J Supercomput (2018) 74:1378–1393
https://doi.org/10.1007/s11227-017-2034-6

An analytical method for developing appropriate protection profiles of Instrumentation & Control System for nuclear power plants

Manhyun Chung[1] · Woogeun Ahn[2] · Byunggil Min[2] · Jungtaek Seo[3] · Jongsub Moon[1]

Published online: 13 April 2017

Abstract A very important target of Instrumentation & Control System used in nuclear power plants is to ensure the safe operation of these plants. Until recently, an analog technology has been used for this purpose; however, this is now being replaced by the digital technology. Such replacement is facilitated by the wide use of real-time distribution of data that are collected by sensor devices of machine-to-machine technology. This, however, provides possibility of exposing Instrumentation & Control System to cyber-attack, as was the case for the Iranian Bushehr nuclear power plant, which the centrifuge was destroyed by the malicious code, Stuxnet. Therefore, security products which are exclusively developed for the prevention of cyber-attack on nuclear power plants are particularly needed in the development and operation of Instrumentation & Control System. However, the currently available security guidelines for such Instrumentation & Control System cover only security policies and protocols, without any specific reference urgent issues of cyber-attack. This paper proposes an implementable Instrumentation & Control System analysis model having focus on cyber security and technology evaluation. The model has been already implemented in reactor protection systems that is operating in Republic of Korea.

Keywords Instrumentation & Control Systems · Nuclear power plants · Cyber-attack · Standard Common Criteria · Cyber security

✉ Jongsub Moon
jsmoon@korea.ac.kr

Manhyun Chung
manhyun4@korea.ac.kr

[1] Korea University, Seoul, Republic of Korea

[2] National Security Research Institute, Daejeon, Republic of Korea

[3] Soonchunhyang University, Asan, Choongnam, Republic of Korea

1 Introduction

The Instrumentation & Control System (I&CS) used in a nuclear power plant measures, controls, protects, and monitors the plant to ensure the safe operation of the power plant. This includes both safety and non-safety class systems.

The safety system and non-safety systems are divided into many subordinate systems according to their specific functions [1]. In the past, I&CS consisted of only analog technology. However, the system has begun to incorporate digital technologies such as computers and data networks [1,2]. Currently, nuclear power plants which are in operation have higher ratio of analog technology than the new ones being built, and the ratio is fast growing [1,2].

The importance of cyber security is growing due to the emergence of digital technology. In 2010, the appearance of Stuxnet [3], which destroyed the centrifuge of the Iranian Bushehr nuclear power plant, showed that nuclear power plants are prone to cyber-attack. Those responsible for the safety of these plants then realized that such threats should not be overlooked any longer. Cyber-attack on I&CS can result in system malfunction and data alteration, and if it is not brought under control, it can lead to the reactor core melt down or to cause exposure to radiation that can lead to a large-scale life threatening disaster. In this context, the cyber security of I&CS is an urgent issue.

As a solution to the security of the system, many cyber security guidelines for nuclear power plants are available. However, the security technology recommended in these guidelines is not implementable to currently operating plants, nor to those under construction. Furthermore, the distinct characteristics of I&CS and the difficulty of data collection due to classified nature makes it a challenge to incorporate the cyber security technology used in other IT systems.

For this reason, it is necessary to develop a security technology suitable for nuclear I&C. Therefore, this paper proposes a method to make security technology development requirements by using the Protection Profile (PP) which is a component of the Common Criteria (CC). Per ISO/IEC 15408, CC is a set of criteria used to evaluate the security of IT systems and information security products. Protection Profile of CC is to allow consumer groups and communities of interest to express their security needs. Also it has a set of functions and assurance requirements which stipulates the security objectives of the designated Target of Evaluation (TOE) [4].

To list the PP, it is necessary to state the scope of the product precisely. For this, the environment, security objective and the security function requirements should be identified. Furthermore, the security environment, including potential threats and security policy of the organization, should be analyzed. In addition, it is necessary to focus on all possible threats and to analyze them during risk analysis. In other words, to list a suitable PP, the threats in the operating environment, the security policy of the organization, and the operational assumptions should first be analyzed. Subsequently, the security function requirements should also be defined.

However, even in the CC, there is no specific method for devising security function requirements and performing security environment analysis. It only describes the criteria for security products that apply to general IT systems. An I&CS is different from a general IT environment in which the data collection is readily achieved.

This work proposes an analysis method which is currently used for I&CS in the operating group of a nuclear power plant in Republic of Korea.

The presentation of this paper is as follows. In Sect. 2, discussion is given on current trends in formulating guidelines for strengthening cyber security in the nuclear power plant and the composition process of the PP. Section 3 proposes a system analysis method for security used in I&CS of a nuclear power plant. In Sect. 4, results of the implementation of the proposed method are given. In Sect. 5, conclusions are made and discusses the future work.

