Risk Assessment Methods for Cybersecurity in Nuclear Facilities: Compliance to Regulatory Requirements

Lilis Susanti Setianingsih[1], Reza Pulungan[2], Agfianto Eko Putra[3], Moh Edi Wibowo[4], Syarip[5]
Department of Computer Science and Electronics, Universitas Gadjah Mada, Yogyakarta, Indonesia[1,2,3,4]
BAPETEN, Nuclear Energy Regulatory Agency, Jakarta, Indonesia[1]
BATAN, National Nuclear Energy Agency, Yogyakarta, Indonesia[5]

***Abstract*—As strategic infrastructures, nuclear facilities are considered attractive targets for attackers to commit their malicious intention. At the same time, for efficiency, those infrastructures are increasingly implemented, equipped with, and managed by digitally computerized systems. Attackers, therefore, try to realign their attack scenarios through such cyber systems. It is crucial to understand various existing risk assessment methods for cybersecurity in nuclear facilities to prevent such attacks. Risk assessment is designed to study the nature of the originated attack threats and the consequences implied. This paper studies a series of risk assessment methods implemented for security related to cybersecurity of strategic infrastructures, including nuclear facilities. Extended from cybersecurity, the required concepts in nuclear security cover defense-in-depth, synergy of safety and security, and probabilistic safety/risk assessment. Selecting cybersecurity risk assessment methods should integrate these three essential concepts in their evaluation. This paper highlights the suitable and appropriate risk assessment methods that meet security requirements in the nuclear industry as specified in the national and international regulations.**

***Keywords*—Risk assessment; cybersecurity; nuclear facilities; security requirements; regulatory requirements**

I. Introduction

As critical infrastructures containing extremely hazardous materials, nuclear facilities have to operate flawlessly to avoid predicaments and unwanted catastrophes. Even a small failure cannot happen in such facilities, let alone mistakes or oversights committed by their operators. To reach this high level of standards, the International Atomic Energy Agency (IAEA) has provided guidance and recommendations for the management of nuclear facilities. At the same time, IAEA member states are obliged to follow the IAEA regulatory frameworks in providing in-line regulation, authorization, licensing, and inspection to ensure compliance to nuclear energy implementation to national and international standards. Nowadays, concerns regarding nuclear facilities include not only nuclear safety and nuclear safeguard but also nuclear security. Cybersecurity has emerged as a crucial issue among the different aspects of nuclear security as more hardware and software are composed of cyber-physical systems in nuclear facilities.

Cybersecurity is a fundamental issue not only in nuclear facilities but also in any computer-based systems in general. IAEA has provided a guideline for computer security [1] to cope with cyberattacks that can potentially penetrate information systems at nuclear facilities. Cybersecurity focuses on the protection of assets, including humans, data, systems, and organizations, using recent developments of digital technology and follows technical guidance stated by government regulations [2], [3], [4], [5]. Cybersecurity also analyzes risk information [6], [7], including threats, vulnerabilities, and adversaries, to anticipate various cyberattack scenarios. A cybersecurity plan is constructed to ensure information preservation in terms of confidentiality, integrity, availability, authenticity, and validity [2], [8], system's robustness and (fault) tolerance, and system's protection from any potential attacks [9], [10], [11]. Such a plan, according to the US Nuclear Regulatory Control (USNRC) [12], has to cover: (1) components supporting safety-related functions, (2) elements that contribute as important-to-safety functions, (3) competence to maintain security functions, (4) capability to perform emergency preparedness functions, covering off-site communications, and (5) sustainability of support systems and equipment. Considering the critical role of nuclear facilities, these facilities are expected to implement the best model and the best security practice. Achieving this purpose is not trivial, and more studies must be dedicated to understanding this issue.

The development of precautionary and preventive measures has become an important approach in cybersecurity. In nuclear facilities, such measures are far more preferred than the detection and mitigation of cyberattacks. Cybersecurity risk assessment comprises the continuous process of identifying, analyzing, and evaluating any possible risks in a cybersecurity system. Conforming to the cybersecurity requirements, it considers potential risks, consequences of emerging threats, and acquiring cost due to the consequences [13]. Risk assessment, in this context, plays an important role that can assist the understanding, analysis, and evaluation of risks [14] exposed by critical infrastructures. Therefore, various impacts caused by undesired events and attacks can be calculated, anticipated, and minimized [15].

This paper presents a study on risk assessment methods of cybersecurity that have been recently proposed for nuclear facilities, with the purpose of providing a comprehensive understanding of how risk assessments have typically been conducted. It is expected to serve as helpful information for nuclear regulatory agencies in performing their task for regulatory control. Its scope is to provide a unified, collective overview of the current state of knowledge and highlight an inclusive

foundation on risk assessment methods for cybersecurity in nuclear facilities. This study is limited to the compliance and conformity of selected suitable risk assessment methods to the nuclear energy regulatory system.

The rest of the paper is organized as follows: Section II discusses related work on cybersecurity and cyberattacks in general and specifically in nuclear facilities. Section III highlights cybersecurity risk assessments in critical infrastructures, comprising the need for synergy of safety-security and the application of the defense-in-depth concept in security aspects. Section IV focuses on assorted methods of cybersecurity risk assessment methods recently proposed for nuclear facilities. The section also discusses the conformity of the selected risk assessment methods to the regulatory aspects, specifically those concerning nuclear facilities. Section V concludes the paper and offers future works.

II. Related Work

A. Cybersecurity and Cyberattacks

Cybersecurity deals with risks and is expected to meet its objective in protecting assets, including humans, data, systems, and organizations. Cybersecurity, to this end, involves the management of five aspects: data/information, software/hardware, procedures, human resources, and communication, each of which plays an essential role in establishing system integrity.

Table I provides summarized descriptions of the five aspects of cybersecurity management. Data encryption serves to enhance cybersecurity by eliminating the possibility of eavesdropping, data falsification, and data tempering [16], [17], [18]. Software and hardware must follow a strict quality assurance, for example, to avoid getting infected by viruses or worms from wider networks [2], [19]. Cybersecurity procedures include strategies, security principles, security guarantees, guidelines, and risk management approaches [20]. Human resources relate to personnel that has to be equipped with skills and knowledge that are up-to-date and are continuously refreshed through training [21] (otherwise, the personnel can also turn into a threat [22]). Communication integrates all of the aspects mentioned earlier in cybersecurity systems.

