Cybersecurity Framework for IIoT-Based Power System Connected to Microgrid

Ji Woong Jang[1], Sungmoon Kwon[2], SungJin Kim[2], Jungtaek Seo[3], Junhyoung Oh[4] and Kyung-ho Lee[5*]

[1] Graduate School of Information Security, Korea University
Seoul, 02841 - Republic of Korea
[e-mail: creative@kpx.or.kr]
[2] Department of Computer Engineering, Ajou University
Suwon, 16499 - Republic of Korea
[e-mail: calmcombat@gmail.com(SM.K), ksjskyblue@ajou.ac.kr(SJ.K)]
[3] Information Security Engineering, Soonchunhyang University
Asan, 31538 - Republic of Korea
[e-mail: sjtgood7@gmail.com]
[4] Institute of Cyber Security & Privacy, Korea University
Seoul, 02841 - Republic of Korea
[e-mail: ohjun02@korea.ac.kr]
[5] Department of Cyber Defense & School of Information Security, Korea University
Seoul, 02841 - Republic of Korea
[e-mail: kevinlee@korea.ac.kr]
*Corresponding author: Kyung-ho Lee

Received December 9, 2019; revised February 8, 2020; accepted March 8, 2020; published May 31, 2020

Abstract

Compared to the past infrastructure networks, the current smart grid network can improve productivity and management efficiency. However, as the Industrial Internet of Things (IIoT) and Internet-based standard communication protocol is used, external network contacts are created, which is accompanied by security vulnerabilities from various perspectives. Accordingly, it is necessary to develop an appropriate cybersecurity guideline that enables effective reactions to cybersecurity threats caused by the abuse of such defects. Unfortunately, it is not easy for each organization to develop an adequate cybersecurity guideline. Thus, the cybersecurity checklist proposed by a government organization is used. The checklist does not fully reflect the characteristics of each infrastructure network. In this study, we proposed a cybersecurity framework that reflects the characteristics of a microgrid network in the IIoT environment, and performed an analysis to validate the proposed framework.

Keywords: Cybersecurity Framework, microgrid, industrial internet of things

"This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2020-2015-0-00403)supervised by the IITP(Institute for Information &communications Technology Planning &Evaluation)"

http://doi.org/10.3837/tiis.2020.05.020 **ISSN : 1976-7277**

1. Introduction

The current infrastructure network uses Industrial Internet of Things (IIoT) for efficiency management, which extends IoT to connect the industrial control systems with external networks. Thus, the network of an industrial control system also becomes susceptible to cyberattacks. Especially, the US ICS-CERT reported that a total of 295 security accidents occurred because of cyberattacks on the industrial control system environment in 2015, indicating an over seven-fold increase from 40 security accidents in 2010. The number of security accidents is on the rise every year. Accordingly, the cybersecurity of the microgrid environment connected to IIoT becomes more important. Microgrid is a small-scale independent power grid that can autonomously provide energy to a small community. This next-generation power system integrates renewable energy sources, such as sunlight and wind power, with an energy storage system (ESS). As the market of renewable energy and consequently, its demand are activated, small resources also increase. In this situation, microgrids connected to IIoT technologies are required to apply innovative techniques for realizing advanced power systems and flexible networks throughout the whole power industry, and to provide information about power generation and demand to the central EMS, which monitors and controls the entire power system in real time. However, the path or connection between the central EMS and microgrids has not been sufficiently studied yet. The lack of security analysis for each communication section may result in diverse security threats. To overcome or avoid the security threats generated by the direct connection of a microgrid to EMS, in this study, we derive the security requirements and countermeasures, which will be useful to develop future security techniques and establish security measures. This type of security requirements and countermeasures for security threats to a system and a network are only a part of a full-fledged procedure of ensuring the security of the system. Apart from these requirements and countermeasures, a systematic process of implementing them is required for effective security reinforcement. Accordingly, a cybersecurity guideline reflecting the characteristics of microgrid-based infrastructure network is an essential security element to react to cyberattacks and reinforce the security of the microgrid-based infrastructure network, “Framework for Improving Critical Infrastructure Cybersecurity” [1] of National Institute of Standards and Technology (NIST) and “Cybersecurity Capability Maturity Model (C2M2)” [2] of Department of Energy (DoE) are representative standards and guidelines that can be used to develop such guidelines. However, many parts of those documents need to be reinterpreted and modified for situations of each organization; thus, it is difficult for each organization to develop its own guideline. Accordingly, many infrastructure-related organizations use the cybersecurity guideline proposed by a government organization by adjusting some parts to reality. This guideline does not sufficiently reflect the characteristics of an infrastructure network, i.e., a special environment in which the existing legacy equipment and new IIoT are used. To resolve such problems, in this study, we attempted to develop a cybersecurity guideline, which reflects characteristics of IIoT and microgrid infrastructure network. Relevant standards and microgrid infrastructure networks were analyzed. Based on the analysis results, a development plan of a cybersecurity guideline was presented and validated.

The remainder of this study is organized as follows. Section 2 examines the application cases of cybersecurity guidelines and analyzes the microgrid security. Section 3 analyzes the cybersecurity threats to IIoT-based power systems. Section 4 used the analysis result of the previous section to clarify cybersecurity requirements and countermeasures for the microgrid infrastructure networks. Section 5 presents a framework for microgrid cybersecurity in IIoT environment and a validation method. Finally, Section 6 concludes the discussion.

