Hindawi
Mobile Information Systems
Volume 2020, Article ID 8878088, 11 pages
https://doi.org/10.1155/2020/8878088

Research Article

Investment Priority Analysis of ICS Information Security Resources in Smart Mobile IoT Network Environment Using the Analytic Hierarchy Process

Jiho Shin,[1,2] **Ilsun You**,[2] **and Jung Taek Seo**[2]

[1]*Police Science Institute, Korean National Police University, Asan, Republic of Korea*
[2]*Department of Information Security Engineering, Soonchunhyang University, Asan, Republic of Korea*

Correspondence should be addressed to Jung Taek Seo; seojt@sch.ac.kr

Received 16 July 2020; Revised 9 September 2020; Accepted 5 November 2020; Published 27 November 2020

Academic Editor: Vinod Karar

Copyright © 2020 Jiho Shin et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The industrial control system (ICS) inherits the attributes of the traditional information system, but because it has its own characteristics that availability of triad (CIA) of information security should be a top priority, it needs to be set differently from the traditional information security requirements. In response to the issue, TTAK.KO-12.0307 (Standard for Industrial Control System Information Security Requirements) proposed by the National Security Research Institute (NSRI) and established by the Telecommunications Technology Association (TTA) is being used. However, it is difficult to apply security requirements of TTAK.KO-12.0307 uniformly because of the reason that the characteristics of the ICS in each layer are different. There is also a limit to invest the security resources with equivalent priority for all requirements and ICS layers. It is still unresolved in the previous research studies which are related to information security resources, for example, Choi (2013), Ko et al. (2013), and Nah et al.'s (2016) studies. Therefore, this study tried to focus on what a top priority of information security requirements by the ICS in each layer is, using the analytic hierarchy process. As a result, we derived that the top priority requirement in the operation layer is "Identification Authentication Access Control," in the control layer is "Event Response," and in the field device layer is "Physical Interface Protection" with the highest importance. The results of this study can be utilized as a guideline for the security strategy and policy design by determining security requirements that should be prioritized in each layer of the ICS.

1. Introduction

Our society has achieved rapid industrial development based on the use of the industrial control system (ICS) in the core infrastructure such as automated processes, power generation, energy supply, transportation, and smart cities and factories [1]. ICS with closed characteristics (air-gap) from the external network that is completely different from the traditional information systems were considered relatively safe from cyberattacks and did not consider security in system design and deployment. However, in recent years, the ICS has been actively adopting IT technologies [2]. Although the digital transformation of ICSs represents the foundation for resource-efficient and flexible industrial plants, this change increases the attack surface, leading to the emergence of new threats [3]. The convergence of the ICS and the latest IT technology creates more complex problems in the security environment, and the emergence of Internet of things (IoT) technology, in particular, makes the need related security functions (e.g., key management, intrusion detection, access control, privacy protection, and wireless sensor networks security) [4, 5] more urgent [6]. IoT technologies such as beacons, for example, may have security vulnerabilities such as spoofing, DoS, and hijacking [7]. Substantial recent investment for the ICS has been directed towards the development of the ICS, that is, relies on the creation of a bridge between digital and physical environments through IoT technologies, as well the ICS itself [8]. In other words, many IoT devices are installed in the field device layer area of the ICS system and are operated based on communication with the control layer. In response, the ICS includes a smart IoT mobile environment that supports IoT-based mobility, so secure computing should be guaranteed. If the ICS is exposed to cyber threats, serious disasters can occur throughout society. In 2010, 1,000 centrifuges were destroyed in an attack on Iran's nuclear facilities using Stuxnet, known as the first malicious code for the ICS, in which the programmable logic controller (PLC), a controller that controls field devices at nuclear facilities, was infected [9]. A lot of research studies on information security of the ICS have been invested, and a lot of efforts have been made to apply relevant security measures since the Stuxnet incident case.

It is necessary to develop and apply exclusive security requirements because the security requirements for the traditional information system are not applicable to the ICS. The biggest differences between the ICS and the information system are the purpose of cyberattacks and the priority of information security triad (CIA). In IT systems, the security is generally defined in terms of three key principles: confidentiality, integrity, and availability (also known as the CIA triad). Confidentiality focuses on ensuring assets are not disclosed to those entities who are not authorized to view it; integrity relates to protecting assets from unauthorized modifications; and availability is defined in terms of making the assets accessible to authorized entities at all permitted times [8]. Availability is known as a top priority and is also the main target of cyberattacks, as the collapse of the ICS could cause great damage. Availability is known as a top priority and is also the main target of cyberattacks, as the collapse of the ICS could cause great damage. In response to the issue, the National Security Research Institute (NSR) proposed Security Requirements for Industrial Control System by defining the features of the ICS, and it was established as a standard (TTAK.KO-12.0307) [10] by the Telecommunications Technology Association (TTA).

However, it is difficult to apply uniformly security requirements of TTAK.KO-12.0307 because the features of the ICS in each layer are different, and security resources are always not enough. In addition, it is still unresolved in the previous research studies which are related to information security resources, for example, Choi [11], Ko et al. [12], and Nah et al. [13]. Choi proposed an appropriate security assessment methodology and a checklist for the ICS, but the checklist does not provide a priority based on the characteristics of the devices; so, it is difficult to determine which areas focus more in terms of security resources. Ko et al. proposed an assessment method for measuring the security threat on smart grid based on the priority, but a limit of their study was the mean time-to-compromise (MTTC) model; they used to determine simply the number of security vulnerabilities that exist on the attack path when calculating an important weight. HoonNah and JungChan suggested the need to establish an ICS security standard same as TTAK.KO-12.0307, but there is no specific discussion of what level of security each component or layer should respond to. So, it is necessary to prioritize and apply security requirements with the standard TTAK.KO-12.0307. In particular, the ICS is a huge system divided into layers which are operated by exchanging data with each other.

