Nuclear Engineering and Technology 51 (2019) 138–145

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants

Jong Woo Park, Seung Jun Lee[*]

Department of Nuclear Engineering, UNIST, 50, UNIST-gil, Ulsan, 44919, Republic of Korea

ARTICLE INFO

Article history:
Received 27 April 2018
Received in revised form
4 August 2018
Accepted 14 September 2018
Available online 17 September 2018

Keywords:
Probabilistic safety assessment
Cyber security
Cyber-attacks
Nuclear power plant
Critical digital asset

ABSTRACT

With the application of digital technology to safety-critical infrastructures, cyber-attacks have emerged as one of the new dangerous threats. In safety-critical infrastructures such as a nuclear power plant (NPP), a cyber-attack could have serious consequences by initiating dangerous events or rendering important safety systems unavailable. Since a cyber-attack is conducted intentionally, numerous possible cases should be considered for developing a cyber security system, such as the attack paths, methods, and potential target systems. Therefore, prior to developing a risk-informed cyber security strategy, the importance of cyber-attacks and significant critical digital assets (CDAs) should be analyzed. In this work, an importance analysis method for cyber-attacks on an NPP was proposed using the probabilistic safety assessment (PSA) method. To develop an importance analysis framework for cyber-attacks, possible cyber-attacks were identified with failure modes, and a PSA model for cyber-attacks was developed. For case studies, the quantitative evaluations of cyber-attack scenarios were performed using the proposed method. By using quantitative importance of cyber-attacks and identifying significant CDAs that must be defended against cyber-attacks, it is possible to develop an efficient and reliable defense strategy against cyber-attacks on NPPs.

1. Introduction

Over the recent decades, analog instrumentation and control (I&C) systems in a nuclear power plant (NPP) have been replaced with digital I&C systems. Digital technologies provide various benefits such as the possibility of software utilization, high-speed data processing capability, and fault detection or fault tolerance techniques. However, new threats that did not exist in analog systems have been introduced such as a cyber-attack. There have been reports of cyber-attacks on the I&C systems of infrastructures that adopted supervisory control and data acquisition (SCADA) systems, industrial control systems (ICS), and distributed control systems (DCS) [1]. The annual report from the U.S. industrial control systems cyber emergency response team (ICS-CERT) states that the number of cyber-attacks on energy systems increases year after year [2]. In 2011, global energy and oil firms were cyber-attacked by a combination of variable routes [3]. Even in NPPs which are designed to decidedly ensure physical and cyber security, there have been attacks that could have severe consequences. A practical example is “Stuxnet”, which was a malware released in 2010 in the Iranian nuclear facility to destroy the components physically. In NPPs, digital I&C systems have been adopted not only in safety systems such as reactor protection systems (RPS), engineered safety features actuation systems (ESFAS), safety instrumentation systems, and safety monitoring systems, but also in non-safety systems such as instrumentation control systems, information processing and monitoring systems, and non-safety monitoring systems [4]. There have been many reports on I&C system vulnerabilities and various attack paths [5], and it means that they might be targets of cyber-attacks.

To protect NPPs against cyber-attacks, in 2009 and 2010, 10 CFR 73.54 “Protection of Digital Computer and Communication Systems and Networks” [6] and RG 5.71 “Cyber Security Programs for Nuclear Facilities” [7] were published by the US Nuclear Regulatory Commission. They defined CDAs which are defined as digital assets that are safety-critical assets to be protected in any situations, and it is required NPP licensees to submit a cyber-security plan for protecting CDAs. Accordingly, studies on CDA identification or cyber-attack detection on NPPs have been performed in recent years. However, it is difficult to protect all CDAs because that CDAs in an NPP are numerous. Moreover, even if it is possible to cover all CDAs,

[*] Corresponding author.
E-mail address: sjlee420@unist.ac.kr (S.J. Lee).

https://doi.org/10.1016/j.net.2018.09.009

it is not easy to develop a perfect cyber security system against cyber-attacks. In general, a new cyber-attack monitoring or protection system is programmed to detect previously known types of cyber-attacks. When a new cyber-attack is observed, the cyber security system is updated using the information of the new attack. That means new types of cyber-attacks are difficult to be detected and protected. However, this imperfect defense is impermissible for safety critical systems such as NPPs which could be cause serious consequences. If only known attacks are defendable, in case of a new type of cyber-attack with new malicious software, the security system is not useful. In addition, malicious software or viruses can be latent; it can lead to the loss of safety functions in the event of an accident. Therefore, importance analysis of cyber-attacks should be performed on feasible cyber-attack scenarios to develop efficient defense strategies using risk information. However, the studies to analyze importance of cyber-attacks or develop risk-informed security strategies are not yet mature.

In this work, a framework for identifying significant CDAs and analyzing importance scenarios of cyber-attacks on an NPP was proposed based on probabilistic safety assessment (PSA) approach. To demonstrate the applicability of the proposed framework, case studies were performed by developing PSA models of cyber-attacks on an NPP and quantitatively evaluating the effect of the attacks. The risk information obtained from the proposed method could be used to identify important CDAs. Consequently, more efficient risk-informed cyber security strategies and development of regulation PSA models for cyber-security could be possible.

2. PSA-based quantitative importance analysis method for cyber-attacks

2.1. Probabilistic risk assessment for cyber-attacks

There are various methods for evaluating the risk or reliability of general energy systems such as solar power systems, smart grids systems, and NPPs [8,9]. One of the widely used methods to evaluate the risk of an NPP is PSA. In this study, we utilize PSA models to evaluate the importance of a cyber-attack.

