Applicability of STAMP/STPA to the Multi-unit Human Failure Event Analysis for the Multi-unit Accident Safety Assessment

Seong Woo Kang[a], Sung-Min Shin[a], Jong Woo Park[a], Jinkyun Park[a*]
[a]Korea Atomic Energy Research Institute (KAERI), Daejeon, Republic of Korea
*Corresponding Author: kshpjk@kaeri.re.kr

Abstract: The Fukushima Daiichi accident raised many challenges in performing realistic risk estimation for commercial nuclear power plant (NPP) sites with multiple units. One key difference between the traditional single-unit probabilistic safety assessment (PSA) and multi-unit PSA (MUPSA) is that the MUPSA must consider the dependencies across the reactor units within a same plant site. Since human resources and equipment may be shared across multiple units during emergency responses for the multi-unit accident, list of human failure events (HFEs) identified from traditional fault tree analysis (FTA) and their subtasks extracted from traditional human reliability analysis (HRA) may not be enough for the MUPSA.

In this study, STAMP/STPA (Systems-Theoretic Accident Model and Processes/Systems-Theoretic Process Analysis) is applied to perform detailed analysis on multi-unit HFEs during general multi-unit emergency responses involving shared equipment, with 1MW mobile generator as a case study. Traditional hazard analysis methods break down the target system into components and analyze each part separately, assuming the properties of each component do not change significantly when looking at the system as a whole. However, STPA is a hazard analysis method based on the systems theory, assuming that a system can be more than sum of its parts. Based on a premise that an accident stems from control problems, STPA provides a structured systematic approach for the hazard analysis that include not just the component failures but also the interaction failures and flawed controller requirements. Through this research, it is shown that potential hazards stemming from complex inter-organizational interactions of the emergency response organizations (EROs) and shared equipment during a general multi-unit accident can be identified using STPA by systematic identification of unsafe control actions (UCAs) through qualitative systematic approach.

Keywords: STAMP/STPA, multi-unit accident, human failure events, organizational failure events

1. INTRODUCTION

Probabilistic safety assessment (PSA) technique was developed to provide realistic risk estimates of the commercial nuclear power plants (NPPs). Traditionally, PSA has been performed to find a risk of a single NPP unit, assuming independence in human operator actions, safety systems, and other equipment among different units. However, the Fukushima Daiichi accident showed that dependencies across reactor units that are in a same NPP site also must be considered to estimate a realistic risk of the NPPs, contrary to the traditional PSA approaches. Furthermore, human resources during the NPP accident management may be shared among different units. Therefore, multi-unit PSA (MU-PSA) and multi-unit human reliability analysis (MU-HRA) is required for more accurate NPP risk estimation.

Multi-unit accident scenarios contain complicated interactions among different organizations (e.g., Technical Support Center) and mobile equipment (e.g., 1MW mobile generator). Based on the systems theory, STAMP/STPA (Systems-Theoretic Accident Model and Processes/Systems-Theoretic Process Analysis) can be used to analyze not just the failures of components in a system but also properties and characteristics that arise from interactions between components [1]. Since multi-unit accident responses are composed of interactions between multiple organizations and equipment, one need to analyze both individual failures of each organization/equipment as well as failures from the integrated environment. The STAMP/STPA can be a useful basis for deriving HRA for multi-unit accident scenarios (i.e., analysing the catalog of subtasks included in a specific HFE with the associated human error modes).

In this study, STAMP/STPA is applied to perform detailed analysis on multi-unit human failure events (HFEs) during general multi-unit emergency responses involving shared equipment, with “1MW mobile generator failure” selected as a case study.

2. METHODOLOGY: APPLYING STAMP/STPA TO IDENTIFY HRA ELEMENTS

The STAMP technique was originally developed at Massachusetts Institute of Technology (MIT) as an accident causality model [2] based on the systems theory, viewing a given system as a greater than sum of its parts. STAMP visually expresses the target system using connections between many control loops, where each control loop is composed of a controller (including control algorithm and process model), controlled process, feedbacks (FBs), and control actions (CAs). Figure 1 illustrates these elements, and Table 1 summarizes the key elements included in the control loops.