2. Background and Related Work

Various organizations have conducted studies on microgrid network architectures and communication, "Common Microgrid Reference Model" published by Korea Smart Grid Association provides a general introduction to the microgrid by specifying each component and explaining communications of components in details [3]. Qiang Fu, et al. identified the physical layers, protocol, and standards for microgrid communication [4]. Jin, Dong, et al. presented an SDN-based microgrid network architecture, thereby examining a model for future development of microgrid network communication [5]. Many other academic studies including that of Franklin E. Pacheco focusing on the microgrid use cases have been performed [6].

Junjian Qi et al. dealt with the microgrid security issue. They proposed a framework of responding to attacks, which aimed to protect microgrid infrastructures from malicious cyberattacks and ensure the reliable and stable integration of DER [7]. Potential cyberattacks were also mentioned; however, they were briefly introduced. Besides, the section connecting the central EMS and microgrids was not dealt with; thus, it was necessary to identify the security risk of that section. The microgrid cybersecurity reference architecture presented by Sandia National Laboratories focused only on the internal part of a microgrid and excluded its connection with the central EMS [8]. Accordingly, the security of this section can be guaranteed by deriving the security threats, analyzing the security requirements, and developing a cybersecurity framework based on the analysis results.

"Framework for Improving Critical Infrastructure Cybersecurity" [1] of NIST, C2M2 [2] of DoE, and NERC CIP [9] are the representative standards and guidelines for developing a cybersecurity framework. However, many parts of these documents need to be reinterpreted and modified for situations of each organization; thus, it is difficult for each organization to develop its own guideline. Accordingly, many infrastructure-related organizations partially modify and use the cybersecurity framework distributed by the government. However, this framework does not sufficiently reflect the characteristics of an infrastructure network. Thus, in this study, we analyze the connection between microgrids and EMS, derive security threats and requirements, and propose a cybersecurity framework for the IIoT-based microgrid and EMS-connected environment using the analysis results and requirements.

3. Cybersecurity Threats in IIoT-based Power Systems

Despite the diverse studies introduced in Section 2, the connection between the central EMS and microgrid has not been sufficiently examined. In this section, we aim to identify the basis for security requirements and countermeasures for the connected sections. To achieve this, cybersecurity threats, which can occur when the central EMS and a microgrid are directly connected, are discussed based on the characteristics of each component and communication.

3.1 Microgrid Components and Communication Characteristics

As the central EMS supports operations of power plants and substations around the country, a microgrid also requires a system that manages various facilities in the grid. This system is referred to as a microgrid EMS. In other words, the microgrid EMS comprehensively manages load characteristics and power source conditions for efficient operation. Similar to a state/regional EMS managing one country or region, the microgrid EMS has the functions of power generation management, system operation, and monitoring/control. However, the load fluctuation is significant and power sources with diverse characteristics are used; thus, more functions are to be considered for quick decision-making and stable operation. Consequently, not only economic feasibility should be considered to optimally operate the distribution resources, but also the connection with the existing power system and composite control of various distribution resources are to be reflected and managed. Figure 1 shows the systems constituting a microgrid.

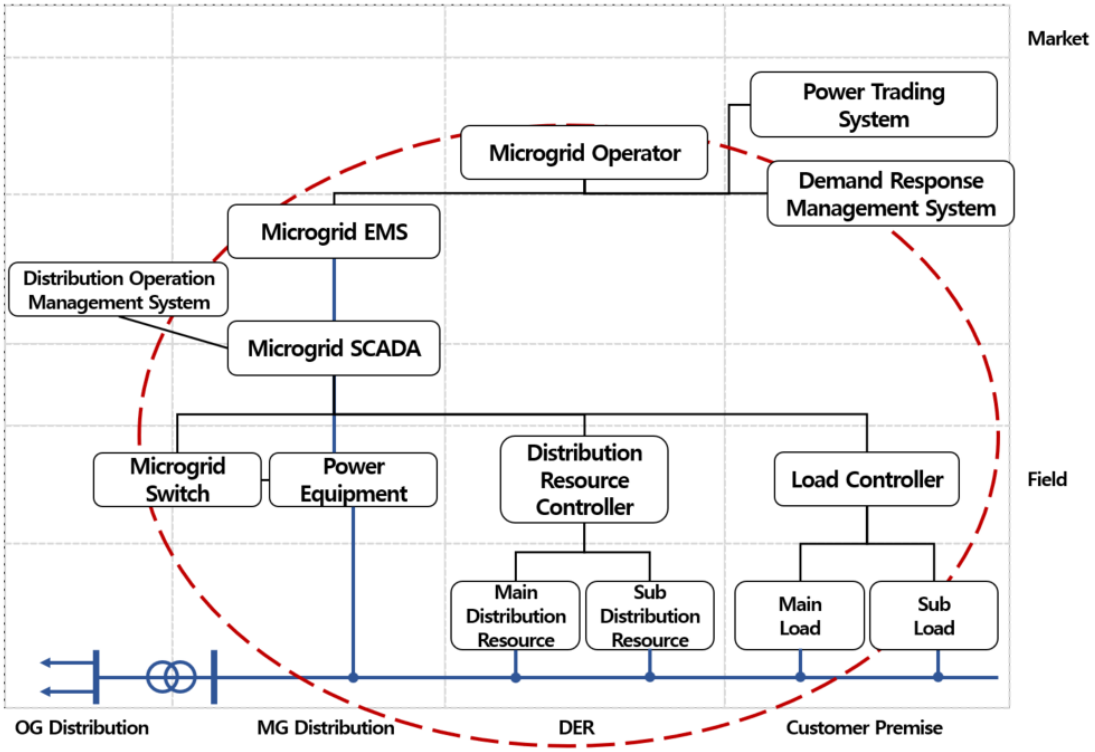

Fig. 1. Configuration of a microgrid

As shown in **Fig. 1**, the microgrid is an abridged form of power installation. This study focuses on the related microgrid EMS and communication sections. **Table 1** presents those communication sections, data transferred in each section, and relevant communication standards.

