A Comparative Study on Nuclear Power Plant Cyber Security Assessment Models Based on Risk Assessment Standard Guideline

Kookheui Kwon*, Aram Kim, Subong Lee
[a]*Korea Institute of Nuclear Nonproliferation and Control, Daejeon, Republic of Korea*
**Corresponding author: vivacita@kinac.re.kr*

ABSTRACT

International efforts to strengthen nuclear cyber security and revision of international guidelines have been underway, with the primary goal of identifying digital assets and implementing security controls after assessing cyber risks. International standards require organizations to assess the probability of information security risk, the impact of risk, and determine the level of risk. Since it is almost impossible to quantify security risk by considering all relevant cases, it is common to assume limited conditions and compare qualitative or semi-quantitative results to prioritize. In this paper, we analyze representative cyber risk assessment models for nuclear power plants and compare their strong and weak points.

I. Introduction

Since the airgap attack known as Stuxnet on Iran's nuclear facilities in 2010, cyberattacks have gone beyond information theft and manipulation and have physically adverse impact, and the need for industrial control system security has increased.

Accordingly, from the beginning of 2010, efforts to strengthen international cyber security for nuclear power plants and related international guides were revised. The main content is to perform security controls after identifying target digital assets and assessing cyber risks.

Cyber risk assessment has been a long-requested activity in the field of information security, and according to ISO/IEC 27001, the likelihood and impact of information security risks are evaluated and the risk level should be determined. The likelihood of occurrence can be evaluated as a combination of security threats and vulnerabilities, and the evaluated risk level is compared with the risk criteria set in the relevant facility to be taken in order of priority.

The cyber risk assessment concept required for nuclear power plants is not much different from this, but it is different in that it must be applied consistently and practically in the site and that documented justification is requested in detail regarding security quality management.

Since it is almost impossible to quantify considering all relevant cases when evaluating security risks, it is common to identify priorities by assuming limited conditions and comparing qualitative or semi-quantitative results.

In this paper, we analyze representative nuclear power plant cyber security assessment models based on the main elements of NIST SP 800-30 and compare their strong and weak points. The results of this analysis are expected to be used in various studies, such as improvement studies to complement the limitations of each model, optimized model design studies, and model verification criteria studies, considering the weaknesses of each model.

II. Analysis of Cyber Security Risk Assessment Models

2.1 NUREG/CR-6847

It is a cyber security self-assessment methodology for nuclear power plants, developed by the U.S. Nuclear Regulatory Commission (NRC) in 2004 through Pacific Northwest National Laboratory (PNNL) and industry experts. Recognizing the difficulty of assessing the probability of cyber risk of assets or communication pathways based on threats and vulnerabilities, it devised a susceptibility category based on a combination of physical/logical exposure and effectiveness of protection measures. The result is a methodology that categorizes cyber security risk levels into a combination of an asset's impact level and susceptibility level to manage cyber risk based on the nuclear facility's strategy.

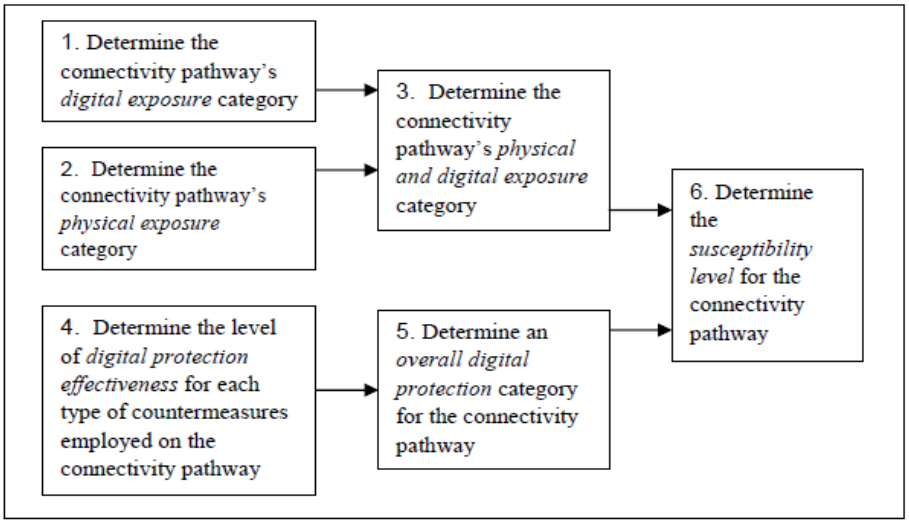

Fig. 1. Susceptibility Assessment Determination Process [1]

2.2 STPA-SafeSec

It is a security assessment methodology based on System-Theoretic Process Analysis (STPA) introduced by MIT in 2012. Basically, the STPA recognizes that as modern systems become more complex in function and configuration, events are often caused by control issues between systems or components rather than component failures. Therefore, when analyzing a system, STPA structures and understands the system around the critical relationships and interactions that affect it rather than listing and combining all components or functions.

