Computers, Materials & Continua
DOI:10.32604/cmc.2021.015632
Article

Tech Science Press

Management of Schemes and Threat Prevention in ICS Partner Companies Security

Sangdo Lee[1] **and Jun-Ho Huh**[2,*]

[1]Cyber Security Center, Korea Midland Power Co., Ltd., Boryeong, Korea
[2]Department of Data Informatics, (National) Korea Maritime and Ocean University, Busan, Korea
[*]Corresponding Author: Jun-Ho Huh. Email: 72networks@kmou.ac.kr
Received: 30 November 2020; Accepted: 28 April 2021

Abstract: An analysis of the recent major security incidents related to industrial control systems, revealed that most had been caused by company employees. Therefore, enterprise security management systems have been developed to focus on companies' personnel. Nonetheless, several hacking incidents, involving major companies and public/financial institutions, were actually attempted by the cooperative firms or the outsourced manpower undertaking maintenance work. Specifically, institutions that operate industrial control systems (ICSs) associated with critical national infrastructures, such as traffic or energy, have contracted several cooperative firms. Nonetheless, ICT's importance is gradually increasing, due to outsourcing, and is the most vulnerable factor in security. This paper proposes a virtualized security management scheme for the resident cooperative firms in the industrial control infrastructure. Since such companies often cannot afford adequate investment in security, the scheme is to let an ICS company provide the virtualized system. One of its merits is the convenience of controlling a VDI server at the center. The cooperative firms were classified, based on their respective security levels, and statistics were collected throughout a four-year period for the results. This paper analyzes the policies and virtualization systems that have been applied to the security of the partner companies, which engaged in ICS security. A suitable model for ICS security was then proposed by analyzing their effects on the system efficiencies, based on the comparisons of the security inspection results obtained before and after virtualization. The proposed system is expected to contribute to industrial safety.

Keywords: Nuclear power plant; nuclear power plant security; virtual machine; SCADA; ICS; ISO27001; VDI based security; software engineering

1 Introduction

We are now witnessing the emergence of the fourth Industrial Revolution, by building on the third one [1], the digital revolution that has been taking place since the middle of the last century. This revolution is characterized by a fusion of technologies, which blur the lines between the physical, digital, and biological spheres [2].

An analysis of the causes of the security incidents that involve a control system, showed that most had been caused by employees of partner companies who provide maintenance services for the relevant facilities, and not by those operating the system itself. One of the reasons is that the institutions or organizations managing the industrial control systems (ICSs) of major national infrastructures associated with traffic, water resources, or energy systems, have been outsourcing such tasks to partner companies, whose roles are becoming increasingly important. Even though the importance of security has increased, following the expansion of those institutions' workload, their security and management systems are still insufficient, due to a lack of budget and adequate security awareness, leading to security incidents caused by hackers. This study was presented as part of the continuous research on security management schemes for such problems [3–7].

It was reported in the 2017 ICS-CERT that the number of cases involving infringement on national infrastructure ICSs is rapidly increasing, due to active cyber-attacks that could cause not only simple financial loss, but also devastating social damage or chaos, often caused by their malfunction or unexpected interruption. Some of the typical examples include the blackout incident in Ukraine (Dec. 2015) [8–10], the power facility shutdown, caused by the USB-embedded malignant code at a German nuclear power plant (Bavarian State, Apr. 2016), and the cyber-threat against Korea Hydro and Nuclear Power (Dec. 2014) [11–15].

Radiation leaks or interruption of power supply could occur with control malfunctions or sudden disruption of a control system of a nuclear plant, caused by a cyber-attack. In such cases, the nation's sovereign rating could sharply be dropped, leading to massive socio-economic loss and confusion. The existing cyber-security systems have been focusing on shutting off external attack routes. However, the current measures are more concerned with sabotage, deliberate attack, or information leaks by insiders or related workers. Moreover, as the number of cases involving accidents in critical infrastructure, due to such personnel, is steadily increasing, so the establishment of an efficient response system between cooperative firms is urgently required.

In this paper, a security index was developed in terms of administrative and physical aspects for the security management of the partner companies to induce voluntary efforts and investment in an attempt to strengthen their competency in information protection in the special area of "Industrial Control." The partner companies were classified into a "Class", which is based on their respective competency levels and is subject to periodic security inspections. Nonetheless, as the vulnerabilities of the resident partner companies persist every year, we attempted to propose an innovative improvement plan that deals with cyber-threats by constructing a virtual environment as a technological measure.

2 Related Work

2.1 International Information Security Management System (ISO 27001)

Both domestic and foreign information protection/management systems were studied to check for most of the control regulations for the management of partner companies. Their contents were investigated once they had been identified. For example, information security certification ISO27001 evaluates the security regulations for certification by each relevant area, whereas ISO/IEC27001 originates from Britain's BS7799. As a typical standard for implementing an Information Security Management System (ISMS), this is being widely adopted by global companies as a procedure for assessing their adequacy/capability in security policy and its execution, as well as the ability to deal with security threats. This certification standard also assists an organization or a firm in constructing a framework for adopting and implementing a Plan–Do–Check–Action

(PDCA) model when establishing and executing an ISMS to perform security monitoring, review, maintenance, and improvement measures [16,17].

Information protection management is divided into 14 areas, with 114 subcategories under each area, in compliance with the information security policy. This management system is one that guarantees the confidentiality, integrity, and availability of information and contributes to the improvement, monitoring, examination, and maintenance of the entire management system (Tab. 1).

Table 1: ISO27001 security categories

Domain		Category
1	Information security policies	Management direction for information security
2	Organization of information Security	Internal organization, mobile devices, and teleworking
3	Human resource security	Prior to employment, management responsibilities, termination and change of employment
4	Asset management	Responsibility for assets, information classification, media handling
5	Access control	Business requirements for access control, user access management, user responsibilities, system and application access control
6	Cryptography	Cryptography controls
7	Physical/Environmental security	Secure areas, equipment
8	Operations security	Operational procedures & responsibilities, protection from malware, backup, logging and monitoring, control of operational software, technical vulnerability management, information systems, audit considerations
9	Communications security	Network security management, information transfer
10	System acquisition, development & maintenance	Security requirements of information systems, security in development and support processes, test data
11	Supplier relationships	Information security in supplier relationships, supplier service delivery management
12	Information security incident management	Management of information security incidents and improvements
13	Information security aspects of business continuity management	Information security continuity, redundancies
14	Compliance	Compliance with legal and contractual requirements, information security reviews

2.2 Korea's Information Security Management System (ISMS)

The ISMS certification system of the Republic of Korea (ROK) is being managed by the Korea Internet and Security Agency (KISA), whose operations include a series of information security protection activities, based on the establishment of information protection policies and their management protection ranges, risk management, implementation, and follow-up controls (5-steps), all of which are aimed at maintaining the confidentiality, integrity, and availability of the information assets that need to be preserved. All the information protection and management systems are subject to such processes and will be certified by the relevant certificate authorities or review services [18]. The ISMS consists of 12 certification criteria for the 5-step information protection and the other 92 criteria for 13 areas, or a total of 104 items, on which a policy should be established and operated. In the process, all the activities should be documented, and information protection measures should be implemented by conducting risk analysis. Recently, ISMS certification has changed to ISMS-P, after additionally including a personal information certification.

Following the introduction of such a certification system, the institutions or organizations that have been successfully certified, are using their security capability as an important tool for marketing by giving an impression to consumers that they are a safe company. Nevertheless, the question about the insufficiency of quality, concerning the effectiveness of the certification, remains [18–20].

2.3 Current State of Industrial Technology Leaks

A leak of industrial technologies results in enormous economic losses or paralysis of business. A company's competitiveness or the national image will be seriously damaged if a technology that is developed through years of hard work has been leaked to a competitor, then reported by the media. A negative influence on various areas, including sales volume, stock price, etc., can be expected as well [21].

The subject of technology leaks is usually either an insider or an outsider, and it has been found that the former has often attempted to leak the critical information or electronic documents stored in a personal computer or a work system through web, electronic mails, or Internet messengers as an attachment or, in the case of offline documents, leak copies through fax or other available means. On the other hand, outsiders leak electronic information by hacking the system through the network or breaking into the company illegally to leak the information system assets or the offline documents that are generated by printers or copiers. There have been many cases of large-scale electronic information leaks attempted by outsiders who had stolen critical assets or offline documents. The media outlets that have been used to leak the industrial information, can be largely divided into online and offline media. Moreover, the former employs a variety of methods following the rapid development of IT technology, including transmission through electronic mail, and illegal sharing, through peer to peer (P2P) sites, such as Webhard or Internet messengers. Most of the offline information leaks have been attempted by stealing a laptop or illegally carrying out a portable storage when surveillance was weak. The number of attempts made when the management of offline documents or copies was not properly performed, or access privileges were loosely provided, is increasing [21–25].