Table 1. Data transferred and communication standards in each microgrid communication section

Section	Information	Standard
Microgrid SCADA ↔ Microgrid EMS	▪ Voltage and power factor profile ▪ Measurement and condition ▪ Control command	▪ IEC 61850 ▪ IEC 61970 ▪ IEC 61968-100 ▪ OPC-UA
Microgrid EMS ↔ Microgrid operator	▪ Measurement and condition ▪ Forecast ▪ Control command	▪ IEC 61970 ▪ IEC 61968 ▪ IEC 61968-100
Microgrid EMS ↔ Power trading system	▪ Tender and contract ▪ Power price	▪ IEC 61970 ▪ IEC 62325 ▪ OpenADR 2.0 ▪ IEC 61968-100 ▪ OpenADR 2.0b ▪ OPC-UA
Microgrid EMS ↔ Demand response management system	▪ DR implementation ▪ Customer information ▪ Forecast	▪ IEC 61970 ▪ OpenADR 2.0 ▪ IEC 61968-100 ▪ OpenADR 2.0b ▪ OPC-UA

3.2 Analysis of Security Threats to the Connection between Microgrid and Central EMS

If the central EMS is affected by the security threat to microgrid, a large-scale accident like an outage over a wide area may happen. For this reason, it is absolutely necessary to analyze security threats and consider countermeasures when a microgrid is connected to the central EMS. As for internal security threats of microgrids, “Microgrid cyber security reference architecture version 1.0” published by Sandia National Laboratories is currently available. However, no security threat has been derived for the connected section of microgrid and the central EMS [8].

As for the direction connection of EMS, if the connection between the central EMS and a microgrid is considered before analyzing threats, only the microgrid EMS is connected to the central EMS. Since the microgrid EMS operates the overall microgrid, the central EMS does not require any communication with individual components. In addition, as the microgrid EMS has the same function in a microgrid as the central EMS, it is expected that all the information collected by the microgrid EMS will be transferred to the central EMS. Based on the above information list for each microgrid communication sections and the microgrid security threats pointed out by Microgrid cyber security reference architecture of Sandia National Laboratories, security threats related to the connection between the central EMS and the microgrid EMS have been derived as in **Table 2** [10].

Table 2. Cybersecurity threats for IIoT-based microgrid and EMS-connected environment

Security threat	Description
Denial-of-service (DoS)	▪ Normal use or management of network or network devices is interrupted or stopped. ▪ If a server executes excessive requests generated by multiple microgrid EMSs connected to the central EMS, the service can be denied. In this case, the number of requests is too high for a service to respond to those requests in time.
Network sniffing	▪ An attacker, who approaches a wired or wireless data channel that is exposed and used to transfer data to the central EMS, uses network sniffing to identify components, resources, and protection. ▪ An attacker uses a commercial or free software, which can scan the domain (neighbor and boundary) of an organization, to improve his/her ability and obtain deeper information about the IT infrastructure facilities.
Gathering open information about independent power producers or related parties	▪ Open accessible information is investigated to collect the information system of independent power producers, business procedures, individual users, and their external relationship, which could be used for future attacks.
Eavesdropping	▪ Manual monitoring for acquiring data including qualification for certificate between the central and microgrid EMSs. ▪ An attacker uses a monitoring software and a local IP network access to record data exchange between the clients and server. This type of data includes usernames of clients and passwords, which are transferred as plain texts.
Fabrication of fake certificate	▪ An attacker forges or damages a certification authority to make a malicious code or a connection request, which is transferred to the central EMS, look legitimate.
Man-in-the-middle (MITM)	▪ Network communication between two legitimate users is intercepted. ▪ After being qualified for certificate and acquiring data, an attacker disguises himself as a legitimate microgrid EMS. ▪ After recording a message for inactivating a target power generation unit using the microgrid EMS, an attacker transfers a copied message whenever attempting to inactivate the unit.
Malicious code transfer to the central EMS	▪ An attacker acquires an access to the microgrid EMS and uses a more sophisticated transfer mechanism (web traffic, instant messaging, FTP, and so on) to deliver a malicious code to the central EMS
Insertion of Malicious code in downloadable software or commercial IT product	▪ An external attacker inserts a malicious code into a common firmware, shareware or a commercial IT product on an open website, or the website of an operator managing the microgrid EMS to figure out a simple access to an internal system.
Attack using cross-network information flow	▪ Cross-network information flow (e.g., e-mail connection, removable storage device) can be used to attack an internal information system. Using this information flow, an attack might be able to acquire and leak sensitive information across the boundary.
Damaging the main information systems through physical access	▪ An attacker physically approaches a relevant unit to a microgrid EMS or the central EMS and destroys or modify it.