STPA-SafeSec is a methodology that adds a security component to the STPA methodology for security analysis. STPA-SafeSec models the system and analyzes the security of the system based on the following procedures;

- Structuring the system and defining the control layer
- Identify the Hazardous Control Actions in the system
- Define the control layers for system components
- Define Hazardous Scenarios
- Perform safety and security analysis and identify mitigation measures [2].

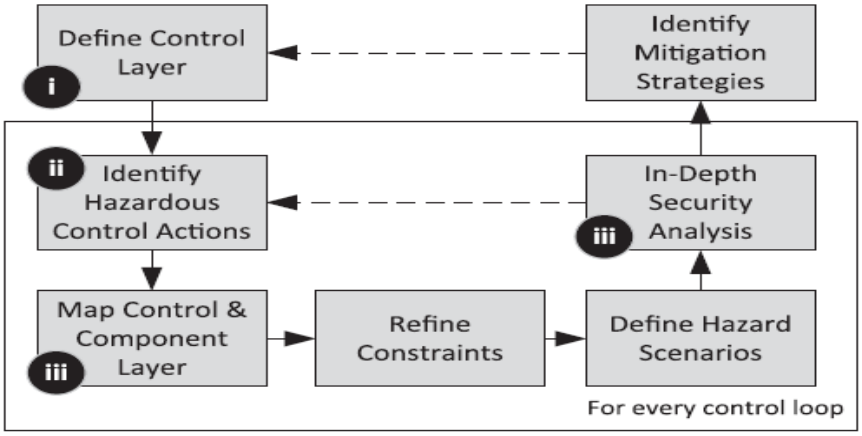

Fig. 2. Assessment Process of STPA-SafeSec [2]

2.3 NEI 13-10 (rev.6)

It is a cyber security assessment methodology developed by the Nuclear Energy Institute (NEI) in 2013 to meet U.S. NRC regulatory guide and finally endorsed by the NRC. The model categorizes digital assets according to their impact on the facility among cyber risks and then devises a process for applying cyber security controls to eliminate possible attack vectors for each asset instead of assessing the probability of occurrence.

It is a methodology that applies baseline security controls to digital assets with relatively low impact and provides security controls to eliminate attack vectors/attack pathways by digitalized type such as sensors, indicators, and controllers for assets that directly affect nuclear power plant safety to assess and apply [3].

Security Impact	Non-Direct CDA			Direct CDA					
	EP CDA	BOP-CDA	Indirect CDA	A.1	A.2	A.3	B.1	B.2	B.3
				Non-Communication Capa.			Communication Capa.		
Classification Criteria	Only EP functions & Alt. means exists	Operation Impact (Transient, Trip)	Non-adverse Impact to Safety/Security Functions	firmware	operational parameter	config. setting	serial com. port,	serial com. port, program	program, upgrade, com. port
Technical Controls	○ 4 baseline controls	○ 7 baseline controls	○ 7 baseline controls	 6 controls	 28 controls	 34 controls			 44 controls
Operational/ Management Controls	baseline processes to eliminate attack vectors			Establish site-specific processes (Procurement process, acceptance test, change control, etc.)					

Fig. 3. Consequence-based Security Assessment by NEI 13-10 [8]

2.4 EPRI TAM

Cyber Security Technical Assessment Methodology (TAM), developed by the U.S. Electric Power Research Institute (EPRI) in 2018, is a semi-quantitative cyber security assessment methodology that identifies attack pathways through a combination of vulnerable attack points and attack vectors for each digital asset and then assigns appropriate security controls to satisfy the allocated security controls score.

The risk assessment process using the TAM consists of three main steps. The first step is to identify attack pathways, exploit mechanisms, and exploit objectives according to the attack surface. Each exploit sequence identified through these combinations represents a particular attack scenario. In the second step, security controls for the exploit sequence are identified, which can be selected by the assessor based on the characteristics of the sequence, and the effectiveness of the selected security controls can be identified by assigning quantitative scores in terms of protection, detection, response/recovery, and technical, operational, and management aspects. In the third step, if there is a residual risk that remains despite the security controls applied in the previous phases, additional shared security controls that take into account the relationship with other assets are applied to mitigate the residual risk [4], [5], [6].

