EPRI Technical Assessment Methodology Analysis based on Risk Assessment Standards

Janghoon Kim, Aram Kim, Kookheui Kwon*
Korea Institute of Nuclear Nonproliferation and Control
**Corresponding author: vivacita@kinac.re.kr*

1. Introduction

Nuclear facilities are replacing existing analog systems with digital systems for the purpose of efficiently performing measurement, control, monitoring, and communication functions. However, the inherent vulnerabilities in digital systems bring challenging cybersecurity concerns to nuclear facilities. Accordingly, the cybersecurity field is demanding risk assessment activities to identify, analyze, and evaluate possible risks in digital systems and mitigate them.

To this end, risk assessors desire to select the most appropriate risk assessment techniques, but it is challenging to determine suitability among various approaches.

This study presents criteria for applying risk assessment techniques depending on their facility characteristics based on NIST and ISO standards. In addition, we provide an analysis of the EPRI Technical Assessment Methodology (TAM) used for nuclear facilities' risk assessment.

2. Criteria based on Risk Assessment Standards

Chapter 2 analyzes NIST SP 800-30 and ISO 31010, which are representative risk assessment-related standards, and presents criteria that can be used for risk assessment technique analysis.

2.1 NIST SP 800-30

NIST SP 800-30 provides guidance for organizations that provide services using information systems to implement risk assessments efficiently. The risk assessment process for NIST SP 800-30 is divided into Prepare, Conduct, Communication and share, and maintain. In particular, in the Prepare stage, the criteria for risk assessment models and analysis methods are presented in Figure 1 and Table I below [1]. In this study, this criterion is used to analyze risk assessment techniques.

Table I: Risk analysis approaches

Threat-oriented	An analysis method that constructs a cyber threat scenario based on the threat source and threat event identification and identifies the impact based on the attacker's intention.
Vulnerability-oriented	Starting with identification of Vulnerability and Predisposing condition, an analysis method that identifies possible threat events and their effects and constitute a scenario.
Asset/Impact-oriented	An analysis method that identifies the threat related to this based on the impact on assets and assets and constitutes a scenario.

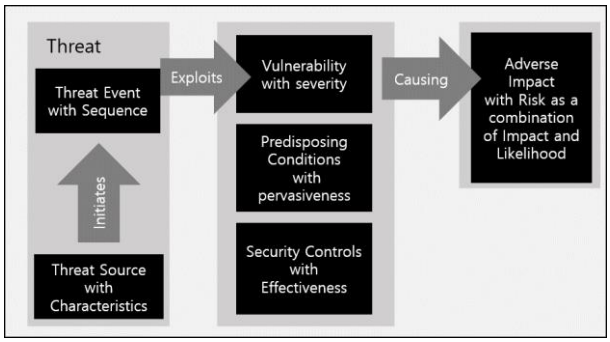

Fig. 1. Risk assessment model

2.2 ISO 31010

ISO 31010 is based on the ISO 31000 risk management process structure and provides guidance on selecting and applying assessment techniques to help understand risks. Procedures for implementing risk assessment are divided into "Plan the assessment", "Manage information and development models", "Apply risk assessment techniques", "Review the analysis", "Apply results to support decisions", "Record and report risk assessment processes and outcomes". In particular, at the Apply risk assessment techniques stage, considerations for selecting techniques and criteria for the characteristics of the risk assessment technique are presented in Table II and Table III below [2]. Table IV is an example of the results of analyzing the Bayesian network assessment technique according to the characteristics of the assessment technique. In this study, this criterion is used to analyze risk assessment techniques.

Table II: Consideration for selecting techniques

Purpose of assessment	Consideration of the selection of assessment techniques based on the assessment purpose
Needs of stakeholders	Consideration of the stakeholder requirements
Requirements	Consideration of legal, regulatory and contractual requirements
Environment and scenario	Consideration based on operating environment and assessment scenarios
Importance of decision	Consideration based on the importance of decision-making
Decision criteria	Consideration based on decision criteria
Time for decision	Consideration over time for decision-making
Information	Consideration based on available information
Complexity of situation	Consideration based on the complexity of the assessment situation
Expertise	Consideration based on assessor expertise

Table III: Characteristics of techniques

Application (Ap)	Application of review, identification, analysis, judgment, etc.
Scope (Sc)	Scope of assessments of institutions, departments, equipment, etc.
Time horizon (Ti)	Apply to short-term, medium-term, long-term risks, or any time
Decision level (De)	Risk determination at strategic, tactical, and operational levels
Starting info/data needs (St)	Level of information required for assessment
Specialist expertise (Sp)	Expertise of experts using assessment technology
Qualitative-Quantitative (Qu)	Analysis method
Effort to apply (Ef)	Time and cost required for application of assessment techniques

Table IV: Application of categorization of techniques (Bayesian network)

Ap	Sc	Ti	De	St	Sp	Qu	Ef
Identify Estimate	Any	Any	Any	M	H	Quant	M

3. EPRI TAM Analysis

Chapter 3 analyzes EPRI TAM based on the analysis criteria of risk assessment technique presented in Chapter 2. Through the analysis, results are derived to ensure that risk assessor understand the TAM assessment technique and properly consider the TAM assessment technique in the risk assessment process.