Therefore, security requirements priorities should be derived and applied for each layer suitably. For this, the security requirements of TTAK.KO-12.0307 are used to analyze the priority of security requirements for each layer in this paper. Based on this, it is intended to help determine where the portion of information security resources investment should be prioritized. The results of this study provide a guideline to avoid uniform security requirements for all layers. Prioritization can be derived through the assessment of security requirements for each layer using the analytic hierarchy process method, thereby contributing to effective investment in information security resources. The results of this study are also expected to be an important contribution to IoT security and privacy protection as well as to the ICS. To discuss this, ICS security and prior research are discussed in Section 2, and the design of the research model to be used for priority analysis using AHP is discussed in Section 3, and empirical analysis conducted based on this is discussed in Section 4. The implications of the analysis results are discussed in Section 5 and finally concluded in Section 6.

2. Background

2.1. Information Security of ICS. The ICS basically inherits many attributes of the traditional IT system. However, in order to derive an information security investment priority, we need to look at a variety of different aspects from the traditional IT system [6]. First, in hardware and software aspects, the IT system operates on a short-term replacement cycle, but the ICS has at least 15 years of long-term replacement cycles generally. The IT system also uses universal operating systems (general-purpose) such as Windows and Linux, but the ICS uses exclusive operating systems. In addition, maintenance and repair, such as system patches, on the ICS are more difficult than traditional IT systems. At last, in network performance aspect, the IT system focuses on overall performance, such as the reliability of responses is important and tolerability exists for some communication delays, but the ICS focuses on real-time responsiveness and is inflexible for communication delays. For risk management objectives, the ICS does not allow the control device to be shut down, and system availability is very important, but the integrity of the data is more important, and some failures can be allowed in the IT system. As a result, the IT system can end up with relatively minor economic damage, such as inconvenience or delay, due to cyberattacks or incidents caused by its own defects. However, the ICS could immediately halt operations at industrial sites, leading to human casualties and massive disasters, which could result in huge social and economic damages. This means that among the CIA triad of information security, the traditional IT system should prioritize "Confidentiality" and "Integrity," while the ICS should prioritize "Availability."

These characteristics set the cyberattacker's goals differently. While cyberattacks on the traditional IT system were primarily aimed at leaking classified information, attacks targeting on the ICS are mainly focused on operational paralysis. This is because stopping the ICS will cause great damage. In the 2010 Stuxnet case, the attack was carried out by infecting Siemens PLC to paralyze operations by manipulating the number of rotations of connected centrifuges, and the main objective in subsequent series of major cyberattacks against the ICS was to disrupt normal operations.

2.2. Literature Review. The past ICS was recognized as safe by configuring an independent network, but the vulnerability was revealed in a bypass attack by the malicious code. In order to respond, HoonNah and JungChan insisted that comprehensive and systematic security measures are needed to defend themselves in depth from cyberattacks and specifically suggested the need to establish standards for security of the ICS. Particularly important is that they took the same argument as this paper, judging that it is unrealistic to take measures at an equal security level for all vulnerabilities [13]. However, there is a limit to driving their arguments because there is no specific discussion of what level of security each component or layer should respond to.

Since the ICS operates in various environments, including major national infrastructure and social overhead capital facilities, the security assessment and security resource investment are of great importance. Therefore, the security assessment of the ICS should be carried out using an objective and feasible inspection process. Choi [11] proposed an appropriate security assessment methodology and checklist for the ICS, taking into account the characteristics of the ICS environment, devices, and operation methods. However, its usefulness could not be verified because there were no examples to verify the proposed methodology, and moreover, the proposed methodology does not provide a checklist that should be prioritized based on the characteristics of the devices; so, it is difficult to determine which areas to focus more on security resources.

Ko et al. proposed an assessment method for measuring the security threat on smart grid [12]. In particular, the ICS network has a hierarchical structure, and security sensitivity of the produced data by each layer is different; so, they suggested that it is necessary to make a level as layers with similar data sensitivity into one area. And they used these levels (consumer level, advanced metering infrastructure head end level, and control center level) to prioritize what needs to be protected in that network. They explained that if protection is relatively unnecessary or if it is difficult for an attacker to access for attack, they can increase efficiency by excluding it from the vulnerability target. Their research can be seen as a previous study of the need investment priorities of information security resource for the ICS to be discussed in this paper. They used a quantified network model to assess security threats applied to advanced metering infrastructure and validated the security threat assessment for the proposed model using mean-time-to-compromise (MTTC) proposed by Leversage and Byres [14] for the resulting attack scenario. However, there is a limitation that the evaluation method using MTTC does not evaluate the overall security threat to the ICS. This is because MTTC simply determines that the number of security vulnerabilities that exist on the attack path is an important weight.

As such, many methodologies for security assessment are important to effectively respond to security threats for the ICS. Although many studies have been conducted, it is difficult to find a discussion that the security assessment uses the information security standard for the ICS. This is because there has been no definition of specific information security requirements to the ICS. It is also understood that although there are already established ICS information security requirements, there is a lack of discussion on the methodology for applying them to each ICS. Therefore, in this paper, we want to provide guidelines for efficient investment of security resources by analyzing the priorities of each layer when using TTAK.KO-12.0307.

