A Research on the Application of Entropy Theory to Identify the Impact of Nuclear Facility Cyber Security Controls

Ka-kyung Kim[a*], Seong-su Yoon[a], Joon-seok Kim[a], Do-yeon Kim[a], Ieck-chae Euom [a]
[a] *Chonnam National University System Security Research Center, 77 Yongbong-ro 138beon-gil, Gwangju, 61186*
[*]*Corresponding author: iceuom@jnu.ac.kr*

Keywords : Nuclear Power Plant Digital System Security, Cyber Security Control Impact, ICS System Requirement, Cyber-Physical System, Information Entropy

1. Introduction

As analog-based systems in existing nuclear facilities are being replaced by digital systems, the cyber-attack surface in nuclear facilities is expanding. KINAC (The Korea Institute of Nuclear Nonproliferation and Control) has developed Regulation RS-015 on computer and information system security for nuclear facilities.

RS-015 provides guidelines for establishing, implementing, and maintaining a cyber security plan and for responding to and recovering from emergency events. However, the effectiveness of cyber security controls implemented for nuclear facility computers and information systems, including RS-015, is difficult to determine due to the nature of the environment.

It is based on the dilemma of allowing real-world vulnerabilities in nuclear facilities to validate the effectiveness of cyber security controls, and the concern that increased security can create a value conflict with safety. On safety systems with constrained performance, building in security features can delay response times. If the response time of safety systems is delayed due to security enhancements, it can negatively impact the security, safety, and emergency preparedness (SSEP) capabilities of essential digital assets.

To address these issues, this research identifies the impact of cyber security controls on system performance. The impact on system performance is predicted based on the probability of violation of industrial control system security requirements. Proposed method to identify cyber security controls that can degrade the performance of digital systems and quantitatively compute the probability of ICS requirement impacts due to the implementation of cyber security controls.

2. Research background

2.1 Define the issue

SSEP functions, as defined in RS-015, are "the safety, security, and emergency response of a nuclear facility as functions that must be protected against cyber-attacks." Some of the negative impacts of Nuclear Facility Cyber Security Controls on SSEP include reduced system functionality due to increased system response time and complexity.

The licensee shall ensure that the nuclear facility's computer and information systems are adequately protected against cyber-attacks that are included in the Design Basis Threat (DBT). Security controls to counter cyber threats have the potential to conflict with the value of safety and require careful judgment on the part of the operator. Safety is the prevention of adverse effects of the system on the environment, while security is the prevention of adverse effects of the environment on the system. Systems designed to prioritize safety do not support high-performance computing capabilities, and therefore may conflict with safety when attempting to enhance cyber security.

In fact, the impact of cyber security controls on the security requirements of industrial control systems can result in system overload or downtime. In particular, systems designed to prioritize safety have many performance constraints that limit the implementation of security features. As a result, they can cause serious damage to power plant operations.

The problem addressed in this research is to identify which cyber security controls can disrupt the security requirements of industrial control systems. It also aims to use entropy to quantify the impact of cyber security controls on ICS security requirements.

2.2 Related Research

According to the purposes of this study, the five papers that identify and evaluate the impact of cybersecurity measures to enhance security were analyzed.

Junhee Lim [12] analyzed the communication independence requirements of nuclear facility systems according to IEEE 7-4.3.2 [11] and identified and presented RS-015 [1] security action items that can affect communication independence requirements.

Chanyoung Lee [13] argued that depending on the digital devices and their security feature requirements, cybersecurity controls can lead to deficiencies. It proposed a methodology for evaluating the impact of security measures based on the complexity of software changes and the entropy model of security controls.

Radek [14] focused on cryptographic algorithms and presented the relationship between security, safety, and performance based on requirements established in standards such as IEC 62443 [17] and NIST SP 800-82 [6]. This research evaluated the impact of different

cryptographic algorithms on security, safety, and performance.

Shin-Hae Um [15] proposed a method to estimate the effectiveness of RS-015 security controls in terms of defense against hostile attacks. This is a methodology to assess the positive impact of cybersecurity measures.

Gu Tingyang [16] Gu Tingyang [16] argued that the enhancement of security requirements in cyber-physical systems may be in conflict with safety requirements. It suggests that if safety measures and security measures are opposite in the same situation and target, the requirements of the two values may conflict.