Brute-force attack to infer password	▪ An attacker guesses a password randomly or systematically by using a password crack program, acquires the management authority of a microgrid operator, and attempts to influence the microgrid EMS.
Inappropriate cybersecurity process or practice for both internal and external employees	▪ As a staff or a microgrid operator may inactivate the firewall after installing a new software that requires the blocked port, the security cannot be intended or be degraded intentionally. ▪ The new software can fulfill its function properly; however, this operation has a negative effect on the security profile of the information system.
Inappropriate definition of the network boundary	▪ The system for command and control is not completely separated from the work network that provides an access to email, Internet, or other services. ▪ As the manager of the central EMS or a microgrid EMS opens a suspicious email with a malicious attachment file and activates the malicious code, this code uses a vulnerable point of the system to allow the attacker to approach on the Internet.
Vulnerability of old industrial protocols	▪ Control and power systems have many old communication protocols, which are vulnerable to even well-known attacks. Especially, unpatched or out-of-date protocols exhibit serious vulnerability. ▪ An attacker with physical access to the bus of Profibus virtual token ring can execute an MITM or DoS attack on the token ring. Other protocols also have no embedded mechanism to diminish such vulnerabilities.

4. Cybersecurity Requirements and Countermeasures

This section describes the cybersecurity requirements and countermeasures against the main security threats mentioned in Section 3. The major cybersecurity items for the requirements for security threats can be summarized as follows:

- Access control: A security requirement for allowing only authorized users for system and network to have access to system, devices, and equipment, and also controlling actions according to access right.
- Security education and training: A security requirement related to education and training for improving staffs' security awareness
- Security auditing: A security requirement related to policy making, data gathering, and inspection process for security inspection
- Security assessment: A security requirement related to a procedure of allowing a microgrid EMS to be connected only to equipment, network, and system, which have undergone security check and been approved.
- Continuity of operation: A security requirement for establishing a countermeasure to prevent the shutdown of a system, equipment, and network
- Identification and certification: A security requirement related to normal identification and certification of a system, equipment, network, and users
- Document security: A security requirement for protecting documents concerning system operation
- Intrusion response: A security requirement related to detection and response to intrusion
- Storage protection: A security requirement for protecting the storage media used in a system, device, and network facility from cyber threats

- Physical security: A security requirement for protecting facility, place, and field units from penetration
- Personnel security: A security requirement related to organization and management of personnel
- Risk management: A security requirement related to risk analysis and management of a system, equipment, and network
- System and communication protection: A security requirement for the technical aspects of a system, equipment, and communication
- System and information integrity protection: A security requirement for protecting the integrity of a system, software, and information

Countermeasures are derived by matching the above 14 items with each security threat [11]. Security requirement items for each security threat are as follows:

- DoS: Access control, continuity of operation, and intrusion response
- Network sniffing: Access control, system and communication protection, system and information integrity protection, and risk management
- Gathering open information about independent power producers or related parties: Access control
- Eavesdropping: Access control, and identification and certification
- Fabrication of fake certificate: Access control, identification and certification, document security, and system and information integrity protection
- MITM attack: Access control, identification and certification, and intrusion response
- Malicious code transfer to the central EMS: Access control, identification and certification, and risk management
- Insertion of malicious code in downloadable software or commercial IT product: Access control, security inspection, security assessment, identification and certification, and system and information integrity protection
- Attack using information flow for which cross-net data transfer is allowed: Identification and certification, system and communication protection, and risk management
- Damaging the main information systems through physical access: Physical security, storage medium protection, and risk management
- Brute-force attack to infer password: Access control, security inspection, and identification and certification
- Inappropriate cybersecurity process or practice for both internal and external employees: Security education and training
- Inappropriate definition of network boundary: Identification and certification, and risk management
- Vulnerability of conventional old industrial protocols: Access control, security inspection, identification and certification, and system and information integrity protection

The countermeasures derived above against security threats to the IIoT-based microgrid and EMS-connected environment reflect the analysis of the target environment. Thus, these can contribute to developing a customized cybersecurity framework. Section 5 provides a detailed explanation about the development and application of a cybersecurity framework reflecting the above requirements for the IIoT-based microgrid and EMS-connected environment.

5. Cybersecurity Framework and Analysis

5.1 Cybersecurity Framework for IIoT-based Microgrid and EMS-connected Environment

The concept of cybersecurity framework implies cybersecurity requirement. A cybersecurity framework is not a simple checklist, but a security procedure that is updated and maintained systematically and continuously, "Framework for Improving Critical Infrastructure Cybersecurity" [1] of NIST and C2M2 [2] of DoE are the currently available cybersecurity frameworks. However, many parts of those documents [1] [2] need to be reinterpreted for characteristics of each organization; thus, it is not easy to develop a suitable guideline for each system. As introduced in [1], the following five main essential concepts are commonly applied:

- Identify: Asset identification and risk analysis
- Protect: Application of security to asset
- Detect: Monitoring of security function
- Respond: Response to an intrusion incident
- Recover: Recovery from an intrusion incident

Identify is a step of identifying an object, Protect and Detect correspond to the security checking steps of the identified object, and Respond and Recover are the feedback providing steps of security inspection and improving security. As these main concepts are simply enumerated, they are required to be systematically organized, so that continuous update and security processes can be implemented. Besides, one more step seems to be necessary, where a new vulnerability of an infrastructure network is identified and analyzed. Accordingly, this step is added to derive a four-step guideline.