Typically, the risk of an NPP is represented as the product of frequency and consequence of event [10]. The core damage frequency (CDF) is estimated from level 1 PSA by constructing event trees (ETs) and fault trees (FTs) [11,12]. The ETs illustrate accident sequences from defined initiating events, and the FTs quantitatively evaluate the system failure probabilities [13]. The consequence such as fatalities and properties loss is estimated from level 3 PSA. In the same sense, the risk of a cyber-attack can be represented as the product of the frequencies of cyber-attacks and their consequences. However, since a cyber-attack is conducted intentionally, it is not possible to estimate or predict its frequency. Therefore, this work focused on the consequence analysis for given cyber-attacks. For the consequence of a cyber-attack, the risk change of an NPP such as the change of CDF and conditional core damage probability (CCDP) were used.

The risk induced by a cyber-attack can be represented by the product of cyber-attack frequency, the conditional probability of events for the cyber-attack, and the consequence of the events as represented in Eq. (1):

$$Risk\ of\ cyber - attack = F(cyber - attack) \times P(Event|cyber - attack) \times C(Event) \tag{1}$$

As mentioned above, since a cyber-attack frequency is not quantifiable, this work is focused on the importance analysis including triggered events by a given cyber-attack and the consequence of the events.

2.2. Identification of possible cyber-attacks

NPPs have adopted digital I&C systems such as programmable logic controllers (PLCs). They can be attacked using malicious software through various attack paths such as networks and external devices [5], although NPPs are designed with external and internal networks separately. To develop a PSA model for cyber-attacks, the possible types of cyber-attacks should be identified. In this research, the attacks are categorized into four types as follows:

- **Type 1. Direct attacks:** Attacks on digital systems to render them unavailable or to cause abnormal behavior (e.g., attacks on a digital output module in RPS)
- **Type 2. Indirect attacks:** Attacks on control logics for non-digitalized components such as pumps and valves (e.g., attacks on a PLC which control to analog components)
- **Type 3. Operator failures:** Attacks on information systems to block the information or to switch it with wrong information (e.g., attacks on a monitoring system)
- **Type 4. Initiating events:** Attacks causing initiating events (e.g., LOCA by opening PORV of PZR)

The first type of cyber-attack is direct attacks. In an NPP, there are digitalized systems such as RPS and ESFAS. If hackers attack the digital systems such as input and output modules, the systems can be rendered unavailable or abnormal. For instance, the RPS has multiple digital/analog input modules, processor module, and output modules to decide trip condition and to generate a trip signal for mitigating accidents [14]. If the RPS is failed by cyber-attack (e.g., output modules CCF by a cyber attack), the risk to the NPP will increase consequently.

The second type of cyber-attack is indirect attacks. In a digitalized NPP, some analog components such as pumps and valves are controlled by digital controllers such as PLCs. Although a component is made only of analog parts, if it is controlled by a digital control system, it could be failed to perform a requested function or be physically damaged by a cyber-attack. In an Idaho National Laboratory experiment, it was shown that an emergency diesel generator which is one of the analog components, could be physically damaged by cyber-attacks on PLCs which control the diesel generator [15].

The third type of cyber-attack is operator failures. As observed in the Three Miles Island-2 accident, wrong information could cause inadequate operations by human operators. In the accident, the coolant of the primary side was continuously leaked through the failed safety depressurization valve, and the safety injection system was automatically started to operate. However, the operators did not recognize the correct state of the safety depressurization valve due to the failed indicator, so that they turned off the safety injection system which should have been kept working. This type of error of commission (EOC) could occur due to cyber-attacks by compromising human-machine interface systems. Providing the wrong information might have severe effects on the plant safety in certain situations.

The last type of cyber-attack indicates the cyber-attacks causing initiating events such as loss of coolant accident (LOCA), interfacing systems LOCA (IS-LOCA), and station black out (SBO). This type of cyber-attack may be happened by complex (both direct and indirect cyber-attacks) cyber-attacks. For instance, if PLCs on the letdown valves or safety depressurization valves were cyber-attacked to stuck open, it could lead to coolant loss, causing an intentional LOCA. Similarly, if cyber-attack occurs in PLCs on isolation valves, the radiological material could be released. It is necessary to analyze possible incidents caused by cyber-attacks, because additional initiating events which are not included the current PSA models should be considered.

2.3. Analysis of basic event

2.3.1. Basic events categorization

A cyber-attack on an NPP can be modeled as a basic event or an initiating event according to its type in the PSA model. The target plant of the PSA model used in this work has digitalized RPS, diverse protection system (DPS) and ESFAS. Also, other analog components such as pumps and valves are controlled by digital controllers, PLCs. The events in a PSA model were categorized according to the four types of cyber-attacks. If an event has no relation with any cyber-attack type, then it is screened out. Fig. 1 shows the example of categorization of basic events. After categorization, additional events were added to represent the component failure by cyber-attacks. For example, in case of the digital output module failure in the RPS shown in Fig. 1, a new node for representing the output module failure by a cyber-attack is added.

