Proposal to Modify Types of the Unsafe Control Actions in the STPA for the Detailed Sub-task Analysis of the Human Reliability Analysis

Seong Woo Kang*, Jaewhan Kim, Jinkyun Park, Sung-Min Shin, Ho-Gon Lim

Risk Assessment Research Division, Korea Atomic Energy Research Institute, Daejeon, Korea
**Corresponding author: swkang@kaeri.re.kr*

Keywords: STAMP, STPA, multi-unit accident, HRA, portable equipment

1. Introduction

In a real-world nuclear power plant (NPP), a multi-unit accident can occur not just from internal events but also from beyond design-basis extreme external events (from here on referred to as *external events*) such as earthquakes, wildfires, and tsunamis. In such a case, various accident management organizations are expected to be launched in order to collectively perform preventive and/or mitigative actions. These organizations and workers may cooperate at an inter-unit level, and these inter-unit interactions must be assessed to better estimate the risk of commercial NPPs. In other words, multi-unit human reliability analysis (MU-HRA) and ultimately probabilistic safety assessment (MU-PSA) need to be performed to gain more realistic site-level insight to improve the multi-unit accident management guidelines and practices involving NPP workers/staffs.

One objective of MU-PSA is to gain insights on current accident response practices for the goal of further reducing the multi-unit and site core damage frequency (CDF). One way to reduce such CDF is to reduce the human and organizational errors that may arise during the utilization of the portable equipment during multi-unit accident responses. To gain such insights, human and organizational error probabilities (HEPs and OEPs, from here on will just be referred to as *HEPs*) must first be quantified.

To quantify HEPs, traditional (single-unit) HRA methods generally assume limited to no transfer and sharing of the equipment with other units for the accident management. Traditional HRA also focus on the human operators working for the specific unit (i.e., MCR and local operators) as mainly responsible for the preventive and mitigative actions. These assumptions allowed the HRA practitioners in the past to examine and assess the detailed sub-tasks with respect to specific human failure events (HFEs), without involving complicated situations and interactions involving various inter-unit organizations on a site level.

However, accident response strategies for the multi-unit and site level accidents (such as diverse and flexible coping strategies, FLEX, and multi-barrier accident coping strategy, MACST) may involve deployment of portable equipment that are not pre-installed at the target unit [1,2]. Moreover, these strategies likely will involve interorganizational interactions required to transfer, install, and operate the required portable equipment. Therefore, to conduct the more realistic MU-HRA for the MU-PSA approach, important sub-tasks reflecting interorganizational characteristics that arises from the deployment of these portable equipment must be properly identified without missing critical ones.

Previous research [3] attempted to do so by using concepts from the Systems-Theoretic Accident Model and Processes (STAMP) and Systems-Theoretic Process Analysis (STPA). As one faucet of the systems theory, STAMP was originally developed at Massachusetts Institute of Technology (MIT) as an accident causality model based on the systems theory. Based on STAMP, a four-phase hazard analysis technique called STPA was also developed [4].

However, through the case study, it was found that the utilizing traditional STPA for the purpose of HRA may allow catching critical sub-tasks but also may require large amount of resources which may burden the HRA practitioners (i.e., too detailed results and too much resources). Accordingly, to be better utilized in the detailed sub-task analysis of the HRA, this study proposes simplification/modification of the standard STPA technique.

2. STAMP and STPA

For the detailed examination of a system, STAMP visually expresses the target system using connections of control loops, where each control loop is composed of a controller, a controlled process, feedbacks (FBs), and control actions (CAs), as shown in Fig. 1.

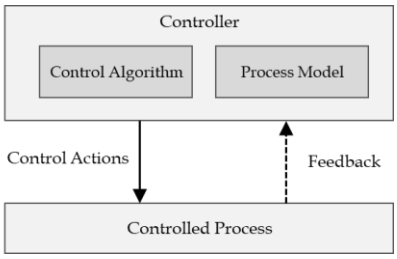

Fig. 1. Typical control loop configuration of STAMP

A "controller" makes decisions and provides control actions for the "controlled process," which can be a physical process or another controller. The controller makes "control actions" based on its "control algorithm." A "process model" is the controller's internal beliefs and other relevant aspects of the system/environment that are used to make decisions, being updated in part by "feedback" that comes from observing the controlled process.

STPA has four phases as shown in Fig. 2 [4]. For the purpose of MU-HRA detailed sub-task analysis, however, up to third STPA phase will be utilized, to examine and extract the catalog of unsafe control actions (UCAs) as detailed sub-tasks of the specific target HEPs.

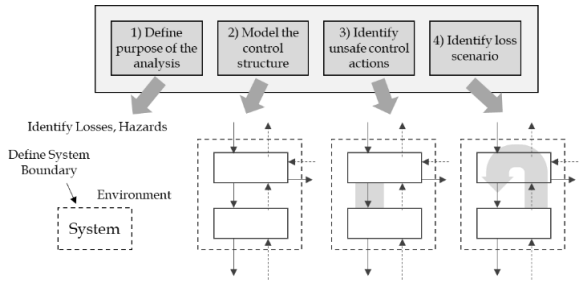

Fig. 2. Generic four phases of STPA

When using the STPA technique, it is recommended for the practitioners to follow the specific format of each UCA [4]. These UCA types are listed in Table 1. The descriptions specified in the UCA regarding the ″controller" and ″control action" are sources of information that may be used for identifying detailed sub-tasks of the specific HFE to be examined.

