Hindawi
Security and Communication Networks
Volume 2022, Article ID 4714899, 13 pages
https://doi.org/10.1155/2022/4714899

Research Article

Compliance-Driven Cybersecurity Planning Based on Formalized Attack Patterns for Instrumentation and Control Systems of Nuclear Power Plants

Minsoo Lee,[1] Hyun Kwon ,[2] and Hyunsoo Yoon[1]

[1] *School of Computing, Korea Advanced Institute of Science and Technology, Daejeon, Republic of Korea*
[2] *Department of Artificial Intelligence and Data Science, Korea Military Academy, Seoul, Republic of Korea*

Correspondence should be addressed to Hyun Kwon; hkwon.cs@gmail.com

Received 18 August 2021; Accepted 12 November 2021; Published 11 January 2022

Academic Editor: Ilsun You

The instrumentation and control (I&C) system of a nuclear power plant (NPP) employs a cybersecurity program regulated by the government. Through regulation, the government requires the implementation of security controls in order for a system to be developed and operated. Accordingly, the licensee of an NPP works to comply with this requirement, beginning in the development phase. The compliance-driven approach is efficient when the government supervises NPPs, but it is inefficient when a licensee constructs them. The security controls described in regulatory guidance do not consider system characteristics. In other words, the development organization spends a considerable amount of time excluding unnecessary control items and preparing the evidence to justify their exclusion. In addition, security systems can vary according to the developer's level of security knowledge, leading to differences in levels of security between systems. This paper proposes a method for a developer to select the appropriate security controls when preparing the security requirements during the early development phase; it is designed to ensure the system's security and reduce the cost of excluding unnecessary security controls. We have formalized the representation of attack patterns and security control patterns and identified the relationships between these patterns. We conducted a case study applying RG 5.71 in the Plant Protection System (PPS) to confirm the validity of the proposed method.

1. Introduction

Recently, the industrial control field has introduced digitalized systems and devices designed to increase ease of use by operators. However, the introduction of digitalized systems can generate a variety of new cyber threats, a prominent example being Stuxnet [1, 2]. After the success of the Stuxnet attack, governments heightened their alertness with regard to the security problem of safety-critical systems and the adverse physical effects on people in the event of a cyberattack. This government-led approach typically involves regulations and requires compliance by system providers and operators. In other words, it is a compliance-driven approach [3].

A typical example of a safety-critical system is the instrumentation and control (I&C) system of a nuclear power plant (NPP). The US government requires operators of an NPP I&C system to comply with RG 5.71, based on 10 CFR 73.43 [4, 5]. RG 5.71 includes not only the requirements for system operation, but also those for technical countermeasures (security controls) [4]. To comply with the regulation, a plant operator should consider providing security functionality in the development phase. Some of the security controls require specific system security functions for compliance. Therefore, security system developers identify these controls and incorporate them into the system requirements in the early stages of development.

There are no system criteria that apply to the code itself. Applying the security controls to the system requires gaining an understanding of the security control requirements, which takes time, because the regulation, which provides the only description of the security controls, is written in natural language. The developer selects the security controls for the system after the system analysis and threat identification are performed, as this approach is supported by security experts based on risk assessment frameworks such as NIST SP 800–13 [6]. In another approach, the developer identifies the system's potential vulnerabilities and selects the security controls by performing a preliminary penetration test [7].

In this paper, we propose a systematic method for selecting the security controls for a given system. The method does not require the participation of a security expert and depends only on the developer. Only when defining the attack patterns is the security expert's participation needed. By defining an attack pattern database that includes existing attack cases and mapping the attack patterns with the system's characteristics, the developer can obtain the appropriate security controls for the target system in an automated manner. The proposed method creates a representation of the system and its operating environment using formalized patterns and then compares the formalized attack patterns with the formalized system characteristics.

The remainder of this paper is organized as follows. Section 2 explains work related to the proposed method. Section 3 provides an overview of the proposed method. Section 4 defines the concept of the security control pattern. Section 5 presents the results of the case study performed. Section 6 discusses the limitations of the proposed approach. Finally, Section 7 concludes the paper.

2. Related Work

Currently, the developer and security experts select the security controls by reviewing individual cases in the NPP domain. In a review meeting, they decide for each individual security control whether it needs to be implemented in the given system [8]. They also perform a preliminary penetration test to find vulnerabilities in the system in order to decrease the cost of addressing such vulnerabilities [7]; this is only a vulnerability response, however, not a method of selecting security controls to satisfy the regulatory guidance [7]. No method has been proposed for systematically choosing the security controls from those listed in RG 5.71.

In information systems security [9–11], there are various security development methodologies, such as MS SDL, Seven Touchpoints, and OWASP CLASP [12–15]. These methodologies depend entirely on security experts, because they define only general processes. There are also open services such as CVE and CWE, which can identify software vulnerabilities and weaknesses [16–18]. Although these services also offer countermeasures, developers can use them after code implementation is complete. Because these methodologies do not consider the operating conditions of the system, they cannot be directly applied to a system, and the assistance of security experts is needed.

Some regulations and standards documents for information systems indicate security threats and countermeasures; ISO 27 001, ISO 15 408, and BSI catalogs are typical examples [19–21]. These standards documents provide security countermeasures similar to RG 5.71, but they do not present methods for applying and implementing them.

The method proposed in this paper differs from the existing methods in three key respects. First, it is a systematic method for selecting security controls that can be applied to meet the requirements of regulatory guidelines in the NPP domain. Second, it can be applied in the early stages of development, and the operational environment can be specified as a parameter. Third, it is a method for choosing specific security countermeasures that considers system-specific characteristics and operational environments.

3. Proposed Method

We propose a systematic method for selecting security controls based on the relationship between attacks and security countermeasures. In RG 5.71, the US NRC requires the application of 143 security controls to a system [4]. In this paper, we focus on the selection of security controls for the specific system targeted. A security countermeasure that can resist a certain type of attack should be applied to the system to protect it from that type of attack. A more in-depth security concept model can express the relationship between the method of attack and the system's security. Figure 1 presents the security concept model of the relationship between attacks and countermeasures.

As shown in Figure 1, an attacker attempts to exploit an attack surface using the knowledge elicited from a history of attacks and their methods. A security engineer decides to apply a security countermeasure based on experience gained from the history of attacks and their methods. We propose a systematic method designed to systematically select a security countermeasure by considering the attack patterns of the target system; it uses an attack formalization method based on the relationship between attack surfaces and security controls. Figure 2 shows the steps involved in the proposed approach.