2.3.2. RAW analysis

Since a cyber-attack is an intended attack and any components digitalized or connected to digital systems could be the target of cyber-attacks, it is not possible to consider all possible attack scenarios. Moreover, there are numerous CDAs in an NPP. Therefore, important components, which have relatively large effect on the plant safety when attacked, need to be identified. In this work, to observe the severity of an attack, risk achievement worth (RAW) was used. RAW is one of the important measures to observe the change in the total system failure probability when a certain component is assumed to fail [16]. Through the RAW analysis, only basic events that affect the risk of NPP significantly are focused in the analysis. The cut-off value was adjusted from 1E-10 to 1E-15 in the RAW analysis in order to reconsider screened-out basic events due to low failure probabilities.

2.4. Development of a cyber-attack PSA model

2.4.1. Failure mode analysis

To develop a cyber-attack risk evaluation model, the failure modes of systems due to cyber-attacks need to be identified. While various failure modes could occur by attack types and paths, it is conservatively assumed that attacked systems are failed and operator with wrong information fail to perform appropriate actions. Table 1 to Table 3 show the example of failure mode analysis mainly focused on their function failures.

Table 1 lists the failure modes of RPS caused by cyber-attacks. RPS has only one failure mode, which is the reactor trip failure [17]. Table 2 and Table 3 list the failure modes of ESFAS caused by cyber-attacks. ESFAS was analyzed based on it actuation signals such as safety injection actuation signal (SIAS), auxiliary feed water actuation signal (AFAS), recirculating actuation signal (RAS), containment spray actuation signal (CSAS), containment isolation actuation signal (CIAS), and main steam isolation actuation signal (MSIS). Further, human actuation failures in both error of omission (EOO) and EOC were considered in this analysis. As shown in Table 2, SIAS, AFAS, RAS, and CSAS have a similar trend in failure modes. However, as given in Table 3, CIAS and MSIS have possible consequences of both core damage and release of radioactive sources.

2.4.2. FT development

To develop a cyber-attack PSA model, the FTs were developed to consider the effect of a cyber-attack. Fig. 2 and Fig. 3 show the example parts of the reactor trip and safety injection in the developed FT model. The basic PSA model is the optimized pressurized reactor-1000 (OPR-1000) PSA model and PLCs for component controls are considered. As mentioned above, the plant used for the model development has digitalized RPS, DPS, and ESFAS, and other analog components or systems are controlled by digital controllers, PLCs. New basic events which marked with color were modeled in Figs. 2 and 3 based on the identification of four possible cyber-attack types as follows:

- Type 1 (Direct Attack): For digital systems, additional failure with yellow marked basic events were added as shown in Fig. 2. Likewise, as shown in Fig. 3, additional failure in ESFAS with yellow marked basic event was included.
- Type 2 (Indirect Attack): As shown in Fig. 3, PLCs failure due to cyber-attack with blue marked basic event was considered in the developed model. This newly considered basic event indirectly effected to analog components.

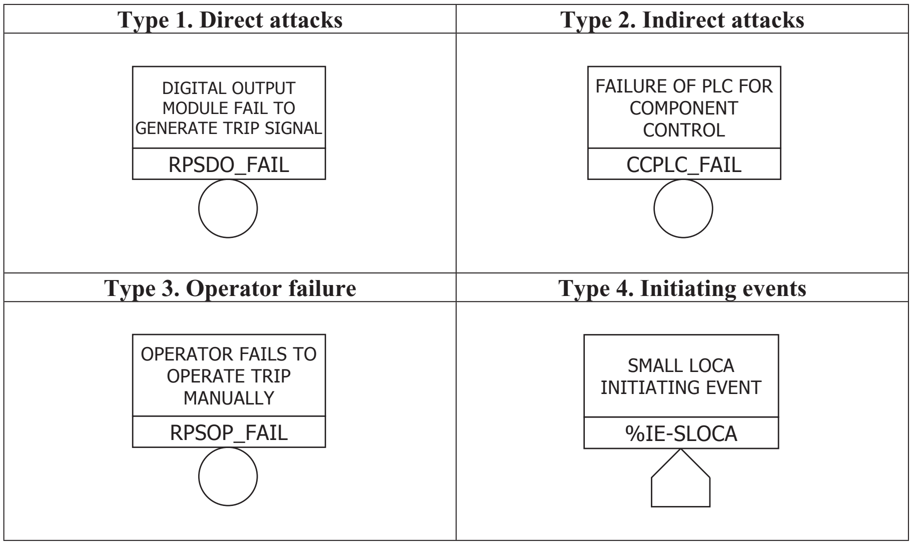
Type 1. Direct attacks
DIGITAL OUTPUT MODULE FAIL TO GENERATE TRIP SIGNAL
RPSDO_FAIL
Type 2. Indirect attacks
FAILURE OF PLC FOR COMPONENT CONTROL
CCPLC_FAIL
Type 3. Operator failure
OPERATOR FAILS TO OPERATE TRIP MANUALLY
RPSOP_FAIL
Type 4. Initiating events
SMALL LOCA INITIATING EVENT
%IE-SLOCA

Fig. 1. Example of the categorization of basic events according by types of cyber-attack.

Table 1
Failure modes of the RPS under cyber-attacks.

System	Signal of Function	Plant State	Failure Mode 1 (Direct Attack)	Failure Mode 2 (Attacks causing operator failure)	Result
RPS	Trip signal	Need to trip	OK	OK	Trip Success
		Need to trip	Digital modules failed by cyber-attack	Operation backup failed by cyber-attack	ATWS[a]

[a] ATWS is anticipated transient without scram, which is the initiating event.

