A VULNERABILITY DIAGNOSIS INTEGRATED MANAGEMENT SYSTEM FOR THE INDUSTRIAL CONTROL SYSTEM OF SOUTH KOREA BASED ON ISO27014

JU-YEON KIM

GECAD-Research Group on Engineering and Intelligent Computing for Innovation and Development Polytechnic of Porto, Porto, Portugal
E-mail:juyeon967@gmail.com

Abstract - Industrial control systems, which are systems applied to major information communication infrastructure, buildings, and airports, are exposed to the threat of cyber security accidents due to linkage with the Internet. However, prior to such a threat, there is no systematic ICS security standard in Korea at present. In this paper, we develop a program to implement the ISO 27014 Governing Body area in order to enhance the systematic security level of the industrial control system in Korea.

I. INTRODUCTION

The Industrial Control System (ICS) is a system applied not only to industrial facilities but also to major information and communication infrastructure, buildings, and airports. The industrial control system consists of various components and types such as Supervisory Control And Data Acquisition System (SCADA), Distributed Control System (DCS), Programmable Logic Controller (PLC) and sensors.

Failure of such an industrial control system to function due to cyber attacks can pose a risk to the safety of citizens and seriously damage the security of the national security and economy.
The initial industrial control system has been separated and operated as an internal and external network, and its own communication protocol has been applied in the control system to construct and operate it in a closed manner. In recent years, however, there has been a tendency to link with the general business system network for various applications, and this has led to a change in convenience for the ICS [2].

In this situation, threats to security incidents in existing Internet networks spread to industrial control systems. In 2010, a Stuxnet malicious code attacking the SCADA system of Siemens was discovered. Stuxnet, aiming at a specific SCADA, has taken control of the system by using security holes that can occur at the contacts of external and internal networks, such as monitoring industrial control systems or generating malicious commands [3].

This paper proposes a program that implements the area of ISO 27014 (Information Security Governance Standard) to enhance systematic security level of industrial control system in Korea. In addition, we conclude that ICS information security governance will be established in Korea in the future through such a program, so that it will be expected to continuously improve the information security level of domestic enterprises / organizations.

II. SYSTEM IMPLEMENTATION ENVIRONMENT

Before describing the system functions of the program, the following system environment is shown in the following table.

Division		Item	Application Details
S/W Development environment	OS	Windows 10	- Work on current operating system - OS in DB Server
	Development environment (IDE)	Eclipse, MySQL Workbench	- Using jsp code and development tools - Server connection
	Development Language	JAVA, JSP, Javascript, PHP	- Interaction process between client and server

III. SYSTEM FUNCTION

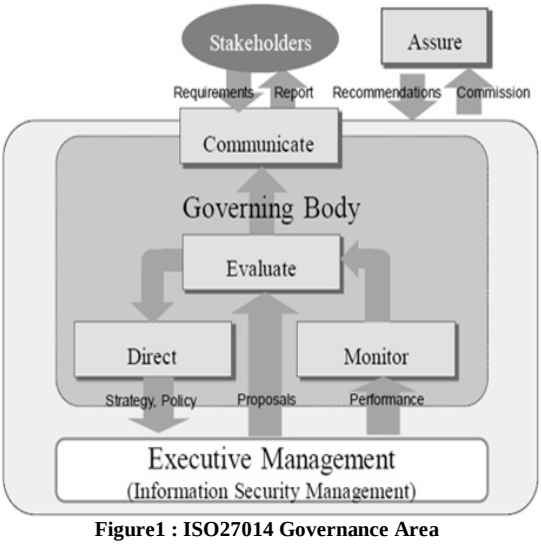


Figure1 : ISO27014 Governance Area

ISO27014 The body of governance is divided into four main functions (Communicate, Evaluate, Direct, Monitor). In this project, this function is applied to the program and implemented [4] Detailed functions of the program combining the four functions of ISO27014 are shown in the following table.

