STPA-SafeSec Evaluation based on IEC 31010 Standard

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

1. Introduction

STPA-SafeSec (System-Theoretic Process Analysis – Safety and Security Analysis), a safety and security risk assessment methodology, is a system theory-based risk assessment methodology and is a methodology to reinforce the shortcomings of STPA-Sec previously proposed. The author of STPA-SafeSec explains that STPA-Sec does not properly consider security for real components because it only considers security from a control perspective, and to this end, they proposed STPA-SafeSec, a methodology that adds analysis of component perspectives to STPA configurations [1]. In addition, researches to analyze STPA-SafeSec and apply it to the industry is also being actively conducted. Using the STPA-SafeSec, the effect of cyber-attacks on the Condensate water system in the nuclear power plant is analyzed [2], and [3] analyzes the effect of cyber-attacks on PPS in the nuclear power plant. In order to compare STPA-Sec and STPA-SafeSec [4], they propose three perspectives: safety and security framework setting, security by design, and threat modeling, and their necessary and sufficient conditions.

However, studies in which STPA-SafeSec is compared to other existing assessment methodologies are found to be insufficient, which is expected to be necessary as a base study for assessors to select STPA-SafeSec when performing risk assessments on security. Accordingly, in this paper, STPA-SafeSec is analyzed and comparable results are derived based on the IEC 31010 standard (Risk management - Risk assessment techniques) that provides guidance on the selection and application of techniques for assessing risk in a wide range of situations [5].

To this end, detailed features are identified by analyzing the composition and procedure of STPA-SafeSec, and criteria based on IEC 31010 are presented. And, based on this, the process of evaluating the characteristics of STPA-SafeSec and its results are presented. This is to allow assessors to make optimal choices by comparing the differences between STPA-SafeSec and other risk assessment methodologies such as TAM (Technical Assessment Methodology) when developing an assessment model.

2. STPA-SafeSec Analysis

STPA-SafeSec is a methodology that adds a process to STPA-Sec for considering security in detail, which identifies a component layer diagram that maps to a control layer diagram and derives a causal factor of a security aspect including malicious intent. The composition and procedure of STPA-SafeSec are expressed as shown in Figure 1.

STPA-SafeSec first defines possible accidents within the scope of assessment. and then derive constraints on the risks that could cause accidents from a safety and security perspective. Then design the control layers associated with the constraints and define the control actions. Within the defined control action, the underlying potential causal factors for the attack are defined and unsafe/unsecure control action is identified. Up to this point, it is the same as the existing STPA-Sec. STPA-SafeSec identifies the component layer that can be mapped to the Control Layer and identifies the security flaw that can pose a risk to consider detailed security constraints here. Based on the derived system flaw, the security constraints are redefined, and based on this, the security perspective is identified as a reinforced Hazard scenario. In addition, mitigation strategies can be established by analyzing threats and vulnerabilities that may exist based on the component layer.

3. Evaluation Criteria based on IEC 31010

IEC 31010 classifies the characteristics of risk assessment technologies, and based on this, it is possible to consider how risk assessment technologies are used for assessment and how many burdens are involved in implementation [5]. Based on this, this paper summarizes the characteristics of the assessment technology as follows.

Table I: Evaluation criteria based on IEC 31010

Application (Ap)	Check assessment technique is applicable to the risk identification, analysis and evaluation process.
Time horizon (Th)	Check assessment technique is applicable for short-term or shutdown periods, and for long-term or operational periods.
Required information(Ri)	Check that the information required to use the assessment technique is readily available.
Required specialist expertise (Rs)	Check that significant training or expertise is required and short training is sufficient to use the assessment technique
Implementation burden (Ib)	Check the time and cost of using the evaluation technique
Analysis method(Am)	Check assessment technique supports quantitative or qualitative assessments