3 Establishment of Security Management System of Partner Companies

3.1 Increasing Security of Industrial Control System (ICS)

In this paper, businesses that are equipped with a SCADA system were selected as research objects. Regarded as a system of high importance in the industrial control area, SCADA or ICS facilities are a representative business in various industries, including construction, power generation, and environmental companies. Moreover, such a facility contributes to all kinds of infrastructure, such as energy production or other types of businesses, teams up with several partners in order to mainly perform operations and management tasks, and consigns additional tasks, such as maintenance, repairmen work, etc., to special partner companies when necessary. Many companies have already outsourced/transferred these tasks to them.

Such movement is expected to increase further in the future. Therefore, managing partner companies will become one of the most important indices that require the establishment of a special security management system to handle security risk efficiently.

In the ICS industry, SCADA facilities have been facing challenges from security threats, such as the power generation interruption incident, due to Stuxnet (Iranian nuclear facility, 2004), or the cyber-attack against a Korean nuclear power plant (2014), and they are endeavoring to establish higher security measures. It will be appropriate to refer to such security models when establishing a security policy for the other ICS areas [26–31].

The partner companies were classified, based on their evaluated management and technological levels. An example of a security system construction, based on the evaluation result, was then used to construct a virtual system that prevented information leaks through hacking attempts or internal conspiracy.

3.2 Establishment of Partner Company Security Management System Model

The security management system of a partner company should have expertise and objective reliability. Since those become important indices when establishing a security control process or conducting a security inspection. In this paper, the security standards of a design model were established to present a security management system model for a partner company, through an actual application case example to improve the effectiveness of its existing system.

Roughly 1,000 companies, within a certain contract period (2014∼2018), were selected among the ICS industry members to come up with a partner company security management model. The number of employees of a partner company and PCs were collected, directly based on their. They were then sorted primarily, according to each company's nature, such as service/construction, manufacturing/wholesale/retail, equipment repairs, or auxiliary equipment (Tab. 2). They were also analyzed in terms of their respective task performance environment, in addition to the possibility and impact of information leaks, based on the value of the information provided to them (Tab. 3).

The impact, in the case of an information leak, depends on the significance of the information provided to the company. As such, not only the contract type, but also the risk of an information leak was considered when grading the partners (Tab. 3).

The analysis criteria for the partner companies' operation environments are presented in Tab. 4, with their specific conditions. They are as follows: whether the partner company is permanently staying in the company with whom they contracted; operating while accessing the internal network; sharing and handling important information; and accessing with a separate Internet network. The partner companies were graded after analyzing their internal/external environments.

Table 2: Classification of partner companies

No.	Type of partner company
1	Service or construction
2	Manufacturing or wholesale/retail
3	Equipment repairs
4	Auxiliary equipment

Table 3: Risk analysis criteria

Criteria	Risk analysis
Impact in case of a leak	Value of information provided
Possibility of a leak	Partner company's operation environment

Table 4: Criteria for analyzing partner companies' environments

No.	Criteria
1	Whether they are permanently stationed in the company
2	Whether they are accessing the internal network
3	Whether they are handling internal technological/technical information
4	Whether they are using external Internet networks while stationed in the company

The level of documents handled by the company should be considered when establishing the criteria for classifying partners. First, the security levels should be set for each drawing, document to apply higher security for those requiring confidentiality or allow sharing of lower-level documents to benefit both parties. Tab. 5 shows the reference standard for determining which document or drawing corresponds to a particular grade/level. A-level includes the key company information that requires special attention/management since the company's fate depends on it, whereas D-level is the lowest security grade and can be disclosed to the public or published, without being harmful to the company.

Tab. 6 presents the terms or conditions when rating the partner companies. If the technical/technological information is rated as either A or B, the partner company will be rated as first-class, regardless of its current status involving the use of internal/external Internet networks, or whether or not it resides within the company. In other words, a company with the highest technical/technological information level should be treated as a priority company. Companies with C-level technical/technological rating can be divided into three categories. Those that correspond to all of these three conditions are rated as a first-level company, whereas those without access to the external (internal) Internet network, are rated as a second- or third-level company. Fourth-level companies do not correspond to all of those conditions. The information that they are handling can be disclosed to the public, without causing any damage to the company.

In addition, the partners were divided into either a high-standard or low-standard company, depending on their status in each environment. This enables improving business efficiency and preventing resistance from the partners.

Table 5: Security levels

Management level		Subject
A	Special mgt.	Major policies or information associated with the technology or core technological development, requiring special protection
B	Limited disclosure	Major technical/technological information having significant value and requiring limited disclosure
C	Internal disclosure	Technical/Technological information necessary for business operation: various types of drawings, documents, procedures, etc.
D	External disclosure	Technical/Technological information that can be open to the employees or the general public, including research, presentations, etc.

Table 6: Criteria for rating partner companies

Technical/ Technological info. Level	Residency	Internal network access	Internet access	Acquisition of security certification	Partner rating
A-Level	N/A	N/A	N/A	N/A	First class
B-Level	N/A	N/A	N/A	N/A	
C-Level	✓	✓	✓	✓	
C-Level	✓	✓		✓	Second class
	✓		✓		
C-Level	✓				Third class
		✓	✓	✓	
		✓			
			✓	✓	
D-Level	N/A	N/A	N/A	N/A	Fourth class

A high-standard company refers to a first or a second-class partner company that maintains the standards in Tab. 6, whereas a low-standard company pertains to a partner company, which keeps the standards for applying for the third- or fourth-class companies. In other words, the former is one that handles technological information, such as drawings or blueprints, at the same level as an ICS company (high security), and the latter is one that supports simple tasks, like supplying equipment and conducting repairs, as well as cleaning, driving, or deliveries. The categorization from classes 1 to 4 depends on the four conditions, including residency, internal network access, Internet access, and acquisition of security certification.

The partner companies were guided for their voluntarily improvement of security levels, by adding a new item, such as the acquisition of security certification for the assessment. Such an effort includes voluntary preparation for acquiring the ISO27001 information security certification.

Those that are required to have a C-level security class or above will be exempted from the information security assessment as one of the benefits (Tab. 6).

Tab. 7 describes the partner companies for each class in detail, based on the rating results in Tab. 6. For example, first-class companies decided to depend on their state of residency and network access, as well as the importance of the information/documents they access. On the other hand, third- and fourth-class companies, base their access to the documents, even though their geographical locations and allowable network access are the same.

Table 7: Categorization of partner companies by class

Class	Description
1st	A partner company handling technical/technological documents under special control, regardless of their residency within the company or level of network access. A partner company handling technical/technological documents subject to limited disclosure, regardless of their residency within the company or level of network access. A partner company that accesses the internal network & Internet network and handles documents, whose disclosure is allowed within the company, only while they are staying in the company.
2nd	A partner company that permanently stays within the company, uses the internal network, and handles documents that can only be disclosed within the company.
3rd	A partner company that does not always stay within the company and handles the company's internal documents, without accessing any networks.
4th	A partner company that does not always stay within the company and handles documents that can be disclosed externally, without accessing any networks.

The test data was collected from 1,042 construction or service companies out of 3,100 partner companies over the period of January 2014–May 2018. As a result, 73 companies were classified as a first-class partner company, whereas 38 (303) (628) companies were categorized as a second-class, a third-class, and a fourth-class partner company (Tab. 8). Based on the standards in Tab. 7, 1st class is the highest-ranking security class, and 73 companies belong to this class. Fourth-class companies with the lowest security level, accounted for about 60% of all partner companies.

Table 8: Partner company classification by class

Class	1st	2nd	3rd	4th	Total
Number	73	38	303	628	1,042

Each company's security level was reviewed using three areas, including administrative, physical, and technological protection measures, with a maximum of 40, 10, or 50 points. A point was then given to each evaluation index, for instance, Information Security Policy had four criteria per item, and it must be applied for both first- and second-class partner companies. There are 12 evaluation indices along with 24 evaluation items and 96 evaluation criteria.

According to ISO27001 and K-ISMS, the evaluation items were categorized in terms of administrative, physical, and technological aspects, and classified into four classes, based on the possibility of information leaks and expected damages. After analyzing previous security incidents, the weights of 50%, 40%, and 10% were applied to technological, administrative, and physical items, respectively, according to ISO27001 (Tab. 9).