3. Cyber Security Control Entropy

This section introduces the methodology presented in this research. The methodology includes the following steps: defining SSEP functions, identifying industrial control system security requirements, identifying RS-015 security controls that can affect industrial control system security requirements, defining information entropy, and defining cyber security controls entropy derived from information entropy. The methodology is schematized in Figure 1.

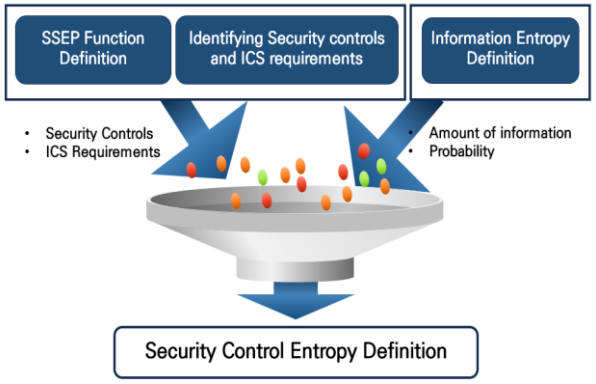

Fig. 1. Proposal Method

3.1 Information Entropy

In information theory, entropy is generally defined as the expectation value of the information contained in each message. Information entropy applies different entropy units based on the logarithmic base definition given by Shannon, Nat, and Hartley. The details are shown in Table I.

Table I : Information Entropy

Category	Logs Under	Indicators
Shannon	Information content of an event that occurs when the probability of two things happening is 1/2.	Bit
Nat	If the probability of that event occurring is 1/e	Nit
Hartley	If the probability of that event occurring is 1/e	Ban

The most used expression for Shannon's information entropy is EQ.1. ‘P(x)’ is the probability mass function of the probability of event 'x' occurring. The reason for taking the logarithm is to make the probability of independent events additive. The base of the logarithm is '2' by definition, which means that the probability of two events occurring is 0.5. E(x) is the sum of all the possible probabilities ‘P(x)’ of ‘x’ occurring, representing the entropy values.

$$(EQ.1) \qquad E(x) = -\sum_{i=1}^{c} P(x) log_2 P(x)$$

Throughput and response time are the main performance metrics of a system. Throughput is the actual amount of data that can be transferred at any given moment, while response time is the amount of time between the initiation of a request and the completion of the system's response to it.

The relationship between throughput and response time depends on the characteristics of the system is generally inverse. The higher the throughput, the slower the system response time, and the lower the throughput, the faster the system response time. In addition, throughput has a threshold that is unique to the system, and response time increases exponentially when the request size exceeds this saturation point. A graphical representation of this is shown in Figure 2.

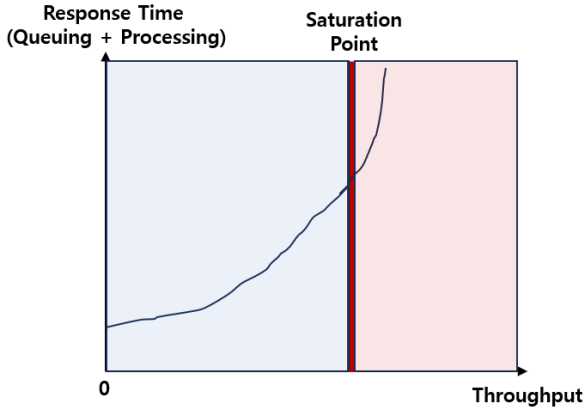

Fig. 2. Association of throughput and response time.

Based on the relationship between throughput and response time, a derivative substitution is made to the theory of information entropy. Throughput in system metrics is described in terms of system performance, while information entropy refers to the amount of information in the number of cases. The quantitative mass of the former is assumed to be on the same line as the probabilistic mass of the latter.

In other words, throughput is substituted for the total amount of information in information entropy, and the probability of a delay in response time due to excessive throughput is substituted for the probability of an event occurring.

Applied to digital systems in nuclear facilities, the security requirements of the relevant industrial control

systems are substituted for the amount of information in the information entropy. The probability of an event is the number of possible impacts on the industrial control system security requirements by performing a specific cyber security control.

Shannon's theory is utilized in this research because the impact of cyber security controls on industrial control system security requirements can be categorized into two scenarios: impacted and unimpacted.