Table1. Detailed functions of the program combining the four functions of ISO27014

Suggest function	Function Details	ISO 27014 area
Control item management	Enter NEI 08-09 based control item Write the importance of each control item	Communicate
Asset valuation based on control items	Select evaluation results for the control items defined in the Communicate area Fill out inspection items and action items	Evaluate
Security evaluation result	Provide action to eliminate vulnerabilities Calculate action priority	Direct
Security Level Management	Quantitative representation of security level	Monitor

First, the communicate registers the management, operation, and technical control items and the so that the user can not modify or delete the data unauthorizedly. If the user modifie importance of each item. Control items are based on NEI 08-09. Users can add, modify, and delete controls based on new threats or analysis. However, the control items and the importance of each item written by the administrator based on NEI 08-09 are registered before the program development s or deletes the control items based on NEI 08-09, it is against the program intention to make more systematic diagnosis of the vulnerability. This step allows each user to exchange information-related information, as well as helping to understand information security requirements.

Second, Evaluate is a function that evaluates whether the user performs the detailed check item in the control item of the asset based on the control item defined in the communicate area with Y / N. This capability allows users to strategically address business objectives by considering and predicting information security performance and results.

Third, Direct is a function that intuitively shows the priority of the action derived through asset priority and item-specific importance, and suggests measures to reduce or eliminate the vulnerability. The security evaluation result is shown only for the data written in Evaluate and the evaluation result is written as 'N'. In the 'Security Assessment Results' tab, you can select two options as required, in order of control item and action priority. By sorting in order of action priority, the calculation is built up using the built-in formula of the program and then sorted in a bottom-up manner, so the user can identify the weakest asset through the calculated action priority. In addition, the user can supplement the vulnerability by implementing security measures accordingly. In other words, this step serves to provide information security objectives and strategic direction.

Fourth, Monitor includes the ability to visually show the results of Direct. Direct graphs the priorities of the control items in the calculation formula used. Also, the number of importance items of the control items checked with 'N' is shown in a graph, so that the indicators can be seen at a glance.