3. Design of Analysis

3.1. Analytic Hierarchy Process Methodology. In this study, the analytical hierarchy process (AHP) method was used to analyze the investment priority of information security resources in the ICS. The AHP was developed by Tomas in the 1970s as part of the decision-making method through the multiple assessment criteria for multiple alternatives [15]. In general, decision-making problems should be solved by choosing the optimal alternative under multiple criteria, and many existing decision-making problems have been solved using statistical models under controlled assumptions [16]. In addition, decision-making problems often include qualitative criteria, which led to the need to quantify criteria with subjective values [16]. In other words, many other real-world problems involve the need to combine quantitative measures with qualitative concerns [17]. This has the problem of prioritizing ICS information security requirements, depending on the responder with different levels of awareness and expertise of information security. In particular, since a big part of information security relates to qualitative and nonfinancial concerns, traditional economic approaches are severely constrained [17]. Saaty developed the AHP to analyze multicriteria decision problems involving both quantitative and qualitative criteria [17–19]. AHP methodology uses the concept of hierarchy to lay out the different elements (purpose, alternatives, and factors) needed to make decisions, thereby providing a more detailed and logical view of the relationship between the different elements [20]. The AHP methodology for performing pairwise comparisons between elements of each layer has been widely used in multidecision-making problems, with two typical advantages: first, weighting between assessment elements can be determined through systematic quantitative procedures. In addition, the choice of optimal alternatives has the advantage of being easier to understand than conventional statistical decisions and being able to use the subjective and objective information of experts comprehensively. Second, it provides indicators to determine the consistency of decision makers (experts). And the analysis procedures are consistent with reasonable decision-making procedures [21].

3.2. Analysis Model Design. In order to analyze the relative investments priorities of information security resource in the ICS, this study has established assessment criteria based on the classification divided in ICS information security requirements (TTAK.KO-12.0307) of TTA. However, the method of prioritizing information security investment for the entire ICS has a wide range of coverage, and there is ambiguity in the selection of priorities. Therefore, it is desirable to perform an analysis of the investment priorities of information security resources by classifying the ICS into each layer.

There are several definitions for layers in the ICS. Irfan Ahmed et al. suggested that information security of ICS/supervisory control and data acquisition (SCADA) should be classified into six layers, based on connectivity between components in the system and connectivity between other networks, such as the system network and the Internet [22]. However, it is difficult to use it as an analysis model because it does not include field devices such as sensors and actuators, and wired and wireless devices are not considered.

On the other hand, TTAK.KO-12.0307 presents the "Security Reference Model" to define the information security requirements of the ICS and is divided into 3 layers which consisted of the "Operation Layer," "Control Layer," and "Field Device Layer" (Figure 1). The "Operation Layer" uses the data received from the control layer to monitor the status of the field devices or send control commands, including engineering workstation (EWS) and human-machine interface (HMI) [10]. The "Control Layer" is responsible for transferring the measured and collected data from the field devices to the operation layer. And the layer is also responsible for controlling the field devices with command from the operation layer, including the PLC, distributed control system (DCS), and remote terminal unit (RTU) [10]. The "Field Device Layer" includes a field device used to measure, collect, and control status data, such as sensors and actuators, and the field device is connected to the control layer by wired and wireless networks or by serial cables [10]. The priority assessment criteria of this paper are based on the classification of TTAK.KO-12.0307.

However, some of information security requirements of TTAK.KO-12.0307 were merged because there were many assessment criteria to be used as the AHP method. Then "Identification Certification" and "Access Control" were merged among security functions on hierarchy I, and "Transmission Data Protection" and "Stored Data Protection" were merged in the same way. Finally, the analysis model to be used for priority assessment is shown in Figure 2.

TTAK.KO-12.0307 set different assessment criteria for the operation layer and control/field device layer. So, there were also two models for investment priority of information security resource analysis. Figure 2 was used in the operation layer, and Figure 3 was used in the control layer and field device layer.

3.3. Analysis Criteria. Table 1 shows the assessment criteria and its descriptions in TTAK.KO-12.0307.

4. Empirical Analysis

4.1. Analysis Method and Tool. The analysis of this study uses the AHP, a hierarchical decision analysis method, but also provides a description of each assessment criteria to help the survey respondents understand. In the AHP analysis method, it is very important to ensure objectivity and expertise in response. The AHP survey was conducted by selecting researchers, practical experts, and a professor related to the ICS, cyber physics system (CPS), and SCADA system. They are affiliated in National Security Research Institute, Electronics and Telecommunications Research Institute (these 2 are government-based research institutes), Incheon International Airport, Naonwork, OnSecurity, Coontec (these 4 are corporations related on ICS information security), and Ajou University.

The assessment criteria were based on TTAK.KO-12.0307 as described above, but there is only one assessment criterion in the network robustness section of the "Operation Layer;" so, the pairwise comparison was not conducted (Figure 2). In addition, as discussed above, "Identification·Authentication" and "Access Control," which are classified as the security functions section, were set by merging into "Identification·Authentication·Access Control" due to similarity in content. In the same way, "Transmission Data Protection" and "Stored Data Protection" were also set by merging into "Data Protection." Finally, the survey was conducted by setting up 3 assessment criteria in hierarchy I and 10 assessment criteria in hierarchy II (but 8 assessment criteria for the "Operating Layer") (Table 1).

4.2. Verification Consistency of Survey Responses. The AHP survey of this study was conducted for a month from December 2019 to January 2020 and was conducted on industry, academia, and research experts related to information security of the ICS. There are a few of discussions regarding the appropriate sample size in order to carry out the AHP analysis. Melillo and Pecchia insisted that smaller sample size is required in case of equally important alternative [23]. The reliability of AHP results is more relevant to the respondents' expertise rather than the number of response samples. In this study, the experts responded to the survey in the field of information security of the ICS with at least more than five years of related experience. A total of 19 experts were surveyed, and 19 responses were collected. AHP analysis of response data used the DRESS tool.