Policy, organization, leadership, security activities, and manpower/asset/essential information management are included in the administrative protection measures (Tab. 10). Although ISO 27001 includes budgets, the partner companies may have a lot of pressure and negative perception.

Physical protection measures are divided into the control of assets, which are being carried in or out, and office security. The latter includes protection measures for office equipment, such as document shredders, document cabinets, access control equipment, and PCs. They are the lowest evaluation index (Tab. 11).

Technological protection measures are mainly associated with the security of information communications, including network separation, data protection measures, and system development security (Tab. 12). It is the highest index among the three indices: Administrative, Physical, and Technological Protection Measures. Most of the major incidents occur because of poor technological protection measures. Therefore, they must be regarded as highly important factors. The infection as a malicious code is the main cause of hacking incidents, so inspection and precautionary measures must be taken seriously. These all must be observed in the evaluation process.

The security level of each partner can be determined by the classification procedure, wherein each company is graded by the index of administrative, physical, or technological protection measures, which are identified as Excellent, Satisfactory, Average, Unsatisfactory, and Vulnerable (Fig. 1). The 1st Class companies will be inspected regularly to maintain their current excellent security level, whereas those that fall short of the standard will be penalized.

After classifying the partners, based on the reference standard, security inspection should be performed next. Fig. 2 shows the sample inspection procedure flowchart of the company's supervising department with a 2nd Class partner or above; a self-inspection is performed by the first partner, and the documented result is then reviewed by the company. In this case, the information security department's role is to support inspection or to provide technical/technological support.

The company's security department conducts inspections by dividing them into spot or regular inspections. For new contracts, an initial inspection will be conducted. For the existing ones, regular inspections will be implemented. In such cases, the partner submits the security report after conducting and diagnosing its security activities. The company's security department reviews the written report and carries out an on-site inspection when such is deemed insufficient (Fig. 3).

If the partner has acquired information security certification (e.g., ISO27001, CoBit, etc.) or complied with the required security process, the on-site inspection can be replaced with other means. Fig. 3 is a detailed security inspection flowchart, starting from the security process as the evaluation result, wherein the partner's security level is determined by the on-site evaluation result.

Table 9: Maximum scores, class coverages, and assigned scores

Classification	Evaluation index	Evaluation item	Evaluation criteria	Class coverage				Assigned score
				1st	2nd	3rd	4th	
Admin. protection measures (40 points)	1. Information security policy	1	4	✓	✓			5
	2. Information security org.	1	4	✓	✓			6
	3. Partner company's information security leadership	1	5	✓	✓			6
	4. Partner company's information security activity	1	5	✓	✓	✓		6
	5. Human resource management	2	10	✓	✓	✓	✓	10
	6. Asset & critical information management	2	7	✓	✓	✓		7
Physical protection measures (10 points)	1. Asset control (In & out)	1	2	✓	✓			2
	2. Office security	3	8	✓	✓	✓		8
Technological protection measures (50 points)	1. Network separation/network access control	4	16	✓	✓			16
	2. PC security mgr.	5	23	✓	✓	✓		22
	3. Protective measures for storing critical data/materials	1	7	✓	✓	✓		7
	4. System development security	1	5	✓	✓			5
Total	12	24	96					100

A total of 1,042 partner companies, which were engaged in industrial control, were classified for empirical analysis. Among them, Company S, which belongs to the 111 first- or second-class companies, was randomly selected along with Company L and Company K, from 303 third-class companies and 628 fourth-class companies, respectively. A security inspection was carried out twice during the period from January to December 2015, by their document management condition and/or on-site inspection to evaluate their performances. Company S was a control

facility maintenance and was allowed to access C-class documents, whereas Companies L and K were in charge of water-quality management and construction work, respectively. Since Company K belonged to the fourth class, it was exempted from both technological and physical inspections. All of these three companies had been selected from the same branch to give them a fair chance for evaluation.

Table 10: Evaluation index: administrative protection measures

Classification	Evaluation index	Item
Administrative protection measures	1. Policy	1.1. Whether a security policy has been established and shared with related parties
	2. Organization	1.2. Whether an information security officer who is responsible for managing the information protection task has been appointed
	3. Leadership	1.3. Whether a plan that is suitable for the objective of the organization has been established and if it continuously supports its activity
	4. Security activity	1.4. Whether matters related to information protection are being inspected autonomously for the service business in terms of manpower, environment, system, etc.
	5. Human resource management	1.5.1. Whether the procedures for information protection are being followed when there is a change in manpower 1.5.2. Whether an information security training plan has been established and is being carried out
	6. Asset/Critical information management	1.6.1. Whether the partner company's information system assets are being managed 1.6.2. Whether the data/materials supplied by the company are being kept safely

Table 11: Evaluation index: physical protection measures

Classification	Evaluation index	Item
Physical protection measures	1. Asset control (In & out)	1.1. Whether the asset control procedure has been established, along with protection measures

(Continued)

Table 11: Continued

Classification	Evaluation index	Item
	2. Office security	2.1. Whether the document shredder and cabinet equipped with a locking device are being arranged within the office 2.2. Whether an office security regulation, such as access control or document management, has been established and if periodic security inspection is performed to check compliance 2.3. Whether protection measures for shared office equipment, such as fax, copier, printer, PC, etc., have been established and are being followed

Table 12: Evaluation index: technological protection measures

Classification	Evaluation index	Item
Technological protection measures	1. Network separation & network access control	1.1. Whether the Internet access or service of the PC that is storing the company's data/materials is being restricted
		1.2. Whether unnecessary services are limited, and if a safe access environment is established when access to the company's internal system is required
		1.3. Whether the existence of any unauthorized bypass networks is consistently checked and if a status check is performed periodically
		1.4. Whether protection measures are being applied when using wireless Internet through wireless LAN
	2. PC security management	2.1. Whether the passwords of internal PCs that deal with critical information comply with the security policy
		2.2. Whether the PCs' OS or applications are constantly updated to block infections from malicious code

(Continued)

Table 12: Continued

Classification	Evaluation index	Item
		2.3. Whether the security policy is observed when installing vaccines or operating systems to protect the company PCs from malicious codes
		2.4. Whether a security solution is included in the company regulations for operation
	3. Protection measures for storing critical data/materials	3.1. Whether safe protection measures are being applied when storing critical information
	4. System development security	4.1. Whether system development/operation tasks are being performed in a safe environment and if access privileges are granted, according to individual tasks

First, all the partner companies were graded by their evaluation results, such as administrative, physical, and technological, as well as their initial scores. Next, the level of security management of each company was determined by its level of technological information and class.

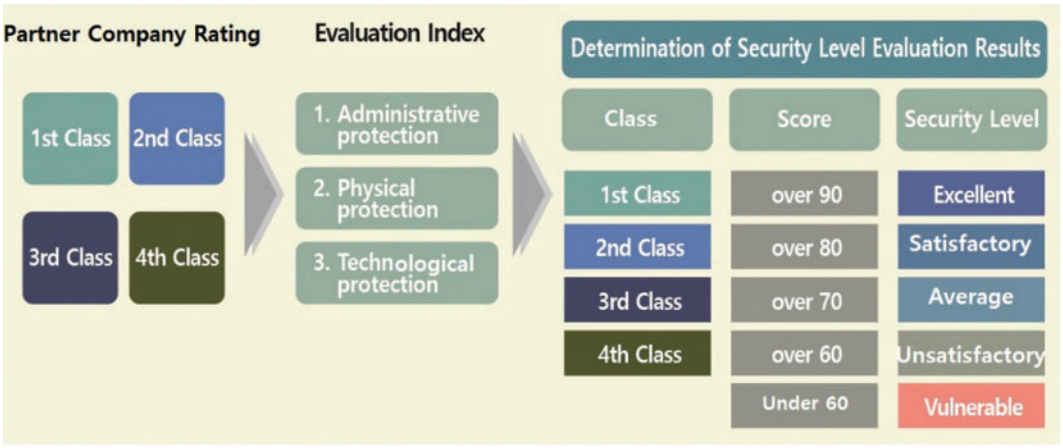

Figure 1: Evaluation standard according to the partners' classes

In Tab. 13, a single typical company was selected separately from groups 2, 3, and 4. For the three evaluation indices, a 50% weight was given to the technological items, whereas 40% and 10% weights were given to administrative and physical indices, respectively. Meanwhile, "Performance Rate by Area" refers to a percentage rate against an evaluation score, whereas "Target Scores" means the individual target values set for administrative, physical, and technological scores. A percent rate of 90% means that the relevant score is an initial target score, which shows the improved security condition. Thus, in Fig. 1, the final scores were put into items, which divided

by individual corresponding scores to define each security level as "Satisfactory," "Average," or "Unsatisfactory." Although all of the target scores for the administrative, physical, and technological indices were supposed to be a perfect score, achieving 90%, which can be regarded as an improved security condition, was set as the primary aim (Tab. 13).