Through this process, the entropy of a cyber security controls can be defined as the sum (E) of the probabilities ($P(x_{ij})$) that an impact on industrial control system security requirements can occur.

3.2 Identifying Security Controls

RS-015 consists of 101 security controls items in three categories: technical, operational, and administrative. For this research, there were two steps taken to identify the security controls to utilize.

First, it excludes operational and administrative security controls that do not actually change system code or performance. Second, it excludes non-digital items from RS-015's technical security controls that simply require nuclear plant operators to "maintain," "manage documentation," "ensure functionality according to design criteria," "oversee operational processes," and so on.The RS-015 security action items identified through the two processes are shown in Table II. The null hypothesis of the methodology proposed in this research is that the 12 security controls listed in Table II should yield higher entropy than the excluded security controls.

Table II: The 12 security controls in RS-015 that identified

Element	Security Control Title	Identification Grounds
1 .1.2	Access Enforcement	May adversely affect the intended functionality of essential digital assets
1 .1.6	Unsuccessful Login Attempts	Reduced system performance, reliability
1 .1.9	Previous Logon Notification	Reduced system performance, reliability
1 .1.11	Permitted Actions without Identification or Authentication	Operations that do not negatively impact SSEP functionality can be used without identification and authentication, although this is not guaranteed.
1.1.12	Network Access Control	Encrypt sensitive information when sending passwords and other sensitive information
1.2.7	Timestamp	Time synchronization can cause failures
1.3.5	Transmission Integrity	Encrypting information
1.3.6	Transmission Confidentiality	Encrypting information
1.3.11	Mobile Code	Approved mobile code use can adversely affect your system
1.5.2	Host Intrusion Detection System	Performing HIDS rules and patching can adversely affect SSEP functionality
1.5.4	Hardware Configuration	The system is SW-unavailable, so it is used for legitimate reasons with the approval of the responsible person, but it may adversely affect the SSEP function.
1.5.5	Installing Operating Systems, Applications, and Third-Party Software Updates	Patches and updates can adversely affect SSEP functionality

3.3 Industrial Control System Security Requirements

IEC 62443, the industrial control system security standard published by the International Electrotechnical Commission (IEC), covers the technical security requirements for industrial control system components in Part 4-2 of IEC 62443. The requirements for each component are shown in Table III. The RS-015 items according to IEC 62443 requirements are categorized according to the stated security controls or details. The justification of the item classification is limited to this research.

Table III : IEC 62443-4-2 Requirements

Category	Requirements	Mapping
Identification and authentication control (a)	• Human user identification and authentication • Software process and device identification and authentication • Account management • Identifier management • Authenticator management • Wireless access management • Strength of password-based authentication	• 1.1.2 • 1.1.6 • 1.1.11 • 1.1.12 • 1.3.5 • 1.3.6 • 1.5.2 • 1.5.5

	• Public key infrastructure certificates • Strength of public key-based authentication • Authenticator feedback • Unsuccessful login attempts • System use notification • Access via untrusted networks • Strength of symmetric key-based authentication	
Use Control (b)	• Authorization enforcement • Wireless use control. • Use control for portable and mobile devices • Mobile code • Remote session termination • Concurrent session control • Concurrent session control • Auditable events • Audit storage capacity • Response to audit processing failures • Timestamps • Non-repudiation • Use of physical diagnostic and test interfaces	• 1.1.2 • 1.1.6 • 1.1.9 • 1.2.7 • 1.3.11 • 1.5.4
System integrity (c)	• Communication integrity • Protection from malicious code • Security functionality verification • Software and information integrity • Input validation • Deterministic output • Error handling • Session integrity • Protection of audit information • Support for updates • Physical tamper resistance and detection	• 1.3.5 • 1.3.6 • 1.3.11 • 1.5.2 • 1.5.4 • 1.5.5
	• Provisioning product supplier roots of trust • Provisioning asset owner roots of trust • Integrity of the boot process	
Data confidentiality (d)	• Information confidentiality • Information persistence • Use of cryptography	• 1.1.12 • 1.3.5 • 1.3.6
Restricted data flow (e)	• Network segmentation • Zone boundary protection • General-purpose person-to-person communication restrictions • Application partitioning	• 1.1.12 • 1.5.2
Timely response to events (f)	• Audit log accessibility • Continuous monitoring	• 1.2.7
Resource availability (g)	• Denial of service protection • Resource management • Control system backup • Control system recovery and reconstitution • Emergency power • Network and security configuration settings • Least functionality • Control system component inventory	• 1.1.6 • 1.1.11 • 1.1.12 • 1.2.7 • 1.3.5 • 1.3.6 • 1.3.11 • 1.5.2 • 1.5.4 • 1.5.5
Software application requirements (h)	• Mobile code • Protection from malicious code	• 1.3.11 • 1.5.2 • 1.5.4 • 1.5.5
Embedded device requirements (k)	• Mobile code • Use of physical diagnostic and test interfaces • Protection from malicious code • Support for updates • Physical tamper resistance and detection • Provisioning product supplier roots of trust • Provisioning asset owner roots of trust	• 1.3.11 • 1.5.2 • 1.5.5