2 Related work

2.1 Trends in cyber security guidelines

The US Nuclear Regulatory Commission (NRC) has published a Regulatory Guide (RG) 5.71 for protection against cyber-attacks on digital computers, communication systems and networks of nuclear facilities. RG 5.71 is a more practical guideline than the cyber security legislation, US Code of Federal Regulations 73.54, whose purpose is to implement comprehensive security control methods and defensive systems in relation to Critical Digital Assets (CDA), in order to handle cyber security threats. Also, it defines the cyber security implementation scope according to the SSEP (Safety, Security and Emergency Preparedness) protocols performing CDA [5]. “Appendix A” in RG 5.71 provides a cyber security scheme, and Appendices B and C list methods to handle potential cyber security threats on the CDA, informed by the National Institute of Science and Technology (NIST) SP 800-53 and 800-82 [6].

The NIST criteria include 100 security requirements which are classified to 18 types. These types are divided into 3 fields: technology, operation and management [7,8].

Nuclear Security Series (NSS) No. 17 describes technical guidance on the implementation and recommendations to ensure security and safety of nuclear facilities. This includes control systems, networks and information systems, cyber threats, etc. In addition, it considers cyber security requirements exclusively for nuclear facilities in tandem with other criteria and ISO 27000 series.

Part I of NSS No. 17 helps to determine cyber security-related policies and administrative structures. Also, to provide a guideline for restrictions on and management of cyber security. Part II provides a technological and administrative guideline for the fulfillment of comprehensive cyber security schemes [9].

2.2 The Protection Profile (PP) of Common Criteria (CC)

The International Common Criteria were established to bring about compatibility among the different evaluation criteria of various countries. It is composed of three sections.

In Sect. 1, general models explain the terms and definitions used in the CC of general models. In Sect. 2, security function requirements classify the security functions needed in security products. In Sect. 3, security requirements elaborate the functions

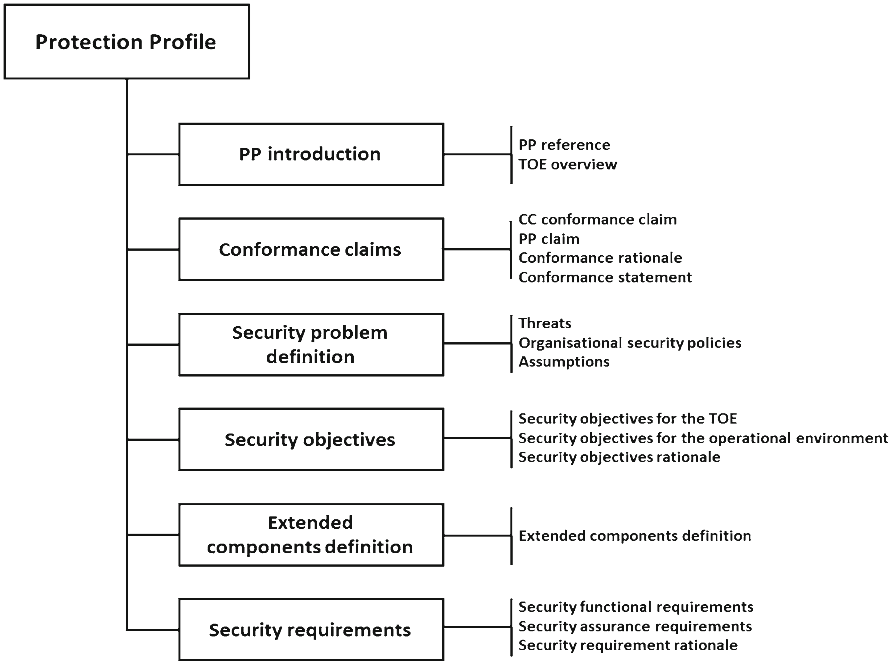

Protection Profile
PP introduction
PP reference
TOE overview
Conformance claims
CC conformance claim
PP claim
Conformance rationale
Conformance statement
Security problem definition
Threats
Organisational security policies
Assumptions
Security objectives
Security objectives for the TOE
Security objectives for the operational environment
Security objectives rationale
Extended components definition
Extended components definition
Security requirements
Security functional requirements
Security assurance requirements
Security requirement rationale

Fig. 1 The contents of Protection Profile [4]

and assurance requirements which information protection systems should perform and meet [4].

The Protection Profile (PP) which constitutes Common Criteria (CC) is a set of functions and assurance requirements which stipulates the security objectives of the designated Target of Evaluation (TOE). The PP of a potential product is first evaluated by the CC evaluation group and documented by a registered institution and is subsequently published. After publication, the product is developed.

Since the PP is a security function requested by users and must have a particular TOE, it should minimize the scope of its technical references, so that they are comprehensible to the user. Figure 1 shows and explains the essential elements of the PP.