IV. SYSTEM FLOW CHART

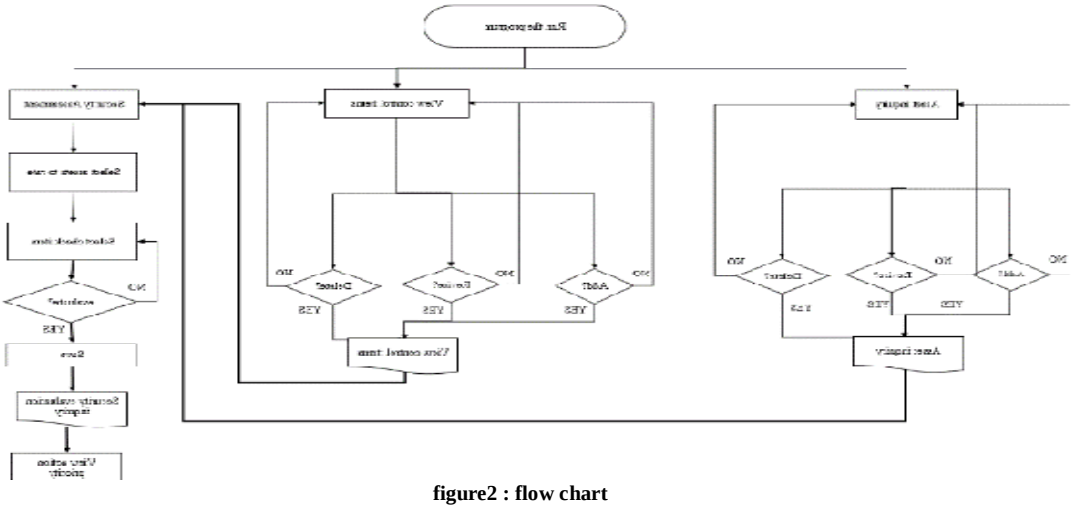


figure2 : flow chart

The above diagram is a system flow chart illustrating the program menu flow. The user can evaluate the assets in turn according to the order of the menu bar at the top of the program. First, when the user executes the vulnerability diagnosis program, the main screen is accessed. In the 'Asset List' menu, the user can register, modify and delete the assets selected by the user. Second, in the 'Asset Evaluation' menu, the user can inquire, add or delete the control items that are the basis of the security evaluation, and finally, it can evaluate the security of the assets through the check items. The user selects the asset and the control item to be evaluated from the 'Asset evaluation' menu and checks whether or not the check item of the asset is implemented. Third, 'security evaluation result' menu only derives non-implemented inspection items based on the result of checking in 'asset evaluation'. In addition, the user can know the action priority of the evaluated asset and the security measure of the action.

V. CRITERIA FOR SELECTING IMPORTANCE BY ITEM

Information security activities within an enterprise are often divided into three categories: vulnerability analysis and response, vulnerability detection and prevention, and vulnerability review and reporting. In this program, the importance (Top, middle, bottom) of the control items was fixed based on the activities classified here. The importance of each control item was determined based on the rating and related research results specified in the Vulnerability Analysis and Evaluation Items of Major IT Infrastructure Facilities.

Table2. The importance criteria for each control item

High	- Establish policies and guidelines related to vulnerability analysis and response procedures - Control items such as access control of ASSET
Middle	- Implementation, approval and supervision of detailed policies and guidelines related to vulnerability detection and prevention - Control items such as supplementary control, alternative supplementary devices, authorization, documentation, implementation and development
Low	- Audit of policies and guidelines related to review and prevention of vulnerabilities - Control items such as monitoring, review / test

The importance criteria for each control item are as follows.

The items designated as 'High' are items such as policy and guidance related to vulnerability analysis and response procedure, and access control of ASSET. This is because the establishment of policies and guidelines is basically a part of governance because it is the foundation that can cover the whole in terms of administrative security. Common weaknesses of industrial control systems are due to the absence and incomplete and inadequate documentation of policies and procedures. [5]

In addition, in the case of physical and logical access control items of ASSET in the aspect of technical and physical security, when unauthorized access and insider leakage occur in ICS, access to important system becomes easy, and access right of control is misused and abused. Therefore, more stringent and strengthened security should be ensured in the management of access rights and the identification of managers in important systems.

The items designated as 'Middle' are related to detailed policy and guidance implementation, approval and supervision, complementary control, replacement and complementary devices, authorization, documentation, implementation and development. This step is relatively insignificant because it is a systematic complement to security rather than a direct cyber attack response.

Finally, the items designated as 'Low' are vulnerability review and reporting phases such as audit, monitoring, review / testing of policies and guidelines. This step can help you understand the future design of the program and the status of ICS, but it does not affect the security of ICS.

VI. CALCULATION OF ACTION PRIORITY

Asset name	Priority
Turbine system PLC	2
Turbine-based monitoring equipment	3
PLC of earthquake monitoring system	2
PLC of nuclear fuel handling system	1
Nuclear steam supply system control device	1

Figure3 : Asset Priority

(By control item)Action Priority
= Asset Priority * {(3 * Number of detailed check items with importance 'high')+
(2 * Number of detailed check items with importance ‘middle')
(1 * Number of detailed check items with importance ‘Low')}
<Equation 1-1>Action Priority Formula

The program adopts a method of automatically calculating the priority of the action through the formula inserted in the program. An example is

shown in <Table 1-1>. <Table 1-2> is the calculation formula derived from the control items in E.12.1. In order to derive the action priority by quantitative value, we assigned 3, 2, and 1 point to the asset priority (1st / 2nd / 3rd) and importance(high / middle / low). Finally, the results for each asset for prioritizing measures are derived by multiplying the weight by asset priority and the sum of weighted control items.