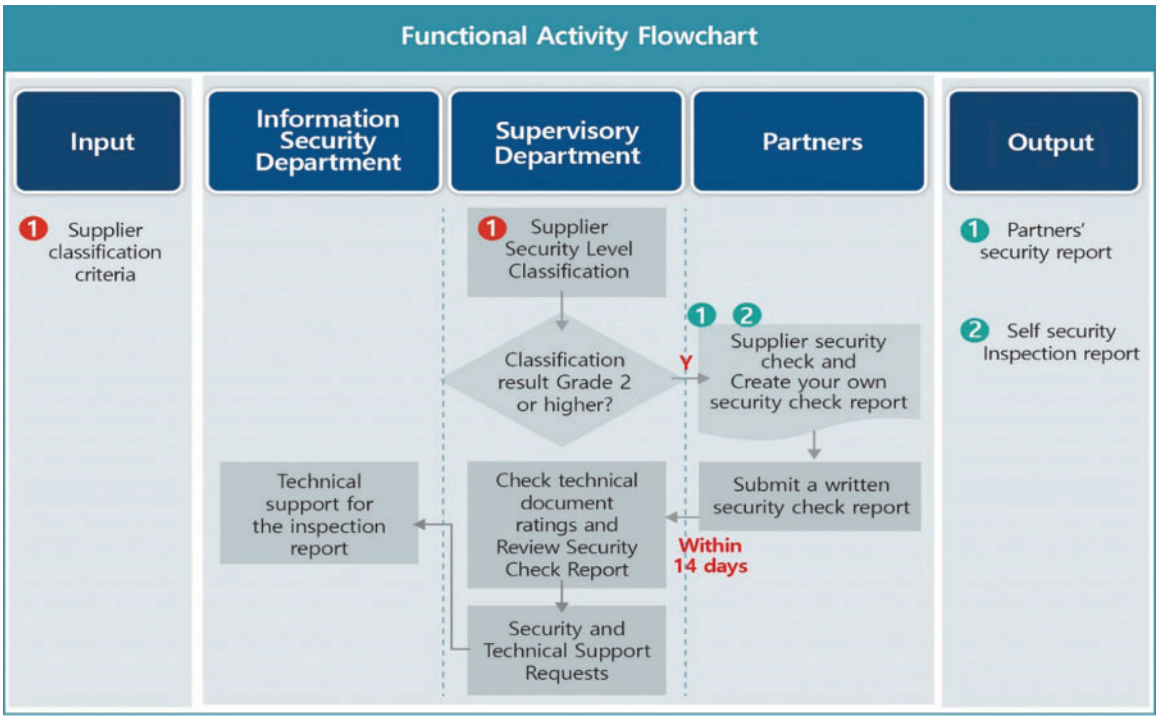

Figure 2: Evaluation standard according to the partners' classes

Fig. 4 depicts the scores in Tab. 13 with a graph. The outer red line indicates the target scores, whereas the blue line represents the current scores.

As a result of analyzing the scores of these three randomly selected partner companies, it was possible to intuitively grasp that both technological and physical security managements for them were inadequate. As such, a security management system was applied to them for the first time.

The partner companies that have completed the evaluation, have to manage their respective scores, through feedback and reflection, in order to maintain their evaluation classes. There are two different types of management methods for the companies, including an excellent evaluation or vice versa. For the former, the number of inspections will be reduced from 2 to 1, whereas the latter (i.e., 3rd and 4th classes) will be subject to occasional inspections or document-based inspections. Moreover, some penalties will be imposed on the latter, including fines, to let them realize that security can be a hefty company expense. These companies will then have no choice, but to find a way to improve their security level by making more investments or reinforcing their manpower.

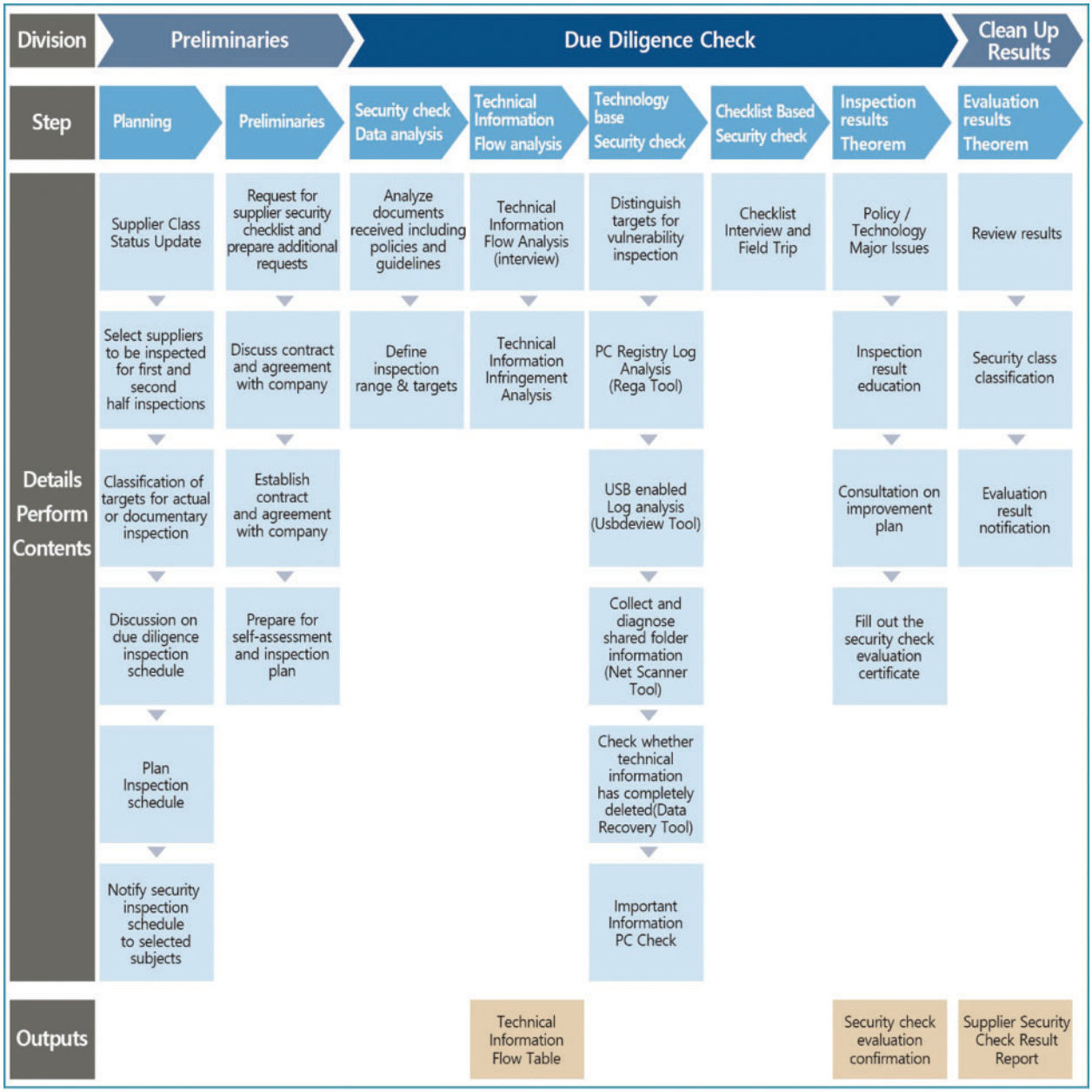

Figure 3: Actual inspection procedure for the partner company's information security

Fig. 5 presents the procedure for imposing penalties on the partner company with an unsatisfactory evaluation result.

The evaluation method was standardized by reflecting the international security standards. The details of security requirements and inspection methods were specified by class, in order to create an effective security inspection procedure.