Table 2
Failure modes of the ESFAS under cyber-attacks (1/2).

System	Signal of Function	Plant State	Failure Mode 1 (Direct or Indirect Attacks)	Failure Mode 2 (Attacks causing operator failure)	Result
ESFAS	SIAS	Need to SIAS	OK	OK	OK
		Need to SIAS	OK	EOC induced by cyber-attack	Lead to SIAS failure
		Need to SIAS	Digital modules failed by cyber-attack	Operation backup	OK
		Need to SIAS	Digital modules failed by cyber-attack	Operation backup failed by cyber-attack	Lead to SIAS failure
	AFAS	Need to AFAS	OK	OK	OK
		Need to AFAS	OK	EOC induced by cyber-attack	Lead to AFAS failure
		Need to AFAS	Digital modules failed by cyber-attack	Operation backup	OK
		Need to AFAS	Digital modules failed by cyber-attack	Operation backup failed by cyber-attack	Lead to AFAS failure
	RAS	Need to RAS	OK	OK	OK
		Need to RAS	OK	EOC induced by cyber-attack	Lead to RAS failure
		Need to RAS	Digital modules failed by cyber-attack	Operation backup	OK
		Need to RAS	Digital modules failed by cyber-attack	Operation backup failed by cyber-attack	Lead to RAS failure
	CSAS	Need to CSAS	OK	OK	OK
		Need to CSAS	OK	EOC induced by cyber-attack	Lead to CSAS failure
		Need to CSAS	Digital modules failed by cyber-attack	Operation backup	OK
		Need to CSAS	Digital modules failed by cyber-attack	Operation backup failed by cyber-attack	Lead to CSAS failure

Table 3
Failure modes of the ESFAS under cyber-attacks (2/2).

System	Signal of Function	Plant State	Failure Mode 1 (Direct or Indirect Attacks)	Failure Mode 2 (Attacks causing operator failure)	Result
ESFAS	CIAS	Need to CIAS	OK	OK	OK
		Need to CIAS	OK	EOC induced by cyber-attack	Lead to CIAS failure
		Need to CIAS	Digital modules failed by cyber-attack	OK (Operator success to backup)	OK
		Need to CIAS	Digital modules failed by cyber-attack	Operation backup failed by cyber-attack	Lead to CIAS failure + possible to release radiological material
	MSIS	Need to MSIS	OK	OK	OK
		Need to MSIS	OK	EOC induced by cyber-attack	Lead to MSIS failure
		Need to MSIS	Digital modules failed by cyber-attack	OK (Operator success to backup)	OK
		Need to MSIS	Digital modules failed by cyber-attack	Operation backup failed by cyber-attack	Lead to MSIS failure + possible to release radiological material

- Type 3 (Attacks causing operator failure): Both operator errors EOO and EOC caused by cyber-attacks were modeled. For instance, manual SIAS generation failure by plant information block is an example of EOO, and inappropriate termination of operating safety injection (SI) by an operator due to wrong information is an example of EOC. They modeled as green and red marked basic events as shown in Fig. 3. For reactor trip failure, only EOO is considered.
- Type 4 (Attacks causing initiating events): This attack is represented by setting a corresponding initiating event as happened. New IE caused by cyber-attack which is not included in the current PSA model is not considered in this work.

2.5. Metrics of importance

In general, CDF is used as a risk metric for level 1 PSA. Since the

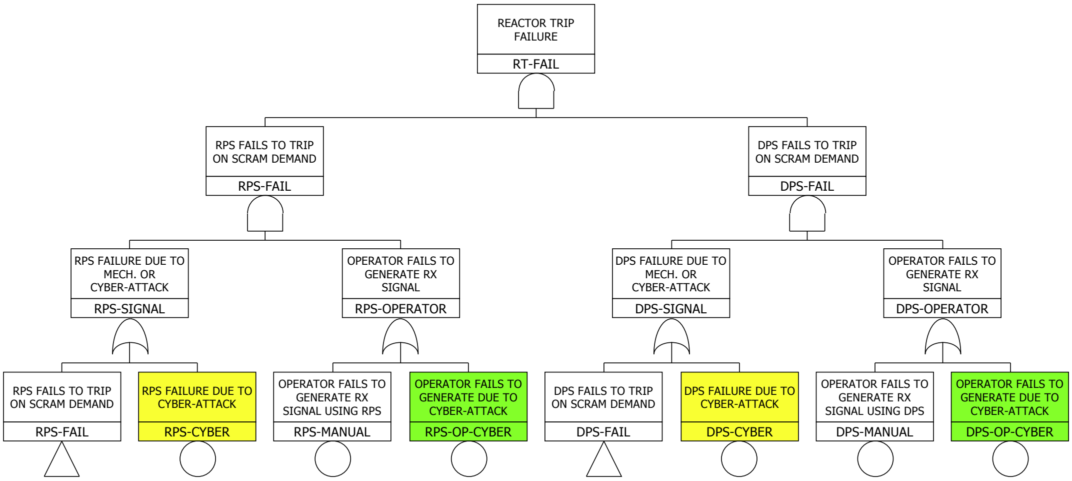
REACTOR TRIP FAILURE
RT-FAIL
RPS FAILS TO TRIP ON SCRAM DEMAND
RPS-FAIL
DPS FAILS TO TRIP ON SCRAM DEMAND
DPS-FAIL
RPS FAILURE DUE TO MECH. OR CYBER-ATTACK
RPS-SIGNAL
OPERATOR FAILS TO GENERATE RX SIGNAL
RPS-OPERATOR
DPS FAILURE DUE TO MECH. OR CYBER-ATTACK
DPS-SIGNAL
OPERATOR FAILS TO GENERATE RX SIGNAL
DPS-OPERATOR
RPS FAILS TO TRIP ON SCRAM DEMAND
RPS-FAIL
RPS FAILURE DUE TO CYBER-ATTACK
RPS-CYBER
OPERATOR FAILS TO GENERATE RX SIGNAL USING RPS
RPS-MANUAL
OPERATOR FAILS TO GENERATE DUE TO CYBER-ATTACK
RPS-OP-CYBER
DPS FAILS TO TRIP ON SCRAM DEMAND
DPS-FAIL
DPS FAILURE DUE TO CYBER-ATTACK
DPS-CYBER
OPERATOR FAILS TO GENERATE RX SIGNAL USING DPS
DPS-MANUAL
OPERATOR FAILS TO GENERATE DUE TO CYBER-ATTACK
DPS-OP-CYBER