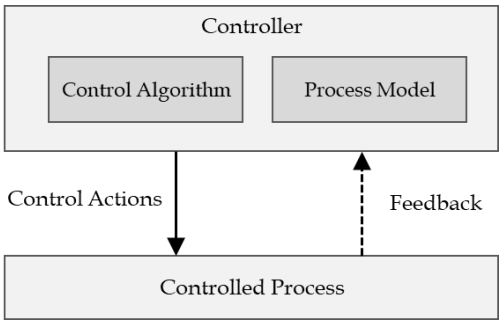

Figure 1. Typical control loop configuration of STAMP

Table 1. Key elements included in a STAMP control loop

Element	Description
Controlled process	Object to be controlled
Feedback (FB)	Information indicating the status of the controlled process
Controller	Subject determines whether a CA is generated or not. Control algorithm: The controller's decision-making procedures or logic Process model: Status of the controlled process understood by the controller (internal belief)
Control action (CA)	Control commands issued by the controller

STAMP is not limited to providing a schematic of physical and functional processes but can also be used for delineating interactive processes including human operators, related organizations, and even non-human resources such as accident management equipment [3-7]. In other words, the CA in STAMP implies not only physical controls by engineered systems such as initiation signals or interlocks but also the managerial or operational controls that are essential for the accomplishment of a required task/function.

STPA is a four-phase hazard analysis technique that utilizes STAMP, as shown in Figure 2 [1]. It should be noted that the second phase in the figure corresponds to the development of the STAMP model, i.e. STAMP is a model that provides a way to scheme and visualize the interactions, and STPA utilizes STAMP.

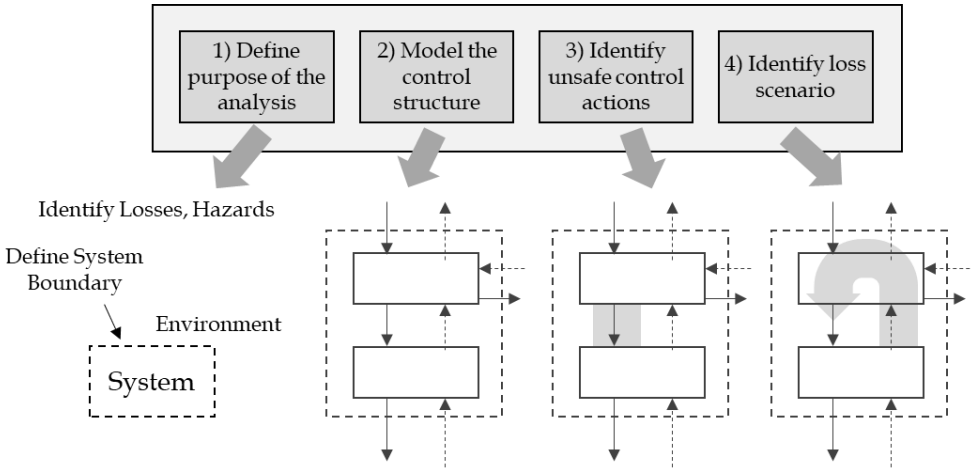

Figure 2. Four phases of STPA [1]

- Developing a STAMP model: First phase of the STPA defines catalog of undesired losses and hazards. A loss can be defined in various ways according to the analysis purpose, such as human death/injury, property damage, environmental pollution, or mission failure. On the other hand, a hazard refers to a single or collective condition of the system that can lead to a predefined loss. It should be noted that losses can be distinguished from hazards because the former denotes a unique status that can no longer be controlled by the system. Along with the definition of losses and hazards, the scope of analysis (boundary of the system) and the associated environment should also be outlined. During second phase of the STPA, causal factors and control flaws are identified through development of a control structure. This is done utilizing elements shown in Figure 1 and Table 1 (FBs, CAs, controllers, and controlled processes). To better understand and represent the complicated subsystems of the overall system, control structure includes a control loop model of each subsystem along with relationships among these subsystems.

- Performing hazard analysis: In the third phase, among the CAs developed in the second phase, a catalog of unsafe control actions (UCAs) is identified that could lead the status of the system to an undesired condition (i.e., hazard). For the sake of clarity, it is recommended that the description of each UCA generally includes the following information: (1) controller, (2) control action, (3) UCA type, (4) context, and (5) relevant hazard. In terms of potential UCA types, Table 2 exemplifies four kinds of UCAs that can be generally applied. In the fourth phase, the causes of the UCAs are analyzed. Through this cause analysis, a scenario leading to one of the predefined losses (i.e., loss scenario) can be clarified by combining three pieces of information such as "UCA cause" – "UCA" – "Hazard" – "Loss". Causes of each UCA may contain diverse aspects including (but not limited to) incorrect feedback, inappropriate requirements, design errors, and component failures.