3 A proposed method for analyzing the Instrumentation & Control Systems of nuclear power plants

This chapter proposes a method for deducing basic information in order to devise the components of PP. Figure 2 shows steps to analyze the Instrumentation & Control of Nuclear Power Plants. The detailed description of each step is as follows.

The first step of the proposed method is to analyze I&CS and identify its characteristics. In this step, various hardware nodes and network connections between nodes using interfaces are identified. Secondly, the analyzed information and iden-

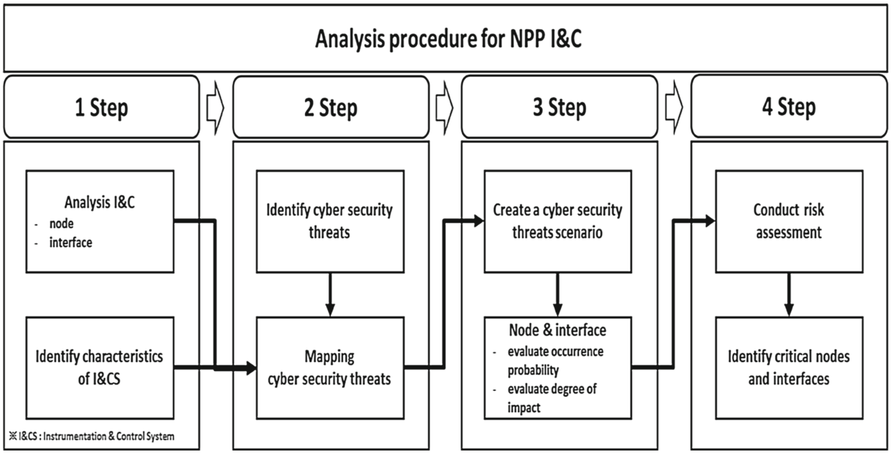

Analysis procedure for NPP I&C
1 Step
2 Step
3 Step
4 Step
Analysis I&C
- node
- interface
Identify characteristics of I&CS
※I&CS : Instrumentation & Control System
Identify cyber security threats
Mapping cyber security threats
Create a cyber security threats scenario
Node & interface
- evaluate occurrence probability
- evaluate degree of impact
Conduct risk assessment
Identify critical nodes and interfaces

Fig. 2 The proposed analysis procedure for NPP I&C

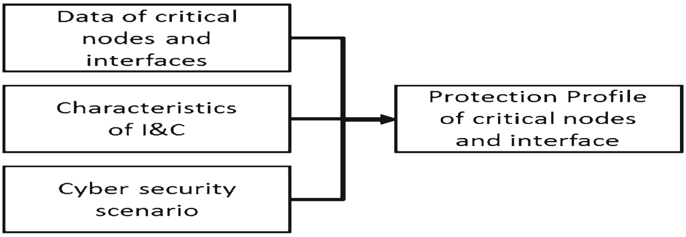

Data of critical nodes and interfaces
Characteristics of I&C
Cyber security scenario
Protection Profile of critical nodes and interface

Fig. 3 Method of devising Protection Profile

tified characteristics from the first step are used to depict cyber security threats. In addition, the second step includes the substance of the cyber threats found through both the interface information and node structure, which were previously analyzed in order to detect them if the threats are actualized. In the third step, an attack scenario is devised, and evaluate its degree of impact and occurrence probability on the node structure and interface proposed in the first step. Finally, a calculation on the degree of the risk with this information is made. The calculated degree of risk to the node structure and interface is used as a basis to decide whether the product should have a Protection Profile or not.

The analyzed data, the system characteristics and the potential cyber threats to the product are used as fundamental data in devising the Protection Profile as shown in Fig. 3.

The summary of the devised PP from Fig. 3 is listed in Table 1.

3.1 Analysis of the Instrumentation & Control System

A I&CS is divided into its safety and non-safety components, each of which has specific subordinate systems. In this section, specific subordinate systems are explained and

Table 1 Analysis results per application

Application	Results
PP introduction, security objectives	System analysis
Security problem definition of the organizations security policy and assumptions	System characteristics
Security problem definition of the threat items	Cyber threats
Degree of risk	Degree of risk
Decision on whether the product should have a PP	

Table 2 Node information form

Name	Explanation
Node definition	Definition of the node functions and characteristics

Table 3 Interface information form

Interface number	Related nodes	Exchanged data
Identifier	Nodes to which the interface is connected	Message information delivered through the interface

then propose a method to analyze their functions and the communication method of I&CS.

First of all, to analyze the structure and the functions of the system, the node structures of various hardware units are classified. For each hardware unit, the functions, hardware types, loaded software, and firmware versions/characteristics should be described. The format of the hardware nodes is shown in Table 2. Furthermore, the network-connected nodes are classified by an interface as shown in Table 3. Each interface is assigned as a unique identifier, and message information is delivered between the nodes.