The AHP analysis method determines consistency index (CI) of the response to ensure reliability of the analysis results. Due to the characteristic of the pairwise comparison, the lower the CI, the more consistent it is, which is related to the respondents' expertise. Generally, responses with a CI value of 10% or less are considered consistent. In this study, 4 surveys with a CI value of 0.1 or higher were excluded from the results analysis, so only 15 responses were used for the analysis.

5. AHP Analysis Result

In this study, the results of AHP analysis were divided into the "Operation Layer," "Control Layer," and "Field Device Layer" for the investment priority of information security resources in the ICS.

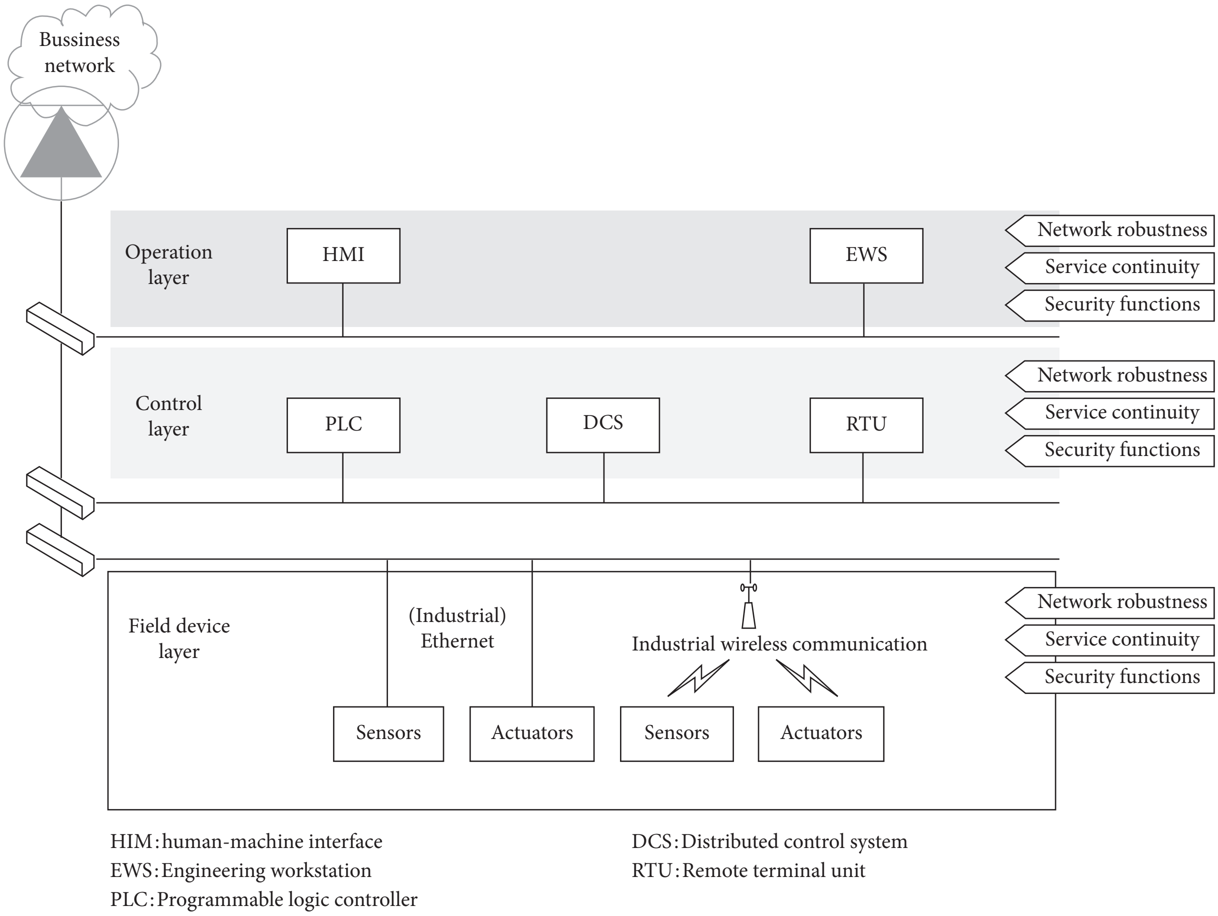

Figure 1: Security reference model of TTAK.KO-12.0307 [13].

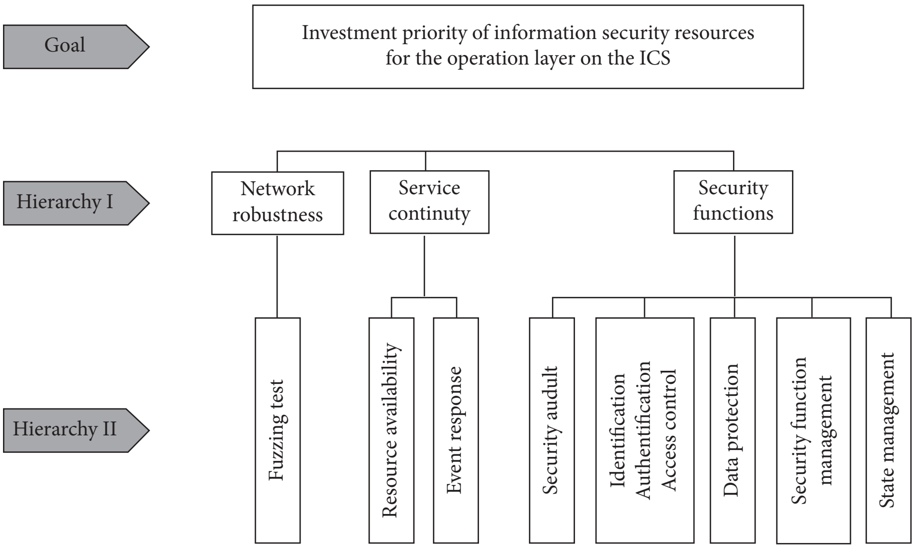

Figure 2: Investment priority of information security resources for the "Operation Layer" on the ICS.