Fig. 2. Reactor trip FT model including cyber-attacks.

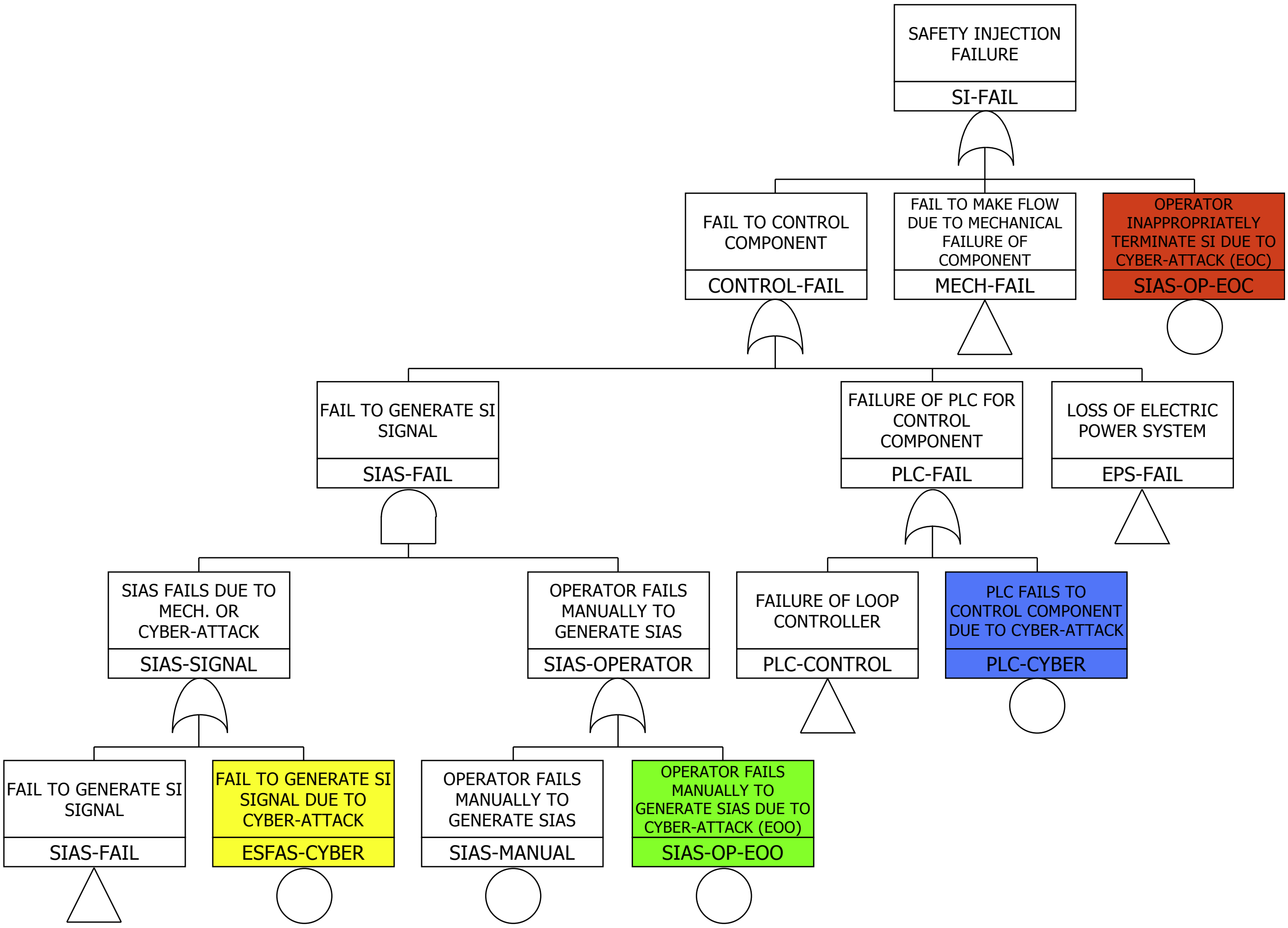
SAFETY INJECTION FAILURE
SI-FAIL
FAIL TO CONTROL COMPONENT
CONTROL-FAIL
FAIL TO MAKE FLOW DUE TO MECHANICAL FAILURE OF COMPONENT
MECH-FAIL
OPERATOR INAPPROPRIATELY TERMINATE SI DUE TO CYBER-ATTACK (EOC)
SIAS-OP-EOC
FAIL TO GENERATE SI SIGNAL
SIAS-FAIL
FAILURE OF PLC FOR CONTROL COMPONENT
PLC-FAIL
LOSS OF ELECTRIC POWER SYSTEM
EPS-FAIL
SIAS FAILS DUE TO MECH. OR CYBER-ATTACK
SIAS-SIGNAL
OPERATOR FAILS MANUALLY TO GENERATE SIAS
SIAS-OPERATOR
FAILURE OF LOOP CONTROLLER
PLC-CONTROL
PLC FAILS TO CONTROL COMPONENT DUE TO CYBER-ATTACK
PLC-CYBER
FAIL TO GENERATE SI SIGNAL
SIAS-FAIL
FAIL TO GENERATE SI SIGNAL DUE TO CYBER-ATTACK
ESFAS-CYBER
OPERATOR FAILS MANUALLY TO GENERATE SIAS
SIAS-MANUAL
OPERATOR FAILS MANUALLY TO GENERATE SIAS DUE TO CYBER-ATTACK (EOO)
SIAS-OP-EOO