TABLE I. Components of Cybersecurity

Component	Description	Precautions to cyberattacks
Data	Information being transferred within the network or internetwork.	Use encrypted data [23], [24].
Software or hardware	The software provides packages of programs, operating systems, including platforms to control the instrumentation and control, which are vulnerable to attacks [25].	Obtain software and hardware from various providers [2]. Secure updating software in accordance with quality assurance (QA) [26].
	Hardware comprises smaller parts as in I&C components and larger devices as the assembly of microprocessors or other peripherals.	Periodic maintenance and regular inspection of hardware [2].
Procedures	Regulations both national and international to follow.	Meet all the requirements as regulated [26], [27].
Human resources	Personnel in charge for the system to run smoothly.	Providing adequate training and regular refresh training [2].
Communication	Interaction inter-device, network, and human-machine interface.	Providing authenticity for communication [28], [23].

All measures implemented in cybersecurity are mainly prepared to anticipate cyberattacks appearing in various forms. Cyberattacks can be defined as attacks on information systems [19] through intrusion conducted by internal [4] or external malicious attackers [16] that may compromise the confidentiality, integrity, and availability [29] of the system or may result in failure and property loss [30], [31] leading to jeopardized safety functions [16], [4], [6]. Cyberattacks have been classified into three categories: active attacks, passive attacks, and cyberwars. Active attacks refer to activities that compromise information systems, including reconnaissance attacks, access attacks, cybercrime, cyber espionage, cyber terrorism, malicious and non-malicious attacks on mobile ad hoc networks and wireless sensor networks. On the other hand, passive attacks do not involve compromising systems but are more on retaining critical information for further use. Most cyberattacks start from cyber scanning followed by enumeration, intrusion attempts, the elevation of privilege, performing malicious tasks, deploying malware/backdoor, deleting forensic evidence, and exiting. Cyber-criminals apply attacks in the forms of cyber vandalism, hacking, denial of service, hijacking the domain name, and even spreading infectious viruses.

In nuclear facilities, cybersecurity issues mainly come from the connectivity between the cyber and the physical systems in the facilities [2]. Current instrumentation and control (I&C) devices are mostly connected to cyber-physical systems. They are distributed control systems (DCS) comprising digitalized automated controllers distributed within the systems, implementing a geographically distributed control loop, and having four main components: controllers, distributed controllers, human-machine interfaces, and communication channels. Nowadays, treating cyber connectivity and physical systems separately is no longer in favor due to more sophisticated and varied cyberattacks [3], [5]. Even though most nuclear facilities are not directly connected to the cyber networks, cyberattacks may still violate system protection [28] in varied forms [32], including denial of services.

B. Cyberattacks at Nuclear Facilities

History has recorded cybersecurity attacks and attempts of attacks at nuclear facilities around the world. Reports have been submitted to IAEA as the international atomic regulatory agency to oversee nuclear energy utilization and ensure the concept of safety, security, and safeguard in nuclear energy implementation.

The David Besse nuclear power plant in the United States was attacked through cyber activity in 2003 [19], [33], leading to the loss of displayed data related to safety and non-safety system for up to five hours. The Slammer worm infected the enterprise workstation through a consultant's network, causing a clogged data traffic connection. The control room personnel could not get the vision of the safety parameter display for four hours fifty minutes.

In 2006, a cyberattack targeted the Browns Ferry nuclear facility in Alabama, United States. The attack resulted in a reactor shutdown because the pump regulating the circulation of demineralized condensate water failed to perform its functions [33]. A programmable logic controller (PLC) controlled the demineralized condensate water, and a variable frequency drive

modulated the circulating pump's speed. Both utilized devices that communicate through a local area network, neglecting the high data traffic that the I&C system could not handle, forcing it to cause malfunction to the PLC and the variable frequency drive. As the recirculating pump was critical to supplying coolant to the reactor, its malfunction could lead to a reactor core meltdown if it failed to support the cooling process. The operator had to manually shut down the operating reactor to avoid further undesired events.

In 2008, the Edwin I. Hatch nuclear facility in Georgia, United States, suffered from a serious incident during a software updating process by an employee [33] on a personal computer in an enterprise network while it was occupied for data input collection to the I&C systems. It led to reset data that should appear on the I&C network. Due to the loss of data display, the systems then considered it an emergency by immediately shutting down to protect the nuclear reactor.

Iran's Natanz uranium enrichment facility suffered from the Stuxnet attack in 2010 [16], [28], [19], [33]. A combination code triggered a PLC in its process control system to send a list of commands to its frequency converter that changed the maximum rotation frequency of the centrifuge, causing the centrifuge to rotate out of its designed range and the rotation speed frequently changed. Due to its operation exceeding the originally designed operational range, the affected centrifuges wore out significantly, reducing the operation period's life and eventually damaging the physical system. The Stuxnet covered its ability by not disrupting the control system's sensor output [51]. It faked the output display and did not interfere with the PLC but gave instructions and commands. It required no connection to the cyber system but used a memory stick instead, plugged into the internal network.

III. Recent Development of Cybersecurity Risk Assessment at Critical Infrastructure

Table II depicts a list of surveyed papers about security, cybersecurity, and risk assessment. Some of them are related to critical infrastructures and, in some cases, to nuclear facilities. As part of the energy sector, nuclear facilities and the electrical supply are classified as critical infrastructures along with finance, transportation, oil and gas industries, water distribution, health care, government services, and emergency installation [52]. However, unlike other critical infrastructures, nuclear facilities are often more attractive to become targets of malicious attacks by different attackers.

A. Synergy of Safety and Security

One major difference distinguishing critical infrastructures such as nuclear facilities from other infrastructures is the requirement to maintain the synergy of security and safety [36], [43]. Any measures taken for security, in this case, should consider their impacts on safety while safety systems in all phases of nuclear energy implementation should not be disturbed. Even though security and safety may oppose one another—for example, security provisions should be kept confidential while safety procedures are to be published as widely as possible—the primary objectives are similar, namely protecting human beings. In any case of the procedures to keep up the synergy of safety and security, safety should be prioritized.

