International Journal of Smart Grid and Clean Energy

Analysis of the impact of cyber attacks on energy management system in smart grid environment

Sangsun Hwang, Pilsung Woo, Sejong Choi, Balho H. Kima

Hongik Univ., Power Economy lab., Sangsu-Dong Mapo-gu Seoul, Korea

Abstract

Smart grids are an integrated solution to recently raised issues in the power industry. To achieve the main objectives of a smart grid, Energy Management System (EMS) must organically connect numerous SCADA systems included in existing power control systems. As such, it is necessary to establish vulnerability classification criteria for cyber security in the large-scale, multi-functional complex architecture of EMS. This paper presents a methodology for classifying cyber threats that can be applied to EMS models in a smart grid environment, and a qualitative analysis of the interactions between each level.

Keywords: Smart grid, energy management system, SCADA system, cyber security

1. Introduction

In response to the recent demand for the modernization of power grids, there have been various discussions regarding the load maps of smart grids. Furthermore, there are ongoing efforts to reform power infrastructure.

According to Arnold [1] and Anderson *et al.* [2], smart grids are an integrated solution to current issues facing the power industry. This concept can be divided into several main elements, viz. power system efficiency, accessibility of information, demand management, reliability of service, renewable energy usage, etc. Because smart grid concepts are of a combined nature, there have been various attempts at modeling smart grids [3], [5]. In the smart grid environment, the characteristics of power control systems can be summarized as extendible, open, and accessible. Because these characteristics make such systems more vulnerable, however, it is important to understand the nature of cyber threats in order to ensure that such they are secure. Moreover, the importance of Energy Management System (EMS) when implementing smart grids is emphasized. Because EMS has a multi-functional, complex architecture with the increasing size of such systems, clear criteria are needed for classifying so-called cyber vulnerability.

In this paper, we examine the classification of cyber threats in the field of Information and Communication Technology (ICT). We establish criteria for classifying cyber vulnerability, such that they are consistent with the characteristics of EMS. Then, we classify cyber threats in accordance with these criteria. Finally, we present a qualitative analysis of the relationship between the cyber threats and each level.

2. Classification of Cyber Threats in ICT

Cyber attacks refer to the paralysis or destruction of a target system, by altering or diverting the stored information through the use of various attack techniques in cyberspace. In ICT, cyber threats are mainly

Manuscript received February 4, 2016; revised October 19, 2016
Corresponding author: Balho H. Kim; *E-mail address*: bhkim0711@gmail.com.
doi: 10.12720/sgce.5.4.245-251

categorized into system-, network- and web-level threats. As a prerequisite to cyber attacks, particular information regarding the target system must be acquired during a so-called information-seeking stage [6].

2.1 System-level attacks

System-level attacks are attacks that attempt to hack into a single computer system. Such attacks aim to procure administrator privileges, or to operate the computer system in an abnormal manner.

2.2 Network-level attacks

Network-level attacks are performed by manipulating the consumption of available resources in a network. When these attacks occur, network services are disrupted, or the data transferred between the user and the network server is diverted, fabricated, or altered.

2.3 Web-level attacks

Web-level attacks are motivated by the appropriation of personal information or cyber-money, by political intentions, or by the malicious desires of individuals. Because these attacks target an unspecified multitude of users through a web server, they are most likely to impact the general public.

2.4 Information-seeking stage

Information seeking is the process whereby the attacker identifies the vulnerable aspects by collecting information regarding the target. This stage comprises three sub-stages: foot printing, scanning, and enumeration.

Based on the explanation above, the following table summarizes the general classification of cyber threats in ICT.

Table 1. General classification of cyber attacks in ICT

Information seeking	System	Network	Web
Foot printing	Password attack	Denial of service attack	Common gateway interface attack
	Buffer overflow attack	Distributed denial of service	
Scanning	Malicious code	Distributed reflection DoS	Attacks using authentication and cookies
	Back door	Sniffing attack	
	Race condition attack	Spoofing attack	
Enumeration	Format string attack	Session hijacking attack	Phishing attack
	Reverse engineering	Man in the middle attack	
	Denial of service attack		

3. Overview of Energy Management System

EMSs perform complex management functions such as real-time monitoring and load prediction through the analysis and processing of power data. Therefore, the role of EMS can be defined as the organic linking of every aspect, including the network, automation, software, and databases [7].