Table 2. Representative UCA types

UCA type		Description format
1	Not providing causes hazard	Hazard occurs because <Controller> *does not provide* <Control Action>
2	Providing causes hazard	Hazard occurs because <Controller> *provides* <Control Action>
3	Too early, too late, out of order	Hazard occurs because <Controller> *provides* <Control Action> *too early, too late, or in the wrong order*
4	Too long or too soon	Hazard occurs because <Controller> *provides* <Control Action> *for too long or too short*

With its systematic approach that can be used for analyzing diverse types of hazards, STPA would be an effective tool for identifying the catalog of HRA elements if one is able to develop a STAMP model that properly describes the interactions among human operators belonging to diverse emergency response organizations. In order to verify this expectation, STAMP/STPA is used to identify the HRA elements (e.g., a list of subtasks with expected human error modes) that are essential for conducting the MU-HRA.

3. CASE STUDY USING THE PROPOSED FRAMEWORK (1MW MOBILE GENERATOR)

In this section, a case study is carried out with respect to the HFE "Failure of starting and running the 1 MWe mobile diesel generator" that corresponds to one of the typical HFEs considered in the progression of a multi-unit ELAP scenario followed by MU-LOOP.

3.1 HFEs and assumptions for the case studies

When a MU-LOOP occurs, MCR operators of each unit should immediately supply electric power to required components by running stand-by EDGs. However, in this case study, it was assumed that all EDGs were not

available due to their simultaneous failures. Then, if electric power recovery using the AAC-DG fails, 1 MWe mobile generators stored onsite at safety center headquarters (SC HQ) can be installed and used as an alternative power source.

In the case study, STAMP/STPA was applied to the HFE "Failure of starting and running the 1 MWe mobile diesel generator," which was chosen from fault trees of the MU-PSA models. For the sake of simplicity, no mechanical failures of the 1 MWe generator were considered. In addition, the following assumptions were made.

- Units: It was assumed that there are six units in total at the site. There are multiple EROs that interact for starting and running the 1 MWe mobile generator, with the developed STAMP/STPA model reflecting on it.
- Systems: It was assumed that each unit has two EDGs (which failed) and one 1 MWe mobile generator, and that the two units share one AAC-DG (which also failed). Starting and running failures of the systems/components were not considered in this case study.
- Organizations onsite: It was assumed that an augmented ERO (e.g., EOF, TSC, and OSC) is convocated for the multi-unit accident response for the case studies. For rest of this paper, aabbreviations EOF, TSC, OSC, MCR, SC, HQ, FO, and CNV_WORK stand for emergency operations facility, technical support center, operational support center, main control room, safety center, headquarters, field operators, and convocated workers (from offsite, outsourcing), respectively. One TSC is assigned to two units, and it has technical responsibility for coping with the progression of the multi-unit accident. The EOF makes decisions on a site-level. The SC and OSC have responsibilities for the installation and maintenance of any mobile equipment, respectively. Both the TSC and OSC are located onsite, but the EOF is installed offsite. Also, with each unit having its own 1 MWe mobile generator, the EOF was not considered in the development of the STAMP for this case study.
- Organizations for each unit: It is assumed that the MCR operators of each unit consist of a senior reactor operator, safety technical advisor, reactor operator, electrical operator, and turbine operator. During the progression of the multi-unit accident, the MCR serves as the initial emergency organization before the convocation of the augmented ERO (e.g., TSC, OSC, and EOF). There are also field operators (FOs) of each unit working onsite. The 1 MWe mobile generator requires not just the FOs (for operation) but also the outsourced workers (convocated from offsite, for moving, installing, connecting, and refueling the equipment).

3.2 Identifying HRA elements for the failure of the 1MWe mobile generator

Successful operation of the 1 MWe mobile generator may require interactions between multiple EROs. Organizations and interactions are defined for the examined HFE identified in a typical MU-PSA model, "Failure of starting and running the 1 MWe mobile diesel generator," that are related to the failure of the installation (i.e. start), operation (i.e. run), and refueling of the 1 MWe mobile generator. In the case study, STAMP/STPA was performed from the perspective of using 1 MWe for unit #1 (referred as 1MW_#1 hereafter).