The second stage is to identify the systems functions and the sequences stages by identifying each functional unit in terms of the use cases. Furthermore, the object, result and protocol of the function have to be identified. At this time, one should discover what is needed to prevent cyber threats from the security point of view by considering confidentiality, integrity and accessibility. All fields and the required content of each field are described in Table 4.

3.2 Identifying the characteristics of the Instrumentation & Control System

Before incorporating cyber security technology into the I&CS of a nuclear facility, an analysis of both the system and its characteristics, policies and operating environment are required. The I&CS also has a different implementation guideline from the func-

Table 4 Use case form

Use case identifier and name	The identifier is a unique number which one can classify from the whole use case list. It is composed of a domain-identifier-classification-sequence number (specific sequence alphabet)
Use case objective	The results of a successful performance of the use case procedure
Use Case explanation	An explanation of the use case objective
Security characteristics of the use case	Elaborates the security characteristics of the use case (the security characteristics should show the cyber threats which can occur in a use case, from the point of view of confidentiality, integrity and accessibility. The security characteristics describe a secure communication technique using an AES algorithm [10,11], an integrity technology like Diffie–Hellman algorithm [12] and/or other security elements)
Use case starting trigger	This explains what conditions are needed to start the use case
Use case scenario	This explains the specific sequential protocol required for the use case to achieve its goal

Table 5 Nuclear pant I&C characteristics

Characteristics	Specific information
Characteristic technology (example: communication protocol information)	Specific explanation of technology (example: safety systems use a Profibus [13], non-safety systems use a Modbus protocol [14])

tional point of view. Furthermore, to ensure the safety level of each sub-system, the I&CS uses multiplexing schemes, so that the malfunctioning of one system does not affect another. Also, the system has various characteristics, including its own unique components.

For the PP of the I&CS, the classification and characteristics of the system analysis described in Sect. 3.1, the policies used by the administrators, communication protocol information, system structure, and safety guarantee conditions should all be described. The format is shown in Table 5. In addition, some necessary items can be added and/or existing items can be extracted according to the characteristics of the system.

3.3 Identifying the cyber security threats and degree of risk of the Instrumentation & Control System

To judge whether or not the I&CS needs its security strengthened, we need to find the possible cyber threats and the degree of risk to the systems node and interface. In this section, we will devise a cyber security threat scenario using the system analysis

Table 6 Form of implementable cyber security threat in nuclear plant I&C

Classification	Cyber security threat
Identifier	Explanation of the cyber security threat

Table 7 Threat scenario form

Object	Threats	Explanation
Node/interface definition	Cyber security threat described in Table 6	Explanation of the potential cyber security threat to the system

resulted in Sects. 3.1 and 3.2 and then identify the characteristics of the cyber security threats. With this procedure, we can determine the degree of risk to the I&CS when the threat occurs.

To identify a potential cyber security threat to the I&CS, the cyber security threat data of IT and ICS from ENISA, US.ICS-CERT, NIST, etc. [7,8,15,16] are analyzed. The risk analysis method cannot be applied directly, but if it is modified to be implementable, it can be used on I&CS. The analyzed security threats are compared with the analysis results of 3.1 and 3.2 above. Then, induce a cyber security threat and classify it using a unique identifier. The induced threat is described as in Table 6.

Also, the threat scenario form is described in Table 7.

The next stage is to calculate the degree of risk of the cyber security threat to the node structure and interface. To calculate the degree of risk, a formula that originated from OWASP, OCTAVE, DREAD, etc., was used [17–19]. For this risk calculation, the cyber security threats degree of impact and degree of risk need to be utilized.

In this paper, the evaluation criteria for a cyber security threat are the boundary at which a cyber attacker or an attacking group can successfully initiate the threat to the system. The attackers ability, system status, attack opportunity, and intrusion detection probability are the elements included in the evaluation. There should be an explanation of the specific conditions and situations in which these elements are manifested. Furthermore, for the elements to be evaluated, their levels and scopes should be classified in advance. For each specific criteria, a score scale of 1–9 according to the occurrence probability was adopted. Scale 1 is the lowest probability, and the highest scale is 9.

Table 8 exhibits an example of the occurrence probability evaluation criteria. The detailed evaluation of an Attacker's techniques indicates the attacker's knowledge of the system. Attacker's techniques are an important evaluation standard for measuring the occurrence probability. It is used together with the results of three other evaluation standards: attack opportunity, intrusion detection possibility and vulnerability availability.

The evaluation criteria for calculating the potential degree of impact of the cyber security threat are the elements which influence the confidentiality, integrity and accessibility of the system. According to the occurrence results and the potential damage level, 1–9 scores are given to the degree of impact of a cyber security threat. 1 is the lowest probability, and the highest is 9. The higher the degree of impact the higher the score. Table 9 shows an example of the evaluation criteria for calculating the degree of impact.