Fig. 3. Safety injection FT model including cyber-attacks.

CDF is not appropriate to represent the risk of a cyber-attack, new metrics need to be proposed. In this work, the change in CDF and CCDP are used as importance metrics.

- Without an initiating event, the change in CDF is used. Since there is no initiating event occurred, the cyber-attack is not lead to core damage. Therefore, in this case, the increase of potential risk of a plant by a cyber-attack is used as the risk measure.
- With an initiating event, CCDP is used. When an initiating event occurred by a type four cyber-attack, the plant risk can be represented as CCDP. This measure means the probability that the given initiating event by an attack leads to core damage. In this case, multiple attacks (e.g., one attack to cause LOCA and the

other simultaneous attacks on RPS and ESFAS) make the CCDP higher.

3. Case study

3.1. Development of scenario for importance analysis

For a feasibility study, case studies were performed. In the case studies, quantitative evaluations for several cyber-attack scenarios were performed through the proposed importance evaluation method. To perform quantitative evaluation, scenario development should be conducted. Although it is the most reasonable way to develop scenarios based on real examples of cyber-attacks on NPPs or test-beds, such data is not enough to develop scenarios [18]. Therefore, we selected several example scenarios for the feasibility study, mainly focused on the digitalized systems such as RPS, DPS and ESFAS by considering four types of cyber-attacks described in section 2.2. To apply this method to an NPP and to identify important CDAs, it is necessary to consider all possible scenarios not only considered events in the current PSA models but also unconsidered events caused by only cyber-attacks.

In a research for qualitative analysis of CDAs for cyber-attacks, CDAs are classified with cyber security levels for a graded approach [4]. For instance, critical systems such as RPS and ESFAS are classified as security level 3, a large display panel and information processing systems classified as security level 2, support systems are classified as security level 1 in order [4]. In scenario development, the security levels of CDA and types of cyber-attacks proposed in this work were considered.

For preliminary quantitative risk evaluations, two represented scenarios were developed. The target systems were RPS and ESFAS. Scenario 1 represents cyber-attacks on RPS, while scenario 2 represents cyber-attacks on ESFAS. Scenario 1 and 2 includes four and five sub-scenarios each. Scenario 1 with four sub-scenarios was constructed as follows:

- Scenario 1-1: Digital output modules common cause failure (CCF) in RPS under a cyber-attack
- Scenario 1-2: RPS signal generation and manual backup failure under a cyber-attack
- Scenario 1-3: RPS trip signal generation failure with a small loss of coolant accident (SLOCA) by cyber-attacks
- Scenario 1-4: Scenario 1-3 + operator manual backup failure due to cyber-attacks on information processing system

Scenario 2 with five sub-scenarios was constructed as follows:

- Scenario 2-1: Actuation signal generation failure by digital output modules CCF in ESFAS under a cyber-attack
- Scenario 2-2: ESFAS actuation signal generation failure and manual backup failure (EOO) for HPSI actuation under a cyber-attack
- Scenario 2-3: Scenario 2-1 + SLOCA by a cyber-attack
- Scenario 2-4: Operator manual backup failure (EOO) under SLOCA situation
- Scenario 2-5: Intentional termination of HPSI in all trains by operators (EOC) under SLOCA situation

Both scenarios 1 and 2 are considering the cases with and without an initiating event. Scenarios 1-1 and 2-1 indicate digital output module CCF in RPS or ESFAS due to cyber-attack. It is assumed that RPS and ESFAS have 4 redundant trains and one identical software in all trains. Therefore, there is a possibility of CCF due to cyber-attacks on the identical software. Scenarios 1-2 and 2-2 consider operator manual backup failure with the event of scenario 1-1 and 1-2 respectively. The above scenarios are quantitatively evaluated with change of CDF which is one of the importance metrics. Scenarios 1-3 to 1-4 and 2-3 to 2-5 consider an initiating event caused by a cyber-attack, SLOCA. These scenarios are evaluated with CCDP. Both scenarios 1-3 and 2-3 include digital output module CCF under cyber-attacks with SLOCA. Scenarios 1-4 and 2-4 to 5 consider operator failures due to cyber-attacks. Especially, in scenario 2-4 and 2-5, EOO and EOC are assumed to observe the difference of their effect. After the scenarios were developed, related basic events were updated in the FT models to evaluate the importance.