3.1. Attack Surface.

3.1. Attack Surface. In the field of information security, the term "attack surface" is generally used to mean the points of attack on a target system [22]. Some researchers have assessed software security using the attack surface concept and have achieved good results. We propose representing an attack pattern in the abstract by extending the attack surface concept. The proposed method uses the attack surface and elements related to the operational environment. There are two operation states in the I&C system of an NPP: the operating state and the maintenance state. Figure 3 illustrates the attack surface and in two operational environments.

The notion of the attack surface is deeply related to that of an entry point of the system, because an entry point is an entrance through which an attacker attempts to access the system using a malicious method. As shown in Figure 3, (a) system opens entry points, which are accessible from the outside, to provide a service. A client uses the service through a communication channel using a predefined protocol. The best method for enhancing security is to remove the entry points in a system. This approach is unfeasible, however, because with no entry points, the system

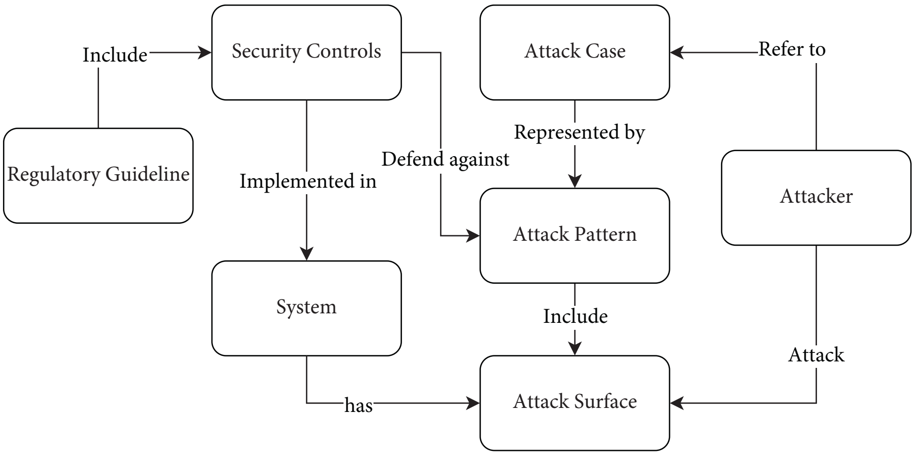

Figure 1: Security concept model.

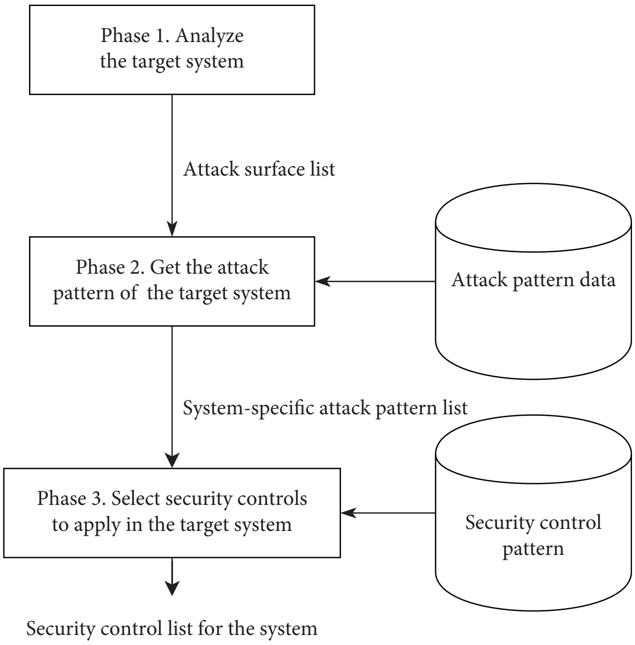
Phase 1. Analyze the target system
Attack surface list
Phase 2. Get the attack pattern of the target system
Attack pattern data
System-specific attack pattern list
Phase 3. Select security controls to apply in the target system
Security control pattern
Security control list for the system

Figure 2: Procedural steps of the proposed method.

cannot provide the service. An alternative method is to develop security countermeasures. In other words, even a system with entry points can be secure if security countermeasures are developed appropriately around the entry points. We use the characteristics of the attack surface and operating environment to formalize an attack pattern. Our model defines three elements to represent the attack surface (AS): external entity (EE), channel (CH), and service (SRV).

An entry point is a network service by which an external system or user can access system. A system can have multiple entry points, which are denoted by $E_1 - E_n$:

$$\text{System} \in \{E_1,\ E_2,\ E_3,\ \text{hellip;}\ E_n\}. \tag{1}$$

An entry point may expose several attack surfaces depending on the service provided. This is represented by the following expression:

$$E_i \in \{AS_1, AS_2, AS_3,\ \text{hellip;}\ AS_k\}. \tag{2}$$

When a system provides an entry point for providing a service to an external system or user, it can be used to attack the service and is thus called the attack surface. We express the attack surface as a system service related to the entry point, an external entity connected to this service, and a communication method:

$$AS = (EE, CH, SRV). \tag{3}$$

3.2. Attack Pattern Formalization. Even a system with an attack surface is not necessarily attackable. Only when additional conditions are satisfied does it become attackable. For instance, when an attacker sniffs data in the communication network, only if the data transmitted through the network include information helpful for carrying out an attack will the system be attackable. We define features to consider this characteristic in our formalization method. The additional elements to express the attack ability condition in the formula are the method (M), attack target (AT), and related data (RD) type. These elements represent the characteristics considered during an attack through an attack surface. M represents the method by which an attacker attempts to attack through the attack surface, AT is the target element attacked by M, and $R\ D$ denotes the type of data exchanged within the elements of the attack surface. Our formalization represents the attack pattern as a tuple that includes these three elements together with AS:

$$\text{Attackpattern} = (AS, M, AT, R\ D). \tag{4}$$

An attack pattern selects the system's attack surface after expressing the specific element of the attack surface and the attack method. The type of related data indicates the type of data transmitted through the attack surface during regular operation. With these elements known, it can be determined whether an attack is possible. Each element's value can be selected from a predefined list, and an example expressing an actual method of attack is given in Equation 5.