Table 13: Security evaluation result of a 3rd-class partner company

Classification	Evaluation index	Evaluation weight (%)	Overall points	Evaluated score	Performance rate by area (%)	Target score (Excellent) (%)	Total score	Evaluation result
Company S	Administrative	40	40	32.583	81	90	68	Unsatisfactory
	Physical	10	10	4.5	45	90		
	Technological	50	50	31	62	90		
Company L	Administrative	40	23	21.333	93	90	75	Average
	Physical	10	8	6	75	90		
	Technological	50	29	17.5	60	90		
Company K	Administrative	100	10	8.333	83	90	83	Satisfactory

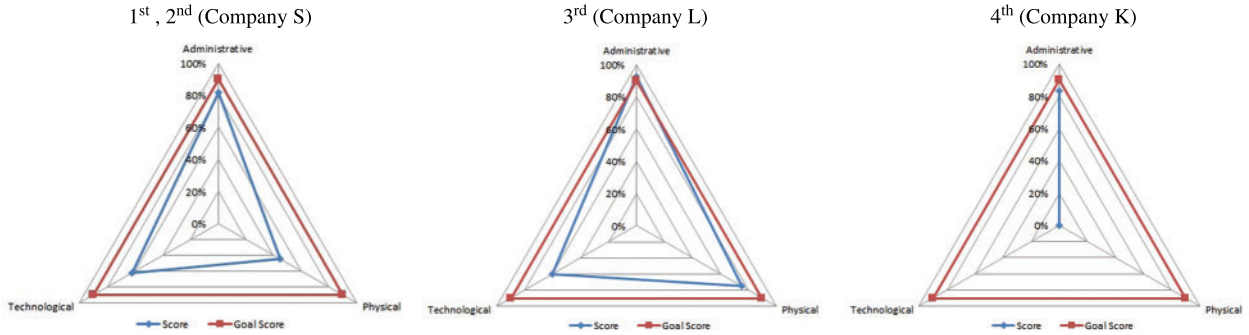

Figure 4: Distribution graph based on the scores

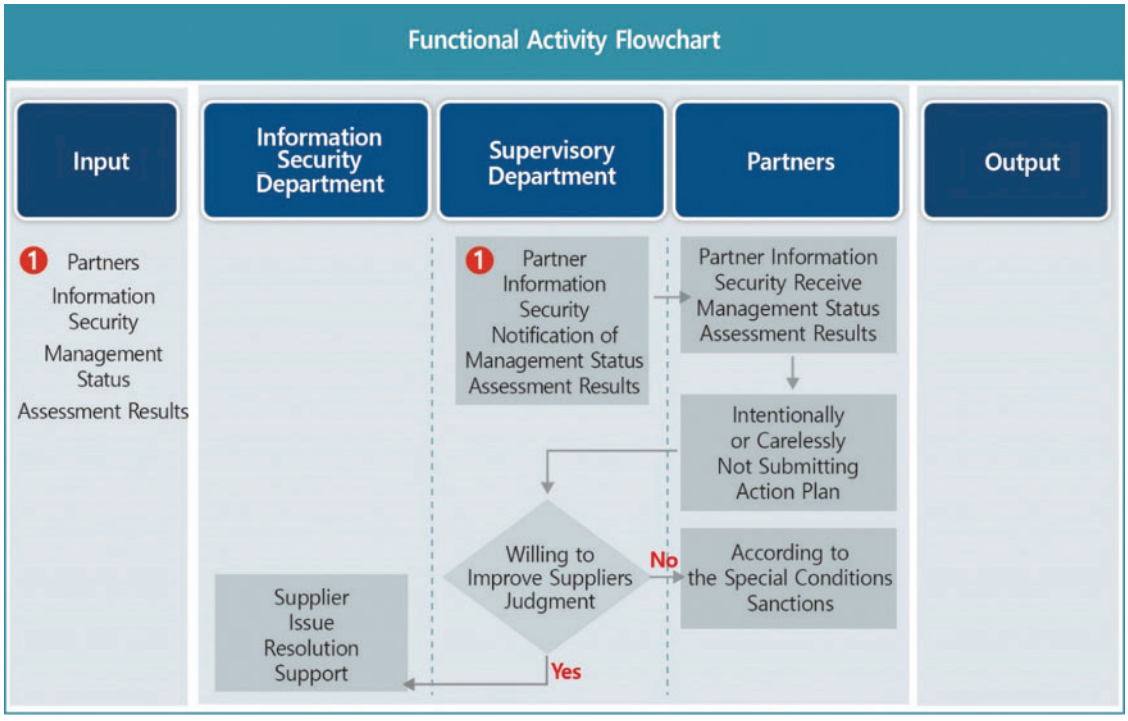

Figure 5: Procedure for imposing penalties on the partner company with an unsatisfactory evaluation result

As a result of initially applying the security management model, it was difficult to manage each company's security management conditions, prior to applying the model, as there were no administrative standards. With the proposed model, every new partner company was classified by the standard after receiving security inspections, based on the evaluation indices, to determine their current security conditions and to perform comprehensive management. Second, about 1,000 partner companies were graded on their security levels, based on the evaluation and inspection results. As a result, (73) (38) (303) (628) companies were rated (A) (B) (C) (D), respectively, with a detailed inspection method applied to each level. A-Level security measures were taken for companies rated as "risky." In the end, the overall security level was improved.

For example, third-class companies, which fall short of this year's standard, were guided in improving their respective status, by strengthening the penalties or increasing the number of inspections. In additional, by presenting them with a security guideline, the risk in business activities was minimized.

As the ICS system is essential, the ICS operating company should invest in constructing a development or a security system, such as the VDI system, by taking the initiative. The ICS operating company should give the terms in the contract that require their partner companies to install a security system properly and by making an agreement for them to be educated about the security system, through consultation and training. Moreover, the ICS operating company needs to organize a periodic meeting for exchanging opinions in order to resolve the operational difficulties in system operation.

3.3 Security Inspection Result

Tab. 14 presents the results obtained from the on-site inspections that are held twice a year, during the period from 2015 to 2018, with the physical location of the partner company subject to the inspections from the selected four Korean branch offices. The branch had a total of 60 partner companies, where 1,800 employees were working.

Table 14: Results of the security inspections conducted from 2015 to 2018

Security item	2015	2016	2017	2018
Possession of unauthorized essential documents	31	24	3	2
Poor password management	18	25	4	3
Vaccines not installed	3	0	0	0
Periodic vaccine-based scanning not performed	14	5	0	0
Major security patches not installed	10	12	6	0
Poor activeX management	5	0	0	0
Screen saver not set	3	0	5	2
Activation of wireless LAN, etc.	62	0	0	1
Use of multi-OS	0	1	1	1
Installation of non-business programs, such as messenger, P2P, etc.	0	8	0	0
PC-lock	0	2	0	3
Poor USB management	0	13	0	0
USB auto-execution not set	0	0	2	0
Total	146	90	21	12

After applying the virtual system, the total number of security issues decreased by 21%, from 146, to 90 in 2015 and 2016, respectively. In fact, the actual application of the system, which was started in 2017 as system construction, was completed in September 2016, and more time was required for the training. The number of security violations dropped from 146 to 12, showing a 50% decrease after the system had been stabilized. Such a decrease was achieved by reinstalling all the security programs and making it impossible to connect to the network without systematizing the network access controls, in addition to checking whether the vaccines had been installed along with security patches or if unauthorized programs or USB devices were used.

Specifically, Active Xs were the main cause of the malicious code, which were able to penetrate the security system. After applying the virtual system, they did not pose any problems. Nevertheless, such a virtual system's uselessness increased, and one of the typical examples was the security violation involving a multi-OS operation. Cases of which have been increasing since 2016. It seems to have been an attempt to bypass the virtual system by installing another OS, which was a weakness of the VDI-based system.

The security inspection result is shown in Fig. 6, with the largest number of violations (62) associated with the use of a wireless LAN in 2015. This was the result of each partner company using its own separate Internet network for its business. However, the effect of the VDI system was immediate, as the number of unauthorized owned documents decreased dramatically. As a whole, the number of security violations dropped, from 146 in 2015, to 21 in 2017, when the system had been stabilized. Then, the major violations involved cases of not setting screen savers or not encrypting the document files properly.