As most safety and security systems are now performed in digital equipment, cybersecurity risks can present in any interface between the two systems. Cybersecurity risk assessment should focus on the people, processes, and equipment related to safety and security. Safety and security digital systems should at least consist of operational technology, as in I&C and information technology. I&C relates to both safety and security systems, while information technology concerns the security system [53].

B. Defense-in-depth Concept

Defense-in-depth is a popular term used in the safety and security field in the nuclear industry. Kim *et al.* [16] initiated a defense-in-depth strategy to strengthen system information and event management (SIEM) in detecting cyberattacks. While dealing with security issues, defense-in-depth SIEM (DID-SIEM) considers all constraints and requirements of nuclear facilities to maintain its safety aspects. DID-SIEM has managed to alleviate technical constraints that can become barriers to security measures. One of the most important technical constraints is that safety function becomes the top priority over security.

Within the DID-SIEM framework, the network is separated into safety, non-safety, and security control levels. The industrial control system network is distantly isolated from the office/enterprise network to eliminate external attack options. Under this security level, no data transfer can be shifted from a lower level to a higher one. It only allows one-way data transmission from safety to non-safety networks. Higher-level DID can deliver command or information to a lower level, but not the other way around. A safety system is isolated within the level where it can share or relay information to a non-safety-related network assigned at a lower level. The monitoring visualization system can only receive data transmission for display from both non-safety and safety log collection and analysis systems.

The defense-in-depth concept can be elaborated into layers of leveled obstructions to prevent any attacks targeting the facilities. The obtained barriers create delays for attackers in accomplishing their missions. These delays can give those in charge of the facilities time to anticipate and prevent the attacks from escalating.

IV. Results and Discussion

A. Cybersecurity Risk Assessment in Nuclear Facilities

Risk can be defined as a combined frequency or probability and consequences of an event or incident that may compromise a system [20], [14]. Another way of expressing risk is the likelihood that a certain vulnerability of a particularly attractive object as the target will be manipulated by a certain threat leading to undesired consequences [54]. Risk can be formulated as a function of (1) the threat for any attack to occur, (2) the vulnerability of the targeted object to endure the attack, and eventually, (3) the damage caused by the threat attack [20], [55], [49]. In a cybersecurity concept, cyber risk is associated with the risk of operational activities in cyberspace, in which the impact can threaten the information systems and assets, the information and communication technology, devices, and peripheral technology resources, and can create

TABLE II. SURVEYED PAPERS ON CYBERSECURITY

Reference	Method	Risk assessment	Cyber-attacks	Critical infrastructure	Nuclear facility
(Kim *et al.*, 2021) [16]	DID-SIEM	Yes	No	Yes	Yes
(Ali, 2021) [2]	Cybersecurity management for DCS	Yes	Yes	Yes	No
(Wang *et al.*, 2021) [34]	Social engineering in cybersecurity	Yes	No	No	No
(Lee *et al.*, 2021) [35]	Estimating security state	Yes	Yes	Yes	Yes
(Yang *et al.*, 2021) [36]	Safety-security risk analysis	Yes	Yes	Yes	No
(El-Genk *et al.*, 2021) [37]	Cybersecurity investigation	Yes	Yes	Yes	Yes
(Yousefnezhad *et al.*, 2020) [38]	Security product lifecycle in IoT	Yes	No	No	No
(Park & Lee, 2020) [6]	Quantitative risk assessment based on difficulty and consequences	Yes	Yes	Yes	Yes
(Lee *et al.*, 2020) [30]	Identifying fault-prone cybersecurity control	Yes	Yes	Yes	Yes
(Syed, 2020) [39]	Cybersecurity vulnerability management	Yes	No	No	No
(Peterson *et al.*, 2019) [40]	Cybersecurity vulnerability assessment	Yes	Yes	Yes	Yes
(Oughton *et al.*, 2019) [41]	Stochastic counterfactual risk analysis	Yes	Yes	Yes	No
(Vessels *et al.*, 2019) [42]	Cybersecurity risk assessment for space systems	Yes	Yes	Yes	No
(Hahndel & Draeger, 2019) [43]	Risk assessment for safety and security	Yes	Yes	Yes	No
(Hashim *et al.*, 2018) [44]	Risk assessment for insider threat	Yes	Yes	No	No
(Lallie *et al.*, 2018) [45]	Evaluating cybersecurity attack graph	Yes	Yes	No	No
(Leszczyna, 2018) [46]	Cybersecurity standards for smart grid	No	No	Yes	No
(Ivanchenko *et al.*, 2018) [47]	Risk assessment of critical infrastructures	Yes	Yes	Yes	No
(Porcedda, 2018) [48]	Regulatory framework on cybersecurity	No	No	No	No
(Zio, 2018) [49]	Future risk assessment	Yes	Yes	Yes	No
(Daria & Massel, 2018) [20]	Risk identification of cybersecurity violation	Yes	Yes	Yes	No
(Lee *et al.*, 2018) [50]	Evaluating the efficacy of cybersecurity control	Yes	Yes	Yes	Yes
(Jana & Ghosh, 2018) [7]	IT2FLC risk assessment model for cybersecurity	Yes	Yes	Yes	No

damage to the tangible and intangible materials [56]. By managing information security risks, good information security practices in cybersecurity are expected to maintain reliable services by the system [57].

Risk assessment plays an important role in understanding and evaluating risks [14] to ensure cybersecurity and to calculate impacts caused by undesired events [15]. Therefore, risk assessment for cybersecurity comprises identifying threats, vulnerabilities, and property assets available within the attack targets [58] and is intended to minimize the negative impacts of potential threats. As the demands for cybersecurity increase to secure data, peripherals, and systems, the need for risk assessment on cybersecurity, especially those implemented at critical infrastructures, including nuclear facilities, also increases.

Table III lists selected risk assessment methods used in nuclear facilities that will be discussed further in this paper. The selected methods relate to security, particularly cybersecurity, in nuclear facilities and critical infrastructures, such as space systems [42] and distributed control systems [2].