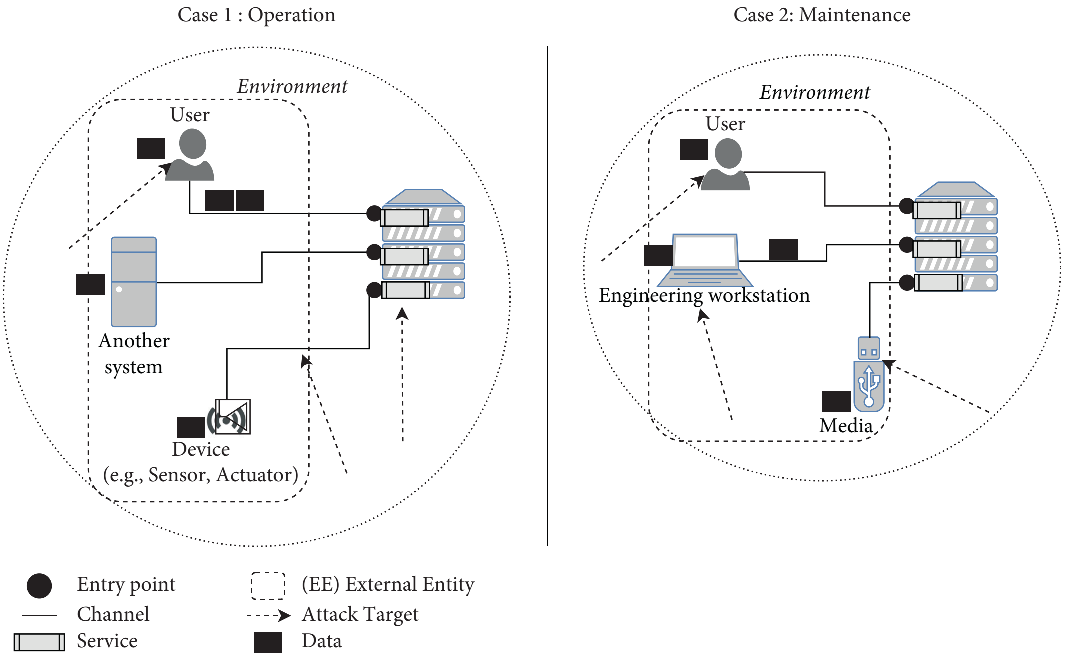

Figure 3: Attack surface in two operational environments.

3.3. Attack Pattern Parameters. An attack pattern is expressed in terms of attack pattern parameters using predefined values, representing a formalized attack pattern recognized by security experts. Figure 4 shows the workflow for defining the attack pattern parameters. These parameters can differ according to the target domain and the phase of the SDLC.

In this paper, we define the parameters that are applicable in the early stages of development of an NPP I&C system. The parameters are defined on the basis of cybersecurity experience in the NPP field, a standard related to nuclear power reactors, and a threat modeling methodology, as follows: the items for the attack surface parameters were determined from experience working in cybersecurity, those for the *M* (method) using the threat categories of Microsoft's STRIDE model, and those for RD (related data) by referring to IEEE 1615 [23]. Table 1 presents the predefined parameters for NPP attack patterns.

This formalized attack pattern can be used to represent an attack method by assigning one of the parameters values to each element. For example, Figure 5 depicts a man-in-the-middle (MITM) attack. The MITM attack is one in which the attacker secretly relays and possibly alters communications between two parties who believe they are communicating directly. In this example, we assume that a user and a web application are communicating to transmit control commands; an attacker attempts to retransmit the commands by tampering with the control data transferred between the systems.

The proposed method represents this attack as a formalized attack pattern. To generate a formalized attack pattern, we use the predefined parameters for the target domain listed in Table 1. The formalized attack pattern of the MITM can be represented as follows:

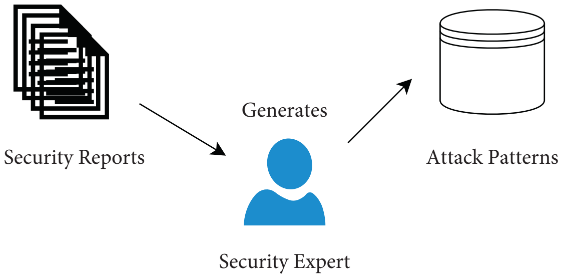

Figure 4: Workflow for generating attack pattern data.

$$AP_{\text{MITM}} = (((S, WN, P), T, CH, C\ D). \tag{5}$$

In this example, the attack surface is represented by the system as the EE, a wired network as the CH, and a platform service as the SRV. The method of attack is tampering, the attack target is the channel, and the type of related data is control data.

By analyzing it in this way, a given attack technique can be expressed as a formalized attack pattern.

4. Security Control Pattern

The security control pattern is a concept map for assigning the security controls of RG 5.71 according to the attack pattern. A security control is a security requirement for a system, described in natural language. The proposed method defines a security control pattern for selecting the appropriate security controls for a given system.

In the classification criteria, RG 5.71 categorizes security controls into technical, operational, and management security controls [4]. Because this regulatory guidance categorization presents only primary properties, a developer

Table 1: Attack pattern parameters for the instrumentation and control (I&C) system of a nuclear power plant (NPP).

Element		Items
Attack surface	EE	User(U), system(S), device(D)
	CH	Direct access (DA), direct wired (DW), wired network (WN), wireless network (LN)
	SRV	Application service (A), platform service (P), maintenance service (M)
M		Spoofing (S), tampering (T), repudiation (R), information disclosure (I), denial of service (D), escalation of privilege (E)
AT		EE, CH, SRV
RD		Nonoperational data (ND), operational data (OD), control data (CD), security and configuration data (SD)

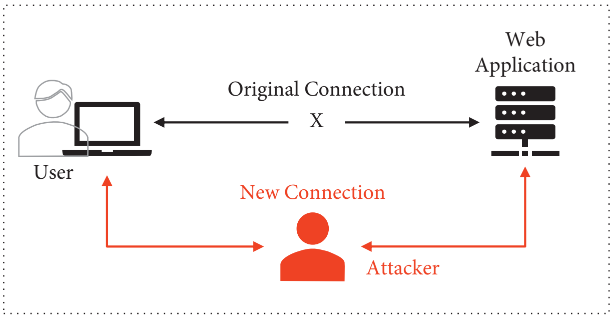

Figure 5: Man-in-the-middle attack.

needs further understanding of the security controls in order to decide whether a given security control is necessary to protect the system in question. We define three classification criteria and their specific items for the security controls as shown in Figure 6.