	• Integrity of the boot process	
Host device requirements (l)	• Mobile code • Use of physical diagnostic and test interfaces • Protection from malicious code • Support for updates • Physical tamper resistance and detection • Provisioning product supplier roots of trust • Provisioning asset owner roots of trust • Integrity of the boot process	• 1.3.11 • 1.5.2 • 1.5.4 • 1.5.5
Network device requirements (z)	• Wireless access management • Access via untrusted networks • Mobile code • Use of physical diagnostic and test interfaces • Protection from malicious code • Support for updates • Physical tamper resistance and detection • Provisioning product supplier roots of trust • Provisioning asset owner roots of trust • Integrity of the boot process • Zone boundary protection • General purpose, person-to-person communication restrictions	• 1.1.12 • 1.5.4 • 1.5.5

3.4 Compute Cyber Security Controls Entropy

The cyber security controls entropy defined earlier is the sum of a probability mass function. The probability mass function describes the probability that a discrete random variable has a particular value. The probability mass function '$P(x_{ij})$' in this research is defined as Eq. 2 below.

$$(EQ.2) \qquad P(x_{ij}) = \frac{SCVR_{i.jSUM}}{SCVR_{ALLSUM}}$$

'$SCVR_{ALLSUM}$' is the total amount of information of the industrial control system security requirements, and '$SCVR_{ijSUM}$' is the sum of the probabilities that the 'i_{-th}' security controls can affect 'j_{-th}' industrial control system security requirement. The sum of the values of the probability mass function $P(x_{ij})$ is the entropy of each cyber security controls, as shown in Equation 3.

$$(EQ.3) \qquad E = -\sum_{i=1}^{c} P(x_{ij}) log_2 P(x_{ij})$$

There are two reasons to use '-log2'. First, because the Shannon definition of information entropy requires that the units of computation consist of '0' and '1'. The logarithmic base of the cyber security controls entropy calculation is similarly '-log 2'. This is because it can be categorized into two situations: those that do not affect the security requirements (0) and those that may affect them (1). Second, it turns the probability of independent events A and B occurring simultaneously into an additive property. Without taking the logarithmic function, the probability of independent events A and B occurring simultaneously is multiplicative.

The '-' is added because the probability mass function $P(x_{ij})$ always has a real value, which becomes negative when logarithmized, and thus to make it positive again. The reason for the '-' in the entropy calculation for cyber security controls in this research is the same as in traditional information theory.

Traditional entropy is an index that indicates the degree of disorder in a result and has a value from '0' to '1'. However, the entropy of cyber security controls defined in this research has only a minimum point of '0' because the more the amount of information that can be violated (industrial control system security requirements) increases, the greater the degree of disorder. The reason why the maximum point is not limited is that the number of security requirements varies depending on the control system environment.

3.5 Identifying and interpreting cyber security controls entropy

The mapping relationship between the RS-015 cyber security controls identified in 3.2 and the IEC 62443 security requirements identified in 3.3 is shown in Table IV below.

Table IV : Association Analysis between Security Control and ICS Requirements

	ICS Requirements										
S.C	a	b	c	d	e	f	g	h	k	l	z
1.1.2	O	O									
1.1.6	O	O					O				
1.1.9	O	O									
1.1.11	O						O	O			
1.1.12	O				O		O				O
1.2.7		O				O	O				
1.3.5	O		O	O			O				

1.3.6	O		O	O			O				
1.3.11		O	O	O			O		O	O	
1.5.2	O		O	O	O		O	O	O	O	
1.5.4		O	O	O			O	O		O	O
1.5.5	O		O	O			O	O	O	O	O

The relevance of RS-015 security controls to each of the industrial control system requirements is not the same. The entropy of a cyber security controls can be expressed as the sum of the entropies of the related security requirements, and the entropy of an individual security controls item can be calculated using Equation 4, based on the foundation described in Section 3.4.