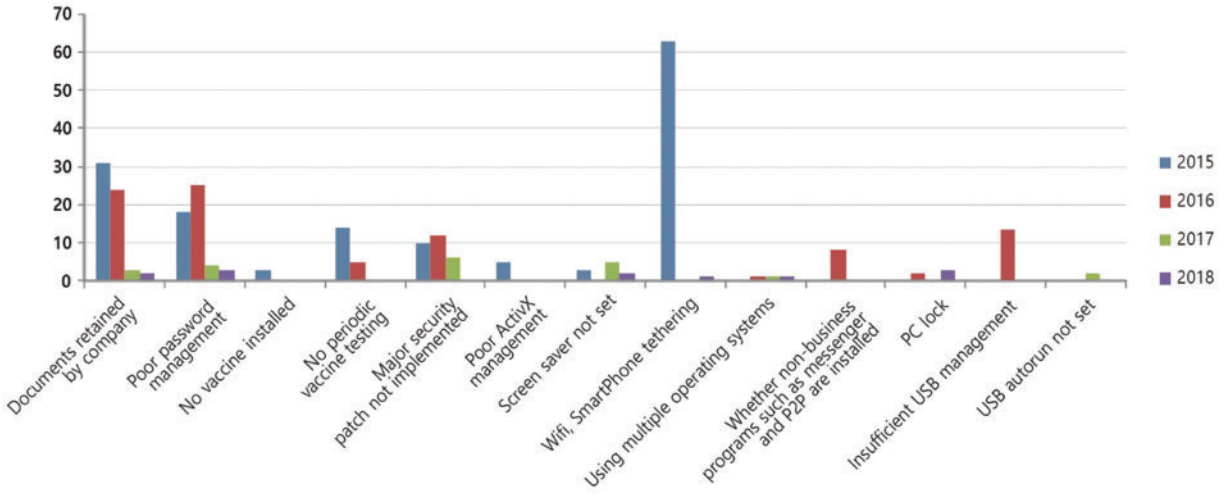

Figure 6: Graph of the security inspection result

The next thing to consider was how to transmit data/materials between networks after physically separating them into a business network and an Internet network. This problem was resolved by constructing a data transmission system that enables data exchange between the VDI network and work PCs. An authorization procedure, that allows the transmission of important drawings or documents after being approved by the supervisor, was prepared, along with the system first filtering a malicious code through security software. Since the ICS industry is based on various types of control systems, it is very sensitive to infections or leaks through the Internet.

Thus, investment in VDI systems may produce a positive, immediate effect on their Return of Investment.

The VDI system plays the role of protecting partner companies from external cyber-attacks and keeping the internal technical/technological documents safe from malicious code. There is a system that distributes these documents between the ICS operating company and their partner companies, in order to conduct business smoothly. Between them, general documents are delivered offline, whereas technical documents, such as blueprints, are distributed through a data transmission system or a mail system, which is connected to the partner companies. One of the important aspects in such cases is guaranteeing the process of a prior approval and allowing it to be tracked afterward, when necessary.

4 Construction of a Partner Company Virtual System

4.1 Status of System and Network

Similar security incidents continuously occurred in the following year. Even though the partner companies had been classified by developing an evaluation index and performing security inspections, the number of malicious code-based infections through the Internet never decreased, despite the constant education or guidance. At the same time, new contracts were awarded to other companies, and regulation violations by their employees did not stop, hence the need for a more systematic approach. A fundamental system, that could minimize such problems, was designed by constructing a virtualization system to minimize Internet access and strengthen data access control.

Preliminary work has to be performed to apply the virtual system to all the partner companies that stay within the company after evaluation and inspection. In other words, it has to be proven that there are no malicious codes within the PCs, which means that their integrity has to be guaranteed at that point. So, the origins of any future virus infections can be traced, thereby ensuring the reliability of the system.

Therefore, all the information systems, including PCs, must be checked, along with the other equipment, for individual integrity. Such tested PCs are called Clean-Zone PCs.

After evaluating and inspecting partner companies, there is an indispensable preliminary process to be performed when applying the virtualization system for all the resident partners in the company: "integrity check." It has to be proven that there are no malicious codes (e.g., worms, viruses, etc.) in the internal PCs as of that moment. Besides, the integrity level should be maintained at a 100% level, so the origins of future infections can be tracked while securing reliability. In this case, all the information systems, including the partners' PCs, are checked with a vaccine program for their integrity, as well as all other equipment/devices, which enter the control system, even if they are to be used for test bed experiments or inspections. Those cleared PCs are called Clean-Zone PCs, which are independent PCs. They are also subject to a vaccine test, before accessing the control network, and are allowed to be brought in after they have been cleared of any abnormalities.

In designing the partner security management system model, controlling outside access was focused on by the company, and requested that users pass the approval process at the point of Internet access. Moreover, a separate exclusive network for the partner company was constructed in a way that it has the same security level as the company (Fig. 7).

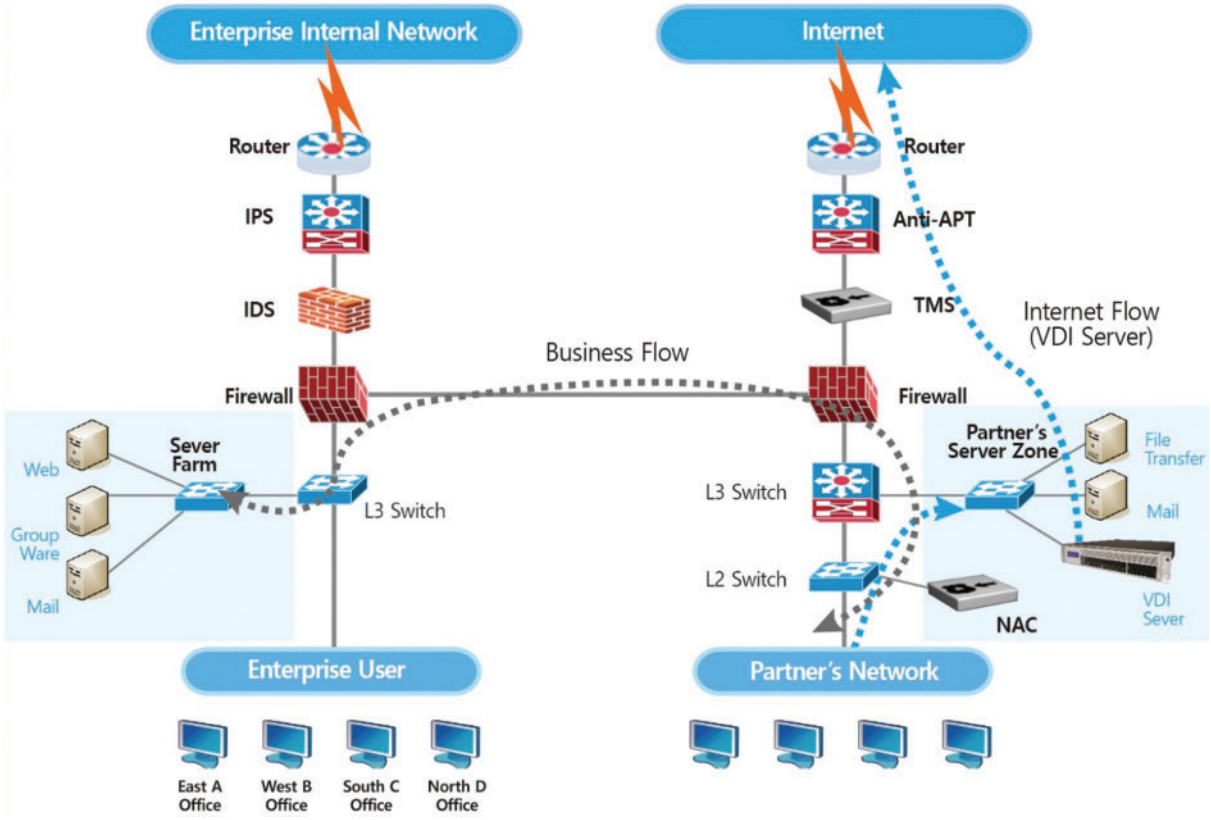

Figure 7: Security management system diagram of partner companies

This is the network configuration, wherein all the partners that are stationed at individual branches, are connected.

Before arranging a partner company system, the partner companies operating in each region were using their own private Internet. As this was not being monitored, the number of security accidents was never reduced, and problems, such as document leaks, had become unmanageable. Thus, it became necessary to establish a centralized security system network. In an attempt to reduce the number of malicious code-based accidents recurring after the centralization, a plan of introducing virtualization was designed.

The networks that were connected from each area, only allowed outside access after passing through the central security system, where all the data that is exchanged by the partners will be checked by the spam mail server and advanced persistent threat (APT) detection system. Meanwhile, each user is able to protect himself/herself from malicious code or information leaks, by establishing access through an Internet browser with his/her own designated account. For network security, the security system for network control consists of a firewall, an intrusion prevention system (IPS), and network access control (NAC) security equipment. A new mail server is provided to the partners. It is possible to use their own mail server, but those, which are stationed within the company, must be provided by the company only, as it is essential for the important materials leaving the company to be monitored and approved. Such a system is quite important during designing. It also is necessary for inspecting the high-level security documents to correspond for A, B, or C level.