Table 8 Occurrence probability evaluation criteria

Evaluation elements	Attacker′s techniques	
Explanation	The evaluation of the attacker′s technical level	
Criteria	Knowledge of the design and internal structure of the I&CS and attack code development ability	Evaluation score
		1
	Professional knowledge of hacking and techniques related to PT	Evaluation score
		3
	The ability to use open source attack tools	Evaluation score
		7
	Knowledge of IT	Evaluation score
		9

Table 9 Example of degree of impact evaluation criteria

Evaluation elements	Accessibility damage	
Explanation	Evaluation of the damage and node (system)/interface out-of-service period	
Criteria	Node (system)/interface normal operation	Evaluation score
		1
	Node (system)/interface temporarily out of service	Evaluation score
		5
	Node (system)/interface completely out of service	Evaluation score
		9

The elements of occurrence probability and the degree of impact can be added to or extracted from the system. There are many methods for risk calculation [7,19,20]. This paper uses the most common formula (1), which is:

$$\text{Risk} = \text{occurrence probability(likelihood)} * \text{impact}. \tag{1}$$

The average value of the likelihood and the average value of the impact are used to derive Eq. 2. Professionals from the nuclear and cyber security fields should devise the boundaries to delineate the criteria for degrees of impact, which are high, medium, and low risks.

$$\text{RISK} = \frac{1}{N}\left(\sum_{i=1}^{N} L_i\right) \times \frac{1}{M}\left(\sum_{j=1}^{M} I_j\right) \tag{2}$$

- L_i: Score of each Likelihood
- I_j: Score of each Impact
- N: Number of elements of Likelihood
- M: Number of elements of Impact
- i: $1, \ldots, N$
- j: $1, \ldots, M$

4 Example of the implementation of an Instrumentation & Control System analysis method

This chapter demonstrates the I&CS analysis method explained in chapter 3 and implements it on a reactor protection system [21,22]. The reactor protection system (RPS) constantly monitors the safety variables. If their values exceed the predefined safety boundary, it quickly halts reactor operation and maintains the integrity of the reactor coolant system. RPS consists of a bi-stable processor (BP), coincidence processor (CP), automatic test and interface processor (ATIP), and a cabinet operator module (COM) similar to PLCs and industrial PCs.

4.1 Analysis of the reactor protection system

The structure of the nodes is comprised of three PLCs and one industrial PC, as shown in Table 10. In addition, between the nodes or between a node and a system, there are

Table 10 Nodes of reactor protection system

System name	Explanation
BP	The PLC which decides whether to send a trip signal depending on the process measurement value or the digital input
CP	The PLC which emits the reactor stop signal and the ESF-CCS by receiving trip signals from its own channel BP or others
ATIP	The PLC which collects status information of modules and tests if they are operating properly
COM	The system which collects information from the ATIP and delivers it to the operator

Table 11 Interface of reactor protection system

Interface number	Related systems		Exchange data
E1	BP	CP	Trip information
E2	BP	ATIP	BP status information and test results
E3	CP	ATIP	CP status information and test results
E4	ATIP	OM	ITP collection information
E5	ATIP	BP, CP	Status test trigger information
E6	CP	ESF-CCS	Trip trigger information

Table 12 Reactor Protection System (RPS) Use case

RPS-1-01 domain
Objective
Trip decision depending on the conditions configured by the internal BP
Explanation
The input module receives a process measurement value or a digital input, compares it with the condition and configuration, then decides whether a trip signal should be sent or not
Security characteristics
Confidentiality confidentiality service is needed to prevent sensor data leakage. Confidentiality means the use of an encryption/decryption method in the course of data communication
Integrity integrity service is needed to prevent the sensor data from being tampered with. The method includes a simple hash function like MD5 to Diffie–Hellman algorithm
Accessibility the BP receiving module should run continuously and the communication equipment and network infrastructure should operate normally. There should be secondary systems to ensure fault tolerance
Trigger condition
If one piece of input data does not satisfy the configuration condition, a trip takes place
Scenario
1. Sixteen sensor data reception via hard-wired circuits
2. Comparison logic performance in the trip configuration device of the internal BP
3. If one of the channels does not satisfy the comparison logic from the received data, a trip is initiated
4. Trip status information is sent to the CP via SDL

six interfaces as shown in Table 11. Among six interfaces, one example is presented in Table 12.

4.2 Identifying the characteristics of reactor protection system

An example of the characteristics and policies guiding the operation of the RPS is described in Table 13, which is the result of our analysis of the system and of input from the nuclear specialist who operates the system. The format of Table 13 was derived from Table 5.

