost that can be directly linked to the supply interruption cost.

Human assets comprise the direct and the indirect costs for the human resources utilized to recover from or prevent a cyber-attack in addition to the costs incurred from the leakage of consumer power information or personal information in the smart grid system.

The subordinate components of each type of asset include all assets susceptible to damage. Such an asset is formulated as

$$A=\sum_{i=1}^{n}(A_P^i)+\sum_{j=1}^{n}(A_I^j)+\sum_{k=1}^{n}(A_H^k) \tag{4}$$

where $\mathbf{A}$ represents the system's total assets (KRW); A_P represents the system's physical assets (KRW); A_I represents the system's intellectual assets (KRW); A_H represents the system's human assets (KRW); $\mathbf{i}$ represents the type of physical asset; $\mathbf{j}$ represents the type of intellectual asset; and $\mathbf{k}$ represents the type of human asset.

5. Case Study

5.1. Composition of the model power information control system

For the model power information control system of this study, a next-generation EMS was installed at a power control command center to supervise the power system throughout the year. The SCADA system involved generation, transformation, and distribution, and subordinate components of the SCADA system included three MTUs with five RTUs and ten FDs (Fig.5)

The risk amplification factors α, β, δ, and γ were assumed to increase by a factor of four for each one-notch increase from γ; the corresponding data are presented in Table 2. The first term (αX_i) of (3) refers to the vulnerability of the EMS; the second term (βX_i) represents the vulnerability of the MTU; the third term (γX_i) represents the vulnerability of the RTU; and the last term (δX_i) represents the vulnerability of the FD.

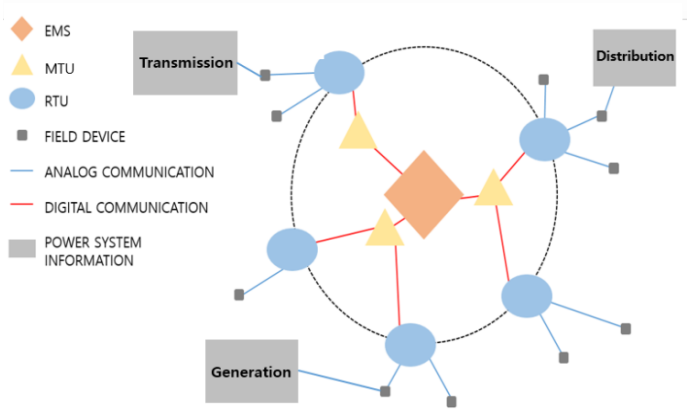

Fig. 5. Components of the model power information control system.

Table 2. Risk amplification factor data for different types of communication equipment

Type of communication equipment	Web-based open	Digital parallel	Analog parallel	Analog serial
Risk amplification factor	α	β	γ	δ
	64	16	4	1

To calculate the degree of a threat, the individual contribution of various components must be calculated while considering the frequency of cyber-attacks and consequent damage on the power information control system. However, for the sake of convenience, the number of attacks and the degree of impact for each threat were constant for all attacks on all power information control systems in this case study. The degree of the threat was calculated as shown in Table 3 while considering the effectiveness of the threat based on the results of preceding studies [10]-[12] and an EMS exposed to all threats.

Table 3. Threat data for various components of the power information control system

	EMS	MTU	RTU, FD
Threat	1	0.77	0.46

5.2. Case study analysis

In the structure of the power information control system, four cases were built for the EMS, MTU, RTU, and FD and were separately expanded in each unit to calculate the increase in the total risk. Table 4 shows the composition of the power information control system for each case. Case 1 is a power information control system assumed to possess two regional control centers and two EMSs. In case 2, four SCADA systems are assumed, whereas for cases 3 and 4, terminal control equipment of the RTU and FD are added.

Table 4. Constitution of power information control system for various cases

Case	EMS	SCADA		
		MTU	RTU	FD
Standard	1	3	5	10
Case 1	2	3	5	10
Case 2	1	4	5	10
Case 3	1	3	6	10
Case 4	1	3	5	11

The previously assumed parameters were introduced in an algorithm to calculate the vulnerability described in Section 3 and determine the final risk. The results for the rate of risk increment in each case are presented in Table 5.

Table 5. Risk increment rate for various cases

Case	Risk increase rate
Case 1	83.156%
Case 2	33.054%
Case 3	19.992%
Case 4	10.000%

The results of the case study reveal the highest risk increment rate for case 1, wherein the risks in the regional control centers increased to 83.156%. For the other cases, the risk increment rates are remarkably lower with values of 33.054%, 19.992%, and 10.00%.

6. Conclusions

This study defined cyber-attack threats to power systems and the notion of risk, which have previously received only superficial attention, to establish a quantitative methodology for the risk assessment of power control systems.

The degree of openness in the communication resource connected to the control volume of individual control equipment components in a power information control system was weighted for the risk-quantitative methodology. The results of the case study demonstrate that EMS is exposed to the greatest risk for damage during a cyber-attack. The results also reveal that the importance of control equipment is highest for EMS, followed by MTU, RTU, and FD, in that order. These results are useful as basic data for establishing security requirements to provide the groundwork for a reasonable decision-making process in establishing a cyber-security system based on a specific power system's risk index.

More meaningful results considering the weight of each cyber-attack and the quantification of each asset are envisaged in future research.

Acknowledgments

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

References

[1] National Intelligence Service, *National information protection white paper 2016*. September 2017.
[2] Negrete-Pincetic M, Yoshida F, Gross G. Towards quantifying the impacts of cyber-attacks in the competitive electricity market environment. Presented at: PowerTech, 2009 IEEE Bucharest.
[3] Lee KS. A study on KEPCO AMI system security policy in compliance with domestic legal regulations and standards. MS thesis. Department of Cyber Security, Korea University. Korea; 2015.
[4] Woo PS. A study on quantitative methodology to assess cyber security risks of SCADA systems. MS thesis. Department of Electrical and Control Engineering, Hongik University. Korea; 2014.
[5] Ministry of Knowledge Economy. Smart grid roadmap. 2017.
[6] Massoud Amin S. Cyber and critical infrastructure security: Toward smarter and more secure power and energy infrastructures. Presented at: Canada-U.S. Workshop on Smart Grid Technologies, 2010.
[7] Lee JH. Localization status and expectation effect of EMS. *Journal of Electrical World Monthly Magazine*, 2015; 1226–0665.
[8] Thomas MS, McDonald JD. *Power System SCADA and Smart Grids*. CRC Press; 2015.
[9] Yazar Z. *A Qualitative Risk Analysis and Management Tool-CRAMM*. SANS Institute; 2002.
[10] Hwang SS, Woo P, Choi S, Kima BH. Analysis of the impact of cyber-attacks on energy management system in smart grid environment. *International Journal of Smart Grid and Clean Energy*, 2016; 5(4): 245–251.
[11] Srinivasan S, Kotta U, Ramaswamy S. A layered architecture for control functionality implementation in smart grids. Presented at: 2013 10th IEEE International Conference on Networking, Sensing and Control (ICNSC).
[12] Ten CW, Liu CC, Manimaran G. Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, 2008; 23(4): 1836–1846.