International Journal of Smart Grid and Clean Energy

Risk analysis of power information control system based on smart grid security standardization

Pil Sung Woo[a], Balho H. Kim[b]*

[a] *Korea Electric Safety Corporation, 12, Ogong-ro, lseo-myeon, Wanju-gun, Jeollabuk-do, 55365, Rep. of Korea*
[b] *Hongik University, 94, Wausan-ro, Seoul, 04066, Rep. of Korea*

Abstract

The smart grid has emerged to meet the rapidly increasing power demand and solve environmental problems through sustainable development. Advanced power networks are being developed to improve the efficiency of power system operation and energy utilization. The advancement of power networks enables us to collect power information in real time, build a database, and optimally control it by utilizing various applications of organically constructed energy management systems. Currently, the rapid change in power infrastructure necessitates security, and the establishment of a cyber security system is essential. Therefore, this paper analyzes the functions of the power information control systems and calculates the risk level for each component by applying the security risk estimation criteria in the Korean Smart Grid security standard (SGSF-121-1-1).

Keywords: Smart grid security standard, Power system, Risk assessment, Power information constrol system, Cyber security

1. Introduction

The power industry is facing various environmental changes both within and outside the country. Changes in the infrastructure of the power industry due to the construction of a smart grid and the activation of new and renewable energy have inevitably driven the technological advancement of the power information control system [1]. This technological advancement has improved the efficiency of power system operation and produced various issues in the power industry. For example, when a smart grid is constructed and operated, the power system will be exposed to various cyber threats in the information technology (IT) field [2]. Furthermore, cyber attacks are increasing in key global industries. In 2014, a Korean anti-nuclear weapons group (Who Am I) leaked the internal information of Korea Hydro & Nuclear Power Co., Ld. (KHNP) through cyber attacks using malicious codes in an e-mail [3]. In the same year, the world's largest hacking event (DEFCON) announced a variety of hacking methods for intelligent watt-hour meters, and demonstrated that watt-hour meters are actually vulnerable to security by introducing simple information leaks to more complex methods of acquisition devices [4]. In 2015, a cyber attack in Ukraine caused a malicious code to spread to the internal network of a power plant, resulting in the suspension of the power information control system. This incident cut off the power supply to 80,000 households [5]. Owing to the physical characteristics of electricity, a power system requires strong real-time features and a high level of availability, and the cyber security problem is likely to cause greater complex, large damage than in the existing IT field. Therefore, it is vital to establish a security system suitable for the smart grid. This paper analyzes the function of each component of the power information control system and calculates the risk of each component by applying the security risk estimation criteria proposed in the smart grid security standard of South Korea (SGSF-121-1-1).

2. Structure of Power Information Control System

The components of the power information control system are defined as EMS (Energy Management

* Manuscript received April 23, 2018; revised January 8, 2019.

doi: 10.12720/sgce.8.2.140-148

System), SCADA (Supervisory Control And Data Acquisition System), MTU (Master Terminal Unit), RTU (Remote Terminal Unit), and FD (Field Device), and the functions of each component were analyzed [6]. Figure 1 illustrates the structure of the power information control system.

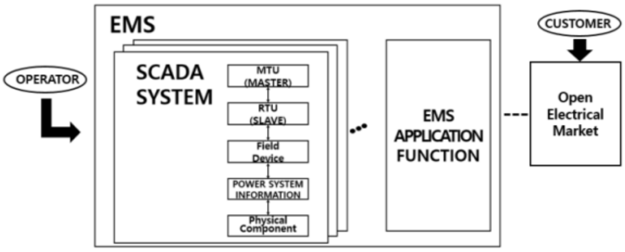

Fig. 1. Structure of power information control system.

2.1. EMS

EMS is the main agent that performs the core functions of power information control system (monitoring, control, analysis, planning, etc.) and is in charge of the optimum system operation based on an organic combination of diverse application programs. EMS is composed of a SCADA system, generation control and planning application program, power system analysis application program, etc. It plays an important role in the operation of power systems by regularly performing system stability evaluations and credible accident analyses based on an off-line study.