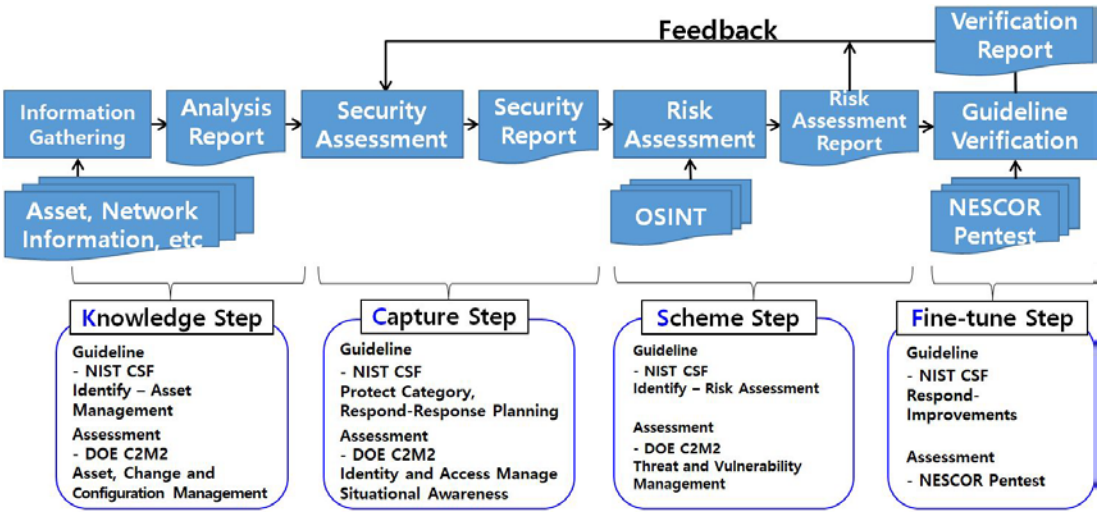

Fig. 2. Cybersecurity framework for IIoT-based microgrid and EMS-connected environment

As shown in **Fig. 2**, this study configures a cybersecurity framework with four steps and eight detailed items. Thus, the main essential concepts and requirements can be rearranged for each step, and the proposed security procedure enables a systematic and continuous update and maintenance operations. Each step is described in next sub-section.

5.1.1. Knowledge step

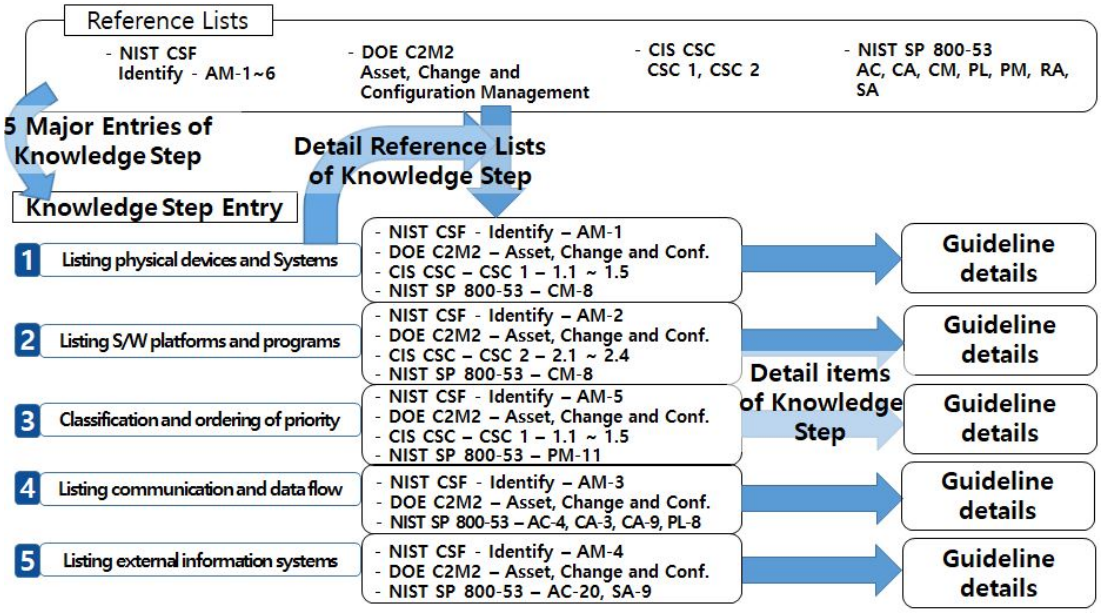

Fig. 3. Cybersecurity Framework - Deduction Process of Knowledge Step

Fig. 3 shows deduction process of Knowledge step. Various information including network diagram, H/W asset list, system list, S/W and version list, policy and procedure documents, network monitoring information, wireless network information, information flow diagram of the system, and system manager and user information are collected, and an object analysis report is prepared.