Figure 3 shows a schematic of organizations involved for successful installation (connection), operation, and refueling of the 1MW_#1. In the figure, interaction lines in blue, green, and orange correspond to required interactions for installation(connection), operation, and refueling of the 1MW_#1, respectively. These EROs may interact with all units and other organizations during multi-unit accident management and mitigation.

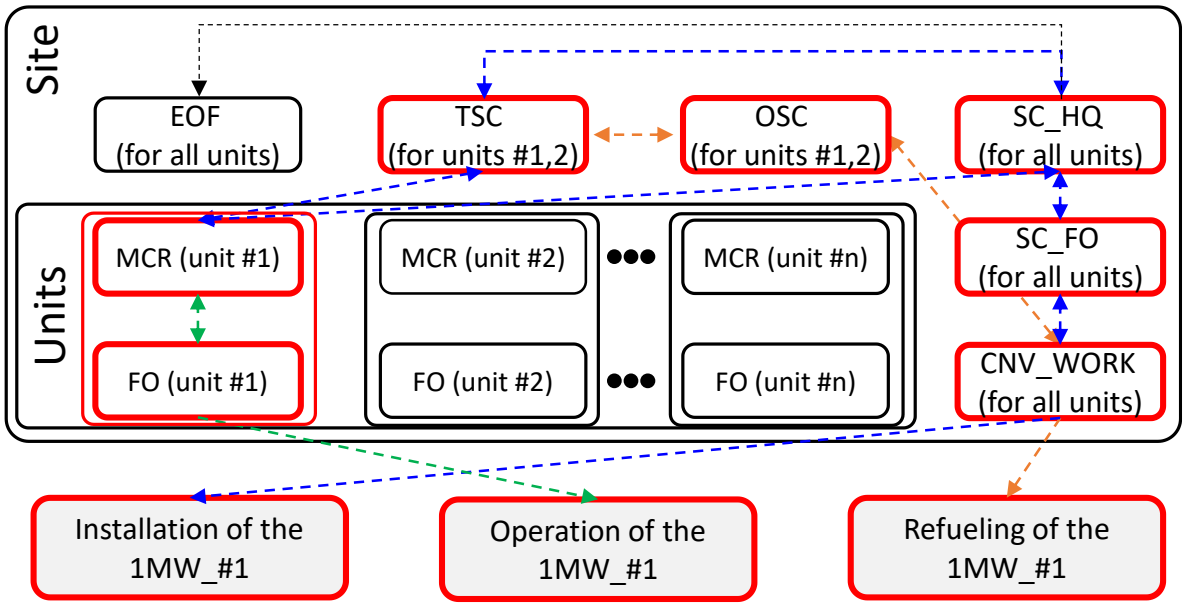

Figure 3. Schematic of the organizations involved in the successful installation, operation, and refueling of the 1 MWe in perspective of the unit #1 (highlighted in red)

After defining the interactions between EROs involved in the successful installation, operation, and refueling of the 1MW_#1, the fourth step of the framework were taken to develop a STAMP model in the perspective of unit #1 for using 1MW_#1. The developed STAMP model is shown in Figure 4.

Following the last step of the proposed framework, HRA elements need to be identified after deriving the UCAs through STPA. In the case study, "Failure of electric power supply using the 1MW_#1 for unit #1" was defined as a loss. Also, three kinds of hazards were defined in this case:
(1) Failure to connect the 1MW_#1,
(2) Too late in its connection, and
(3) Failure to maintain the operation of the 1MW_#1.

These hazards are indicated as H-1, H-2, and H-3, respectively. Based on these hazards, four types of UCAs were found through STPA for the 1MW_#1 case study from Figure 4, with the results shown in Table 3. Unsafe control actions (UCAs) identified in the case study (1MW_#1 failure).

Based on the analysis of the UCAs from STAMP/STPA, detailed analysis for the subtasks of the examined HFE can be performed. In Table 3. Unsafe control actions (UCAs) identified in the case study (1MW_#1 failure), there are 26 UCAs identified in the case study. Out of these UCAs, for feasibility analysis of Type 4 UCAs when the 1MW_#1 is running, the operators stopping 1MW_#1 too soon or stopping refueling too soon may not be likely when only considering the HRA elements (i.e. not considering environmental conditions or component failures). Then, one can see that most UCAs occur when corresponding organizations do not take required actions (i.e. Type 1) or take actions too late (i.e. Type 3).