2.2. SCADA

SCADA system can be seen as the concept of EMS's sub-routine, which consists of MTU and RTU to control the power plant and substation of power system. First, the basic function of SCADA is to collect general generation, transmission, and distribution data from RTU. Based on the collected data, power plants and substations that are organically connected with EMS are controlled. The SCADA system structure generally has one or more MTU and subordinate MTUs and RTUs exist under the main MTU.

2.3. MTU

MTU is a control system that is equivalent to the brain of the SCADA system. It is a control system that has an active input and output system and enables a real-time monitoring and control of the power system through the connected RTU. In short, it 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 order.

2.4. RTU

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

2.5. FD

The FD plays the role of connecting the physical layer and the power information control layer of a power system. It is subject to the final control of the main MTU and is the equipment that collects the essential information of the power system. This essential information includes the status value (circuit breaker, disconnector, ground switch, open/shut state of valves, etc.), control value (on/off condition of different power equipment and IT equipment), measurement value (pressure, fluid pressure, voltage, current, phase angle, frequency, etc.).

3. Criteria for Estimating Risk from Identification of Security Threats

This study uses the risk estimation method of the smart grid security standard (SGSF-121-1-1) established in South Korea in 2014 [7], and this chapter summarizes the risk estimation criteria presented in the standard. This standard provides a procedure for ensuring the security of smart grid standards, which is applied to smart grid standards that require minimum security functions and interoperability to ensure security.

3.1. Identification of security targets

The smart grid security standard proposes identification of three types of security targets: security targets based on the objects of standardization; security targets based on the risk estimation criteria; and security targets based on communication, network, and data characteristics. If any system meets one of these three criteria for identification, its security must be ensured. To estimate the risk of a smart grid, this study adopts the second method, which is to identify the security targets based on risk estimation criteria. The criteria for identification are the risks of availability, integrity, and confidentiality, which are outlined in Table 1.

Table 1. Criteria for identification of targets for standardization based on risk criteria

Security Goal	Potential Impact		
	Low	Medium	High
Confidentiality	Unauthorized information leakage is expected to have a limited negative impact on the organization's operations and assets or on individuals.	Unauthorized information leakage is expected to have a serious negative impact on the organization's operations and assets or on individuals.	Unauthorized information leakage is expected to have an extreme or disastrous negative impact on the organization's operations and assets or on individuals.
Integrity	Unauthorized modification or destruction of information is expected to have a limited negative impact on the organization's operations and assets or on individuals.	Unauthorized modification or destruction of information is expected to have a serious negative impact on the organization's operations and assets or on individuals.	Unauthorized modification or destruction of information is expected to have an extreme or disastrous negative impact on the organization's operations and assets or on individuals.
Availability	Suspension of access to and use of information systems is expected to have a limited negative impact on the organization's operations and assets or on individuals.	Suspension of access to and use of information systems is expected to have a serious negative impact on the organization's operations and assets or on individuals.	Suspension of access to and use of information systems is expected to have an extreme or disastrous negative impact on the organization's operations and assets or on individuals.

3.2. Identification of security threats

The smart grid security standard presents 11 security threats and recommends that smart grid standard developers should estimate risk through the identification of security threats. Table 2 lists the 11 security threats presented in this standard, and the identification criteria for the major security threats defined in the standard are as follows. First, the damage of information and its ripple effects are outlined in Table 3, which are the criteria for analyzing the threat of security violation against information from (T1) through (T6) of the 11 security threats. Table 4 lists the evaluation criteria for identification of physical security threats. Table 5 defines the criteria for the importance of the standard targets. Finally, Table 6 classifies 11 security threats according to the estimation of risk in terms of confidentiality, integrity, and availability for five standard targets.