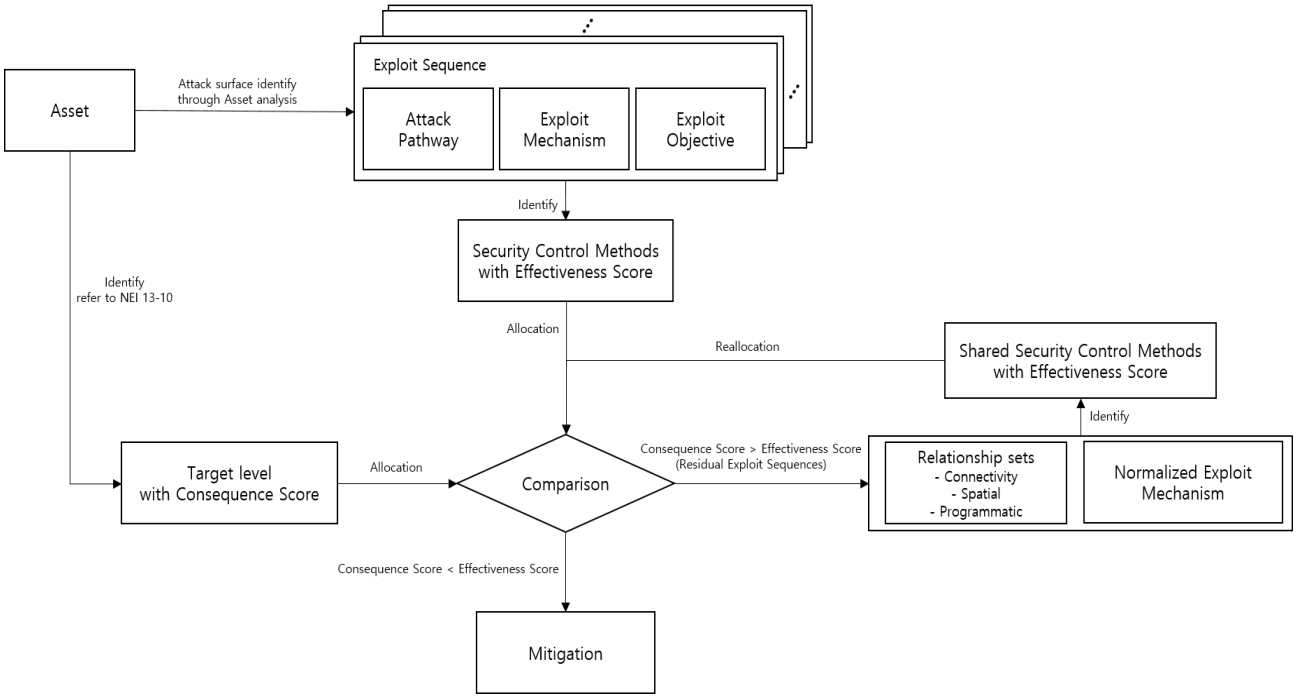

Fig. 4. General Process of EPRI TAM Methodology

III. Comparison of Cyber Risk Assessment Models

General risk assessment requirements are proposed by IEC, ISO, NIST, etc. and in this paper, we compared the models analyzed above with the main elements of security risk assessment presented in NIST SP 800-30 (Guide for Conducting Risk Assessment, 2012), a standard guideline for information security risk assessment in the U.S. [7], [8].

Through the analysis of each criterion, we identified the strong and weak points of the characteristics of each assessment model, and found that all models consider threats, vulnerabilities, and impacts, but in different ways and to different degrees. The TAM model assesses risk in a detailed, semi-quantitative manner, but requires a lot of preliminary resources and relies highly on the assessor's expertise, while the NEI 13-10 model reflects a primary attack vector/attack pathways analysis within itself and does not require separate threat and vulnerability assessments, making it relatively less dependent on the assessor's expertise.

The STPA-SafeSec model is a methodology based on safety analysis, so it is a security assessment centered on control signals/components, which has limitations in holistic security assessment. The NUREG/CR-6847 model can be effectively assessed with a relatively simple

procedure, but limitations can be identified such as risk reversal for low-critical assets and continuous changes in susceptibility and risk due to improvements in security controls.