TABLE III. CYBERSECURITY RISK ASSESSMENT METHODS FOR NUCLEAR SECURITY

Reference	Methods applied
(Kim *et al.*, 2021) [16]	Method of risk assessment to detect cyberattack; then manage, collect, analyze security information and events, called system information and event management (SIEM) defense in depth. Defense-in-depth is a strategy implemented for nuclear security.
(Lee *et al.*, 2021) [35]	Estimating security state for an integrated response to cyberattacks in nuclear power plants.
(El-Genk *et al.*, 2021) [37]	Cybersecurity investigation.
(Park & Lee, 2020) [6]	Risk assessment is performed by evaluating the risk based on the difficulty and consequences caused by cyberattacks through implementing a Bayesian belief network and probabilistic safety assessment.
(Lee *et al.*, 2020) [30]	Development of a quantitative method for estimating fault-proneness of cybersecurity controls.
(Peterson *et al.*, 2019) [40]	Cybersecurity vulnerabilities in nuclear power plants.
(Lee *et al.*, 2018) [50]	Mean Time To Compromise (MTTC) quantifies the abstract concept of efforts linked to Common Vulnerability Scoring System (CVSS). MTTC value is the estimated figure of the time required for the valid attack. CVSS is one method assigning numerical scores to vulnerabilities based on severity and difficulty to exploit.

B. Estimating Security State

Lee *et al.* [35] developed a probabilistic safety assessment to assist operators in conducting safety-related security evaluations. This method allows operators to conduct cause investigation and security impact analysis. The developed security state evaluation can calculate security failure probability, accounting for the damage probability of critical data assets. Quantification of cyberattack-induced impact is typically carried out by fault tree and event tree analysis. An initiating or basic event relates to the response function failure in the event tree analysis. In contrast, the top event represents the control's functional failure linked to the basic events using logical gates. The top event's probability can be calculated provided that all basic events' probabilities are available, typically obtained from fault tree analysis.

Security state evaluation can lead to the estimation of functional performance impact due to cyberattacks progress. Security state estimation proceeds by observing the target system, developing a hidden Markov model based on the observation, and inputting the model to the evaluation module. The attack level is determined for its minimum and maximum values after being estimated by the evaluation module. The decoding module then uses the selected model from the evaluation module to provide a state-transition path to estimate the current security state.

C. Risk Assessment for Difficulty and Consequences of Cyberattacks

Each cyberattack scenario has its difficulty and produces different impacts that depend on the existing protection systems. This observation gives rise to methods that assess the difficulty and consequences of cyberattacks and consider various aspects from the adversary's point of view. Park and Lee [6]

demonstrated a risk evaluation method based on difficulties and consequences of cyberattacks that combines Bayesian belief network (BBN) and probabilistic safety assessment (PSA) [4].

The BBN method offers quantitative measurements for the attack difficulties level by considering the number of targets and cyberattack scenarios for calculating the conditional cyberattack probability. The number of targets indicates the vulnerability points of the system. Conditional cyberattack probabilities can incorporate the vulnerabilities and failure modes due to the cyberattacks. PSA, on the other hand, evaluates the consequences of the assessment. Using the selected basic events constructed as event trees or fault trees, PSA uses the Boolean logic in analyzing the sequence of basic events to a system failure.

This research also identified several types of cyberattacks based on previous reports of incidents and accidents in nuclear history. These include attacks on man-machine interface systems, attacks related to errors on omission or errors on commission, and attacks that lead to blocked information as well as incorrect displayed information.

D. Fault-proneness in Cybersecurity Control

Lee *et al.* [30] developed a quantitative method to estimate fault-proneness in cybersecurity control by implementing: (1) an analysis of fault prediction models, (2) adoption of the software change entropy model, and (3) development of the security control entropy model. Achievement of high-level quality assurance through consistent attempts, fault proneness, and software complexity correlates to the focus of study for this particular method. Fault proneness can be predicted by software modules exploiting software complexity and fault data recorded in history. Cybersecurity control in the nuclear industry can use the change entropy model to identify the fault-prone in planning and preparing for future issues. To do so, it needs a definition of the amount and complexity of information regarding cybersecurity control.

Nuclear facilities, including nuclear power plants, must provide cybersecurity control in their I&C systems covering intrusion detection systems, surveillance, and access control [19], [35], [37], [40]. For that purpose, the I&C system needs to be modified and extended to comply with the security requirements. The more robust and complex the system coupling is, the more vulnerable are the operating system and application programs to cyberattacks. A proper software development life cycle is expected to increase the security level, although it requires efforts to provide quality assurance for keeping the fault-proneness at a minimum. Information on the software development life cycle can be used to estimate the software failure probability from the number of hidden faults and fault activation probabilities. Software failure probability is then used to anticipate the damage in critical data assets that can jeopardize the safety functions of the nuclear facility.

E. Cybersecurity Vulnerability Assessment

Peterson *et al.* [40] suggested that a risk assessment on a nuclear facility should cover [12]: (1) digital system inventory, (2) penetration testing, (3) vulnerability database and software, (4) modernized discussion of risk, and (5) ongoing risk assessment. They also noted that the assessment should also include the vulnerability assessment. Assessment of cybersecurity vulnerability at nuclear facilities assumes that most incidents occur due to insufficient cybersecurity procedures or unintentional avoidance of the facilities' security measures. History of successful cyberattacks in nuclear facilities, in some manners, involved ingenuous insider participation and the digitalization of I&C in nuclear facilities. Thus, it is vital to pay special attention to such particular attack vectors involving humans, insiders, or technological changes.

F. Cybersecurity Investigation

El-Genk *et al.* [37] noted that the main concern arising in the digitalization of I&C systems in nuclear facilities is the vulnerability of being targeted by cyberattacks. PLCs for I&C in pressurized water reactors face the threat of disturbance caused by cyberattacks, which can manipulate data display collected from data sensors used for safety monitoring. Such an attack can be executed through a false data injection attack. They strongly advised that nuclear facilities need to provide high fidelity analyses in investigating the response and identifying the vulnerabilities to the threat of cyberattacks.