Moreover, a data transfer system can control malicious codes in a VDI environment, and the data/materials downloaded from the Internet will be tested for viruses or released outside, through the Internet, only after obtaining approval from the supervising department [32–40].

The partner companies configure their security equipment into networks, PCs, and mail server sections. The work PCs aim to block the data/material being carried out without authorization by installing media controls, an antivirus, and output security software, along with an unauthorized data transfer-blocking system. The security level can be enhanced by installing security products identical to those used by the mother company, if the budget allows. Network security systems, such as firewalls, anti-APTs, and NACs are installed first, followed by spam mail blocking and DLP for mail server security (Tab. 15).

Table 15: Security system of partner companies

Classification	Sec. system	Description
PC	Media control (Endpoint protector)	Block leaks of the data that is unauthorized by PCs, by controlling the Read/Write function for USBs and CDs
	Blocking unauthorized transfer	Locks down the PC when an authorized user attempts to access networks without any approval
	Print security	Displays printout information in a printed document
	Antivirus	Virus treatment vaccine, such as malware
	Data right management (MGR)	Encrypts documents containing personal information
Network	Firewall	Only approved services or IPs can be used
	Network access control (NAC)	Installs essential security programs and blocks any attempted network access by unauthorized users
	Harmful site blocking	Blocks access to harmful sites, including commercial mail, Webhard, or messengers
	Anti-APT	Responds to APT attacks
E-Mail	Spam filter	Blocks incoming spam mail
	Data loss prevention (DLP)	Authorization process for sending attached files

4.2 VDI System Configuration

Tab. 16 compares the merits and demerits of the virtualization method of a VDI system. Due to the decisive problem of the PC-based network separation being vulnerable to malicious code and difficulty of being controlled by the partner company, VDI-based network separation was applied. Since the PC-based method shares a single hard disk, it is not suitable for industrial control systems, due to its vulnerabilities to malicious code, such as advanced persistent threat (APT). Meanwhile, the VDI-based method has its own vulnerabilities to some of the bypassing malicious code. However, it is known to be safer than the PC-based method.

Table 16: Comparison between VDI-based and PC-based network separations

Classification	VDI-based network separation	PC-based network separation
Virtualization method	A virtual PC with hypervisor-based client and separate OS	Logically separate the application executions by distinguishing them as a hosting area or a protection area, through the virtualization of the client's OS kernel
Location of virtual PC	Run on the server	Run on the PC
Security system	Dedicated protocol security SSL VPN solution and additionally available 2-factor security authentication, etc.	SSL VPN solutions
Merits	-Provide users with an environment where they can consistently process tasks regardless of place or ability to access equipment -Internet control using a virtual server -Convenient to manage data, by concentrating the major business data at the center	-Existing resources can be utilized and are easier to construct, as there are no H/W installations, with low costs involved -Guarantee the performance or work efficiency by utilizing the local resources of the user PC
Demerits	-Initial server construction cost can be high -There is an issue of slowdown, in case of simultaneous use -Data access or storage will be limited in case of network interruptions -User adjustment period is necessary	-Vulnerable to malicious code, as a single hard disk is shared -Lack of compatibility of various types of PC environments -Application change may be required following OS upgrades
Product	Citrix [41], Vmware [42], etc.	Ahnlab [43], MirageWorks [44], etc.

A VMware product was used in this study as a server virtualization tool for the configuration of the VDI system. The number of viewers and performance of the server affect the system load, as virtualization that is performed on the server side for all the clients. The VDI server was designed to include all the partner company's viewers. The server, VDI, network, and mail server were all configured, based on 900 simultaneous user connections. Tab. 17 shows the server specifications for constructing a test environment.

The network configuration is located within the DMZ (De-Militarized Zone) section so that external hacking attempts are dealt with by the firewall, the IPS, spam filter, and the anti-APT that are installed in the upper network. As a secondary future task, network forensics will be introduced to trace the path of malicious code generation and use it as material in the inspection process when data has been leaked. There are two areas in a user PC, including the local areas, where paperwork can be performed, and the VDI area for Internet. People can use e-mail or

perform a web search through the Internet by accessing VDI and logging in with the assigned account.

Table 17: Server specifications for constructing a test environment

Classification	Designation	Qty.	Specifications	Remarks
H/W	VDI server	19	-CPU: 2.4 GHz, 2P/28Core, MEM: 192 GB, HDD: 300 GB ∗ 2, Type: Blade	CPU: 532 Core MEM: 3,648 GB
	VDI management server	2	-CPU: 2.4 GHz, 28Core, Memory: 192 GB, HDD: 300 GB ∗ 2, Type: Blade	-
	Network	-	-10G ∗ 2EA, FC: 8G ∗ 4EA	-
	VDI storage	1	-OS (Windows) SSD: 33.6TB, DATA SAS: 8.3TB, Cache MEM: 128 GB	-
S/W	VDI server OS	9	-Microsoft windows server 2012	-
	VDI DBMS	1	-Microsoft SQL server 2016	-
	VDI solutions	1	-Desktop VDI (Concurrent: 900 users)	-
	Electronic certification	1	-Email 2-factor certification	-

The existing partner companies are vulnerable to hacking attempts, as they often use external Internet. For most cases, their systems are not connected to a safe security system, which is linked to the head office or is installed with a limited security program. Specifically, several small companies are operating their PCs without any security software, due to lack of security awareness or budget. It is only a matter of time before important company files leak outside if they have been stored in them. The partner company, that is working in the ICS space, must at least have a security system the same as the ICS company's system, in order to share important documents together. In that sense, the VDI system can be regarded as a system that minimizes the possibility of the partner company leaking the information, which are shared within the same space.

5 Conclusions

In this paper, a security management system for the partner companies, which are working together at industrial sites operating an ICS facility, was designed to propose an appropriate model, along with an adequate technical/technological plan. The model worked flexibly during its full implementation. The necessity of strengthening the security management capability is often emphasized when developing an industrial control system in addition to constructing a technologically error-free security system. Thus, this study presented a method of classifying the partner companies that often remain in a blind spot of security management, based on the major security elements, along with the management system appropriate for individual security levels. Moreover, the virtualization solution, VDI, was applied to allow the partners to securely use the

Internet, by preventing information leaks or protecting their system from any infections or attacks originating from the hackers by malicious code. The results are shown as follows:

First, the partner companies should be graded by classifying the value of individual information and must be managed by the respective classes. In other words, they need to be classified by considering the information provided to them in their internal/external environment in a special area, for example, industrial control systems. The evaluation model considering the individual partner company classes and contract forms can only be effective when their various security-level elements are reflected in the model. The security level can be evaluated by conducting both document-based and actual inspections by class. This paper presented a management plan for each partner company, based on the evaluation results. It is also important that the items in the evaluation indices be adjusted by varying security policy standards and their limits.

Second, security infrastructure for the prevention of damages, which are caused by information leaks or malicious code, should be constructed as cases of data/material leaks, through the partner companies, are still increasing. There have been many hacking incidents perpetrated through them as well. Nonetheless, providing security training or simply performing security inspections will not totally block the persistent threats. The significance of control systems is too high for almost every industry that the security management problem should not be left to the partner companies only. In that sense, it is necessary to provide proper security infrastructure to each of them for adequate management. VDI can be an excellent option, since it was designed to circulate important materials only after preventing any possibility of infection and approval has been given. It is essential to have a paradigm shift for the partner companies. For example, making an investment in security infrastructure is not "fruitless", but rather a "future-oriented investment" that enhances the value of the companies engaged in control systems.

Third, a means of providing work convenience is required. Although security is considered to be one of the priorities in the industrial control, simply emphasizing it in an environment where a lot of value is being placed on the convenience of work would produce a contrary result. Thus, a business program, that not only emphasizes security, but is also suitable for the existing work process, should be provided in the security infrastructure. The security competency of the partner companies has been improved. Moreover, it also reduces the negative effects by providing them with a data transmission system that offers virtualization capabilities and transferring data between businesses by e-mail and messenger systems, which are used for communication between employees. Fourth, the partner companies should be motivated to voluntarily comply with the security policy to continuously improve their security levels. It is necessary for a company to develop some external factors that would encourage the partner companies' security activities by establishing a penalty and incentive system.