Table 13 Reactor protection system characteristics

Classification	RPS characteristics
Implemented policies	An in-depth protection strategy is used depending on the importance of the node (communication originating from a lower level and directed to a higher level is prohibited)
	Remote access is not possible
System composition status	In the case of industrial PCs, real-time operating system is used
	Dual network is established
Communication protocol	The industrial communication protocol (Profibus, etc.) is used
	Deterministic transmission structure is used
Safety guarantee conditions	Designed to process error situations (Watch dog)

Table 14 Reactor protection system threats list

Types	Cyber security threats
T_1	Denial of service
T_2	Malicious code propagation
T_3	System data leakage
T_4	System data alteration
T_5	Malicious code infection via portal media or external H/W
T_6	Physical access attack

Table 15 Reactor protection system cyber security threat scenarios

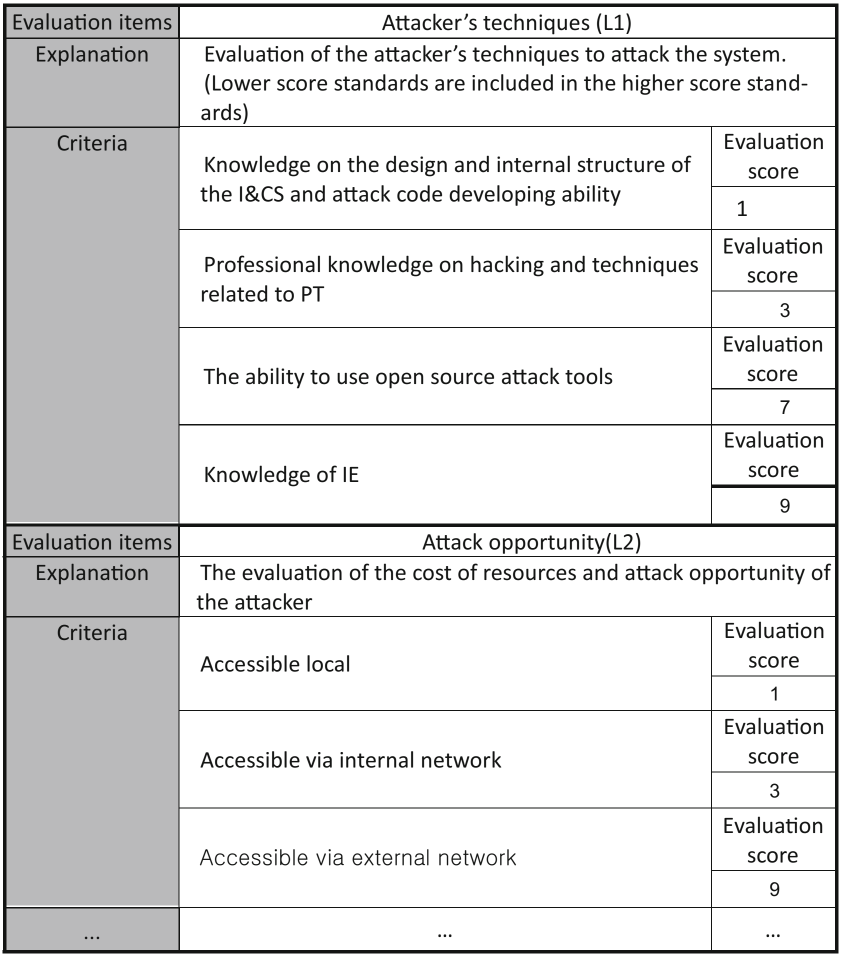
Target	Threat	Explanation
BP	System data alteration	The BP analyzes the channel information and sends a trip signal to the CP when needed
		The attacker deletes the trip signal and sends a normal signal when a trip signal is actually needed (E1)
		–
–	–	–

4.3 Identifying threat to reactor protection system and calculating degree of risk to the system

To determine a cyber security threat to the I&CS, this paper employed the threats suggested in the Threat Landscape published by ENISA and the ICE vulnerability information published by ICS-Cert [15,16]. With the analysis method described in Sect. 4.2, six possible threats to the RPS were identified, which are shown in Table 14.

Table 15 shows one of twelve possible attacks scenario using the threats described above to the node structure and interface of the RPS.

Table 16 Two examples (attack technique and attack opportunity) of likelihood evaluation criteria of cyber security threat