The method of this cybersecurity investigation is applied for program emulated for PLC in the physics-based transient prototype of pressurizer. The pressurizer adapts and controls both system pressure and required water level in a pressurized water reactor type. Setpoints of pressure magnitude and accustomed water level within the pressurizer are preprogrammed. The PLC performs any opening water spray nozzle changes while controlling the charging and adjusting speed levels of letdown water. The on/off position is based on the command of electrical power changes controlled by a PLC.

Such cybersecurity investigation can also be implemented for cases other than pressurizers within the PLC and I&C systems. History showed that several cyberattacks in nuclear industries interfered with the sensor display, leading to immediate shutdown compromising the safety-supporting system.

G. Intrusion-tolerance-based Cybersecurity Index

Another risk assessment method was proposed by Lee *et al.* [50], namely the intrusion-tolerance-based cybersecurity index (InTo-CSI). This method is performed through the reduction of the ratio probability that a cyberattack can damage the target. As safety is the primary concern in nuclear facilities, the intrusion tolerant concept can be a popular option in the evaluation method. Attack difficulty is used to determine the failure probability of intrusion-tolerant strategy in terms of resistance strategy [7], [47]. Attack difficulty depends strongly on unexpected and abstract factors covering attackers' skills and ability to access target system information. Quantifying abstract attempts to attack can be modeled by mean time to compromise (MTTC) based on the assumption of time required for an attack to proceed. Later, MTTC is linked to a common vulnerability scoring system (CVSS) to examine the scores of vulnerabilities based on their severity and level of difficulty to exploit.

The InTo-CSI can be calculated based on the failure probability of each state of the security system by taking into account the failure probability of the existing system from cyberattacks and the failure probability of the upgraded

system. In the upgraded system, the failure probability of securing the system tends to be smaller than that of securing the system before upgrading. There are five intrusion tolerant strategies that should be considered in using the InTo-CSI: (1) a resistance strategy to see the vulnerability difficulties, (2) a detection strategy in detecting a valid attack during the exploitation phase, (3) a backup strategy to provide redundancy in case of error service, (4) an elimination strategy to reduce the risk sources, and (5) a graceful-degradation strategy to keep the essential system functions despite the degraded less important functions.

H. Discussion

From the papers discussed in Sections III and IV, several cybersecurity aspects can be highlighted:

1. The defense-in-depth concept has been recognized as a comprehensive approach for keeping cyberattacks' impacts at a minimum level.
2. The synergy of safety and security has become one of the most important basic requirements in the nuclear industry. Protection of human beings, in this case, comes before protection of properties and assets.
3. The probabilistic approach has emerged as a prominent method of cybersecurity risk assessment. The probabilistic approach can help evaluate the consequences based on the likelihood or probability of the fault propagation as composed in attack scenarios [59].

Draeger & Hahndel [43] proposed a unified risk assessment for both aspects to accommodate the need to maintain a balance between safety and security. The proposed framework provides a simulation that generates paths of sequenced state events. Risk measurement based on the paths is then conducted to predict the criticality and probability of each branch leading to its successor state. The risk assessment itself is modeled to be dynamic and time-dependent [60]. It covers both sides of time response for the defender as the target and the time frame available for the attacker to perform their action in threatening the system [61].

Probabilistic risk assessment (PRA) is an assessment method inspired by the probabilistic safety assessment (PSA) and commonly implemented in nuclear facilities. It provides a combination of quantitative and graphical analysis (fault trees or event trees) to ensure system protection. It can express the basic manifestation of possible attacks scenarios, indicate vulnerabilities, and assist with preparing anticipation before the occurrence of attacks. Since cyberspace is subjected to severe attacks with drastic consequences at a very high speed and complete anonymity [62], modeling threats and vulnerabilities using a probabilistic approach in risk assessment might deliver a better prospect for the entire security system. PRA also includes analysis of adversaries that can be performed based on their capability, opportunity, and intent to build behavioral characteristics [18].

Past experiences in the nuclear industry and several other critical infrastructures, cyberattacks variedly depending on the initial intention of the attackers [17], [63]. In attempting attacks, the adversaries always try to find vulnerabilities in the protected systems. The capability of the adversaries determines the severity level of the impact after attacks. The adversaries can consist of terrorists, criminals, extremists or demonstrators, outsider agents, and insider agents [18], [64], [44], [65], [66], with their respective capacity and capability based on their financial and technical assets. The better the capacity of the adversaries to execute the attack, the more significant is the probability of the attack succeeding.

The selected candidates of cybersecurity risk assessment for nuclear facilities are compared to examine their compliance to the nuclear security aspects required in all facilities. Table IV highlights the conformity of each risk assessment candidate to the three aspects: defense-in-depth, the synergy of safety and security, and implementation of PSA/PRA. All three aspects are highly recommended to be considered in developing or selecting cybersecurity risk assessment. As can be seen from the table, all the listed cybersecurity risk assessment methods have considered the synergy of safety and security during the assessment process. In most methods, the procedures employ distinct parts of assessment for each safety and security-related section.

TABLE IV. ASPECTS OF NUCLEAR SECURITY CONFORMITY

Method	Ref.	DID	Synergy Safety & Security	PSA/PRA
DID-SIEM	[16]	√	√	
Security state estimation	[35]		√	√
Cybersecurity investigation	[37]		√	
BBN PSA/PRA	[6]		√	√
Fault proneness estimation	[30]		√	
Cybersecurity vulnerability assessment	[40]	√	√	√
MTTC-CVSS InTo-CSI	[50]	√	√	√

In analyzing the balance between cybersecurity measures and safety systems simultaneously, the fault-prone estimation method requires that all security controls be evaluated before implementation to ensure that none of the safety and emergency preparedness systems is negatively affected by security measures. This method, however, is not equipped with probabilistic analysis tools nor has instruments to evaluate the implementation of the defense-in-depth concept. The BBN-PSA method does not evaluate the defense-in-depth concept either. However, this method is still more complete because it can conduct probabilistic analysis for the risk assessment. Mirroring this situation, both the cybersecurity investigation and the DID-SIEM methods have the instruments to evaluate the defense-in-depth concept and the synergy between security and safety. However, they do not support probabilistic analysis of risks. The DID-SIEM method, in particular, conducts steps of risk assessment based on levels of priority to put safety concerns as main objectives and separate the safety-network section and the non-safety-network section.