Table. 1. Comparison Table of Cyber Risk Assessment

Mothed / Elements	NUREG/CR-6847	STPA-SafeSec	NEI 13-10	EPRI TAM
Threat	Partially considered (Consider 6 security measures within Susceptibility to mitigate attack vectors)	Partially considered (Consider network threats primarily from a control perspective)	Considered (Suggest security measures to mitigate this attack vector)	Considered (Considers attack vectors/scenarios including attack vectors)
Vulnerability	Partially considered (Consider physical/logical exposure within Susceptibility)	Alternatives considered (Consider hazardous scenarios)	Alternatives considered (Suggest security measures to mitigate the vulnerability)	Alternatives considered (Consider attack vectors/scenarios including attack surface)
Impact (Consequence)	Considered (Attack impact is included in the risk categorization)	Partially considered (Consider system-localized impacts due to control signal compromise)	Considered (Differentiate security measures based on attack impact)	Considered (Reflect attack impact on security goal level)
Security Controls	Partially considered (Consider the effectiveness of 6 security measures)	Partially considered (Consideration of security measures for the network from a control perspective)	Considered (Present security measures by impact and type)	Considered (Comparing the effectiveness score of goal score)
Assessment Approach	Qualitative assessment (based on qualitative metrics)	Qualitative assessment (Identify mitigation measures per risk scenario)	Qualitative assessment (based on qualitative impacts, typology)	Semi-quantitative assessment (based on qualitative metrics using quantitative scoring)
Analysis Approach	Sensitivity and impact-based analysis	Partial impact-based analysis	Impact-based analysis	Impact-based analysis
Information Availability	Medium preliminary information required	High preliminary information required	Low preliminary information required	High preliminary information required
Complexity	Relatively simple procedure	Complicated procedure with various signal analysis	Relatively simple procedure	Complicated procedure due to various factors considered
Risk Assessor	-Consistency of results across assessors -Medium reliance on evaluator expertise	High reliance on evaluator expertise	Low reliance on evaluator expertise	High reliance on evaluator expertise
Strong Point	-Only a small number of security measures and sensitivities can be assessed	-Allows detailed analysis of control signals within components	-No need for separate threat and vulnerability assessments as attack vector/path analysis is primarily reflected in the methodology -Many application cases	-Differentiate scores for different types of security measures -Considers various factors such as security measure effectiveness, implementation burden, shared security measures, etc.
Weak Point	-Risk reversal for low-critical assets -Improvements in security measures have a lasting impact on sensitivity/risk changes	-Based on safety analysis methodology, limited to holistic security assessment -Oriented toward control systems -Requires a lot of resources (information, manpower, etc.)	-Requires evaluation of additional security measures after categorizing assets by impact and type -Need to prepare rationale for some alternative measures, non-implementation	-Requires a lot of resources (information, time, manpower, etc.) -Difficult to understand how formulas, calculations work -Few application cases

IV. CONCLUSIONS

In this paper, representative cyber security assessment models for nuclear power plants were analyzed based on the elements of NIST SP 800-30, and their advantages and limitations were compared. As a result of the analysis, it was found that all models consider threats, vulnerabilities, and impacts, but in different ways and to different degrees. In addition, due to the difficulty in assessing the probability of cyber risk occurrence, various methods such as susceptibility analysis, assessment of security controls by asset type, and comparison of security control effectiveness scores are being considered. It is expected that these analysis results can be used for various studies, such as improvement studies to complement the limitations of each model, optimized model design studies, and model verification criteria studies, considering the weaknesses of each model.

ACKNOWLEDGEMENT

This work was supported by the Nuclear Safety Research Program through the Korea Foundation of Nuclear Safety (KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission (NSSC) of the Republic of Korea. (No. 2106012)

REFERENCES

[1] U.S. Nuclear Regulatory Commission, Cyber Security Self-Assessment Method for U.S. Nuclear Power Plant, NUREG/CR-6847, 2004.

[2] Journal of Information Security and Applications, STPA-SafeSec: Safety and security analysis for cyber-physical systems, Journal of Information Security and Applications 34, 183-196, 2017.

[3] U.S. Nuclear Energy Institute, Cyber Security Control Assessment Revision 6, NEI 13-10, 2017.

[4] U.S. Electric Power Research Institute, Cyber Security Technical Assessment Methodology: Risk Informed Exploit Sequence Identification and Mitigation Revision 1, EPRI, 2018.

[5] IEEE Access, D. Jung, J. Shin, C. Lee, K. Kwon, J. Seo, Cyber Security Controls in Nuclear Power Plant by Technical Assessment Methodology, 2023.

[6] Korea Institute of Information Security and Cryptology, J. Kim, A. Kim, K. Kwon, Technical Assessment Methodology based on IEC 31010, 2022.

[7] U.S. NIST, Guide for Conducting Risk Assessments, NIST SP 800-30 rev1, 2012.

[8] Korea Institute for Information and Communications Technology Promotion, K. Kwon, Security by Design for Nuclear Cyber Security, IITP Weekly Technology Trends 1982, 15-27, 2021.