Transactions of the Korean Nuclear Society Spring Meeting

EPRI Technical Assessment Methodology Analysis based on Risk Assessment Standards

Janghoon Kim [1], Aram Kim [1], Kookheui Kwon [1*]
[1] *Korea Institute of Nuclear Nonproliferation and Control, Republic of Korea*
**Corresponding author: vivacita@kinac.re.kr*

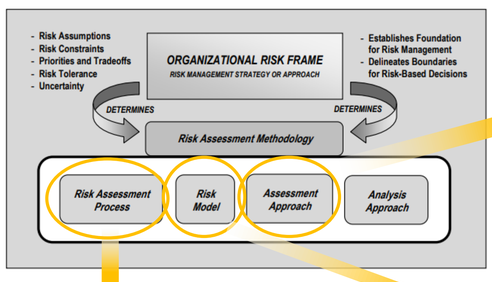
OVERVIEW

- Nuclear facilities are **replacing existing analog system with digital system** for efficiently performing measurement, control, monitoring, etc.
- However, the **inherent vulnerability in digital systems bring cybersecurity concerns** to nuclear facilities.
- Accordingly, **the cybersecurity field is demanding risk assessment activities** to evaluate possible risks in systems and mitigate them.
- For this requirement, **Assessors desire to select the most appropriate risk assessment technique, But, it is challenging.**
- So, **this study presents criteria for selecting risk assessment technique** depending on their facility characteristics.
- And, **we provide result of EPRI TAM analysis based on criteria** that refer to ISO, NIST standard.

RISK ASSESSMENT STANDARD ANALYSIS

NIST SP 800-30 Analysis

- NIST SP 800-30 provides guidance for organizations that provide services using information system to implement risk assessment efficiently.



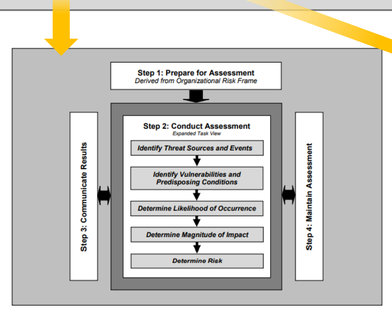
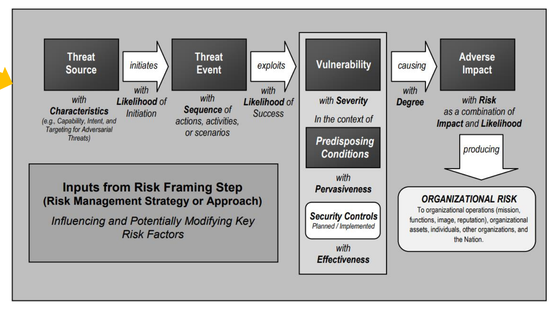


Table I: Risk analysis approaches

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.



ISO 31010 Analysis

- ISO 31010 provides guidance on selecting and applying assessment techniques to help understand risks.

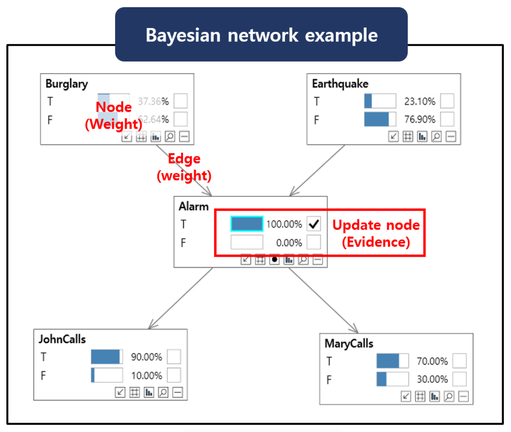
Table III: Characteristics of techniques

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 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

Applying



Evaluating

Selecting

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

EPRI TAM ANALYSIS RESULT BASED ON REQUIREMENTS OF STANDARD

- TAM was developed for the purpose of assessing security controls for power plants in EPRI.
- Analyzes the technical composition of assets to identify possible cyber risks and derive security controls to mitigate them.
- In addition, utilization can be increased in conjunction with regulatory requirements such as NEI 13-10, R.G. 5.71, NERC-CIP, etc.
- Currently partially used at Vogtle and UAE Barakah nuclear power plants

- TAM is an Asset/Impact-oriented technique
- TAM can be derive security controls to mitigate the exploit sequence and apply them to the consequence to determine the current risk level
- TAM is analyzed according to the characteristic criteria of the ISO 31010

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
Sc	TAM is judged as a system or device because it is the target of analyzing components and data composed of assets
Ti	Since it is assumed that the TAM consider all risks that may be occurred, it can be determined as any
De	The risk is determined only by considering the technical composition of the asset, so it can be determined in terms of operation
St	It may be determined according to the TIA level of the TAM
Sp	It basically, a high level is required
Qu	The risk level and mitigation are determined using quantitative values, so it can be determined quantitatively
Ef	It can be determined according to the TIA level

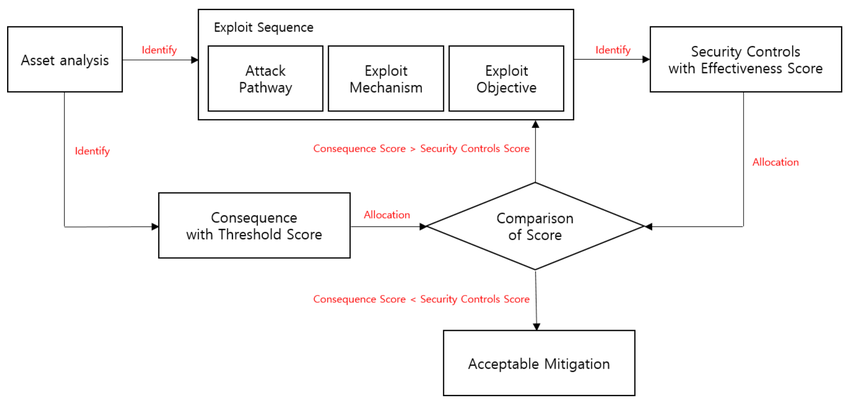


Table V: Application of categorization of techniques (TAM)

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

CONCLUSION

- 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.

KINAC
KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
한국원자력통제기술원