The main objective of EMS is to deliver an optimal quantity of power with guaranteed economic viability to consumers.

The architectural characteristic of EMS comprises five different frameworks in a multifunctional architecture, wherein various applications ranging from power-generation planning to system analysis operate organically.

A schematic summary of the architectural characteristics of EMS is shown in Fig. 1 [8].

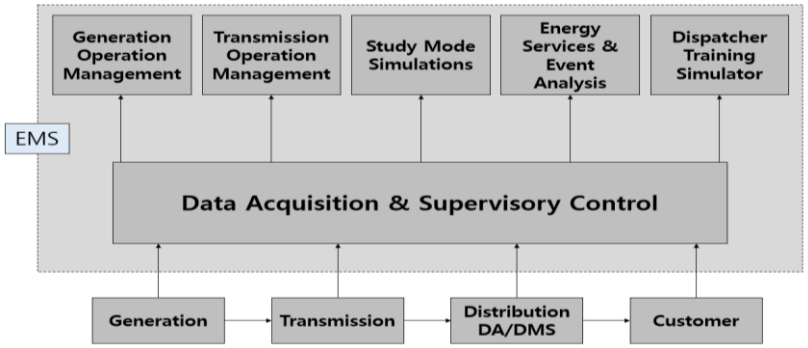

Fig. 1. EMS framework.

3.1 Generation operation management

Generation operation management should include the following:

- Load forecasting (LF)
- Unit commitment (UC)
- Hydrothermal coordination (HTC)
- Real-time economic dispatch and reserve monitoring (ED)
- Real-time automatic generation control (AGC)

3.2 Transmission operations management

Transmission operation management should include the following:

- Network configuration/topology processor (TP)
- State estimation (SE)
- Contingency analysis (CA)
- Optimal power flow and security constrained optimal power flow (OPF, SCOPF)
- Islanding of power systems

3.3 Study mode simulations

Study mode simulations should include the following:

- Power flow (PF)
- Short-circuit analysis (SC)
- Network modeling

3.4 Energy services and event analysis

Energy services and event analysis should include the following:

- Event analysis
- Energy scheduling and accounting
- Energy service providers

3.5 Dispatcher training simulator

A dispatcher training simulator (DTS) provides a training environment to the administrator for real-time contingency management. This involves running an application to model the generator, prime movers, and the controllers of the actual system.

4. Classification of Vulnerability and Cyber-Attacks Specific to EMS

In this section, we propose the criteria for the classifying the vulnerability of EMS to cyber threats,

owing to the characteristics of EMS.

4.1 Vulnerability classification criteria for cyber security in EMS

Whereas the functionality of EMS is highly complicated, they ultimately consist of a communication network between independent single units, such as computers and other units.

Moreover, one of the important objectives of a smart grid is the bidirectional communication between the provider and the consumer. Therefore, the web and the system must be connected at a web access point, and it must be possible to announce and utilize the various information regarding power at these points.

Therefore, the classification criteria for the cyber vulnerability of EMS must consider the system, network, and web. In this section, these are referred to respectively as the component, communication, and web access point, out of consideration for the unique characteristics of power systems.

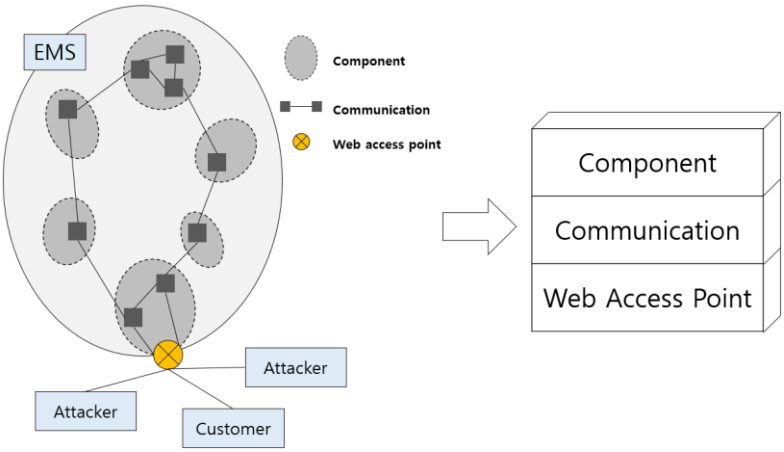

Fig. 2. Configuration of a power control system and classification criteria.