5.1.2 Capture Step

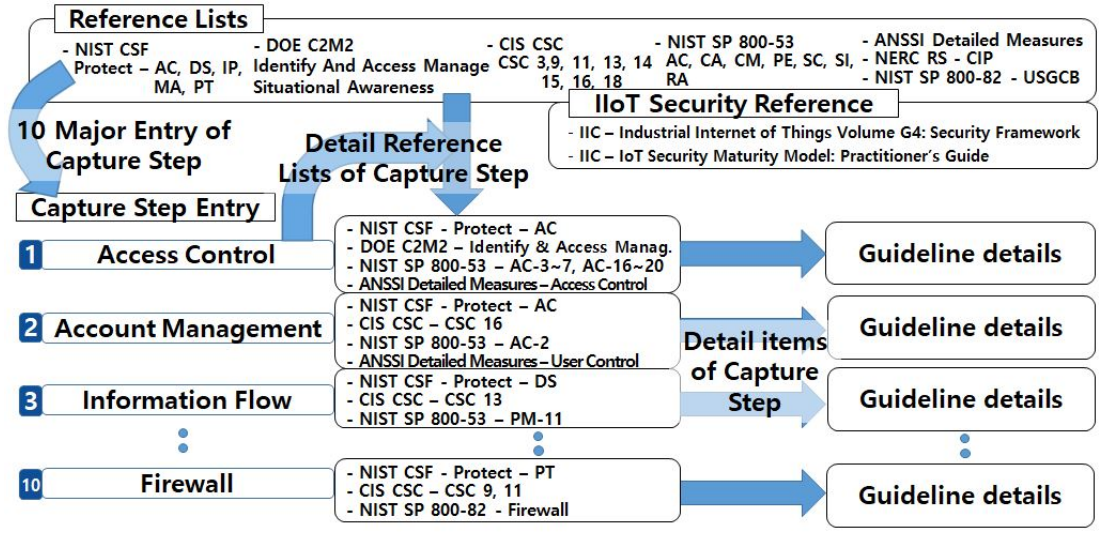

Fig. 4. Cybersecurity Framework - Deduction Process of Capture Step

Fig. 4 shows deduction process of Capture step. Major security items are inspected for networks/systems/programs identified by the above analysis report produced in the Knowledge state. A security inspection report is also prepared. The security inspection items contain the major security requirements derived in Section 4 and IIoT security factors from IIC's IIoT security guidelines. In addition, these security requirements are not static, but dynamic items, which will be continuously added considering the new vulnerabilities identified in the Fine-tune step.

5.1.3 Scheme step

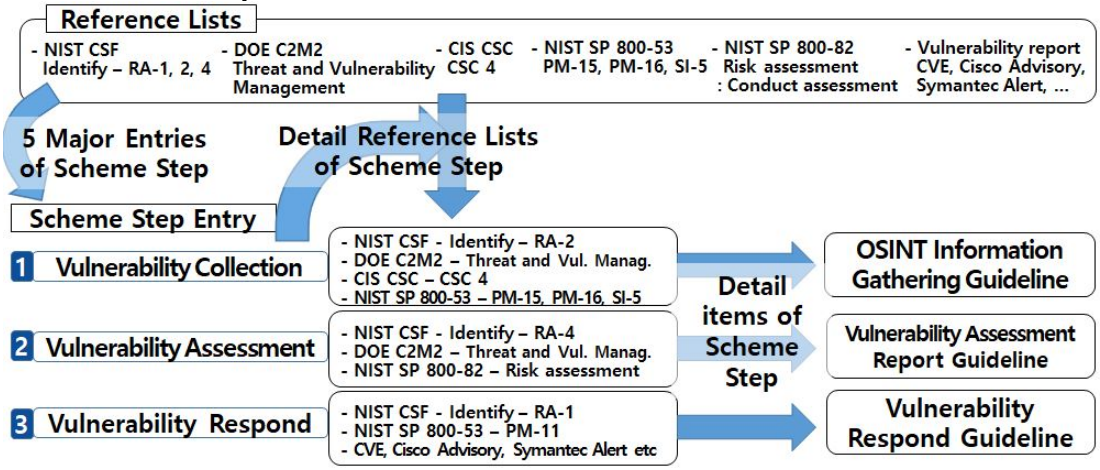

Fig. 5. Cybersecurity Framework - Deduction Process of Scheme Step

Fig. 5 shows deduction process of Scheme step. Open vulnerability information, i.e., the OSINT data is collected using the keyword of asset information. New threats and vulnerabilities are reinterpreted for each organization, and a corresponding threat and vulnerability report is prepared. New security inspection items are added to those of the Capture step.

5.1.4 Fine-tune step

A simulated penetration experiment is conducted for the same network range as that of the inspection object in the previous step. In this way, the guideline is validated and feedback is provided. In comparison with the security inspection items and the vulnerabilities identified by the risk analysis report, a report of the simulated penetration experiment is prepared. Newly identified vulnerabilities are added as security inspection items of Capture step, and a feedback work is performed.

As for the security requirements of each step, apart from those proposed in [1], [2], and Section 4 above, not only "Center for Internet Security Critical Security Controls (CIS CSC)" [12], NISP SP 800-53 [13], both of which specify IT security requirements, but also "ANSSI (Agence nationale de la sécurité des systèmes d'information) Cybersecurity for ICS Detailed Measures" [14] and NIST SP 800–82 [15], which deal with security requirements for infrastructural environment, are available. For the IIoT security requirements, Industrial Internet Consortium(IIC) IIoT guidelines [16] [17] are available. NERC CIP [9] can also be used, which presents reliability requirements for power systems.