3.2. Result analysis of importance evaluation

Table 4 and Table 5 show the evaluation results. Since the events of system or operator failures without initiating events in scenarios 1-1 to 1-2 and 2-1 to 2-2, the risks are represented as the change of CDF. As expected, the CCF of the RPS digital output modules due to cyber-attack greatly affected to the change of CDF. It increased about 40 times. In the preceding situation, if the operator cannot operate manual backup due to compromised information by a cyber-attack, the change of CDF dramatically increased about 125 times. Also, in scenario 2-1, actuation signal generation for all engineered safety features is failed by a cyber-attack, in result, the CDF increase about 5 times. And operators cannot operate the HPSI manually due to wrong information, the CDF increases more than RPS cases because basic error probability of operator's manual backup for ESFAS is much lower than that of RPS.

This evaluation result means that it is highly important to prevent the simultaneous failures of RPS or ESFAS and operator manual backup. One of the possible cyber security strategies to prevent these simultaneous events is to provide analog information systems for important plant parameters to operators for diversity.

In scenarios 1-3 to 1-4 and 2-3 to 2-5, the risks are represented by CCDP because an initiating event by a cyber-attack is considered. In the case of the RPS scenario, it was analyzed to have a CCDP value of about 1~2% as shown in Table 4. In this case, because the DPS is available, the CCDP and the effect of manual backup failure of the operator due to the cyber-attack is relatively low. In the case of ESFAS, the scenario of CCF of digital output modules in ESFAS due to cyber-attack showed similar result to RPS case as shown in Table 5. Scenario 2-4 and 2-5, which considered EOO and EOC respectively showed very distinct differences in CCDP. In the scenario for EOO

Table 4
Case study results of cyber-attacks in the RPS scenario.

Risk metric	Scenario 1-1	Scenario 1-2
CDF[a] changes	Increases 40.9 times	Increases 125 times
Risk metric	Scenario 1–3	Scenario 1–4
CCDP[b] with SLOCA	1.23%	1.41%

[a] CDF is core damage frequency.
[b] CCDP is conditional core damage probability.

Table 5
Case study results of cyber-attacks in the ESFAS scenario.

Risk metric	Scenario 2-1		Scenario 2-2
CDF[a] changes	Increases 5.32 times		Increases 1502 times
Risk metric	Scenario 2-3	Scenario 2-4	Scenario 2-5
CCDP[b] with SLOCA	Less than 1%	Less than 1%	16.5%

[a] CDF is core damage frequency.
[b] CCDP is conditional core damage probability.

Table 6
Case study results of CCF case for several CDAs due to cyber-attacks.

Effect of Cyber-Attacks	System	CDA	Detailed description of failure modes	Changes of CDF
Common Cause Failure	RPS	All bistable processor (BP) modules	CCF of all BP modules in RPS	1243%
		All coincidence processor (CP) modules	CCF of all CP processing modules in RPS	248%
		All watchdog timers (WDTs)	CCF of all WDTs in RPS	No effect
	DPS	All DPS processor modules	CCF of all processor modules in DPS	132%
	ESFAS	All coincidence logic (CL) modules	CCF of all CL modules in ESFAS	557%
		All digital input (DI) modules	CCF of all DI modules in ESFAS	416%

Table 7
Case study results of single failure case for several CDAs due to cyber-attacks.

Effect of Cyber-Attacks	System	CDA	Detailed description of failure modes	Changes of CDF
Single Failure	RPS	Single BP module	One BP module fails to generate trip signal	No effect
		Single CP WDT	The WDT in one CP processor module fails to detect a fault	No effect
	DPS	Single DPS processor module	One DPS processor module fails to generate trip signal	132%
	ESFAS	Single CL module for pump controller	One CL module for one pump group controller fails to provide output	19%
		Single CL module for valve controller	One CL module for one valve group controller fails to provide output	19%
		Single DI module for pump controller	One DI module for one pump group controller in one ESFAS channel fails to provide output	No effect
		Single DI module for valve controller	One DI module for one valve group controller in one ESFAS channel fails to provide output	No effect

showed a very low CCDP value of less than 1%, but the scenario for EOC showed an extremely high CCDP value of 16.5%. While EOO was analyzed to have no significant impact because ESFAS was assumed to work normally, EOC was found to have a significant impact because it caused the termination of HPSI pumps automatically actuated. This situation is a similar situation with the TMI-2 accident. Therefore, cyber security strategies should be proposed to prevent EOC due to cyber-attack.

Based on the cyber-attack risk model, the importance of each system can be obtained as the change of CDF. Tables 6 and 7 shows an example of importance analysis of CDAs in RPS, DPS, and ESFAS. As shown in Tables 6 and 7, CCFs caused by cyber-attacks have high effects on the plant safety in almost all cases. While the components which have direct relation with system functions such as output modules have great effects, components for system monitoring such as watchdog timer have low effects.

Tables 6 and 7 show an example of CDA importance analysis results for digitalized components. As shown in the tables, single component failure in RPS and ESFAS have low effect to the changes of CDF compared to CCFs because RPS and ESFAS are designed with redundancy concept: four redundant channels for 2-out-of-4 voting logic and two processor modules for each channel. However, in case of DPS, DPS has only two channels with 2-out-of-2 voting logic. If one signal processor in the two DPS channels is failed by cyber-attack, the effect of single component failure due to cyber-attack is same as CCF case.