(i) Applicable target: this item is the abstract-level component of the system and its environment. It is a target entity in which a security control can be implemented. Tags: user, platform and OS, application, and channel.

(ii) Security principle: this item is the security principle that can defend against STRIDE threats [24]. We additionally include "hardening," defined as a system security enhancement regardless of the threat. Tags: authentication, authorization, nonrepudiation, confidentiality, integrity, hardening, and availability.

(iii) Life stage: this item identifies the phase in the system's life cycle. Because the regulation describes the security controls from an operational point of view, the developer needs to identify the items to be considered during the development and maintenance phases. Tags: development stage, operation stage, maintenance stage, and disposal stage.

These three criteria can be used to categorize each security control, and each classification result can be linked to an attack pattern parameter. We defined the criteria with consideration of the parameters of the formalized attack pattern and whether the security control is applicable. We applied the tags to the security controls in RG 5.71 using a heuristic approach.

The relationship between the three dimensions of the security control pattern and the elements of the attack pattern is shown in Figure 7. This relationship provides the foundation for the systematic selection of specific security controls for a given system.

Figure 7 shows the relationship between the attack pattern and the security control pattern. The applicable target of the security control pattern is the component where the security requirements are fulfilled within the system and its operational environment; it is related to the attack target of the attack pattern. In other words, the applicable target element should have security functionality.

The life cycle of the security control pattern comprises four stages: development, operation, maintenance, and disposal. This element limits the application of security controls by the stage of the system's life cycle.

The security principle of the security control pattern is a technical feature of the security control. It supports selection of the proper method of defense against the threat, as the security controls should be applied differently depending on the method of attack. The security principle is mapped from the attack method of the attack pattern. Our method uses the STRIDE threat categories and their corresponding security properties [24].

In the proposed approach, the attack method is used to select the security principles to apply to the system. Once the method of attack is determined, the security principles are chosen automatically. Table 2 shows the security principle corresponding to each method of attack. This relationship is based on the STRIDE methodology [24].

The RD type is used to determine whether the attack pattern is valid in the target system. If the importance of the data type is low, this element allows us to determine that the security control is unnecessary for the target system. The attack surface and RD type determine whether the attack pattern is valid in the target system. The attack target is the component in which the security control should be implemented. The life stage determines when the security control should be developed. Figure 8 shows the relationship between the attack target of the attack pattern and the applicable target of the security control pattern.

5. Case Study: Plant Protection System (PPS) Application

To demonstrate the effectiveness of the proposed approach, we applied the method to an I&C system of a nuclear power plant. Typically, information related to the design and architecture of NPPs is not publicly available. Therefore, we conducted the case study using the information in a

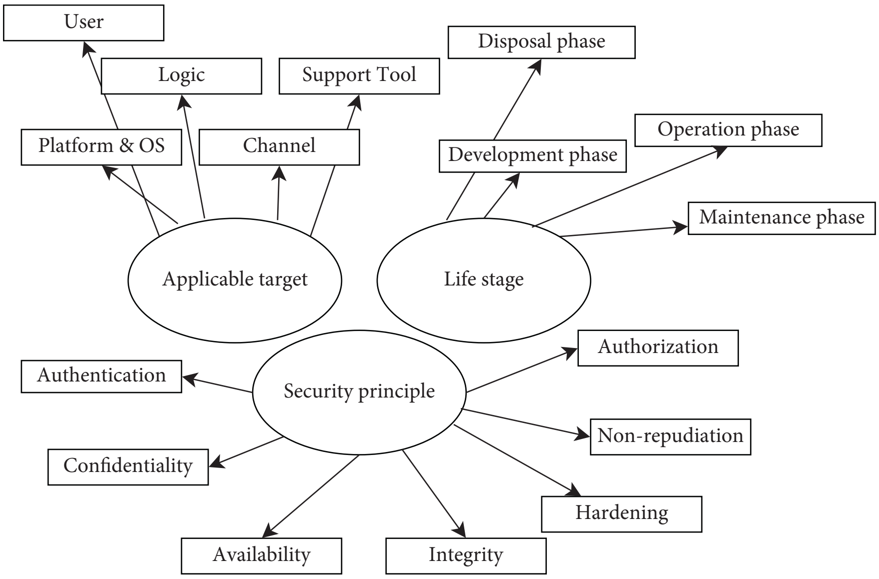

Figure 6: Classification criteria.

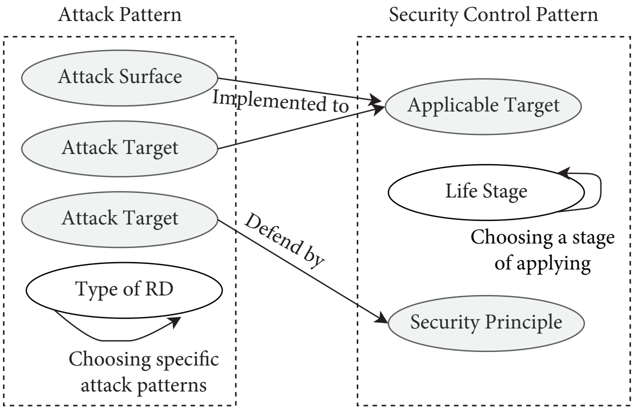

Figure 7: Relationship between attack pattern and security control pattern.

Table 2: Mapping between methods of attack and security principles.

Attack Method	Security principle
Spoofing	Authentication
Tampering	Integrity
Repudiation	Nonrepudiation
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization
-	Hardening

published paper by Song et al. [8], which describes the Plants Protection System (PPS) used in their security analysis, which we chose as our target system.

We performed the case study in three phases:

(i) *Phase 1.* Analyzing the target system

(ii) *Phase 2.* Identifying attack patterns for the specific system

(iii) *Phase 3.* Selecting the candidate set of security controls.

5.1. Overview of Target System. We conducted the case study selecting the security controls for an NPP I&C system. In [8], Song et al. introduced the high-level concepts of the Plant Protection System (PPS) for modeling security. The published description provides sufficient information about PPS to use in applying our method to it. Figure 9 provides an overview of PPS based on the information presented in the paper.