5.2 Cybersecurity Framework Analysis

The application of the proposed cybersecurity framework is analyzed as follows. In the Knowledge step, a target network is set, various information about the network is gathered, and an analysis report is prepared by listing 29 items. In this study, the available items include network diagram, H/W asset list, system list, S/W and version list, policy and procedure documents, network monitoring information, wireless network information, information flow diagram of system, and system manager and user information. Thus, the resultant analysis report is used not only for the next step but also for security inspection considering the use of permitted equipment/SW/communication and an abnormal data flow-like transfer of the upper security data to a lower security device. In the Capture step, the analysis report produced in the Knowledge step is used for security inspection through capture security inspection items corresponding to each device, network, and S/W. A security inspection report is also prepared. In the Scheme step, threats and vulnerabilities, which have been opened through the main information (such as S/W name and version) of assets, are collected based on the analysis report prepared in the Knowledge step. Thus, the threats and vulnerabilities gathered should be reinterpreted by considering the conditions of each organization. Thus, a threat and vulnerability report is prepared and added to the security inspection items of the Capture step. In the Fine-tune step, a simulated penetration experiment is conducted for identifying vulnerabilities in the target network. Accordingly, a guideline is validated in terms of security improvement and an additional vulnerability is identified, for which a feedback is provided. For such simulated penetration experiments, “Guide to Penetration Testing for Electric Utilities” [18], which specifies the procedure of a simulated penetration experiment for the power control system of National Electric Sector Cybersecurity Organization Resource (NESCOR), and the procedure and method for embedded equipment, network communication, operating system, and applications, which are proposed by “Guide to Vulnerability Assessment for Electric Utility Operations Systems” [19], can be used. The procedure of the simulated penetration experiment consists of the following steps: the synchronization step of the assessment team determines the main threats. The information gathering step collects information about the target network and systems. The enumeration step determines the experimental equipment and identifies the essential user and account information for the experiment. The exploration step checks a vulnerability scanning tool and performs the scanning process. The identification and documentation step prepares documents about identified vulnerabilities. Finally, the escalation and repetition step determines the order of priority for the documents prepared and checks if an additional test is required. The simulated penetration experiment method for each equipment type presents the test equipment types and techniques for each type. **Fig. 6** illustrates NESCOR penetration testing process. This type of simulated penetration experiment shows if the guideline has adequately improved the previously identified vulnerabilities. In addition, countermeasures and security requirements for additional vulnerabilities are derived and added to the security inspection items of the Capture step, and a feedback is also provided. Thus, the guideline is not a static checklist, but is being continuously developed through the basic security inspection using security items of the Capture step, information gathering of opened vulnerabilities in the Scheme step, and the simulated penetration experiment of the Fine-tune step. This type of architecture of the cybersecurity framework can continuously compensate and use the guidelines even if new vulnerabilities are opened or identified.

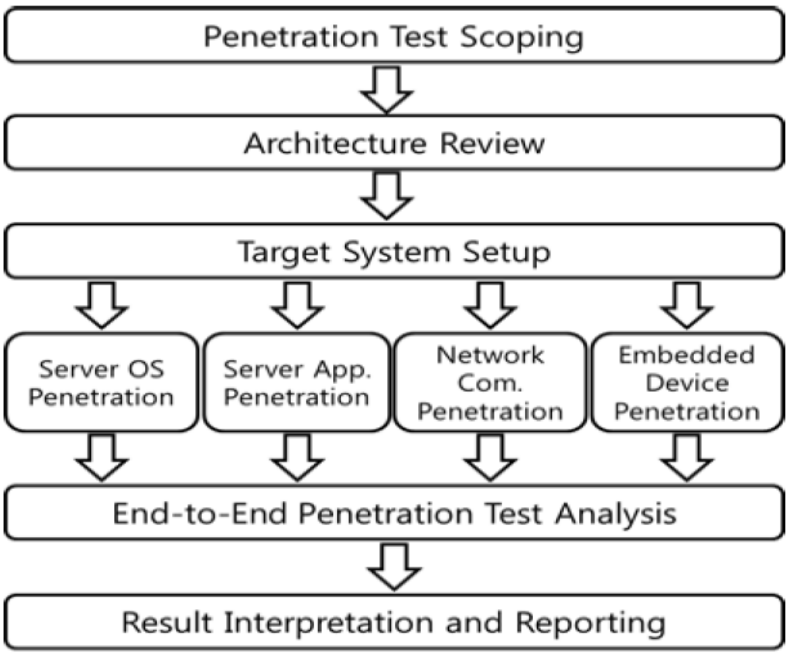

Fig. 6. NESCOR penetration testing process

6. Conclusion

In this study, we analyzed cybersecurity threats to IIoT-based microgrid environment and proposed the corresponding cybersecurity requirements and countermeasures. Based on the cybersecurity frameworks for conventional systems and networks, such as the cybersecurity framework of US NIST, a cybersecurity framework applicable to IIoT-based microgrid environment has been derived, and an analysis was performed for validating the proposed framework. The proposed cybersecurity framework of this study derived main items related to the IIoT environment from the perspective of cybersecurity of the infrastructure network. Accordingly, each organization can develop its own cybersecurity guideline, which has a wide application scope including organizational management and policy. The static cybersecurity guideline proposed by government organizations does not reflect characteristics of infrastructure networks, while the development method proposed in this study enables each infrastructure organization to reflect the characteristics of microgrids connected to the IIoT environment and continuously develop its own guideline. Thus, the security of a microgrid infrastructure network can be improved by adopting the proposed method. For future works, the proposed cybersecurity framework can be applied to a real microgrid site and its operation result can be analyzed further.