5.1. Operation Layer. The AHP results for the analysis of investment priority of information security resource by the "Operation Layer" of the ICS are as follows.

An analysis result of the priority on hierarchy I showed that "Security Functions" was the highest priority with an importance 0.371, "Service Continuity" was the second priority with an importance 0.358, and "Network Robustness" was the third priority with an importance 0.271 (Table 2).

In "Security Functions" section, which was ranked the highest priority in hierarchy I, "Identification·Authentication·Access Control" was the highest priority with an importance 0.291, "Security Function Management" was the second priority

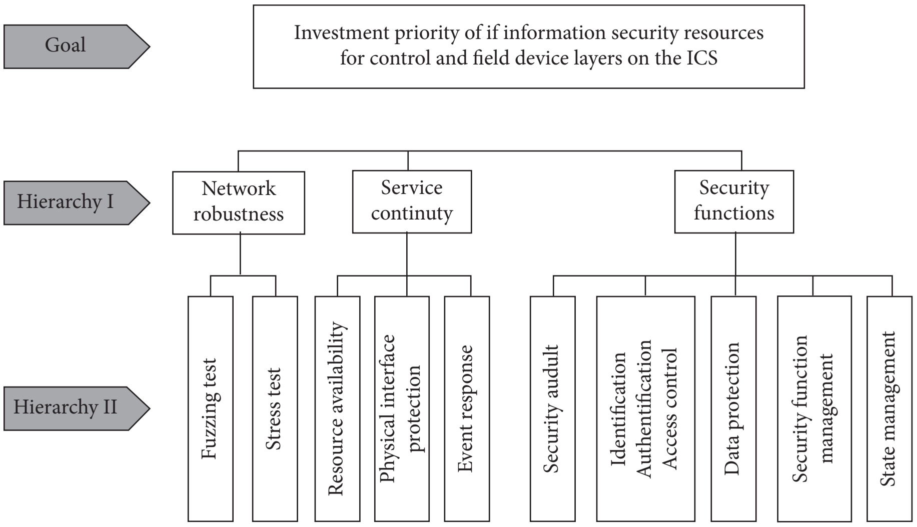
Goal
Investment priority of if information security resources for control and field device layers on the ICS
Hierarchy I
Network robustness
Service continuty
Security functions
Hierarchy II
Fuzzing test
Stress test
Resource availability
Physical interface protection
Event response
Security audult
Identification Authentification Access control
Data protection
Security function management
State management

Figure 3: Investment priority of information security resources for the "operation layer" on the ICS.

Table 1: Criteria and descriptions of ICS security requirements.

	Hierarchy I		Hierarchy II	
	Criteria	Description	Criteria	Description
ICS security requirements	Network robustness	Require network robustness against external cyberattacks or internal abnormal behavior	Fuzzing test	Require handling capability to sustain the ICS service when receiving abnormal network packet
			Stress test	Require providing ICS service even when overloading the network traffic
	Service continuity	Require stable and continuous service	Resource availability	Require resource management procedures, such as backup and recovery, so that resources can perform their normal functions
			Physical interface protection	Require resource management procedures, such as backup and recovery, so that resources can perform their normal functions
			Event response	Require checking the status of devices, systems, and networks in real-time and responding to failures
	Security functions	Require security features such as component identification, authentication, and access control	Security audit	Require security audits through creating and encrypting audit-logs for major events
			Identification, authentication, and access control	Require separation or restriction about identification and access authority of devices/users with a user authentication procedure
			Data protection	Require confidentiality and integrity of sensitive transmission or stored data
			Security functions management	Require network and security settings of the control software, secure encryption algorithms, and key management
			State management	Require state management such as integrity verification of the execution code, normal operation test, and vulnerability response

with an importance 0.195, and "Data Protection" was the third priority with an importance 0.194, followed by "State Management" and "Security Audit" in order (Table 3). In "Service Continuity" section, which was ranked the second priority in hierarchy I, "Event Response" was the highest priority with an importance 0.534 and "Resource Availability" was the second priority with an importance 0.466. In "Network Robustness" section, which was ranked the third priority in hierarchy I, there is only one assessment criterion, which is the "Fuzzing Test" in the sector, so the pairwise comparison survey was not

Table 2: AHP result of hierarchy I on all layers.

Layer	Operation layer		Control layer		Field device layer	
Hierarchy I	Importance	Priority	Importance	Priority	Importance	Priority
Network robustness	0.271	3	0.281	2	0.258	3
Service continuity	0.358	2	**0.439**	**1**	**0.463**	**1**
Security functions	**0.371**	**1**	0.280	3	0.279	2
Consistency index	0.02		0.02		0.03	

The highest priority of each layer is shown in bold.

Table 3: AHP result of hierarchy II on the operation layer.