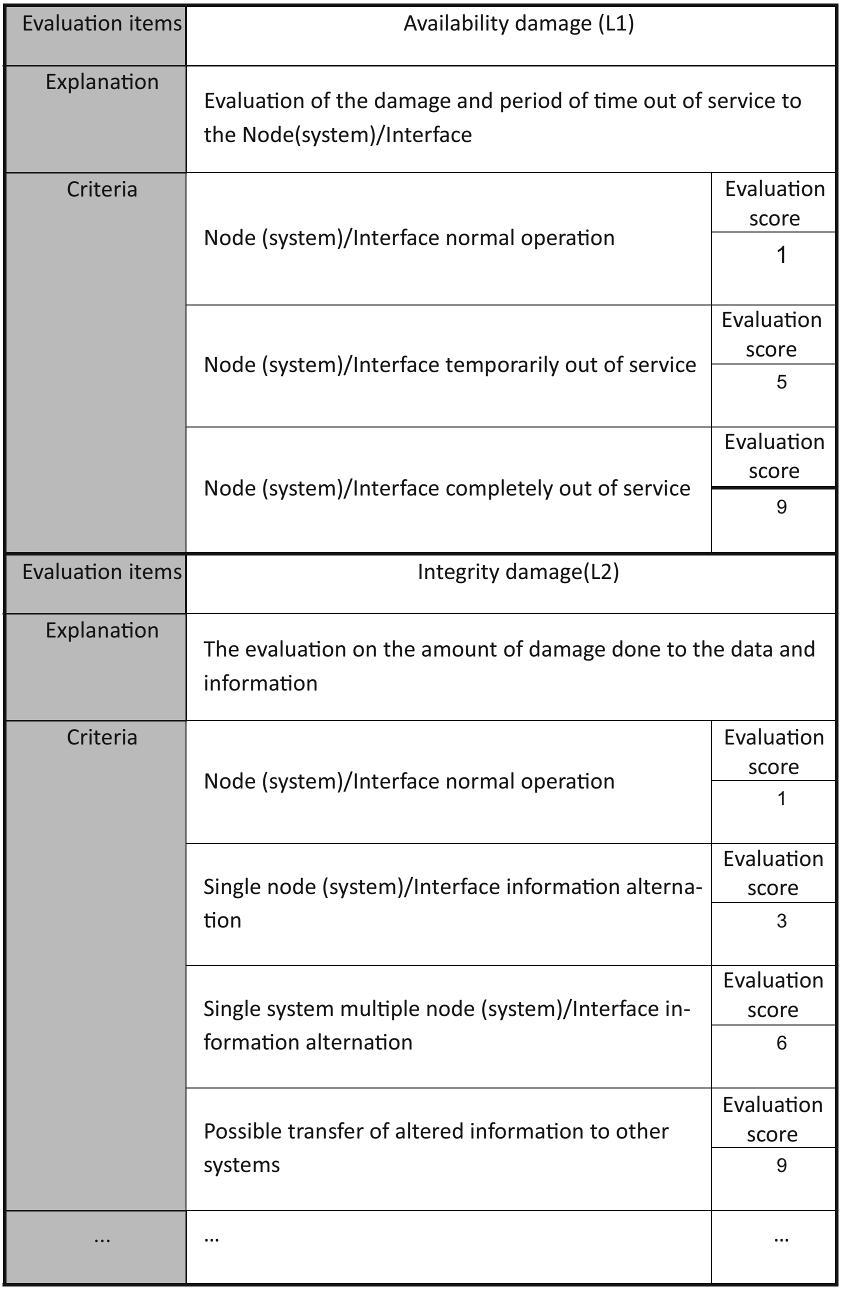


Evaluation items	Attacker's techniques (L1)	
Explanation	Evaluation of the attacker's techniques to attack the system. (Lower score standards are included in the higher score standards)	
Criteria	Knowledge on the design and internal structure of the I&CS and attack code developing ability	Evaluation score
		1
	Professional knowledge on hacking and techniques related to PT	Evaluation score
		3
	The ability to use open source attack tools	Evaluation score
		7
	Knowledge of IE	Evaluation score
		9
Evaluation items	Attack opportunity(L2)	
Explanation	The evaluation of the cost of resources and attack opportunity of the attacker	
Criteria	Accessible local	Evaluation score
		1
	Accessible via internal network	Evaluation score
		3
	Accessible via external network	Evaluation score
		9
...	...	...

For the calculation of the degree of risk, criteria for calculating the occurrence probability were established. The occurrence probability consists of four evaluation items, namely attack technique, attack opportunity, intrusion detection possibility, and vulnerability, in order to devise specific criteria and to evaluate them. The impact evaluation criteria consisted of items that evaluated confidentiality, integrity, and accessibility. In this example, an evaluation criteria of the occurrence probability and impact of the cyber security threat were established. This is shown in Tables 16 and 17, respectively, with two examples each.