In current PSA practices, HFEs and their HEPs for actions going MCR→FO, FO→1MW, and CNV_WORK→1MW are accounted in a typical MU-PSA model. However, for MU-HRA, following groups of the control actions may have not been accounted (with the corresponding UCAs bold in Table 3).

- Requests for 1MW (CA1, CA2)
- Convocation of the SC workers and outsourced workers from offsite (CA3)
- Installation of the 1 MW (CA4, CA5, CA6)
- Requesting/ordering refueling of 1 MW (*CA1, *CA2)

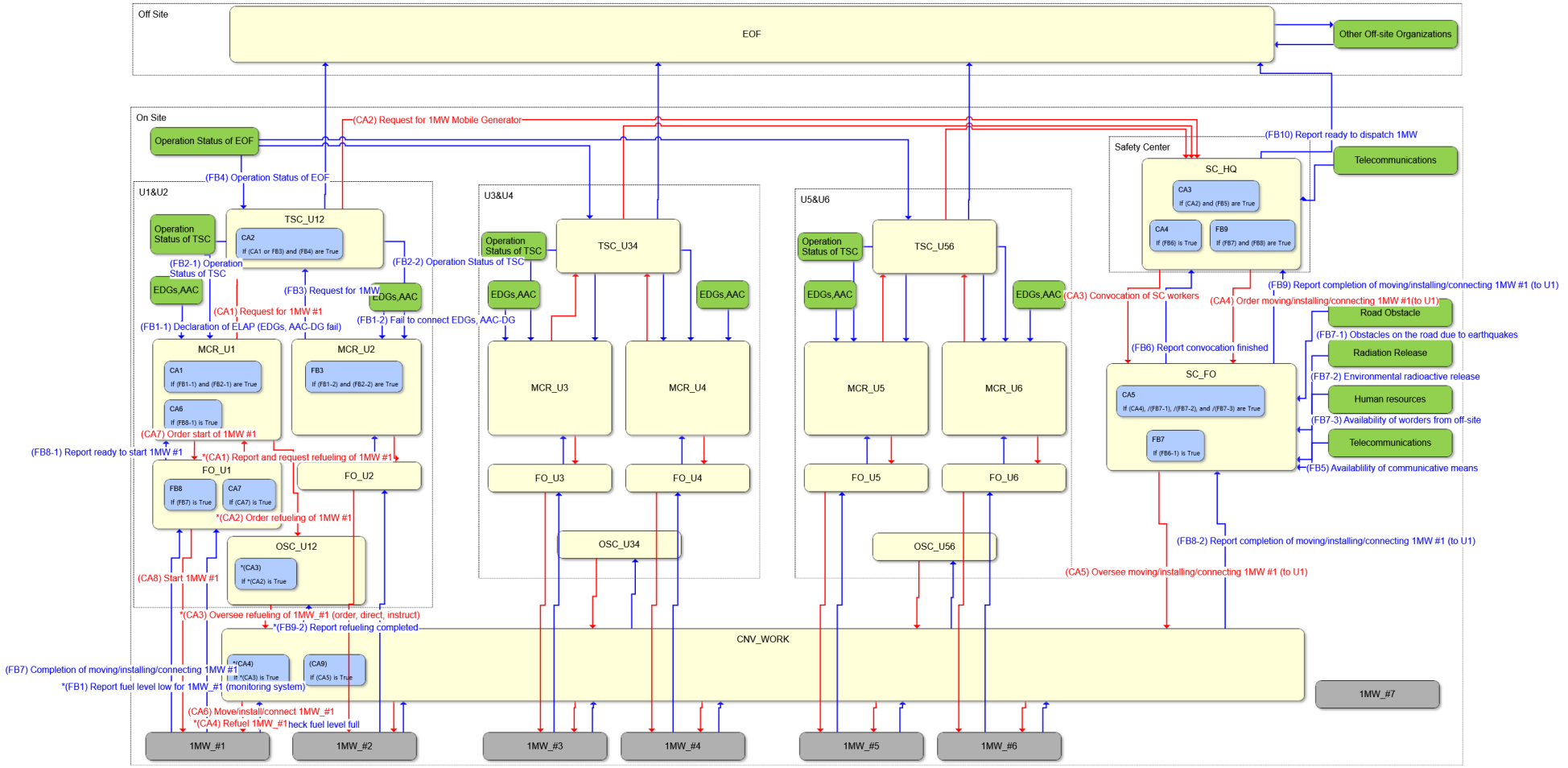

Figure 4. STAMP for successful installation, operation, and refueling of the 1 MWe in unit #1 (i.e. 1MW_#1), where lines in red and blue are control actions and feedbacks, respectively, between a) controllers (e.g. TSC for units 1 & 2, convocated workers from offsite, etc.), b) controlled processes (e.g. 1MW_#1), and c) environmental conditions (e.g. when there are no environmental radiation releases and when there are telecommunication devices available)