PPS is composed of three programmable logic controllers (PLCs) and two industrial PCs. They connect through an N-to-N network and a one-to-one network. An engineering workstation (EWS) performs the logic update and system configuration for the PLCs through a dedicated maintenance port during the sole maintenance phase. The OM and MTP, based on industrial PCs, provide the human-machine interface.

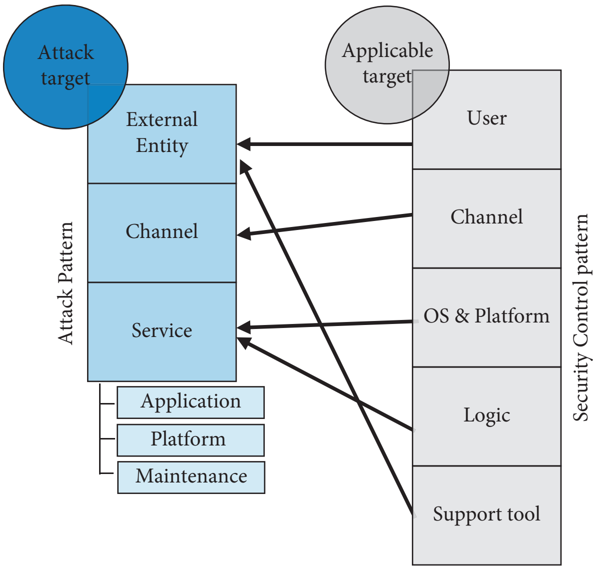

Figure 8: Relationship between attack target and applicable target.

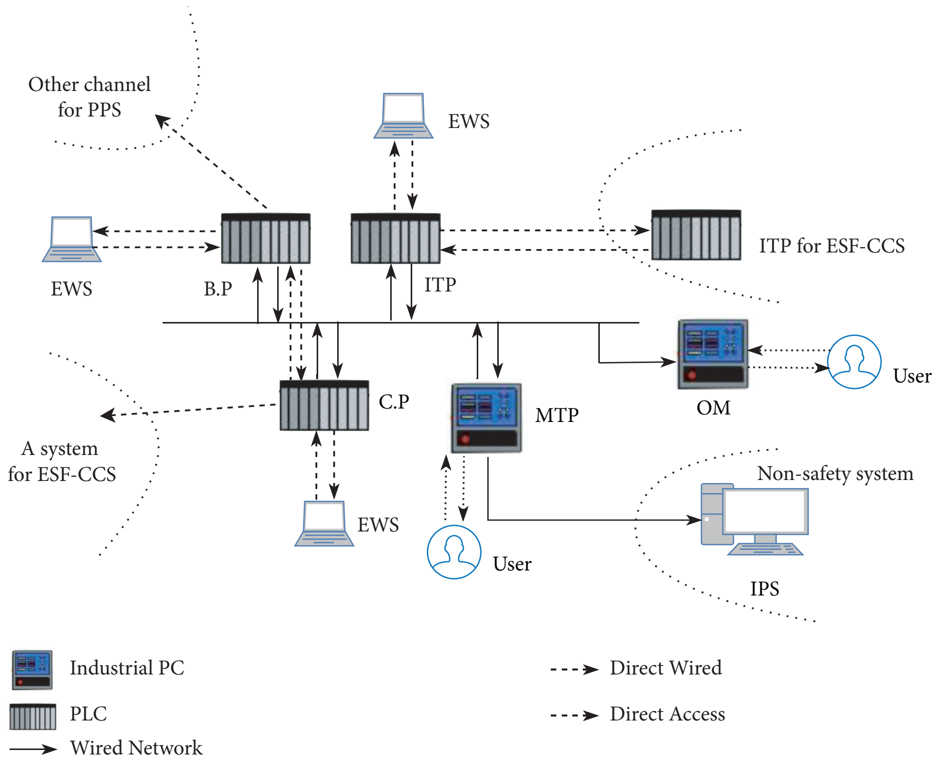

Figure 9: Overview of plant protection system (PPS).

5.2. Attack Pattern Data. The proposed method assumes that a security expert has generated customized attack pattern data for the target system on the basis of known attack cases. For the case study, we reviewed cases of attacks on the industrial control system and vulnerability analysis reports because vulnerabilities of NPP I&C systems are generally not made public [25–27].

It is challenging to apply our method using vulnerability analysis reports because specific information about the system is necessary. Therefore, we used data presented by the SANS Institute to generate the attack patterns for this case study [25]. Table 3 gives an example of an attack description from the SANS report [25].

The report is also written in natural language. If a system has a human-machine interface (HMI), the attacker can attack by accessing the interface directly. We can identify the attack pattern from the HMI description as given in Table 4.

Table 3: Example of an attack description.

Human-machine interfaces (HMIs)
- Can be a traditional indicator and switch-based - Can be serial interface based - Can be network-based - Most modern HMIs are now web interfaces - Some leverage web services to a user front-end - Some older ones may use RPC calls - If we can gain access to the HMI, we can often control the system

Table 4: Example of an attack pattern expression (human-machine interfaces (HMIs)).

SUB-ID	Attack surface			M	AT	RD
	EE	CH	SRV			
SANS–ICS–01-01	User	Authorization	Application, platform	EP	SRV	CD
SANS–ICS–01-02	System	Authorization	Application, platform	EP	SRV	CD
SANS–ICS–01-03	System	Authorization	Application, platform	EP	SRV	CD

5.3. Phase 1: Analyzing the Target System. This section provides the results of the attack surface analysis performed in the first phase of our method. In this phase, we analyzed each subsystem of the PPS. The result includes the input/output connections of the subsystem and enumerates them. We used the description of PPS in Song et al.'s paper to analyze its subsystems [8]. Figure 10 shows the analysis target subsystems of PPS.

We performed the analysis for six PPS subsystems: BP, ITP, CP, MTP, OM, and EWS. We analyzed only one EWS because all EWSs have the same connectivity.

5.4. Phase 2: Identifying Attack Patterns for the System. In the second phase, we identified the attack patterns for each subsystem according to the element of the AS. Our review focused on all entry points. A number of attack patterns were extracted for each subsystem; the counts are shown in Figure 11.