Hierarchy I	Hierarchy II	Importance	Priority	C.I.
Network robustness	Fuzzing test	—	**1**	—
Service continuity	Resource availability	0.466	2	0.00
	Event response	**0.534**	**1**	
Security functions	Security audit	0.153	5	0.07
	Identification authentication access control	**0.291**	**1**	
	Data protection	0.194	3	
	Security function management	0.195	2	
	State management	0.168	4	

The highest priority of each hierarchy on operation layer is shown in bold.

conducted, but the importance can be very high. Because TTAK.KO-12.0307 security requirements require network robustness even in the following cases through the "Fuzzing Test." (1) In case of the order of the field in packets is changed, (2) in case of a part of the field in packets is cut, (3) in case of the field size in packets is different, (4) in case of the fixed value of the field in packets is different, and (5) in case of the value of the field in packets is not within the valid range [10].

As a result of the priority pairwise comparison of all criteria in the "Operation Layer" of the ICS, "Identification·Authentication·Access Control" was the highest priority with an importance 0.171, "Event Response" was the second priority with an importance 0.168, and "Resource Availability" was the third priority with an importance 0.122, followed by "Security Function Management," "State Management," "Data Protection," "Fuzzing Test," and "Security Audit" in order (Table 4).

5.2. Control Layer. The AHP results for the analysis of investment priority of information security resource by the "Control Layer" of the ICS are as follows.

An analysis result of the priority on hierarchy I showed that "Service Continuity" was the highest priority with an importance 0.439, "Network Robustness" was the second priority with an importance 0.281, and "Security Functions" was the third priority with an importance 0.280 (Table 2).

In "Service Continuity" section, which was ranked the highest priority in hierarchy I, "Physical Interface Protection" was the highest priority with an importance 0.362, "Resource Availability" was the second priority with an importance 0.336, and "Event Response" was the third priority with an importance 0.302 (Table 5). In "Network Robustness" section, which was ranked the second priority in hierarchy I, the "Fuzzing Test" was the highest priority with an importance 0.510, and the "Stress Test" was the second priority with an importance 0.490. In "Security Functions" section, which was ranked the third priority in hierarchy I, "Identification·Authentication·Access Control" was the highest priority with an importance 0.256, "State Management" was the second priority with an importance 0.215, and "Security Function Management" was the third priority with an importance 0.203, followed by "Data Protection" and "Security Audit" in order.

As a result of the priority pairwise comparison of all criteria in the "Control Layer" of the ICS, "Event Response" was the highest priority with an importance 0.128, "Resource Availability" was the second priority with an importance 0.122, and "Identification·Authentication·Access Control" was the third priority with an importance 0.119, followed by the "State Management," "Physical Interface Protection," "Security Function Management," "Data Protection," "Stress Test," "Security Audit," and "Fuzzing Test" in order (Table 6).

5.3. Field Device Layer. The AHP results for the analysis of investment priority of information security resource by the "Field Device Layer" of the ICS are as follows.

An analysis result of the priority on hierarchy I showed that "Service Continuity" was the highest priority with an importance of 0.463, "Security Functions" was the second priority with an importance 0.279, and "Network Robustness" was the third priority with an importance 0.258 (Table 2).

In "Service Continuity" section, which was ranked the highest priority in hierarchy I, "Physical Interface Protection" was the highest priority with an importance 0.375, "Event Response" was the second priority with an importance 0.333, and "Resource Availability" was the third priority with an importance 0.292 (Table 7). In "Security Functions" section, which was ranked the second priority in hierarchy I, "State Management" was the highest priority

Table 4: Final priorities among all criteria on the operation layer.

Hierarchy I	Hierarchy II	Importance	Priority	C.I.
Network robustness	Fuzzing test	0.095	7	
Service continuity	Resource availability	0.122	3	0.75
	Event response	0.168	2	
Security functions	Security audit	0.094	8	
	Identification authentication access control	**0.171**	**1**	
	Data protection	0.113	6	
	Security function management	0.120	4	
	State management	0.118	5	

The highest priority among all criteria on the operation layer is shown in bold.

Table 5: AHP result of hierarchy II on the control layer.

Hierarchy I	Hierarchy II	Importance	Priority	C.I.
Network robustness	Fuzzing test	**0.510**	**1**	0.00
	Stress test	0.490	2	
Service continuity	Resource availability	0.336	2	0.02
	Physical interface protection	**0.362**	**1**	
	Event response	0.302	3	
Security functions	Security audit	0.123	5	0.04
	Identification authentication access control	**0.256**	**1**	
	Data protection	0.203	4	
	Security function management	0.203	3	
	State management	0.215	2	

The highest priority of each hierarchy on the control layer is shown in bold.

Table 6: AHP result of hierarchy II on the control layer.

Hierarchy I	Hierarchy II	Importance	Priority	C.I.
Network robustness	Fuzzing test	0.061	10	
	Stress test	0.080	8	
Service continuity	Resource availability	0.122	2	0.08
	Physical interface protection	0.103	5	
	Event response	**0.128**	**1**	
Security functions	Security audit	0.078	9	
	Identification authentication access control	0.119	3	
	Data protection	0.097	7	
	Security function management	0.101	6	
	State management	0.112	4	

The highest priority among all criteria on the control layer is shown in bold.

Table 7: AHP result of hierarchy II on the field device layer.