For example, the priority calculation result derived from the item 'E.12 Cyber Risk Assessment and Management', which is a control item of 'Turbine System PLC', is 2 (Asset Priority) X Sum of Weights 22 points) = 44 (points).

Table3. Table of calculation formula

Division	Weight (importance)			total
	3point(high)	2point(middle)	1point(low)	
Number of items checked by control item	3 (37%)	2 (25%)	3 (37%)	8 (100%)
Sum of weights	9	4	3	16

The program adopts a method of automatically calculating the priority of the action through the formula inserted in the program. An example is shown in Table 1-1. <Table 1-2> is the calculation formula derived from the control items in E.12.1. In order to derive the action priority by quantitative value, we assigned 3, 2, and 1 priority to the asset priority (1st / 2nd / 3rd) and importance (top / middle / bottom) Finally, the results for each asset for prioritizing measures are derived by multiplying the weight by asset priority and the sum of weighted control items. For example, the priority calculation result derived from the item 'E.12 Cyber Risk Assessment and Management', which is a control item of 'Turbine System PLC', is 2 (Asset Priority) X Sum of Weights 22 points) = 44 (points).

VII. PROGRAM IMPROVEMENT DIRECTION

According to the "Radiation Emergency Preparedness Act," cyber security drills must be carried out from 2016 as laws and regulations for physical protection training of nuclear operators are legislated.

In addition, while establishing cyber security training plans, it is necessary to develop training scenarios first and regulatory agencies should carry out adequacy assessment, but Korea lacks guidelines and manuals to evaluate training scenarios. Therefore, by adding these four functions to the program, I seek to improve the quality of the training plan by presenting training scenario evaluation guidelines.

Table4. Suggest function

Suggest function	Function Details
Emergency incident management	•Emergency incident registration and Calculation of importance by item by cyber attack route entry •Major components: year, city, country, institution, event name, cyber attack damage level, summary of events, cyber attack path, control item importance
Scenario Management / Evaluation	• Register / View / Modify / Delete scenarios according to level of cyber infringement by derived vulnerability • Main components: Infringement incident level, ICS facility name, Initial condition, Scenario summary, Time Line, Phase, Activity, Organization R & R,
Infringement response training management	• Main components: type of training (physical / practical training), training schedule, training place, training department, scenario, training by date

VIII. RESULTS AND DISCUSSION

In this paper, I developed a vulnerability diagnostic program based on the tendency of preventing and managing the importance of industrial control system due to the nature of non - stop operation. Currently, Korea is developing with a focus on CCE (Checking for Vulnerability of Pattern Matching Method for Regulatory Compliance). However, in the days when intelligent attacks are increasing, CVE method is also needed to detect vulnerabilities themselves and respond to actual attacks . The program was also developed with a focus on CCE. Future developments combining CVE and CCE methods are considered to be a research task in ICS security field.

REFERENCES

[1] ISO / IEC, "ISO 27014 Governance of Information Security", ISO / IEC, 2013

[2] Son, Kyung Ho, "Analysis of Security Evaluation and Certification Trends in Industrial Control System", Korea Institute of Information Security, 2014

[3] Kim, Il-Taek Lim, Ji-Bum Park, Jae-Pyo Park, "Effective Network Security Management Model in Industrial Control System Environment", Korea Academia-Industrial

[4] Cho, YH, Lee, Eun-Kyung, "A Study on the Design of Information Protection Management System for Industrial Control System", Korea Computer Information Association, 2016

[5] Kim, Jeong-Deok, Lee, Sung-Il, "International Standardization of Information Protection Governance and Domestic Case Study", Korea Information Security Society, 2012

[6] Kim, Do-yeon, "Vulnerability Analysis for Cyber Security of Industrial Control Systems", JKIECS, vol. 9, no. 1, pp. 140, 2014

★★★