The remaining risk assessment methods in Table IV support the consideration of all three cybersecurity aspects. For the implementation of the defense-in-depth concept, the security state estimation method evaluates whether safety-critical components are secured from any cyberattack. This technique also examines system vulnerabilities while it analyses the progress of the estimated cyberattacks, which meets the requirements in probabilistic risk assessment. The security state estimation method helps the security personnel keep the safety state during the operational period and conduct cause analysis while

establishing cyberattack responses at the right moment.

The InTo-CSI method implements the defense-in-depth strategy comprising the capability to protect, detect, respond, and recover during cyberattacks. The method utilizes event trees to evaluate existing protection functions and supports vulnerability analysis should successful attempts penetrate the protected systems. The combination of the defense-in-depth concept and the probability risk assessment is well implemented in the InTo-CSI method. The event trees generated in the method can show vulnerability areas and identify possible intrusion and attacks to the systems.

The cybersecurity vulnerability assessment method also supports the defense-in-depth concept and the probabilistic risk assessment. This method focuses on the lack of cybersecurity procedures that may lead to cybersecurity incidents originated from unintentional actions. Meanwhile, the possibility of cyberattacks involving insider threats also exists [2], [44]. A typical case of applying this method is the modernization of digital control, including I&C, which is unavoidable anymore in the nuclear industry. The assessment and analysis, in this case, require a dynamic process as the data involved should be reliable and updated [22]. They also need the engagement of all relevant stakeholders with better access to intelligent information.

The conformity to nuclear aspects and compliance with nuclear energy regulations are essential in finding suitable cybersecurity risk assessment methods. Such methods can deliver the best performance in securing the protected system and still fulfill the requirements specified in regulations.

Risk assessment methods for cybersecurity discussed in this paper have been implemented at nuclear facilities in various countries. The methods were designed to align with regulations released both by national and international regimes, such as IAEA and USNRC. The Korean Hydro & Nuclear Power, for instance, has implemented a cybersecurity risk assessment within the scope of nuclear facilities of nuclear power plants. The assessment has been conducted for Generation III and Generation III+ reactors, which are more digitized, like AP 1000. A similar assessment will be used in the United Arab Emirates for the APR 1400 units installed by South Korea.

In Indonesia, BAPETEN, as the Nuclear Energy Regulatory Agency, has been determined to include risk assessment in supervising nuclear energy utilization [67]. However, the tools used by the regulator to perform risk assessment are not always available. In 2012, BAPETEN released Regulation no. 6 to regulate the computer systems in nuclear facilities to comply with its requirements to support safety and security aspects [68]. The regulation emphasizes that immediate attention to any impending threats through early detection can revive the sustainability of proper cybersecurity in the nuclear industry.

V. Conclusion

Nuclear energy implementation should cover pillars of safety, security, and safeguard. They should be considered in selecting the most suitable risk assessment. The safeguard aspect has been declared earlier at the national level by ratifying the non-proliferation treaty to implement nuclear energy for peaceful purposes. Thus, we need to ensure that both safety and security aspects are well-maintained for operational during commissioning in nuclear facilities. Proper risk assessment can enhance cybersecurity in nuclear facilities. Risk assessment in cybersecurity for nuclear facilities is expected to keep the aspects of security and safety simultaneously.

Basic concepts that should be examined in nuclear security implementations include the synergy of safety-security and the defense-in-depth aspect. Moreover, security risk assessments in nuclear facilities should also implement commonly used PSA/PRA to integrate the attack scenario graphs. Cybersecurity vulnerability assessment is a viable method based on the selection process we have carried out in the previous section. The method puts together the defense-in-depth, the synergy of safety and security, and the application of PSA/PRA along with the scenario graph analysis. We believe that cybersecurity vulnerability assessment conforms to the stated requirements in regulations for nuclear energy implementation.

It is important to note that cybersecurity risk assessment is a must in nuclear energy utilization for peaceful use. Existing technologies of the I&C system, including PLCs, are vulnerable as they are attractive targets for the cyberattack threats. Appropriate risk assessment can enhance strong cybersecurity for providing preventive measures in avoiding potential cyberattacks.

This research will continue the in-depth study of the topics by focusing on cybersecurity and vulnerability aspects and include them in the PSA/PRA analysis generally implemented in nuclear facilities.

Authorship Contribution Statement

Lilis Susanti Setianingsih: methodology, writing, and original draft. Reza Pulungan: conceptualization, validation, supervision, writing-review, and editing. Agfianto Eko Putra: validation, supervision, review, and editing. Moh. Edi Wibowo: validation, supervision, review, and editing. Syarip: validation, supervision, review, and editing.

Acknowledgment

The authors would like to thank BAPETEN (Indonesian Nuclear Energy Regulatory Agency), and Universitas Gadjah Mada. This research is partially funded by Universitas Gadjah Mada's Rekognisi Tugas Akhir program in 2020.

References

[1] "Computer security at nuclear facilities: Technical guidance reference manual," *IAEA Nuclear Security Series No. 17*, pp. 1–69, 2011.

[2] S. Ali, "Cybersecurity management for distributed control system: Systematic approach," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–13, 2021.

[3] M. Alali, A. Almogren, M. M. Hassan, I. A. Rassan, and M. Z. A. Bhuiyan, "Improving risk assessment model of cyber security using fuzzy logic inference system," *Computers & Security*, vol. 74, pp. 323–339, 2018.

[4] J. Shin, H. Son, and G. Heo, "Cyber security risk evaluation of a nuclear I&C using BN and ET," *Nuclear Engineering and Technology*, vol. 49, no. 3, pp. 517–524, 2017.

[5] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Computers in Human Behavior*, vol. 48, pp. 51–61, 2015.

[6] J. W. Park and S. J. Lee, "A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence," *Annals of Nuclear Energy*, vol. 142, p. 107432, 2020.

[7] D. K. Jana and R. Ghosh, "Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security," *Journal of Information Security and Applications*, vol. 40, pp. 173–182, 2018.

[8] C. O'Halloran, T. G. Robinson, and N. Brock, "Verifying cyber attack properties," *Science of Computer Programming*, vol. 148, pp. 3–25, 2017.