Table 3. Unsafe control actions (UCAs) identified in the case study (1MW_#1 failure)

Control Action	Type 1	Type 2	Type 3	Type 4
(CA1) Request for 1MW #1 MCR_U1 → TSC_U12	**(UCA-1)** **MCR_U1 fails to request 1MW_#1 to TSC_U12 during ELAP** **(Comm: ODL) [H-1]**	N/A	**(UCA-2)** **MCR_U1 is too late to request 1MW_#1 to TSC_U12 during ELAP** **(Comm: ODL) [H-2]**	N/A
(CA2) Request for 1MW Mobile Generator TSC_U12 → SC_HQ	**(UCA-3)** **TSC_U12 fails to request 1MW_#1 from SC_HQ after receiving request of 1MW_#1from MCR_U1** **(Comm: ODL) [H-1]**	N/A	**(UCA-4)** **TSC_U12 is too late to request 1MW_#1 from SC_HQ after receiving request of 1MW_#1from MCR_U1** **(Comm: ODL) [H-2]**	N/A
(CA3) Convocation of SC workers & outsourced workers SC_HQ → SC_FO SC_HQ → CNV_WORK	**(UCA-5)** **SC_HQ fails to order convocation of SC_FO after receiving request of 1MW_#1 from TSC_U12** **(Comm: ODM/OSM) [H-1]**	N/A	**(UCA-6)** **SC_HQ is too late to order convocation of SC_FO after receiving request of 1MW_#1 from TSC_U12 (Comm: ODM/ OSM) [H-2]**	N/A
(CA4) Order moving/installing/ connecting 1MW #1(to U1) SC_HQ → SC_FO	**(UCA-7)** **SC_HQ fails to order 1MW_#1 installation to U1 to SC_FO after receiving request of 1MW_#1 from TSC_U12** **(Comm: ODM / OSF) [H-1]**	N/A	**(UCA-8)** **SC_HQ is too late to order 1MW_#1 installation to U1 to SC_FO after receiving request of 1MW_#1 from TSC_U12** **(Comm: ODM / OSF) [H-2]**	N/A
(CA5) Oversee moving/installing/ connecting 1MW #1 (to U1) SC_FO → CNV_WORK	**(UCA-9)** **SC_FO fails to oversee installation of 1MW_#1 by CNV_WORK after SC_HQ ordered installation of 1MW_#1 to SC_FO** **(Comm: ODM / OSF) [H-1]**	N/A	**(UCA-10)** **SC_FO is too late to oversee installation of 1MW_#1 by CNV_WORK after SC_HQ ordered installation of 1MW_#1 to SC_FO U12** **(Comm: ODM / OSF) [H-2]**	N/A
(CA6) Move/install/ connect 1MW #1 CNV WORK → 1MW_#1	**(UCA-11)** **CNV_WORK fail to install 1MW_#1 after receiving order to install 1MW_#1 from SC_FO** **(Comm: ISF) [H-1]**	N/A	**(UCA-12)** **CNV_WORK is too late to install 1MW_#1 after receiving order to install 1MW_#1 from SC_FO** **(Comm: ISF) [H-2]**	N/A
(CA7) Order start of 1MW #1 MCR_U1 → FO_U1	(UCA-13) MCR_U1 fails to order start of 1MW_#1 to FO_U1 after receiving report that 1MW_#1 installation is completed from FO_U1 (Comm: ODM) [H-1]	N/A	(UCA-14) MCR_U1 is too late to order start of 1MW_# to FO_U1 after receiving report that 1MW_#1 installation is completed from FO_U1 (Comm: ODM) [H-2]	N/A
(CA8) Start 1MW #1 FO_U1 → 1MW_#1	(UCA-15) FO_U1 fails to start 1MW_#1 after receiving an order to start 1MW_#1 from MCR_U1 with 1MW_#1 installed by CVN_WORK (Comm: ISF) [H-1]	N/A	(UCA-16) FO_U1 is too late to start 1MW_#1 after receiving an order to start 1MW_#1 from MCR_U1 with 1MW_#1 installed by CVN_WORK (Comm: ISF) [H-2]	(UCA-17) FO_U1 stops 1MW_#1 too soon after starting 1MW_#1 (Comm: ISF) [H-3]