Table 2. Eleven security threats of the smart grid security standard

Security threats	Subdivision
(T1) Leakage of data stored in devices and systems	(T1-2) Low-priority data (T1-3) High-priority data
(T2) Leakage of communication data	(T2-2) Low-priority communication data (T2-3) High-priority communication data
(T3) Deletion of data stored in devices and systems	(T3-2) Deletion of low-priority data (T3-3) Deletion of high-priority data
(T4) Falsification of data stored in devices and systems	(T4-2) Falsification of low-priority stored data (T4-3) Falsification of high-priority stored data
(T5) Falsification of communication data	(T5-2) Falsification of low-priority communication data (T5-3) Falsification of high-priority communication data
(T6) Forgery of communication data	(T6-2) Forgery of low-priority communication data (T6-3) Forgery of high-priority communication data
(T7) Manipulation of equipment through physical access	(T7-1) Physical access to devices with low physical attack threat (T7-2) Physical access to devices with high physical attack threat and low ripple effect (T7-3) Physical access to devices with high physical attack threat and high ripple effect
(T8) Unauthorized access to the network of devices and computing devices	(T8-2) Unauthorized access to field network (T8-3) Unauthorized access to operation network
(T9) Denial of act	(T9-2) Denial of act causing damage to individuals and measuring devices (sensors) (T9-3) Denial of act causing damage to groups, industries, countries, etc.
(T10) Use of prohibited features by persons in charge, devices, processes, etc.	(T10-1) Use of prohibited features related to data reading (T10-2) Use of prohibited features related to data creation or manipulation (T10-3) Use of prohibited features related to control
(T11) Excessive use of resources	(T11-2) Excessive use of general system resources (T11-3) Excessive use of network resources or important systems

Table 3. Criteria for damages and ripple effects of information

Grade	Damage level	Ripple effect
High	Damage to information related to operations and system control such as control information and operation information, or personal information	The damage can spread to a city or large areas
Middle	Damage to setup information such as devices, systems, services, protocols	The damage can spread to relevant systems, devices, protocols, and services, as well as peripheral systems and devices
Low	Damage to information related to small amounts of data, etc., among general statistical data and data collected from multiple sensors for generation of statistics	The damage occurs only to the relevant systems, devices, protocols, services, etc.

Table 4.Criteria for evaluating the accessibility, physical security level and the spreading level of device damage at the installation site

Grade	Accessibility	Physical security level	Spreading level of device damage
High	Installed in an external space that is easily accessible by anyone	Personal authentication devices such as biometrics and access card and physical security devices such as CCTV that are operated 24/7 are installed.	The damage is spread to a city or larger areas.
Middle	Installed in an external space, but it is accessible only by the help of special equipment Installed in an independent space or in a space whose entrance is easily accessible by anyone	There are physical locking devices such as padlocks, and physical security devices are constructed in such a manner that, although CCTVs exist, 24/7 monitoring is not performed.	The damage is spread to the relevant devices and some peripheral devices.
Low	Installed in an independent space that is accessible only by limited people	There are no special physical security devices except for locks for devices and systems.	Services can be provided even if the devices do not work.

Table 5. Criteria for importance of standard targets

Grade	Importance of standard targets
High	The damage is spread to a city or larger areas.
Middle	The damage is spread to the relevant device and some peripheral devices.
Low	Services can be provided even if the devices do not work.