Hierarchy I	Hierarchy II	Importance	Priority	C.I.
Network robustness	Fuzzing test	0.473	2	0.00
	Stress test	**0.527**	**1**	
Service continuity	Resource availability	0.292	3	0.02
	Physical interface protection	**0.375**	**1**	
	Event response	0.333	2	
Security functions	Security audit	0.115	5	0.05
	Identification authentication access control	0.243	2	
	Data protection	0.219	3	
	Security function management	0.167	4	
	State management	**0.256**	**1**	

The highest priority of each hierarchy on the field device layer is shown in bold.

with an importance 0.256, and the “Identification·Authentication·Access Control” was the second priority with an importance 0.490, followed by “Security Function Management” and “Security Audit” in order. In “Network Robustness” section, which was ranked the third priority in hierarchy I, “Network Robustness” was the

Table 8: AHP result of hierarchy II on the field device layer.

Hierarchy I	Hierarchy II	Importance	Priority	C.I.
Network robustness	Fuzzing test	0.074	9	0.07
	Stress test	0.081	8	
Service continuity	Resource availability	0.110	3	
	Physical interface protection	**0.159**	**1**	
	Event response	0.105	5	
Security functions	Security audit	0.069	10	
	Identification authentication access control	0.118	2	
	Data protection	0.105	4	
	Security function management	0.087	7	
	State management	0.090	6	

The highest priority among all criteria on the field device layer is shown in bold.

Table 9: Implication of the AHP analysis result on the ICS in each layer.

Considerations	Layers	Operation layer	Control layer	Field device layer
Practical environments	Security aspect	A lot of user accesses that need to be identified for security	Various events of devices, systems, and networks that need to be handled for service continuity	Control end-point devices along with ethernet or the IoT network
	Risks	Social engineering attacks or user carelessness	Service abort or collapse availability	Manipulating command attack to end-point devices
Top priority for security resources investment	Hierarchy I	Security functions	Service continuity	Service continuity
	Hierarchy II	Identification Authentication Access control	Event response	Physical interface protection
TTAK.KO-12.0307 standard		Based on Priority analysis		Analytic hierarchy process

highest priority with an importance 0.527, and the "Fuzzing Test" was the second priority with an importance 0.473.

As a result of the priority pairwise comparison of all criteria in the "Field Device Layer" of the ICS, "Physical Interface Protection" was the highest priority with an importance 0.159, "Identification·Authentication·Access Control" was the second priority with an importance 0.118, and "Resource Availability" was the third priority with an importance 0.110, followed by the "Data Protection," "Data Protection," "State Management," "Security Function Management," "Stress Test," "Fuzzing Test," and "Security Audit" in order (Table 8).

5.4. Implications. It is difficult to deploy effective resources in applying the uniform security requirements because the ICS has a wide range of areas and, above all, different characteristics of each layer. In this study, it was intended to avoid applying the uniform security requirements for ICS and to contribute to the effective investment in information security resources by deriving the priority of security requirements for each layer on the ICS.

As a result of analyzing the priority of assessment criteria for each layer using AHP, "Identification Authentication Access Control" was the most important security requirement that should be prioritized on the "Operation Layer." This emphasizes that these criteria are the most important to prepare for information security from the risks of social engineering attacks or exposure due to user carelessness, mainly because the operation layer has a lot of user access. "Event Response" was the most important security requirement that should be prioritized on the "Control Layer." This emphasizes the need for various events in the control layer to be properly handled in order for the service to continue to operate. Because "Event Response" is an item that requires real-time identification of the status of devices, systems, and networks and is responsive in the event of various failures. "Physical Interface Protection" was the most important security requirement that should be prioritized on the "Field Device Layer." The "Field Device Layer" has a variety of devices, including sensors and actuators, and is an important layer of control over end-point devices using industrial ethernet or wireless IoT networks, requiring a high-level protection from the physical interface accessible to this layer (Table 9).

On the contrary, it is also necessary to point out the commonly lowest assessment criteria for investment priority of information security resources for the ICS. "Security Audit" was analyzed with the lowest importance in the "Operation Layer" and "Field Device Layer." In terms of investment of information security resources, "Security Audit" performs audits by creating audit log for major events and encrypting the log data, mainly as part of long-term security functions rather than real-time response or service continuity, so "Security Audit" can be analyzed as

Table 10: Comparison of the approaches for the ICS information security.

Parameters	Approaches				
	Choi [12]	Ko et al. [13]	Hoon Nah and Na [11]	TTAK.KO-12.0307 [10]	Proposed approach
Proposed exclusive security requirements	No	Yes	Partially yes	Yes	Yes
Utilization of a standard	No	No	Yes	Yes	Yes
Concept of ICS layers	Not considered	3 levels (according to data sensitivity)	Not considered	3 layers (security reference model)	3 layers (security reference model)
Security requirements priority analysis	Yes	Yes	Not considered	Not considered	Yes
Security resource investment decision	Using the risk evaluation checklist	Using the number of vulnerabilities in the attack path	Not considered	Not considered	Using the priorities
Usability as a guidelines	Partially possible	Partially possible	Partially possible	Impossible	Possible

relatively low importance due to the availability aspect in the ICS.

In summary, we have successfully derived security investment priorities using AHP techniques and TTAK.KO-12.0307 standards for ICS information security priorities that have not been addressed in our previous research. The biggest advantage of this result is that it can be used as a guideline when establishing ICS security policies. In addition, the results of this study contribute significantly to the effective distribution of information security resources that were not addressed in previous studies (Table 10).

6. Conclusion and Further Research

The ICS inherits the attributes of the traditional information system, but because it has its own characteristics such as availability and continuity, it needs to be set differently from the information security requirements of the traditional information system. For appropriate information security requirements and assessment on the ICS, TTAK.KO-12.0307 proposed by the NSR and established by the TTA is being used.