5.5. Phase 3: Selecting the Security Controls Candidate Set

5.5.1. Parameters for Selecting Security Controls. Our approach chooses security controls based on the attack target and attack method of the attack pattern elements (Figure 8). The parameters assigned for the attack pattern groups in this case study are listed in Tables 5–7.

5.5.2. Security Controls for BP. By applying the proposed method to BP, it was determined that security controls should be applied in (1) the BP logic applications and (2) the BP channels. Figure 12 illustrates the application of security controls in these target components of the BP network architecture. BP needs to implement the security controls in the BP Logic and communication channel as presented in Tables 8 and 9.

5.5.3. Security Controls for MTP. By applying the proposed method to MTP, it was determined that security controls should be applied in (1) the MTP logic and (2) the MTP platform. Figure 13 illustrates the application of security controls in these target components of the MTP network architecture. MTP needs to implement the security controls in the MTP Logic and Platform as presented in Tables 10 and 11.

5.5.4. Security Controls for EWS. By applying the proposed method to EWS, it was determined that security controls should be applied in (1) the EWS logic and (2) the EWS platform. Figure 14 illustrates the application of security controls in these target components of the EWS network architecture.

EWS also needs to implement the security controls related to the user interface. In many attack cases, the access privileges of an unauthorized user are expanded because EWS provides an interface for configuring the PLC. Tables 12 and 13 list the security controls that should be applied to each component.

5.5.5. Effectiveness Comparison. Although it is difficult to perform a quantitative evaluation by comparing the method presented in this paper with the process, we can discuss its effectiveness by comparing the numbers of people who need to be involved in the project.

Under the expert review method (the method in use today), many system developers and security experts are involved in analyzing a system (e.g., PPS), and this group of experts participates in multiple review meetings. Considering the scope and complexity of a nuclear power plant's I&C system, the time cost of review meetings is very high. In addition, it is not easy to apply a method in a domain in which many experts proceed simultaneously, because of the need to maintain consistency of security for compliance with regulations.

The proposed method, on the other hand, can be performed with a minimal number of people once the initial analyses, such as the attack surface analysis and domain attack pattern analysis, have been completed. Thus, this

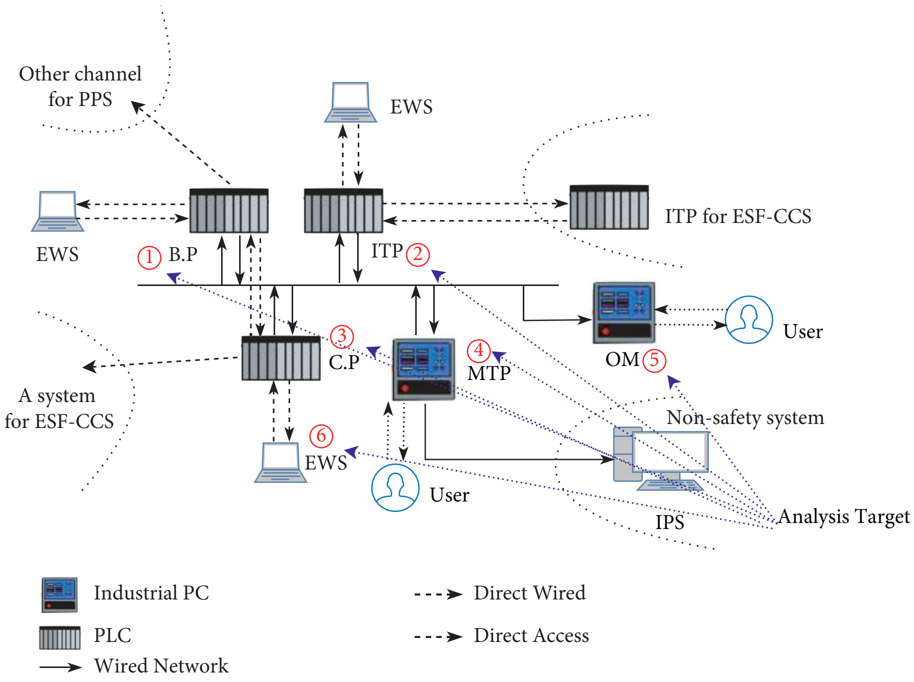

FIGURE 10: Analysis target subsystems of PPS.

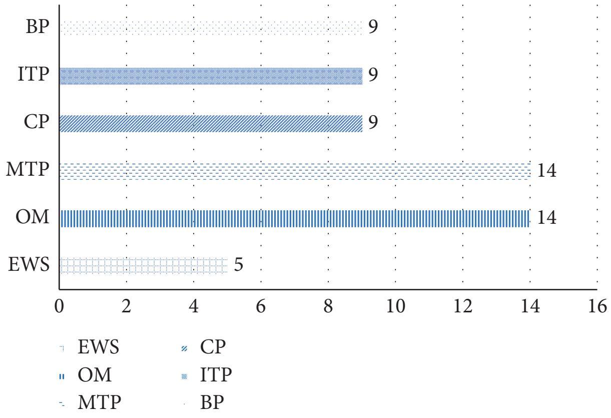

FIGURE 11: Count of attack patterns for each subsystem.

TABLE 5: Parameters for BP, ITP, and CP.

Attack surface	Parameter of the security control		
	Applicable target	Security principle	Life stage
(S,DW,M)	Logic	Authorization	Development
(S,DW,A)	Logic	Authorization	Development
	Logic	Authorization	Development
(S,WN,A)	Logic	Authentication	Development
	Channel	Confidentiality	Development

Table 6: Parameters for MTP and OM.

Attack surface	Parameter of the security control		
	Applicable target	Security principle	Life stage
(S,WN,A)	Logic	Authorization	Development
	Logic	Authentication	Development
(U,DA,A)	Logic	Authentication	Development
	Logic	Authorization	Development
(U,DA,P)	OS and platform	Authorization	Development

Table 7: Parameters for engineering workstation (EWS).