Table 6. Criteria for risk estimation for standard targets depending on the identification of security threats

Damage area	Level	Device	System	Protocol	Service	Data
Confidentiality	1	-	-	-	-	-
	2	T1-2 T2-2	T1-2 T2-2	T2-2	T1-2 T2-2	T1-2 T2-2
	3	T1-3 T2-3	T1-3 T2-3	T2-3	T1-3 T2-3	T1-3 T2-3
Integrity	1	-	-	-	-	-
	2	T3-2 T4-2 T5-2 T6-2 T9-2	T3-2 T4-2 T5-2 T6-2 T9-2	T5-2 T6-2 T8-2 T9-2	T3-2 T4-2 T5-2 T6-2 T8-2 T9-2	T4-2 T5-2 T6-2 T8-2 T9-2
	3	T3-3 T4-3 T5-3 T6-3 T9-3	T3-3 T4-3 T5-3 T6-3 T9-3	T5-3 T6-3 T8-3 T9-3	T3-3 T4-3 T5-3 T6-3 T8-3 T9-3	T4-3 T5-3 T6-3 T8-3 T9-3

Availability	1	T7-1 T10-1	T7-1 T10-1	-	T10-1	T10-1
	2	T3-2 T7-2 T10-2 T11-2	T3-2 T7-2 T10-2 T11-2	T11-2	T3-2 T10-2 T11-2	T3-2 T10-2 T11-2
	3	T3-3 T7-3 T10-3 T11-3	T3-3 T7-3 T10-3 T11-3	T11-3	T3-3 T10-3 T11-3	T3-3 T10-3 T11-3

4. Risk Evaluation Based on the Structure of the Power Information Control System

This chapter evaluates the risk based on the security threats for each component of the power information control system by applying the criteria defined in the smart grid security standard mentioned in Chapter 3.

4.1. Identification of security threats for each component of the power information control system

The security threats of each component of the power information control system were identified based on 11 security threats. First of all, Table 7 shows the threats of security violations for information (T1 ~ T6) among the 11 security threats. In Table 7, importance was applied as the top criterion for the damage level and ripple effect. Furthermore, the information assets were matched to (T1) to (T6) depending on the presence or absence of the security threat, and the standard security threat was determined as the top criterion.

Table 7. Identification of security threats of the power information control system related to information

Target	Damage level	Ripple effect	importance	T1	T2	T3	T4	T5	T6
EMS	High	High	High	T1-3	-	T3-3	T4-3	-	-
SCADA	High	High	High	T1-3	-	T3-3	T4-3	-	-
MTU	Middle	High	High	T1-2	T2-3	T3-2	T4-2	T5-3	T6-3
RTU	Middle	Middle	Middle	-	T2-3	-	-	T5-3	T6-3
FD	Low	Low	Low	-	T2-2	-	-	T5-2	T6-2

Next, Table 8 shows the identification of physical access security threats, and Tables 9 and 10 show the identification of security threats (T10) and (T11), respectively. Finally, the unauthorized access to network (T8) and the denial of act (T9) are defined in Table 11.

Table 8. Physical access security threats

Target	Place risk	Damage spreading	T7
EMS	Low	High	T7-1
SCADA	Low	High	T7-1
MTU	Middle	Middle	T7-2
RTU	Middle	Middle	T7-2
FD	High	Low	T7-2

Table 9. Threats for using prohibited features

Target	Function type	Accessibility	T10
EMS	Active control	Impossible	-
SCADA	Active control		-
MTU	Active control	Possible	T10-2
RTU	Passive control		T10-1
FD	Data collection		T10-1

Table 10. Treats for using excessive resources

Target	Resource type	Importance of standard target	T11
EMS	System	High	T11-3
SCADA	System	High	T11-3
MTU	Device	Middle	T11-2
RTU	Device	Middle	T11-2
FD	Device	Low	T11-2

Table 11. Threats for unauthorized access to network and denial of act

Target	Unauthorized access to network (T8)	Denial of act (T9)
EMS	T8-3	T9-3
SCADA	T8-3	T9-3
MTU	T8-2	T9-2
RTU	T8-2	T9-2
FD	T8-2	T9-2

4.2. Risk evaluation of the power information control system

This chapter summarizes the security threats identified in Chapter 4.1 in a single table and the risk of each component of the power information control system is estimated. EMS and SCADA were classified as systems, and MTU, RTU, and FD were classified as devices. Then the risk of each component was estimated. For EMS and SCADA, the risks of confidentiality, integrity, and availability were all estimated as level 3. For MTU, RTU, and FD, which were classified as devices, the risks were estimated as level 3 for confidentiality and integrity and level 2 for availability.