In this study, the priorities of assessment criteria by hierarchy were analyzed to enhance the efficiency of investment in information security resources on the ICS. There are many difficulties in operating an industrial control system to establish security policies for all the requirements set forth in the standards. Therefore, the results of this study can be used to design security strategies and policies by selecting the security elements that should be relatively prioritized for each layer in the operation of the industrial control system. It can also be used as a guideline for determining the investment priority of security resources to the ICS that are currently in operation or are being redesigned. However, in the course of carrying out this study, experts who responded to the survey commented on whether TTAK.KO-12.0307 standard, which was used as assessment criteria, was suitable for the security requirements, so it will remain a future research.

Data Availability

The data used to support the findings of the study are available at Security Requirements for Industrial Control System (TTAK.KO-12.0307) and Telecommunication Technology Association http://www.tta.or.kr/data/weeklyNoticeView.jsp?pk_num=5621.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2020-2018-0-01799) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation) and supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT: Ministry of Science and ICT) (NRF-2020R1A2C1012187).

Supplementary Materials

Supplementary figures of the survey sheet are provided as a separate file under the Supplementary Materials section (Figures 1–3). (*Supplementary Materials*)

References

[1] S. Keith, V. Pillitteri, and S. Lightman, *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication, National Institute of Standard and Technology, Gaithersburg, MD, USA, 2015.

[2] J.-H. Lee and W.-N. Kim, "Security requirements for industrial control system," *Telecommunication Technology Association*, vol. 173, pp. 62–66, 2017.

[3] M. Eckhart, B. Brenner, and A. Ekelhart, "Quantitative security risk assessment for industrial control systems: research opportunities and challenges," *Journal of Internet Service and Information Security*, vol. 9, no. 3, pp. 52–73, 2019.

[4] H. Hui, X. An, and H. Wangetal, "Survey on blockchain for internet of things," *Journalof Internet Service-andInformationSecurity*, vol. 9, no. 2, pp. 1–30, 2019.

[5] V. Korzhuk, A. Groznykh, and M. Alexander, "Identification of attacks against wireless sensor networks based on

behaviour analysis," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 10, no. 2, pp. 1–21, 2019.

[6] M. StJohn-Green, R. Piggin, and J. A. McDermid, "Combined security and safety risk assessment—what needs to be done for ICS and the IoT," in *Proceedings of the 10th IET System Safety and Cyber-Security Conference*, pp. 1–7, Bristol, UK, 2015.

[7] H. K. Almathami, A. Majed, and E. Vlahu-Gjorgievska, "An analytical approach to using and implementing beacons: opportunities and challenges," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 10, no. 1, pp. 57–74, 2019.

[8] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *Journal of Manufacturing Systems*, vol. 47, pp. 93–106, 2018.

[9] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *Proceedings of the IECON 2011—37th Annual Conference of the IEEE Industrial Electronics Society*, pp. 4490–4494, Melbourne, Australia, November 2011.

[10] TTA, Security Requirements for Industrial Control System, *TTAK.KO-12.0307, Telecommunication Technology Association*, 2015, http://www.tta.or.kr/data/weeklyNoticeView.jsp?pk_num=5621.

[11] M. Choi, "A study on security evaluation methodology for industrial control systems," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 23, no. 2, pp. 287–298, 2013.

[12] J. Ko, S. Lee, and T. Shon, "Security threat evaluation for smartgrid control system," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 23, no. 5, pp. 873–883, 2013.

[13] J. HoonNah and N. JungChan, "Industrial control system security standardization trend," *Review of the Korea Institute of Information Security & Cryptology*, vol. 26, no. 4, pp. 28–35, 2016.

[14] D. J. Leversage and E. J. Byres, "Estimating a system's mean time-to-compromise," *IEEE Security & Privacy*, vol. 6, no. 1, pp. 52–60, 2008.

[15] L. S. Thomas, "Decision making with the analytic hierarchy process," *International Journal of Services Sciences*, vol. 1, no. 1, pp. 83–98, 2008.

[16] J. Hyo-Jung, "Analysis on the information security manpower policy with analytic hierarchy process," in *Proceedings of the Symposium of the Korean Institute of communications and Information Sciences*, pp. 468–471, Seoul, Republic of Korea, 2003.

[17] L. D. Bodin, L. A. Gordon, and M. P. Loeb, "Evaluating information security investments using the analytic hierarchy process," *Communications of the ACM*, vol. 48, no. 2, pp. 78–83, 2005.

[18] L. S. Thomas, "A scaling method for priorities in hierarchical structures," *Journal of Mathematical Psychology*, vol. 15, no. 3, pp. 234–281, 1977.

[19] L. S. Thomas, *The Analytic Hierarchy Process*, McGraw-Hill, New York, NY, USA, 1980.

[20] T.-S. Kim, "Analysis on information security manpower policy by the analytic hierarchy process," *The Journal of Korean Institute of Communications and Information Sciences*, vol. 31, pp. 486–493, 2006.

[21] W. Sung, "A study on information security policy priority using AHP (analytic hierarchy process)," in *Proceedings of the Symposium of the Korean Association for Public Administration*, pp. 1614–1634, Seoul, Republic of Korea, October 2011.

[22] I. Ahmed, S. Obermeier, M. Naedele, and G. G. Richard III, "Scada systems: challenges for forensic investigators," *Computer*, vol. 45, no. 12, pp. 44–51, 2012.

[23] P. Melillo and L. Pecchia, "What is the appropriate sample size to run analytic hierarchy process in a survey-based research?" in *Proceedings of the International Symposium of the Analytic Hierarchy Process*, pp. 4–7, London, UK, August 2016.