4. Discussions

The study proposed a framework for importance analysis of cyber-attacks on an NPP based on PSA models to provide risk information for efficient cyber security strategy development. Followings are remained research items which should be conducted for more reliable evaluations.

- Failure modes: At this stage, the result of all cyber-attacks was assumed to cause failure of digital components or systems only. However, it is a conservative assumption because some cyber-attacks could cause failure modes which has relatively low effects than entire failure of a system. Therefore, it is necessary to consider possible failure modes according to types of cyber-attacks.
- Identification of initiating events caused by cyber-attacks: The current PRA models consider the initiating events caused by random hardware failure and external events. However, more various initiating events should be considered against cyber-attack because unconsidered or unexpected initiating events can occur according to the knowledge of attackers. Therefore, it is necessary to analyze the possibility of initiating events by cyber-attacks which are not considered in the current PSA models.
- Frequency and complexity: This work is focused on the consequence analysis for the given attacks because it is difficult to estimate the frequency of an intended attack. The frequency concept is not appropriate for an intended attack. Therefore, we are considering to use the complexity or difficulty of a cyber-attack instead of the frequency to evaluate the risk. In future work, the complexity or difficulty of a cyber-attack will be assessed by considering various characteristics of cyber-attacks.

5. Conclusion

The cyber security for safety-critical infrastructures such as an NPP has introduced as one of the emerging issues as digital technology has been widely applied. In fact, for the last decades, a number of cyber-attacks on safety-critical infrastructures have been reported. Stuxnet attack on Iranian nuclear facility showed that it is possible to attack an NPP although it has physically separated internal/external network. However, developing an efficient and perfect cyber security strategy is a challenging issue because of the huge number of CDAs and unpredictable attack paths or methods in large and complex systems. Thus, it could be one of the efficient approaches to develop the strategy based on the risk information of cyber-attacks. In this study, the framework for PSA-based importance analysis of cyber-attacks and CDAs was proposed. In the case studies, the risks of two cyber-attack scenarios were quantitatively evaluated with two risk metrics; CDF and

CCDP. Also, the importance of a component or a system was quantitively analyzed. It is expected to use the proposed method for developing an efficient cyber security strategy by identifying important CDAs and attack scenarios.

Acknowledgment

This work has supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2018M2B2B1065653).

References

[1] J. Song, J. Lee, C. Lee, K. Kwon, D. Lee, A cyber security risk assessment for the design of I & C systems in nuclear power plants 44 (8) (2012) 919–928.

[2] U.S. ICS-CERT, Year in Review 2016, 2016.

[3] A. Nicholson, et al., SCADA security in the light of Cyber-Warfare, Comput. Secur. 31 (2012) 418–436.

[4] J. Park, J. Park, Y. Kim, A graded approach to cyber security in a research reactor facility, Prog. Nucl. Energy 65 (2013) 81–87.

[5] J.G. Song, J.W. Lee, G.Y. Park, K.C. Kwon, D.Y. Lee, C.K. Lee, An analysis of technical security control requirements for digital I&C systems in nuclear power plants, Nucl. Eng. Technol. 45 (5) (2013) 637–652.

[6] U.S. Nuclear Regulatory Commission, Protection of Digital Computer and Communication Systems and Networks, 2009, 10 CFR Part 73.54.

[7] U.S. Nuclear Regulatory Commission, Cyber security Programs for nuclear facilities, Regulatory Guide 5 (71) (2010).

[8] Lan Wu, et al., Reliability evaluation of the solar power system based on the Markov chain method, Int. J. Energy Res. (2017) 1–8, 2017.

[9] J.B. Ko, et al., Towards a novel quantification approach based on smart grid network vulnerability score, Int. J. Energy Res. 40 (2016) 298–312, 2016.

[10] Y. Cherdantseva, et al., A review of cyber security risk assessment methods for SCADA systems, Comput. Secur. 56 (2015) 1–27.

[11] Ernest J. Henley, Hiromitsu Kumamoto, Probabilistic Risk Assessment: Reliability Engineering, Design, and Analysis, *IEEE Press*, New York, 1992.

[12] P.A.S. Ralston, J.H. Graham, J.L. Hieb, Cyber security risk assessment for SCADA and DCS networks, ISA Trans. 46 (4) (2007) 583–594.

[13] U.S. Nuclear Regulatory Commission, Fault Tree Handbook, NUREG-0492, 1981.

[14] D. Lee, J. Choi, J. Lyou, A safety assessment methodology for a digital reactor protection system, Int. J. Contr. Autom. Syst. 4 (1) (2006) 105–112.

[15] Idaho National Laboratory, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, 2016.

[16] M. Van Der Borst, H. Schoonakker, An overview of PSA importance measures, Reliab. Eng. Syst. Saf. 72 (3) (2001) 241–245.

[17] J. Park, Y. Suh, C. Park, Implementation of cyber security for safety systems of nuclear facilities, Prog. Nucl. Energy 88 (2016) 88–94.

[18] P.A.S. Ralstona, J.H. Grahamb, J.L. Hiebb, Cyber security risk assessment for SCADA and DCS networks, ISA (Instrum. Soc. Am.) Trans. 46 (4) (2007) 583–594.