4.1.1 Component

Components are the single units encompassing the independent small-scale systems that perform the necessary functions of a power system. For example, this includes the main computer responsible for the general management of all information from the master station (i.e., EMS), or the intelligent electronic devices (IEDs) that collect the power information from the field.

4.1.2 Communication

Communication refers to the communication between single units, or in other words, the exchange of information between components. Major examples of communication include the I nformation exchanged between the circuit breaker of the transmission line or the controller responsible for switchgear in the substation and the master station of the EMS, and the information exchanged between the IED that collects the power information from the consumer in real-time and the local distribution station.

4.1.3 Web access point

Web access points refer to the access points between the applications that are necessary for the consumer in a smart grid environment in order to obtain the information regarding the power system in real-time. For example, once the participants of the power market apply to a price tender through the web access point, the independent system operator (ISO) synchronizes the supply and demand at the tendered price. In this manner, the ISO establishes the system operation plan, and minimizes the overall system cost under the constraints [9].

4.2 Classification of cyber-attacks based on vulnerability

4.2.1 Cyber-attacks on components

At the component level, the main objective of cyber-attacks is to acquire access permissions to the

system. Attacks that can impact components include password attacks, buffer overflow attacks, malicious code, and denial of service (DoS) attacks. In this case, all attacks involve obtaining the access permissions in order to subsequently destroy the system through malicious code and steal information.

4.2.2 Cyber-attacks on communication

At the communication level, the system is extended through the communication channels connected between various components. Unlike component-level attacks, attacks at the communication level are restricted to the network resources.

The exchange of information comprises a series of steps, such as data processing and identification, along with data transfer. The list of applicable types of cyber-attacks here include sniffing attacks, spoofing attacks, session hijacking attacks, and man in the middle attacks.

4.2.2 Cyber-attacks on web access points

At the web access point, the components are connected to the web, allowing the users to obtain direct access to the power system. The applicable attacks in this case are restricted to the web, among network resources that are relevant in the case of communication-level attacks. For example, such attacks include common gateway interface attacks, attacks using authentication and cookies, and phishing attacks. However, the web is the most generally accessible network service in the world. Because numerous users share information and receive services through the web, this is the most problematic aspect of a smart grid framework from the perspective of cyber security.

The classification of cyber-attacks based on the proposed classification criteria for the constituent elements of a power information control system are shown in Table 2.

Table 2. Classification of cyber-attacks in Smart Grid

Classification standard / Cyber threat	Component	Communication	Web service
Password attack	○	X	X
Buffer overflow attack	○	X	X
Back door	○	X	X
Malicious code	○	X	X
Denial of service attack	○	○	○
Other attacks*	○	X	X
Sniffing attack	X	○	X
Spoofing attack	X	○	X
Session hijacking attack	X	○	X
Man-in-the- middle attack	X	○	X
Common gateway interface attack	X	X	○
Attacks using authentication and cookies	X	X	○
Phishing	X	X	○
Other attacks* : race condition attack, format string attack, reverse engineering, etc.			

5. Analysis of Interactions between Each Level of EMS

Attacks at the component level cause the malfunction of low-level devices such as the IED, resulting in the collapse of the power system. An attack on the EMS will impact the entire power system, leading to power outages and causing economic loss on a large scale.

Meanwhile, attacks on communication can occur during the process of manipulating the power

information collected from field devices at the RTU and the transfer of such information to the master station. Likewise, this is also applicable to the process of delivering the control commands from the control center to various components. Cyber-attacks on network resources distort the function of the SCADA system in power systems, through diversion, fabrication, and alteration of power information.