(EQ.4)
$$\begin{aligned} E(x_{ij}) = -[&P(x_{i.a})log_2P(x_{i.a}) \\ &+ P(x_{i.b})log_2P(x_{i.b}) \\ &+ P(x_{i.c})log_2P(x_{i.c}) \\ &+ P(x_{i.d})log_2P(x_{i.d}) \\ &+ P(x_{i.e})log_2P(x_{i.e}) \\ &+ P(x_{i.f})log_2P(x_{i.f})] \\ &+ P(x_{i.g})log_2P(x_{i.g})] \\ &+ P(x_{i.h})log_2P(x_{i.h})] \\ &+ P(x_{i.k})log_2P(x_{i.k})] \\ &+ P(x_{i.l})log_2P(x_{i.l})] \\ &+ P(x_{i.z})log_2P(x_{i.z})] \end{aligned}$$

3.6 Visualization and Analysis Cyber Security Controls Entropy

Based on the mapping relationship between the RS-015 security action items identified in 3.5 and the industrial control system security requirements of IEC 62443, the calculated cyber security action entropy value is shown in Figure 3 below.

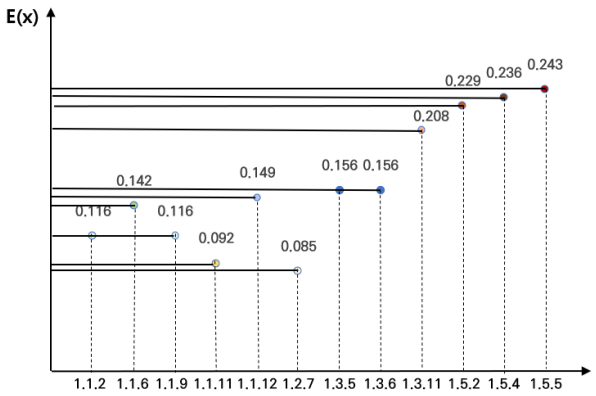

Fig.3. Entropy by Security Control(E)

The higher the entropy value, the more relevant the security controls is to the security requirements of the industrial control system. In other words, it can have many effects. In situations where there are multiple security controls to mitigate a particular vulnerability, a security controls with a high entropy value should be used with more caution.

4. Case studies

4.1 Selecting case study

As a case study, select a PLC used as an industrial control system. Typically, a PLC consists of a microcontroller and a set of input and output channels. Assume that this PLC is using the S7-1500 firmware from Siemens, and that the vulnerability 'CVE-2014-0224' has been identified in production S7-1500s. The details of the vulnerability are shown in Table V below.

Table V : Details Information of 'CVE-2014-0224'

Category	Details
Descriptions	• OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h do not properly restrict ChangeCipherSpec message handling, which could allow a man-in-the-middle attacker to trigger the use of zero-length masters • Injecting keys into certain OpenSSL-to-OpenSSL communications and consequently crafted TLS handshakes, also known as the "CCS injection" vulnerability, could allow hijacking of sessions or obtaining sensitive information
CVSSv3 Score	7.4 (Management target)
Feature	• Attack Vector: Network • Attack complexity: High • Access Privileges: None • User Interaction: None • Scope: Unchanged • Confidentiality: High • Integrity: High • Availability: None

The NVD also lists inadequate encryption strength 'CWE-326' as a security weakness for this vulnerability. Specifically, it states that "sensitive data is stored or transmitted using an encryption scheme that is not strong enough for the required level of protection. Based on this, the security control lines identified in Section 3.2 that could mitigate the vulnerability are assumed to be '1.1.12', '1.3.5', '1.3.6', '1.3.11', and '1.5.5'.

4.2 Identifying and interpreting cyber security controls entropy

The entropy calculation results for the five security controls are shown in Figure 4. Security controls '1.1.12' has the lowest entropy value, and '1.5.5' has the highest entropy value. This means that of the security controls that nuclear operators must implement to mitigate vulnerabilities, '1.5.5' may have the greatest impact on

industrial control system security requirements. Therefore, it can be seen that more careful judgment is required before implementing '1.5.5' than other security controls.