References

[1] National Institute of Standards and Technology, “Framework for improving critical infrastructure cybersecurity,” April 16, 2018. Article (CrossRef Link)
[2] Jason D. Christopher, Fowad Muneer, et al, “Cybersecurity capability maturity model (C2M2),” *Department of Energy*, Feb. 2014. Article (CrossRef Link)
[3] Korea Smart Grid Association, Common Microgrid Reference Model, 2016. Article (CrossRef Link)

[4] Qiang Fu, et al, "Microgrids: Architectures, controls, protection, and demonstration," *Electric Power Components and Systems*, 43(12), 1453–1465, 2015. Article (CrossRef Link)
[5] Dong Jin, et al, "Toward a cyber resilient and secure microgrid using software-defined networking," *IEEE Transactions on Smart Grid*, 8(5), 2494–2504, 2017. Article (CrossRef Link)
[6] Franklin E. Pacheco and James Christopher Foreman, "Microgrid reference methodology for understanding utility and customer interactions in microgrid projects," *The Electricity Journal*, 30(3), 44–50, 2017. Article (CrossRef Link)
[7] Junjian Qi, et al, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Physical Systems: Theory & Applications*, 1(1), 28–39, 2016. Article (CrossRef Link)
[8] Cynthia K. Veitch, et al, *Microgrid cyber security reference architecture*, Sandia National Laboratories: Albuquerque, NM, USA, 2013. Article (CrossRef Link)
[9] North American Electric Reliability Corporation, "Reliability standards for the bulk electric systems of North America," Jan. 2020. Article (CrossRef Link)
[10] VEITCH, Cynthia K., et al., *Microgrid cyber security reference architecture*, Sandia National Laboratories: Albuquerque, NM, USA, 2013. Article (CrossRef Link)
[11] KPX and Soon Chun Hyang University, "Study on the establishment of security measures for the KPX (Korea Power Exchange) based protection issues," Feb. 2018. Article (CrossRef Link)
[12] Center for Internet Security, "The CIS critical security controls for effective cyber defense," Aug. 2016. Article (CrossRef Link)
[13] Ronald S. Ross, Gary Stoneburner, et al, "Security and privacy control for federal information systems and organizations," *National Institute of Standards and Technology*, Apr. 2013. Article (CrossRef Link)
[14] Agence nationale de la sécurité des systems d'information, "Cybersecurity for industrial control system detailed measures," Jan. 2014. Article (CrossRef Link)
[15] Keith Stouffer, et al, "Guide to Industrial Control Systems (ICS) Security," *National Institute of Standards and Technology*, May 2015. Article (CrossRef Link)
[16] Sven Schrecker, Hamed Soroush, et al, "Industrial Internet of Things Volume G4: Security Framework," *Industrial Internet Consortium*, Sep. 2016. Article (CrossRef Link)
[17] Sandy Carielli, Matt Eble, et al, "IoT Security Maturity Model: Practitioner's Guide," *Industrial Internet Consortium*, Feb. 2019. Article (CrossRef Link)
[18] Justin Searle, Galen Rasche, Andrew Wright, and Scott Dinnage, "Guide to penetration testing for electric utilities," *National Electric Sector Cybersecurity Organization Resource*, July 2013. Article (CrossRef Link)
[19] Glen Chason, Scott Dinnage, et al, "Guide to vulnerability assessment for electric utility operations systems," *National Electric Sector Cybersecurity Organization Resource*, Jun. 2014. Article (CrossRef Link)

Jiwoong Jang received the B.S. degree in electrical engineering from Hanyang University and the M.S degree in information security from Korea University. He is now a Ph.d student at the graduate school of information security at Korea University. He has been working for Korea Power Exchange since 2003 and is in charge of critical infrastructure security.

Sungmoon Kwon received B.S. degree in Information and Computer Engineering from Ajou University, Suwon, Korea, in 2013. He is currently pursuing his Ph.D. in Computer Engineering from Ajou University, and is with the Information and Communication Security Lab. His current research interests are smart grid security and industrial control system security.

SungJin Kim received B.S. degree in Information and Computer Engineering from Ajou University, Suwon, Korea, in 2014. He is currently pursuing his Ph.D. in Computer Engineering from Ajou University and is with the Information and Communication Security Lab. His current research interests include Software vulnerability analysis, Machine Learning, Anomaly Detection and Industrial Control System.

Jungtaek Seo received the Ph.D. degree in information security from Graduate School of Information Management & Security, Korea University, (South) Korea, in 2006. In 2000, he joined the Attached Institute of Electrical and Telecommunication Research Institute, Korea, as a researcher, and he was a senior researcher at the research institute. He is currently a professor at the department of Information Security Engineering, Soonchunhyang Univ. Asan, Korea. His research interests include control system cyber security, cyber security for smart grid, network security, DDoS attack mitigation, etc.

Junhyoung Oh received the B.S. degree in electrical engineering from Korea University. He is currently pursuing the Ph.D. degree with the graduate school of information security at Korea University. His research interests include Usable Security, Privacy Framework, and Internet of Things.

Kyung Ho Lee received his Ph.D. degree from Korea University. He is now a professor in the graduate school of information security at Korea University, and has been leading the risk management laboratory in Korea University since 2012. He was a former CISO at Naver Corporation. And he was a CIO, CISO, CPO at Korea University.