[9] X. Fan, K. Fan, Y. Wang, and R. Zhou, "Overview of cyber-security of industrial control system," in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, 2015, pp. 1–7.

[10] D. Young, J. Lopez, M. Rice, B. Ramsey, and R. McTasney, "A framework for incorporating insurance in critical infrastructure cyber risk strategies," *International Journal of Critical Infrastructure Protection*, vol. 14, pp. 43–57, 2016.

[11] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," *International Journal of Critical Infrastructure Protection*, vol. 8, pp. 53–66, 2015.

[12] "Cyber security programs for nuclear facilities," *Regulatory Guide 5.71, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission*, pp. 1–40, 2010.

[13] R. Leszczyna, "Review of cybersecurity assessment methods: Applicability perspective," *Computers & Security*, vol. 108, p. 102376, 2021.

[14] M. Touhiduzzaman, S. N. G. Gourisetti, C. Eppinger, and A. Somani, "A review of cybersecurity risk and consequences for critical infrastructure," in *2019 Resilience Week (RWS)*, vol. 1, 2019, pp. 7–13.

[15] M. R. Asghar, Q. Hu, and S. Zeadally, "Cybersecurity in industrial control systems: Issues, technologies, and challenges," *Computer Networks*, vol. 165, p. 106946, 2019.

[16] S. Kim, S.-m. Kim, K.-h. Nam, S. Kim, and K.-h. Kwon, "Security information and event management model based on defense-in-depth strategy for vital digital assets in nuclear facilities," in *Advances in Computer Science and Ubiquitous Computing*, J. J. Park, S. J. Fong, Y. Pan, and Y. Sung, Eds. Springer Singapore, 2021, pp. 331–339.

[17] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," *Computers & Security*, vol. 68, pp. 81–97, 2017.

[18] S. Moskal, S. J. Yang, and M. E. Kuhl, "Cyber threat assessment via attack scenario simulation using an integrated adversary and network modeling approach," *The Journal of Defense Modeling and Simulation*, vol. 15, no. 1, pp. 13–29, 2018.

[19] H. E. Kim, H. S. Son, J. Kim, and H. G. Kang, "Systematic development of scenarios caused by cyber-attack-induced human errors in nuclear power plants," *Reliability Engineering & System Safety*, vol. 167, pp. 290–301, 2017.

[20] G. Daria and A. Massel, "Intelligent system for risk identification of cybersecurity violations in energy facility," in *3rd Russian-Pacific Conference on Computer Technology and Applications*, 2018, pp. 1–5.

[21] A. Reeves, P. Delfabbro, and D. Calic, "Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue," *SAGE Open*, vol. 11, no. 1, pp. 1–18, 2021.

[22] "Risk informed approach for nuclear security measures for nuclear and other radioactive material out of regulatory control: Implementing guide," *IAEA Nuclear Security Series No. 24-G*, pp. 1–69, 2015.

[23] X. Yao, F. Farha, R. Li, I. Psychoula, L. Chen, and H. Ning, "Security and privacy issues of physical objects in the IoT: Challenges and opportunities," *Digital Communications and Networks*, 2020.

[24] E. H. Riyadi, T. K. Priyambodo, and A. E. Putra, "The dynamic symmetric four-key-generators system for securing data transmission in the industrial control system," *International Journal of Intelligent Engineering and Systems*, vol. 14, pp. 376–386, 2021.

[25] S. Eggers, "A novel approach for analyzing the nuclear supply chain cyber-attack surface," *Nuclear Engineering and Technology*, vol. 53, no. 3, pp. 879–887, 2021.

[26] "IEEE standard criteria for digital computers in safety systems of nuclear power generating stations," *IEEE Std 7-4.3.2-2003 (Revision of IEEE Std 7-4.3.2-1993)*, pp. 1–65, 2003.

[27] "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model," *ISO/IEC 15408-1:2009*, pp. 1–64, 2009.

[28] A. Khalid, P. Kirisci, Z. H. Khan, Z. Ghrairi, K.-D. Thoben, and J. Pannek, "Security framework for industrial collaborative robotic cyber-physical systems," *Computers in Industry*, vol. 97, pp. 132–145, 2018.

[29] S. Abraham and S. Nair, "Comparative analysis and patch optimization using the cyber security analytics framework," *The Journal of Defense Modeling and Simulation*, vol. 15, no. 2, pp. 161–180, 2018.

[30] C. Lee, S. M. Han, and P. H. Seong, "Development of a quantitative method for identifying fault-prone cyber security controls in NPP digital I&C systems," *Annals of Nuclear Energy*, vol. 142, p. 107398, 2020.

[31] J. Shin, H. Son, R. Khalil ur, and G. Heo, "Development of a cyber security risk model using Bayesian networks," *Reliability Engineering & System Safety*, vol. 134, pp. 208–217, 2015.

[32] H. El-Sofany, "A new cybersecurity approach for protecting cloud services against DDoS attacks," *International Journal of Intelligent Engineering and Systems*, vol. 13, pp. 205–215, 2020.

[33] W. Ahn, M. Chung, B.-G. Min, and J. Seo, "Development of cyber-attack scenarios for nuclear power plants using scenario graphs," *International Journal of Distributed Sensor Networks*, vol. 11, no. 9, p. 836258, 2015.

[34] Z. Wang, H. Zhu, and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods," *IEEE Access*, vol. 9, pp. 11 895–11 910, 2021.

[35] C. Lee, Y. Ho Chae, and P. Hyun Seong, "Development of a method for estimating security state: Supporting integrated response to cyber-attacks in NPPs," *Annals of Nuclear Energy*, vol. 158, p. 108287, 2021.

[36] Z. Ji, S.-H. Yang, Y. Cao, Y. Wang, C. Zhou, L. Yue, and Y. Zhang, "Harmonizing safety and security risk analysis and prevention in cyber-physical systems," *Process Safety and Environmental Protection*, vol. 148, pp. 1279–1291, 2021.

[37] M. S. El-Genk, R. Altamimi, and T. M. Schriener, "Pressurizer dynamic model and emulated programmable logic controllers for nuclear power plants cybersecurity investigations," *Annals of Nuclear Energy*, vol. 154, p. 108121, 2021.