Table 12. Risk of EMS

Security threat		T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	EMS
Security threat level		T1-3	-	T3-3	T4-3	-	-	T7-1	T8-3	T9-3	-	T11-3	Risk
Security service violation risk	Confidentiality	3	-	-	-	-	-	-	-	-	-	-	3
	Integrity	-	-	3	3	-	-	-	-	3	-	-	3
	Availability	-	-	-	-	-	-	1	-	-	-	3	3

Table 13 Risk of SCADA

Security threat		T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	SCADA Risk
Security threat level		T1-3	-	T3-3	T4-3	-	-	T7-1	T8-3	T9-3	-	T11-3	
Security service violation risk	Confidentiality	3	-	-	-	-	-	-	-	-	-	-	3
	Integrity	-	-	3	3	-	-	-	-	3	-	-	3
	Availability	-	-	-	-	-	-	1	-	-	-	3	3

Table 14. Risk of MTU

Security threat		T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	MTU Risk
Security threat level		T1-2	T2-3	T3-2	T4-2	T5-3	T6-3	T7-2	T8-2	T9-2	T10-2	T11-2	
Security service violation risk	Confidentiality	2	3	-	-	-	-	-	-	-	-	-	3
	Integrity	-	-	2	2	3	3	-	-	2	-	-	3
	Availability	-	-	-	-	-	-	2	-	-	2	2	2

Table 1.5 Risk of RTU

Security threat		T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	RTU Risk
Security threat level		-	T2-3	-	-	T5-3	T6-3	T7-2	T8-2	T9-2	T10-1	T11-2	
Security service violation risk	Confidentiality	-	3	-	-	-	-	-	-	-	-	-	3
	Integrity	-	-	-	-	3	3	-	-	2	-	-	3
	Availability	-	-	-	-	-	-	2	-	-	1	2	2

Table 16. Risk of FD

Security threat		T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	FD Risk
Security threat level		-	T2-3	-	-	T5-3	T6-3	T7-2	T8-2	T9-2	T10-1	T11-2	
Security service violation risk	Confidentiality	-	3	-	-	-	-	-	-	-	-	-	3
	Integrity	-	-	-	-	3	3	-	-	2	-	-	3
	Availability	-	-	-	-	-	-	2	-	-	1	2	2

5. Conclusion

This study identified the cyber threats of a power information control system, and estimated the risk to each component of the system.

To estimate the security risk of each component, this study applied the standardization target identification criteria and security threat identification criteria presented in the smart grid security standard. To analyze the estimated risks, the EMS and SCADA, which were classified as systems, were estimated to have the highest level of security service violation risk. Thus, more detailed security measures should be prepared for the identified security threats. Furthermore, MTU, RTU, and FD, which were classified as devices, were estimated to have risk level 3for confidentiality and integrity and risk level 2 for availability. In particular, the MTU requires more diverse security measures compared to other devices because it was identified in every security threat owing to its functional characteristics. The results of this study can be used as basic data for establishing the security requirements of a smart grid and will provide a basis for rational decision making in the development of a cyber security system that reflects the characteristics of the power system operating system. In follow-up research, more meaningful results could be obtained by establishing guidelines for security measures based on the risk for each component of the power information control system.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation by 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] Hwang SS, Woo PS, Choi S, Kim 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.

[4] 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.

[5] 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.

[6] Woo PS, Hwang SS, Hwang SH, Kim BH. Risk Assessment for Secruity of Power Information Control System. *International Journal of Smart Grid and Clean Energy*, 2018.

[7] Korea Smart Grid Association. Requirements for Ensuring of Smart Grid Standards (SGSF-121-1-1). *SmartGrid Standardization Forum*, 2014.