Table 1. Representative UCA types in traditional STPA

UCA type	Description format
Not providing causes hazard	Hazard occurs because "controller" does not provide "control action"
Providing causes hazard	Hazard occurs because "controller" provides "control action"
Providing too early, too late, out of order causes hazard	Hazard occurs because "controller" provides "control action" too early, too late, or in the wrong order
Providing too long or stopping too soon causes hazard	Hazard occurs because "controller" provides "control action" for too long or too short

The use of STAMP/STPA is just not limited to developing schematics of physical and functional processes; they can be used for detailed analysis of interactive processes between human operators and non-human resources, such as railways, aircrafts, adaptive software, cybersecurity, NPP digital I&C and protection systems [5,6]. It can also be used to model complex interactions that may arise from multi-unit accident responses [3]. This is because STAMP models not only physical controls by engineered systems (such as initiation signals or interlocks) but also includes the managerial or operational controls that are essential for the accomplishment of a required task and/or function.

The purpose of using STPA is to follow a systematic methodology to avoid "missing" critical UCAs (e.g., detailed sub-tasks in the HRA process). However, for the purpose of HEP quantification, having too much details may make the quantified probabilities extremely conservative, as conservative values of each detailed sub-tasks may snowball (i.e., add up to result in extremely high and possibly unrealistic probability values for the examined HFE). Dividing the specific HFE into too much detailed sub-tasks may also burden the HRA practitioners during the HRA processes, since there are many HFEs in the PSA models.

Therefore, for the purpose of utilizing STAMP/STPA for the HRA (at least in the field of nuclear safety), this research proposes simplified modification of the UCA categories in the STPA.

3. Simplification/modification of the UCA types for the HRA applications

Previous research to apply the STAMP/STPA for the HRA purposes showed that some types of UCAs rarely gets identified for typical NPP accident responses [3]. For the perspective of multi-unit accident management involving portable equipment, *providing control actions correctly* (UCA type 2), *providing too early* (part of UCA type 3) or *providing control actions too long* (part of UCA type 4) generally do not cause problems for the accident mitigation [3]. Furthermore, for the perspective of traditional HRA, not providing or providing too late both counts as similar failure for the sub-task quantification

For the detailed analysis of the HFE sub-tasks involving portable equipment, therefore, it is proposed that the UCA types are to be simplified to

1) not providing / providing too late,
2) out of order causes hazard, and
3) stopping too soon causes hazard

to reduce the amount of time and effort the HRA practitioners may require to follow the technique

procedure. The proposed modified STPA types and descriptions to be used as a guideline for the HRA practitioners are shown in Table 2.

Table 2. Proposed modification to the UCA types and guideline for the detailed HFE sub-task analysis

Modified UCA types	Guideline	Additional details for the HRA practices
Not providing / providing too late causes hazard	(<UCA number>) [<hazard number>] <*Controller*> fails or provides too late <*Control Action*>	after/when <prerequisite *Control Action* and/or *Feedbacks*, if any> when/during <other situational/environmental conditions>
Providing out of order causes hazard	(<UCA number>) [<hazard number>] <*Controller*> provides <*Control Action*> out of order	
Stopping too soon causes hazard	(<UCA number>) [<hazard number>] <*Controller*> provides <*Control Action*> too short	

4. Future Work

For the future work, a case study will be performed on the HFE "failure of deploying the portable diesel generator" to show feasibility of the proposed methodology and to compare with the results from the previous research [3]. Once the detailed sub-task analysis using the proposed simplified STPA is done, the HEP of the examined HFE will ultimately be quantified to compare with other methodologies that quantified the corresponding HFE without accounting for various interorganizational interactions.

Acknowledgement

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea (No. 20224B10200050). This research was also supported by the National Research Council of Science & Technology (NST) grant by the Korea government (MSIT) (No. GTL24031-000)

REFERENCES

[1] NEI. Diverse and Flexible Coping Strategies (FLEX) Implementation Guide. NEI 12-06, Rev. 5, NEI, April 2018.
[2] B. Seong, KHNP Accident Management Plan Accident Management Organization and Response System, Nuclear Safety & Security Information Conference 2023, June 2023.
[3] S. Kang, et al., Applicability of STAMP/STPA to the Multi-unit Human Failure Event Analysis for the Multi-unit Accident Safety Assessment, 17th International Conference on Probabilistic Safety Assessment and Management & Asian Symposium on Risk Assessment and Management (PSAM17&ASRAM2024), October 2024.
[4] Leveson, N. G., Thomas, J. P., 2018. STPA Handbook, MIT.
[5] Shin, S. M., Lee, S. H., Shin, S. K., Jang, I., & Park, J. (2021). STPA-based hazard and importance analysis on NPP safety I&C systems focusing on human–system interactions. Reliability Engineering & System Safety, 213, 107698.
[6] Shin, S. M., Lee, S. H., & Shin, S. K. (2022). A novel approach for quantitative importance analysis of safety DI&C systems in the nuclear field. Reliability Engineering & System Safety, 228, 108765.