5. Conclusions

Because they prioritized safety in the initial system design, there is always the possibility that controls to increase security will conflict with the values they are intended to achieve. Safety and security can have positive and negative effects on each other, and vice versa. They can also be independent of each other, with neither having any impact on the other.

As a result, security personnel in non-disruptive environments should not make decisions based solely on the value of safety or security.

The purpose of this research is to encourage caution when taking steps to increase security, as it can lead to delays in system response time. In order to make prudent judgments, quantitative metrics such as entropy presented in this research can help practitioners make efficient judgments.

The limitation of this research is that it simply analyzes and assumes the impact relationship between security action items and industrial control system security requirements from a semantic perspective. In addition, in general, machine learning makes decisions by reducing entropy, but the entropy in this research is for simple impact identification.

Considering the limitations of this research, future research should identify the common causes of failure (CCF) caused by cyber security controls from the structural perspective of the system and quantify the impact in terms of system reliability.

ACKNOWLEDGMENTS

This work was supported by Institute for Information & communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT)(No.2022-0-01203, Regional strategic Industry convergence security core talent training business)

The results of a study on the supported by Nuclear Safety Research Program through the Korea Foundation of Nuclear Safety (KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission (NSSC) of the Republic of Korea (No.2106061).

REFERENCES

[1] The Korea Institute of Nuclear Nonproliferation and Control, RS-015 Security of computers and information systems at nuclear facilities, 2016
[2] United States Nuclear Regulatory Commission, Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities. 2023.
[3] Nuclear Energy Institute, Endorsement of Addendum 5 to NEI 08-09 Revision 6 Cyber Security Vulnerability and Risk Management, 2018
[4] Nuclear Energy Institute, NEI 13-10 Revision 6 Cyber Security Control Assessments, 2017
[5] Korea Internet Security Agency, Detailed Guide for Analysis and Evaluation of Technical Vulnerabilities in Major Information and Communication Infrastructure, 2021
[6] National Institute of Standards and Technology, NIST SP 800-82 Guide to Operational Technology (OT) Security, 2022
[7] National Institute of Standards and Technology, NIST SP 800-53 Security and Privacy controls for Federal Information Systems and Organizations, 2020
[8] International Electrotechnical Commision, Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems, 2014
[9] International Electrotechnical Commision, Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cyber security, 2016
[10] Institute of Electrical and Electronics Engineers Standards Association, IEEE 603-2018 Standard Criteria for Safety Systems for Nuclear Power Generating Stations, 2018
[11] Institute of Electrical and Electronics Engineers Standards Association, IEEE STD 7-4.3.2 IEEE Standard Criteria for Programmable Digital Device in Safety Systems of Nuclear Power Generating Stations, 2016
[12] Jun Hee Lim, & Huy Kang Kim, A study on the security evaluation considering the design requirements (Code & Standard) for digital systems in nuclear power plants, REVIEW OF KIISC, 30 (2), 59-63, 2020
[13] Chanyoung Lee, Sang Min Han, Poong Hyun Seong, Development of a quantitative method for identifying fault-prone cyber security controls in NPP digital I&C systems, Annals of Nuclear Energy, Volume 142, 2020
[14] R. Fujdiak, P. Mlynek, P. Blazek, M. Barabas and P. Mrnustik, "Seeking the Relation Between Performance and Security in Modern Systems: Metrics and Controls," 2018 41st International Conference on Telecommunications and Signal Processing (TSP), Athens, Greece, 2018
[15] Um Shin-hae. "Correlation Analysis of Attack Techniques and Security Controls for Deriving Priorities." Chonnam National University, 2023
[16] T. Gu, M. Lu and L. Li, "Extracting interdependent requirements and resolving conflicted requirements of safety and security for industrial control systems," 2015 First International Conference on Reliability Systems Engineering (ICRSE), Beijing, China, 2015
[17] International Electrotechnical Commision, Security for industrial automation and control systems, 2016
[18] A. J. Kornecki and W. F. Stevenson, "Impact of Adding Security to Safety-Critical Real-Time Systems: A Case Study," 2011 IEEE 35th Annual Computer Software and Applications Conference Workshops, Munich, Germany, 2011