[38] N. Yousefnezhad, A. Malhi, and K. Främling, "Security in product lifecycle of IoT devices: A survey," *Journal of Network and Computer Applications*, vol. 171, p. 102779, 2020.

[39] R. Syed, "Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system," *Information & Management*, vol. 57, no. 6, p. 103334, 2020.

[40] J. Peterson, M. Haney, and R. Borrelli, "An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants," *Nuclear Engineering and Design*, vol. 346, pp. 75–84, 2019.

[41] E. J. Oughton, D. Ralph, R. Pant, E. Leverett, J. Copic, S. Thacker, R. Dada, S. Ruffle, M. Tuveson, and J. W. Hall, "Stochastic counterfactual risk analysis for the vulnerability assessment of cyber-physical attacks on electricity distribution infrastructure networks," *Risk Analysis*, vol. 39, no. 9, pp. 2012–2031, 2019.

[42] L. Vessels, K. Heffner, and D. Johnson, "Cybersecurity risk assessment for space systems," in *2019 IEEE Space Computing Conference (SCC)*, 2019, pp. 11–19.

[43] J. Draeger and S. Hahndel, "Simulation-based unified risk assessment for safety and security," *arXiv*, vol. abs/1709.00567v2, pp. 1–24, 2019.

[44] N. A. Hashim, Z. Z. Abidin, A. Puvanasvaran, N. A. Zakaria, and R. Ahmad, "Risk assessment method for insider threats in cyber security: A review," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 11, pp. 126–130, 2018.

[45] H. S. Lallie, K. Debattista, and J. Bal, "Evaluating practitioner cybersecurity attack graph configuration preferences," *Computers & Security*, vol. 79, pp. 117–131, 2018.

[46] R. Leszczyna, "Cybersecurity and privacy in standards for smart grids - a comprehensive survey," *Computer Standards & Interfaces*, vol. 56, pp. 62–73, 2018.

[47] O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak, and S. Konovalenko, "Risk assessment of critical energy infrastructure considering physical and cyber assets: Methodology and models," in *2018 IEEE 4th International Symposium on Wireless Systems within the International*

Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), 2018, pp. 225–228.

[48] M. G. Porcedda, "Patching the patchwork: appraising the EU regulatory framework on cyber security breaches," *Computer Law & Security Review*, vol. 34, no. 5, pp. 1077–1098, 2018.

[49] E. Zio, "The future of risk assessment," *Reliability Engineering & System Safety*, vol. 177, pp. 176–190, 2018.

[50] C. Lee, H. B. Yim, and P. H. Seong, "Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept," *Annals of Nuclear Energy*, vol. 112, pp. 646–654, 2018.

[51] M. Yampolskiy, P. Horváth, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits, "A language for describing attacks on cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 8, pp. 40–52, 2015.

[52] M. Ficco, M. Choraś, and R. Kozik, "Simulation platform for cybersecurity and vulnerability analysis of critical infrastructures," *Journal of Computational Science*, vol. 22, pp. 179–186, 2017.

[53] R. Busquim e Silva, J. Piqueira, J. Cruz, and R. Marques, "Cybersecurity assessment framework for digital interface between safety and security at nuclear power plants," *International Journal of Critical Infrastructure Protection*, vol. 34, p. 100453, 2021.

[54] V. Casson Moreno, G. Reniers, E. Salzano, and V. Cozzani, "Analysis of physical and cyber security-related events in the chemical and process industry," *Process Safety and Environmental Protection*, vol. 116, pp. 621–631, 2018.

[55] J. Neeli and S. Patil, "Insight to security paradigm, research trend & statistics in internet of things (IoT)," *1st International Conference on Advances in Information, Computing and Trends in Data Engineering (AICDE)*, vol. 2, no. 1, pp. 84–90, 2021.

[56] G. Strupczewski, "Defining cyber risk," *Safety Science*, vol. 135, p. 105143, 2021.

[57] M. Alohali, N. Clarke, and S. Furnell, "The design and evaluation of a user-centric information security risk assessment and response framework," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 10, pp. 148–163, 2018.

[58] J. Hu, S. Guo, X. Kuang, F. Meng, D. Hu, and Z. Shi, "I-HMM-based multidimensional network security risk assessment," *IEEE Access*, vol. 8, pp. 1431–1442, 2020.

[59] A. Nakai and K. Suzuki, "Risk assessment system for verifying the safeguards based on the HAZOP analysis," *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 10, pp. 48–53, 2014.

[60] F. Arnold, H. Hermanns, R. Pulungan, and M. Stoelinga, "Time-dependent analysis of attacks," in *Principles of Security and Trust*, M. Abadi and S. Kremer, Eds. Springer Berlin Heidelberg, 2014, pp. 285–305.

[61] Y. Zhao, L. Huang, C. Smidts, and Q. Zhu, "Finite-horizon semi-Markov game for time-sensitive attack response and probabilistic risk assessment in nuclear power plants," *Reliability Engineering & System Safety*, vol. 201, p. 106878, 2020.

[62] E. Bou-Harb, M. Debbabi, and C. Assi, "Cyber scanning: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1496–1519, 2014.

[63] P. H. Nguyen, S. Ali, and T. Yue, "Model-based security engineering for cyber-physical systems: A systematic mapping study," *Information and Software Technology*, vol. 83, pp. 116–135, 2017.

[64] K. Geers, "The challenge of cyber attack deterrence," *Computer Law & Security Review*, vol. 26, no. 3, pp. 298–303, 2010.

[65] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & Security*, vol. 72, pp. 212–233, 2018.

[66] M. A. Hawila and S. S. Chirayath, "Combined nuclear safety-security risk analysis methodology development and demonstration through a case study," *Progress in Nuclear Energy*, vol. 105, pp. 153–159, 2018.

[67] "Undang-Undang Republik Indonesia no. 10/1997 (Indonesia Nuclear Energy Act no. 10/1997)," 1997, (In Bahasa Indonesia).

[68] "Peraturan Kepala BAPETEN no. 6/2012 (BAPETEN Chairman Regulation No. 6/2012)," 2012, (In Bahasa Indonesia).