3.1 EPRI TAM (Technical Assessment Methodology)

TAM was developed for the purpose of assessing security controls for power plants in EPRI. TAM is a technique that analyzes the technical composition of assets to identify possible cyber risks and derive security controls to mitigate them [3]. In addition, utilization can be increased in conjunction with regulatory requirements such as NEI 08-09, NEI 13-10, R.G. 5.71, and NERC-CIP, and is currently partially used at Vogtle and UAE Barakah nuclear power plants [4-7].

The TAM consists of identify attack surface and exploit sequence (Step1), identity security control/scoring/allocation (Step2) and identify shard security control/scoring/allocation (Step3). In the first stage, assets are first analyzed according to the technical information availability (TIA) level to understand the composition and flow. Then, based on the asset analysis results, an exploit sequence consisting of attack surface, attack pathway, exploit mechanism, and exploit objective is derived to identify possible risks in the asset. In steps 2 and 3, security controls to mitigate the Exploit Sequence are derived, and the results are compared with the Consequence score of the asset to determine whether to mitigate it [8].

3.2 Results of EPRI TAM Analysis

Chapter 3, Section 2, aims to derive consistent results by analyzing TAM based on the risk assessment technique analysis criteria described in Chapter 2.

According to Chapter 3, Section 1, TAM identifies the possible exploit sequence based on asset analysis and derives the corresponding consequence. Accordingly, it can be determined that TAM is an Asset/Impact-oriented technique proposed in the NIST SP 800-30 standard. In addition, TAM can derive security controls to mitigate the exploit sequence and apply them to the consequence to determine the current risk level and risk mitigation. Accordingly, TAM can be expressed as a risk model in Figure 2 below. In Figure 2, the exploit sequence has the meaning of replacing the threat and vulnerability element of the NIST SP 800-30 risk assessment model. In addition, adverse impact can be determined by the consequence of assets and the security control against exploit sequence. In TAM, it is assumed that an attack occurred because likelihood was not considered, but the TAM uses exploit difficulty as a surrogate for likelihood with the results represented in the security effectiveness score of security controls. As a result, the risk assessment model for TAM can be composed of a security control allocation process to mitigate this by taking consequence as a risk.

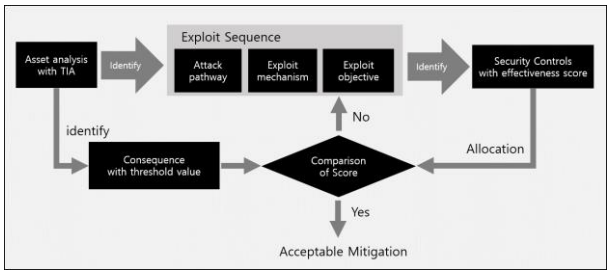

Fig. 2. TAM risk model

If TAM is analyzed according to the characteristic criteria of the ISO 31010 assessment technique, it can be determined in Table V below. In the case of Ap, it is judged as identification because exploit sequence and consequence are derived through asset analysis, and the process of deriving the final risk level by allocating the security control score to the consequence score is judged as analysis. In the case of Sc, TAM is judged as a system or device because it is the target of analyzing components and data composed of assets. In the case of Ti, since it is assumed that the TAM consider all risks that may be occurred, it can be determined as any. In the case of De, the risk is determined only by considering the technical composition of the asset, so it can be determined in terms of operation. In the case of St, it may be determined according to the TIA level of the TAM. In the case of Sp, it basically, a high level is

required. In the case of Qu, the risk level and mitigation are determined using quantitative values, so it can be determined quantitatively. In the case of Ef, it can be determined according to the TIA level.

Table V: Application of categorization of techniques (TAM)

Ap	Sc	Ti	De	St	Sp	Qu	Ef
Identify Analysis	System, Device	Any	Oper	About TIA	H	Quant	About TIA

Finally, it is believed that risk assessors can determine the suitability of TAM based on considerations and TAM analysis results when selecting risk assessment techniques.

4. Conclusions

In this study, the criteria for the risk assessor to understand and apply appropriate assessment techniques according to the assessment situation were presented based on the contents of the NIST and ISO risk assessment standards. In addition, consistent and comparable results were derived by analyzing the EPRI TAM according to the criteria presented. The results can be used as a reference for risk assessors to understand and apply risk assessment techniques. In addition, compared to other assessment techniques, it can be used to select an optimal risk assessment technique according to considerations when selecting.

ACKNOWLEDGMENTS

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

REFERENCES

[1] NIST, Guide for Conducting Risk Assessments, NIST SP 800-30, 2012.
[2] ISO, Risk Management-Risk assessment techniques, ISO 31010, 2019.
[3] J. Daun, S. Jiho, L. Chaechang, K. Kookheui, S. Jungtaek, TAM analysis of cybersecurity assessment methodology for power plants, Korea Institute of Information Security & Cryptology (KIICS), Vol.30, no.5, 2020.
[4] NEI, Cyber Security Plan for Nuclear Power Reactors, NEI 08-09 Rev. 6, 2010.
[5] NEI, Cyber Security Control Assessments, NEI 13-10 Rev. 5, 2017.
[6] NRC, Cyber Security Programs for Nuclear Facilities, R.G 5.71, 2010.
[7] NERC, Critical Infrastructure Protection Standards.
[8] EPRI, Cyber Security Technical Assessment Methodology- Risk Informed Exploit Sequence Identification and Mitigation, 2018.