Finally, for the evaluation of the Cyber Security Occurrence Probability and Impact, the scenario of Table 15 was evaluated with both criteria of Tables 16 and 17. Afterward, the results from formula (1) were implemented and consulted several nuclear

Table 17 Impact evaluation criteria of cyber security threat



Evaluation items	Availability damage (L1)	
Explanation	Evaluation of the damage and period of time out of service to the Node(system)/Interface	
Criteria	Node (system)/Interface normal operation	Evaluation score 1
	Node (system)/Interface temporarily out of service	Evaluation score 5
	Node (system)/Interface completely out of service	Evaluation score 9
Evaluation items	Integrity damage(L2)	
Explanation	The evaluation on the amount of damage done to the data and information	
Criteria	Node (system)/Interface normal operation	Evaluation score 1
	Single node (system)/Interface information alternation	Evaluation score 3
	Single system multiple node (system)/Interface information alternation	Evaluation score 6
	Possible transfer of altered information to other systems	Evaluation score 9
…	…	…

Table 18 Risk of each threat of cyber security of the reactor protection system

Reactor protection system	T_1	T_2	T_3	T_4	T_5	T_6
BP	Low		Low	Low	Medium	Low
CP	Low		Low	Low	Medium	Low
–	–	–	–	–	–	–
E1		Low				
E2		Medium				
–	–	–	–	–	–	–

and cyber security specialists. A score of 9 or below designates a low risk, a score of 10–36 is a medium risk, and a score of 37 or above is considered a high risk. As shown in Table 18, the degree of risk of various threats to the Reactor Protection System was calculated.

5 Conclusion

This paper proposed a method for calculating the degree of risk to a nuclear reactor systems based on multiple factors for the safety purpose. Based on the proposed method, we presented some examples of how to calculate risk factors to nuclear reactor safety systems which may be under cyber-attack targets. Furthermore, using the analyzed information and the security threat mapping table, we have also proposed a method to define and specify security problems. In addition, we found that to generate security profiles, one also needs to analyze environmental elements, security assumptions and the organization's security policy. We also have found that many of the evaluations have resulted in low risks while none of them have received high in risk. This is because the I&CS is isolated from the external network and it is very difficult for a hacker to access the system and acquire information. However, due to the dangers posed by of nuclear power plants, even a low risk assessment can lead to serious consequences. Therefore, the security of I&CS in nuclear facilities needs to be reinforced.

The proposed method provides a foundation on which to develop and incorporate cyber security technology into nuclear power plants. Its main focus is to implement security techniques in currently operating I&CS.

As a future work, more research is needed on the security function and guarantee requirements of the Protection Profile of I&CS.

Acknowledgements This research is supported by a Korea University Grant and the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea (No. 20121510100030).

References

1. Lee C-K (2012) Cyber security technology trends of instrumentation and control system in nuclear power plants. Rev Korean Inst Inf Secur Cryptol 22(5):28–34

2. Koo I-S, Kim K-W, Hong S-B, Park G-O, Park J-Y (2011) Digital asset analysis methodology against cyber threat to instrumentation and control system in nuclear power plants. J Korean Inst Electron Commun Sci 6(6):839–847
3. Symantec Security Response (2011) W32.Stuxnet Dossier, Rev. 1.4
4. CC v3.1. Release 4. http://www.commoncriteriaportal.org/cc/
5. 10 CFR 73.54 Protection of digital computer and communication systems and networks, March 2009
6. NRC Regulatory Guide 5.71. Cyber security programs for nuclear power facilities. US NRC, Jan 2010
7. National Institute of Criteria and Technology (2009) Special publication 800-53, Aug 2009
8. National Institute of Criteria and Technology (2011) Special publication 800-82, June 2011
9. International Atomic Energy Agency (2011) IAEA nuclear security series no. 17, Computer security at nuclear facilities. IAEA, Vienna
10. Suo H, Wan J, Zou C, Liu J (2012) Security in the internet of things: a review. In: 2012 International Conference on Computer Science and Electronics Engineering, pp 648–651, 23–25 March 2012
11. Roman R, Najera P, Lopez J (2011) Securing the internet of things. Comput Mag 44(9):51–58
12. Li N (2010) Research on Diffie–Hellman key exchange protocol. In: Computer Engineering and Technology (ICCET), vol 4, pp 634–637, 16–18 Apr 2010
13. PROFIBUS. http://www.rtaautomation.com/technologies/profibus/
14. MODBUS. http://www.rtaautomation.com/technologies/modbus-rtu/
15. European Network and Information Security Agency (2013) ENISA threat landscape, Jan 2013
16. ICS-CERT. Cyber threat source descriptions. http://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions
17. Microsoft. DREAD. http://msdn.microsoft.com/en-us/library/ff648644.aspx
18. OCTAVE. http://www.cert.org/octave/
19. OWASP. Threat risk modeling. https://www.owasp.org/index.php/Threat_Risk_Modeling
20. International Organization for Standardization. ISO/IEC 27001:2005 (information technology—security techniques—information security management systems—requirements)
21. Lee D-Y, Choi J-G, Lyou J (2006) A safety assessment methodology for a digital reactor protection system. Int J Control Autom Syst 4(1):105–112
22. Song J-G, Lee J-W, Lee C-K, Kwon K-C, Lee D-Y (2012) A cyber security risk assessment for the design of I&C systems in nuclear power plants. Nucl Eng Technol 44(8):919–928