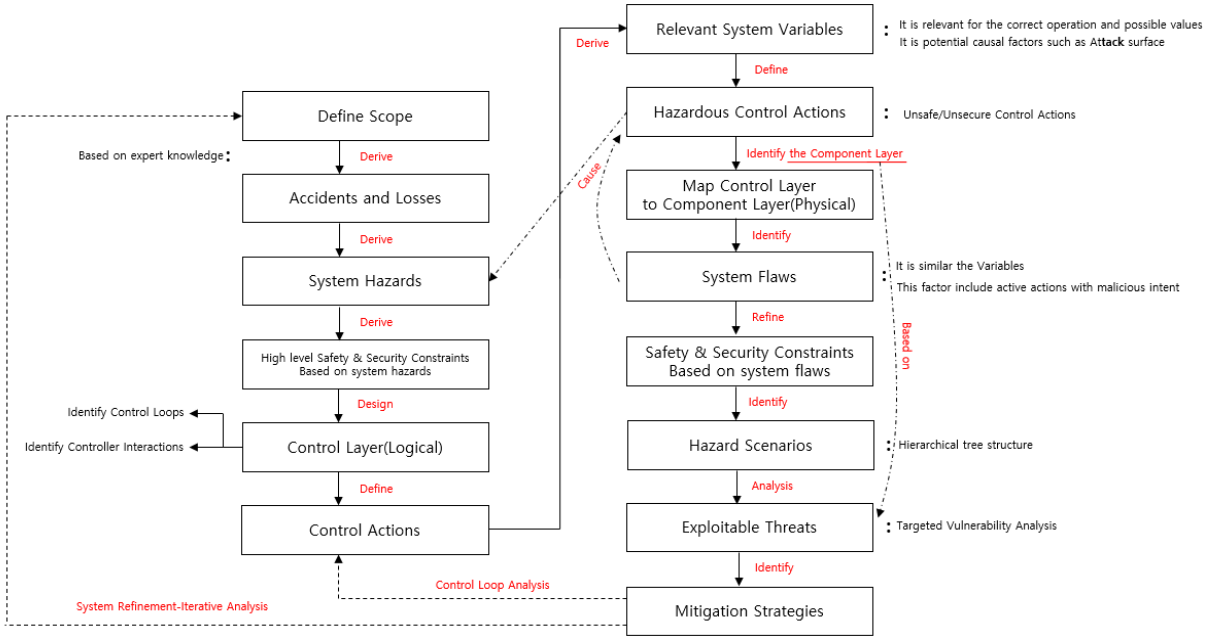

Fig. 1. Composition and procedure of STPA-SafeSec

4. Results of Evaluation

In this chapter, the STPA-SafeSec analyzed in Chapter 2 is evaluated based on the criteria presented in Chapter 3. evaluation is made based on results of existing related studies and the analysis in this paper. In the case of (Ap) of Table I, the risk scenario is derived as a result of the [1], [2], and [3] studies, but it is confirmed that only risk identification is performed because the impact or likelihood of the scenario is not considered. In the case of (Th), since the risk from the control perspective is evaluated, it is confirmed that the risk from the operational side can be considered, not from a simple device. In the case of (Ri), (Rs), (Ib), it is necessary to understand and identify the control process and the components related to control within the assessment range, so detailed information related to the target is required, and a high level of expertise is required to understand the information. In addition, it is confirmed that the burden in terms of time and cost to secure such information, expertise, and implement assessment technology will be high. In the case of (Am), it is confirmed that quantitative analysis is not presented in the STPA-SafeSec process, and [1] also mentions that methods for quantitative analysis can be added to STPA-SafeSec, so it is confirmed that only qualitative assessment is supported.

Table II : Results of evaluating the STPA-SafeSec

Application (Ap)	It is confirmed that only risk identification.
Time horizon (Th)	It is confirmed that the risk from the operational side can be considered.
Required information(Ri)	It is confirmed that the detailed information related to the target is required.
Required specialist expertise (Rs)	It is confirmed that the high level of expertise is required to understand the information.
Implementation burden (Ib)	It is confirmed that the burden in terms of time and cost to secure such information, expertise, and implement assessment technology.
Analysis method(Am)	It is confirmed that only qualitative assessment is supported.

5. Conclusions

In this paper, STPA-SafeSec was analyzed and comparable analysis results were derived by applying IEC 31010 standard-based criteria. Based on the analysis results, assessors can confirm that STPA-SafeSec can be used to identify risks and that operational risks can be considered from a control perspective. In addition, the burden of information, expertise, time, and cost for implementation will be high, and additional methodologies for quantitative analysis can be expected. If differentiation from other methodologies can be confirmed based on this, and various comparison results can be obtained, quantitative comparison criteria can also be presented in the future.

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] I. Friedberg, K.McLaughlin, P.Smith, D.Laverty, and S. Sezer, STPA-SafeSec: Safety and Security Analysis for Cyber-Physical systems, Journal of Information Security and Applications, Vol.34, p.183-196, 2017.
[2] J. Shin, J. Choi, J. Lee, C. Lee, J. Song, Application of STPA-SafeSec for a cyber-attack impact analysis of NPPs with a condensate water system test-bed, Nuclear Engineering and Technology, Vol.54, p.3319-3326, 2021
[3] J. Shin, J. Lee, J. Song, J. Choi, Methodology on Cyber-attack Impact Analysis for PPS by using STPA-SafeSec, Transations of the Korean Nuclear Society Autumn Meeting Goyang, Korea, 2019.
[4] T. Kaneko, Y. Takahashi, T. Okubo, R. Sasaki, Threat analysis using STRIDE with STAMP/STPA, The international workshop on evidence-based security and privacy in the wild, 2018.
[5] IEC, Risk management - Risk assessment techniques, IEC 31010, 2019.