Attack surface	Parameter of the security control		
	Applicable target	Security principle	Life stage
(S,DW,M)	Logic	Authorization	Development
(U,DA,P)	OS and platform	Authorization	Development

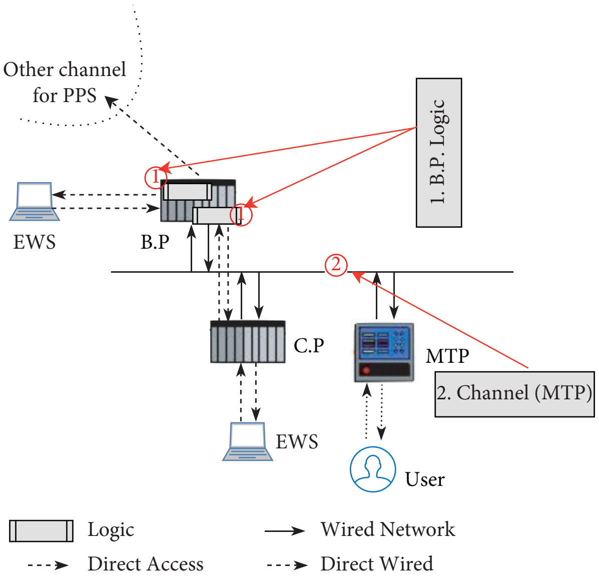

Figure 12: Application of security controls in the target components of BP.

Table 8: Security controls for BP logic.

Target component	Security controls
BP logic	B.1.2 account management B.1.3 access enforcement B.1.5 separation of functions B.1.7 unsuccessful logic attempts B.1.9 Previous logon notification B.1.10 session lock B.3.19 thin nodes B.4.2 user identification and authentication B.4.3 Password requirements B.5.8 authenticator feedback

Table 9: Security controls for BP channels.

Target component	Security controls
Channel (to MTP)	B.3.7 transmission confidentiality B.3.12 transmission of security parameters

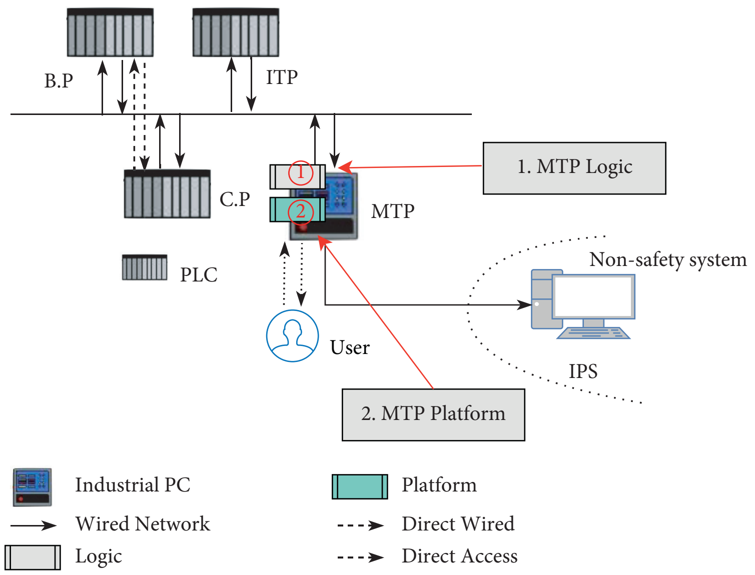

Figure 13: Application of security controls in the target components of MTP.

Table 10: Security controls for MTP logic.

Target component	Security controls
MTP logic	B.1.2 account management B.1.3 access enforcement B.1.5 separation of functions B.1.7 unsuccessful logic attempts B.1.9 Previous logon notification B.1.10 session lock B.3.19 thin nodes B.4.2 user identification and authentication B.4.3 Password requirements B.5.8 authenticator feedback

Table 11: Security controls for MTP platform.

Target component	Security controls
MTP platform	B.1.2 account management B.1.3 access enforcement B.1.5 separation of functions B.1.6 least privilege B.1.7 unsuccessful logic attempts B.1.8 system use notification B.1.9 Previous logon notification B.1.10 session lock B.1.22 use of external systems B.2.9 Protection of audit information B.2.10 nonrepudiation B.3.2 application Partitioning and security function isolation B.3.11 unauthorized remote activation of services B.3.13 public key infrastructure certificates B.3.19 thin nodes

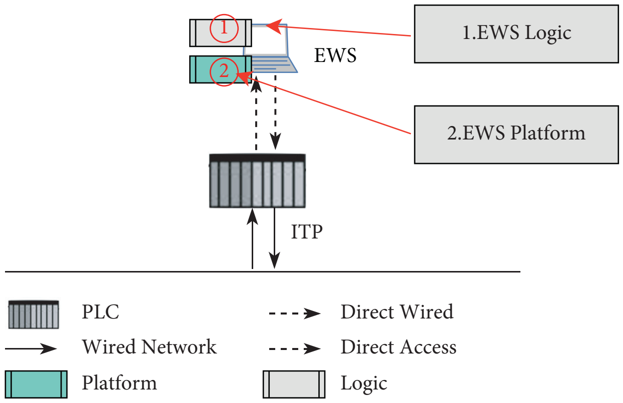

Figure 14: Application of security controls in the target components of EWS.

Table 12: Security controls for EWS logic.

Target component	Security controls
EWS logic	B.1.2 account management B.1.3 access enforcement B.1.5 separation of functions B.1.7 unsuccessful logic attempts B.1.8 system use notification B.1.9 Previous logon notification B.1.10 session lock B.3.19 thin nodes

Table 13: Security controls for EWS platform.

Target component	Security controls
EWS platform	B.1.2 account management B.1.3 access enforcement B.1.5 separation of functions B.1.6 least privilege B.1.7 unsuccessful logic attempts B.1.8 system use notification B.1.9 Previous logon notification B.1.10 session lock

method can reduce the time cost of review meetings and maintain consistency of security across systems.

Because the proposed method can reuse the results of the initial analysis for successive products, it is cost effective. In addition, safety-critical systems such as NPP I&C systems are themselves more cost effective because their function does not change significantly.

6. Discussion

The proposed method identifies the appropriate security controls for a target system by examining it from an attacker's point of view. However, the developer has an additional perspective to consider before applying the specified controls. Because an NPP I&C system is a safety-critical system, it is crucial to maintain a safe status. Therefore, after determining whether a control is technically applicable to a system or channel, the developer should employ a method that avoids conflict between safety requirements and security requirements.

For the proposed method to be applied, it is necessary to obtain and maintain the latest attack pattern data. Because the suitability of the security controls selected for the system depends on the freshness of the attack pattern data, obtaining the newest attack pattern data is vital.

The proposed method systematically provides a candidate set of security controls. However, if the method is not available in an automated form, a developer must repeatedly perform the task of selecting security controls manually. Therefore, to improve the practicality of the model, it is necessary to implement it as an automated tool.