An improved control system security management scheme, was proposed in this study, based on the verified results and by supplementing the limitations of the existing security management systems. The object of this scheme is not only to punish the partner companies that do not comply, but also to promote mutual growth between them, through the improved levels of security. Although there have been quite a large amount of research carried out for the subjects associated with control security, research on the security of the partner companies dealing with ICS security has yet to be conducted. This paper can be meaningful to the ICS security sector, as it provides an applicable solution, based on the results that were obtained through the empirical planning, designing, implementation, and validation processes.

Funding Statement: This research was supported by the Energy Cloud R&D Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT (NRF-2019M3F2A1073385).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] E. G. Popkova, Y. V. Ragulina and A. V. Bogoviz, "Industry 4.0: Industrial revolution of the 21st century," in *Studies in Systems, Decision and Control Book Series*, Berlin, Germany: Springer, pp. 1–253, 2019.

[2] L. Yao, S. Zhong, H. Kikuta, J. G. Juang and M. Anpo, *Advanced mechanical science and technology for the industrial revolution 4.0*, Berlin, Germany: Springer, pp. 1–22, 2018.

[3] C. K. Lee, "Trend of technology of instrumentation and control system in nuclear power plants," *KIISC*, vol. 22, no. 5, pp. 28–34, 2012.

[4] I. S. Koo, K. W. Kim, S. B. Hong, G. O. Park and J. Y. Park, "Digital asset analysis methodology against cyber threat to instrumentation and control," *JKIECS*, vol. 6, no. 6, pp. 839–847, 2010.

[5] D. Y. Kim, "Vulnerability analysis for industrial control system cyber security," *JKIECS*, vol. 9, no. 1, pp. 137–142, 2014.

[6] H. O. Jun, I. Y. You and K. H. Lee, "Infrastructure accident and control system standard trends," *Review of KIISC*, vol. 27, no. 2, pp. 5–11, 2017.

[7] C. I. Pub, *Cyber security planning guide*, Federal communications commission, Washington, D.C. USA, pp. 1–50, 2014.

[8] T. S. Kim and D. J. Kang, "A study on identification and classification of cyber security threats on electric power system," *Journal of Security Engineering*, vol. 9, no. 1, pp. 9–11, 2012.

[9] I. N. Fovino, L. Guidi, M. Masera and A. Stefanini, "Cyber security assessment of a power plant," *Electric Power Systems Research*, vol. 81, pp. 518–526, 2011.

[10] KINAC, "Cyber security division annual report," 2016. [Online]. Available: http://www.kinac.re.kr/board/.

[11] S. D. Lee and Y. T. Shin, "A design of cyber security framework for nuclear power plant security management," *Convergence Research Letters*, vol. 3, no. 3, pp. 655–660, 2014.

[12] IAEA Tech, "Computer security at nuclear facilities," IAEA Nuclear Security Series, Vienna Austria, no. 17, pp. 1–67, 2012.

[13] C. I. Cybersecurity, "Framework for improving critical infrastructure cybersecurity," NIST, Maryland, USA, pp. 1–28, 2014.

[14] F. P DRAFT, "Recommended security controls for federal information systems and organizations," NIST, Maryland, USA, pp. 1–17, 2009.

[15] BSI, "Industrial control system security top 10 threats and countermeasures 2016," Federal Office for Information Security, Germany, pp. 1–20, 2016.

[16] R. Sheikhpour and N. Modiri, "An approach to map COBIT processes to ISO/IEC 27001 information security management controls," *International Journal of Security and Its Applications*, vol. 6, no. 2, pp. 13–28, 2012.

[17] H. K. Kim, K. H. Lee and J. I. Lim, "A study on the impact analysis of security flaws between security controls an empirical analysis of K-iSMS using case-control study," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 9, pp. 4588–4608, 2017.

[18] K. Khan, R. Syal and A. Kapila, "Introduction to Voice-over IP Technology," 2004 IT Governance Institute, Information Systems Audit and Control Association, Illinois, USA, pp. 1–11, 2006.

[19] T. Y. Lee and D. G. Park, "K-ISMS based control system information protection management system evaluation standard," *JKIIT*, vol. 12, no. 8, pp. 107–122, 2014.

[20] H. D. Rha and H. S. Chung, "A theoretical comparative study of human resource security based on Korean and int'l information security management systems," *Journal of Convergence Society for SMB*, vol. 6, no. 3, pp. 13–19, 2016.
[21] ITS ISSUE, no. 9, 2013. [Online]. Available: http://www.kaits.or.kr/information/publications/list.do?.
[22] NCI Agency, "HandBook: Advanced industrial technology protection trend," NATO Communications and Information Agency, Brussels, Belgium, pp. 1–22, 2007.
[23] J. M. Lee, Design method of internal control management system to protect industrial technology and prevent leakage: Focusing on improvement cases of security management system of manufacturers, Ph.D. dissertation, Korea University, pp. 1–22, 2013.
[24] G. S. Lee, "A study on the preventing policy of the industrial technology leak crime-focused on the criminal aspect of the united state's economic espionage," *Act*, vol. 9, no. 2, pp. 109–163, 2009.
[25] G. Andrade, M. Mitchell and E. Stafford, "New evidence and perspectives on mergers," *Journal of Economic Persectives*, vol. 15, no. 2, pp. 103–120, 2001.
[26] Y. R. Chen, S. J. Chen, P. A. Hsiung and I. H. Chou, "Unified security and safety risk assessment-a case study on nuclear power plant," in *2014 Int. Conf. on Trustworthy Systems and Their Applications*, Taichung, Taiwan, IEEE, pp. 22–28, 2014.
[27] P. Scoett, "Toward renewed legitimacy? nuclear power, global warming, and security," *Global Environmental Politics*, vol. 3, no. 1, pp. 99–116, 2003.
[28] C. S. Cho, W. H. Chung and S. Y. Kuo, "Cyber physical security and dependability analysis of digital control systems in nuclear power plants," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 46, no. 3, pp. 356–369, 2015.
[29] N. Perlroth, "Hackers are targeting nuclear facilities, homeland security dept. and FBI say," *The New York Times*, 2017.
[30] S. Gandhi and J. M. Kang, "Nuclear safety and nuclear security synergy," *Annals of Nuclear Energy*, vol. 60, pp. 357–361, 2013.
[31] S. D. Lee and J. H. Huh, "An effective security measures for nuclear power plant using big data analysis approach," *Journal of Supercomputing*, vol. 75, no. 8, pp. 4267–4294, 2019.
[32] J. H. Huh, "Smart grid test bed using OPNET and power line communication," *IGI Global*, Pennsylvania, USA, pp. 1–425, 2017.
[33] B. K. Sovacool and S. V. Valentine, "The national politics of nuclear power: Economics, security, and governance," *Routledge*, Oxfordshire, UK: Taylor & Francis, pp. 1–312, 2012.
[34] D. Y. Kim, "Cyber security issues imposed on nuclear power plants," *Annals of Nuclear Energy*, vol. 65, pp. 141–143, 2014.
[35] W. Young and N. G. Leveson, "An integrated approach to safety and security based on systems theory," *Communications of the ACM*, vol. 57, no. 2, pp. 31–35, 2014.
[36] S. D. Lee and J. H. Huh, "A study on threat containment through VDI for security management of partner companies operating at industrial control system facility," in *2019 Autumn Conf. of KIPS at Jeju National University*, Jeju, Korea, pp. 1–4, 2019.
[37] Oracle VM Virtualbox, [Online]. Available: http://www.virtualbox.org/ (accessed on 31 May 2020).
[38] V. Mnih, K. Kavukcuoglu, D. Silver, A. Graves and I. Antonoglou, "Playing atari with deep reinforcement learning," in *NIPS Deep Learning Workshop 2013*, Lake Tahoe, USA, pp. 1–9, 2013.
[39] C. Stergiou, K. E. Psannis, B. B. Gupta and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Sustainable Computing: Informatics and Systems*, vol. 19, pp. 174–184, 2018.
[40] Z. A. Sharif, I. A. Mohammed, M. A. Luay, I. J. Yaser and G. Brij, "Live forensics of software attacks on cyber–physical systems," *Future Generation Computer Systems*, vol. 108, pp. 1217–1229, 2020.
[41] Citrix, [Online]. Available: https://www.citrix.com/ko-kr/ (accessed on 31 May 2020).
[42] VMware, [Online]. Available: http://www.vmware.com/ (accessed on 31 May 2020).
[43] Ahnlab, [Online]. Available: https://global.ahnlab.com/site/main.do/ (accessed on 31 May 2020).
[44] Mirage Works, [Online]. Available: http://www.mirageworks.co.kr/ (accessed on 31 May 2020).