Finally, attacks on web access points can be examined in terms of their influence on the power market. In particular, problems during the settlement of charges can be expected, owing to the inconsistency in market information between the participants of the power market [10].

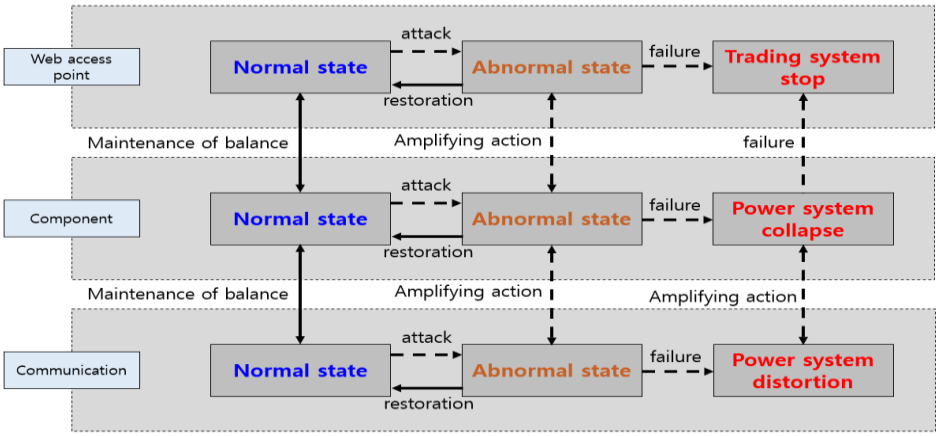

Fig. 3. Qualitative analysis of the interactions between each level of the EMS.

6. Conclusion

Following the recent introduction of IEDs, which can serve as the eyes and ears of EMS, the number of web access points is expected to increase geometrically. Through access points, attackers can deliberately isolate the consumer from the real-time status of the power system, or these attackers can obtain direct access to the internal system of the power grid from a remote location.

In conclusion, there will be inevitable situations in smart grids where the natural connections between components and web access points will lead to more devastating results.

In this paper, we examined the relevant cyber attacks based on the classification of cyber attacks in ICT, and the classification criteria proposed in consideration of the unique characteristics of EMS. Moreover, we derived a more meaningful causality by presenting a qualitative classification of the interactions between each level.

It is widely believed that if a quantification methodology is developed based on the qualitative classification of cyber threats in future research, threats and the extent of damage can be predicted more accurately.

Acknowledgement

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

References

[1] Arnold GW. Challenges and opportunities in smart grid: a position article. *Proceedings of the IEEE*, 2011; 99(6):922-927.

[2] Anderson RN, Boulanger A, Powell WB, Scott W. Adaptive stochastic control for the smart grid. *Proceedings of the IEEE*, 2011; 99(6):1098-1115.

[3] Farag MM, Azab M, Mokhtar B. Cross-Layer framework for smart grid: physical security layer. In: *Proc. of IEEE PES Innovative Smart Grid Technologies Conference Europe*, 2014.

[4] Trefke J, Rohjans S, Uslar M, Lehnhoff S, Nordstrom L, Saleem A. Smart grid architecture model use case management in a large european smart grid project. In: *Proc. of 4th IEEE/PES Innovative Smart Grid Technologies Europe*, 2013.

[5] Srinivasan S, Kotta U, Ramaswamy S. A layered architecture for control functionality implementation in smart grids. In: *Proc. of 10th IEEE International Conference on Networking, Sensing and Control*, 2013:100-105.

[6] Jeong TM, Eom JH, Han YJ, Park SH. *Cyber attack & Security Technology*, 2009:31-106.

[7] Shuguang L. Energy management system architecture based on Internet of Things. In: *Proc. of 32nd Chinese Control Conference*, 2013:8066-8069.

[8] Thomas MS, McDonald JD. *Power System SCADA and Smart Grids*, 2015:177-213.

[9] Kim YC. *Understanding of the Power Industry*, 2012:197.

[10] Kirschen DS, Strbac G. *Fundamentals of Power System Economics*, 2004:49-72.