7. Conclusion

We have proposed a systematic compliance-driven method in this paper. This approach supports the system developer in deciding in the early stages of development whether specific security controls apply to the system. The method can automatically choose a set of appropriate security controls for the system if the developer can identify the attack surface and the data that pass through it. We demonstrated the method's application using a case study. Assuming that the attack pattern data are updated sufficiently often and that security experts perform multiple checks on the security control patterns, the method can enhance the security of NPP I&C systems. Although we did not discuss cost efficiency in this paper, given the human resources required by the existing approach, such as those needed to conduct a preliminary penetration test [7], we can expect that the proposed method will be more cost efficient. This paper deals only with NPPs, but we believe the proposed method would also be highly suitable for application to systems in other government-regulated industries, such as the automotive industry [28].

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request after acceptance.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by National Research Foundation of Korea (NRF) grants funded by the Korea government (MSIT) (2021R1I1A1A01040308) and Hwarang-Dae Research Institute of Korea Military Academy.

References

[1] W. Stuxnet, "stuxnet 2021," August-2021, https://en.wikipedia.org/wiki/stuxnet%202021.

[2] R. Langner, "Stuxnet: dissecting a cyberwarfare weapon," *IEEE Security and Privacy Magazine*, vol. 9, no. 3, pp. 49–51, 2011.

[3] M. Muckin and S. C. Fitch, *A Threat-Driven Approach to Cyber Security*, Lockheed Martin Corporation, MD, USA, 2014.

[4] U.N.R. Commission, *Cyber Security Programs for Nuclear Facilities*, US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Rockville, MD, USA, 2010.

[5] U.N.R. Commission, *Protection of Digital Computer and Communication Systems and Networks*, US Nuclear Regulatory Commission, Rockville, MD, USA, 2009.

[6] R. M. Blank, *Guide for Conducting Risk Assessments*, CreateSpace Independent Publishing Platform, Scotts Valley, CA, US, 2011.

[7] S. Song, M. Lee, T. Kim, C. Park, S. Park, and H. Kim, *A Case Study on Cyber-Security Program for the Programmable Logic Controller of Modern Npps*, IAEA, Vienna, Austria, 2014.

[8] J.-G. Song, J.-W. Lee, G.-Y. Park, K.-C. Kwon, D.-Y. Lee, and C.-K. Lee, "An analysis of technical security control requirements for digital I&c systems in nuclear power plants," *Nuclear Engineering and Technology*, vol. 45, no. 5, pp. 637–652, 2013.

[9] J.-C. Loh, S.-H. Heng, S.-Y. Tan, and K. Kurosawa, "On the invisibility and anonymity of undeniable signature schemes," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 11, pp. 18–34, 2020.

[10] A. Abhishta, W. Van Heeswijk, M. Junger, L. J. M. Nieuwenhuis, and R. Joosten, "Why would we get attacked? an analysis of attacker's aims behind ddos attacks," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 11, pp. 3–22, 2020.

[11] A. L. Marra, F. Martinelli, F. Mercaldo, A. Saracino, and M. Sheikhalishahi, "D-bridemaid: A distributed framework for collaborative and dynamic analysis of android malware," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 11, pp. 1–28, 2020.

[12] Microsoft, *Microsoft Security Development Lifecycle (sdl)*, 2019.

[13] G. McGraw, "Software security," *IEEE Security and Privacy Magazine*, vol. 2, no. 2, pp. 80–83, 2004.

[14] O. Clasp, *Owasp Claps Project*, 2015.

[15] F. Valenza and M. Cheminod, "An optimized firewall anomaly resolution," *Journal of Internet Services and Information Security (JISIS)*, vol. 10, pp. 22–37, 2020.

[16] P. Mell and T. Grance, *Use of the Common Vulnerabilities and Exposures (cve) Vulnerability Naming Scheme*, National Inst Of Standards And Technology Gaithersburg Md Computer Security Div, Gaithersburg, MD, US, 2002.

[17] R. A. Martin, *Common Weakness Enumeration*, Mitre Corporation, Virginia, USA, 2007.

[18] L. König, S. Unger, P. Kieseberg, and S. Tjoa, "The risks of the blockchain a review on current vulnerabilities and attacks," *Journal of Internet Services and Information Security (JISIS)*, vol. 10, pp. 110–127, 2020.

[19] A. Jaschob and L. Tsintsifa, "It-grundschutz: two-tier risk assessment for a higher efficiency in it security management," in *Proceedings of the ISSE 2006 - Securing Electronic Busines Processes, Highlights of the Information Security Solutions Europe 2006 Conference*, pp. 95–101, Springer, Rome, Italy, October 2006.

[20] A. Gillies, "Improving the quality of information security management systems with iso27000," *The TQM Journal*, vol. 23, no. 4, pp. 367–376, 2011.

[21] O. Potii, O. Illiashenko, and D. Komin, "Advanced security assurance case based on iso/iec 15408," in *Proceedings of the International Conference On Dependability And Complex Systems*, pp. 391–401, Springer, Brunów, Poland, June 2015.

[22] C. Theisen, N. Munaiah, M. Al-Zyoud, J. C. Carver, A. Meneely, and L. Williams, "Attack surface definitions: a systematic literature review," *Information and Software Technology*, vol. 104, pp. 94–103, 2018.

[23] S. Tom, D. Christiansen, and D. Berrett, *Recommended Practice for Patch Management of Control Systems*, Technical Report, Idaho National Laboratory (INL), D, USA, 2008.

[24] A. Shostack, *Threat Modeling: Designing for Security*, John Wiley & Sons, J, USA, 2014.

[25] E. C. Sans, *Ics Attack Surfaces*, 2017.

[26] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on scada systems," in *Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, pp. 380–388, IEEE, Dalian, China, October 2011.

[27] K. Stouffer, J. Falco, K. Scarfone, M. Abrams, and A. Hahn, "Guide to industrial control systems (ics) security," *NIST Special Publication*, vol. 800, no. 82, p. 16, 2011.

[28] National Highway Traffic Safety Administration (NHTSA) and Department of Transportation (DOT)., "Cybersecurity best practices for modern vehicles," *Report No. DOT HS*, vol. 812, no. 333, pp. 17–20, 2016.