(*CA1) Report and request refueling of 1MW #1 FO_U1 → MCR_U1	**(UCA-18)** **FO_U1 fails to request refueling of 1MW_#1 to MCR_U1 when 1MW_#1 fuel level is low** **(Comm: ODM) [H-3]**	N/A	**(UCA-19)** **FO_U1 is too late to request refueling of 1MW_#1 to MCR_U1 when 1MW_#1 fuel level is low** **(Comm: ODM) [H-3]**	N/A
(*CA2) Order refueling of 1MW #1 MCR_U1 → OSC_U12	**(UCA-20)** **MCR_U1 fails to order 1MW_#1 refueling to OSC_U12 after FO_U1 reported 1MW_#1 fuel level is low** **(Comm: ODL/ODM) [H-3]**	N/A	**(UCA-21)** **MCR_U1 is too late to order 1MW_#1 refueling to OSC_U12 after FO_U1 reported 1MW_#1 fuel level is low** **(Comm: ODL/ODM) [H-3]**	N/A
(*CA3) Oversee refueling of 1MW (order, direct, instruct) OSC U12 → CNV_WORK	(UCA-22) OSC_U12 fail to oversee CNV_WORK to refuel 1MW_#1 after receiving request of 1MW_#1 refueling from MCR_U1 (Comm: ODM / OSF) [H-3]	N/A	(UCA-23) OSC_U12 is too late to oversee CNV_WORK to refuel 1MW_#1 after receiving request of 1MW_#1 refueling from MCR_U1 (Comm: ODM / OSF) [H-3]	N/A
(*CA4) Refuel 1MW #1 CNV_WORK → 1MW_#1	(UCA-24) CNV_WORK fail to refuel 1MW_#1 after receiving order to refuel 1MW_#1 from OSC_U12 (Comm: ISF) [H-3]	N/A	(UCA-25) CNV_WORK is too late to refuel 1MW_#1 after receiving order to refuel 1MW_#1 from OSC_U12 (Comm: ISF) [H-3]	(UCA-26) CNV_WORK stops too soon the refueling of 1MW_#1 after receiving order to refuel 1MW_#1 from OSC_U12 (Comm: ISF) [H-3]

*** UCA types are listed in Table 2**
**** H-1, H-2, and H-3 denote the first, second, and third hazards identified in this section**
***** For communication abbreviations:**
a) different and same organizations are labeled as O (inter) or I (intra)
b) locations of two organizations having an interaction are labeled as S (same) or D (different)
c) method of communication may be labeled as F (face-to-face), M (mobile phone, including texting), and L (landline)

UCAs for these control actions (bold in Table 3) may be identified as subtasks for the HFE of 1 MWe generator failure, which are missing in current models but may be important in a real-world multi-unit accident situation. These identified UCAs can further be analyzed in detail by the HRA experts, from which HEP quantification (stage 5 of the general HRA process, from Section 1) can be performed to be integrated (stage 6) into the PSA model of a MU-LOOP scenario, which is out of scope for this research and would be performed as a future work. As a guideline, each of the identified UCAs may further be divided into different modes of human errors through detailed analysis (e.g. diagnosis or action) and have their HEPs quantified individually (e.g. using SPAR-H). Once these HEPs for individual UCAs are found, they may be combined as the representative HFE and corresponding HEP can be calculated. If there are too many UCAs, these may be screened or combined through more detailed analysis using Table 3 as a guideline.

4. CONCLUSION

After the Fukushima Daiichi accident, MU-PSA has been emphasized in response to the demand for realistic risk assessment in NPPs. This implies that MU-HRA reflecting the unique features of a multi-unit accident progression is also required because traditional HRA does not sufficiently consider multi-unit dependencies in quantifying the HEP values of HFEs. For example, for a given HFE, traditional HRA does not explicitly consider the series of subtasks pertaining to the decision-making process of diverse organizations. For this reason, in this study, a method was proposed to utilize the concepts of the STAMP/STPA method.

The scope of the HRA elements being considered in this study is twofold: (1) catalog of subtasks that should be modeled for a given HFE, and (2) catalog of human error modes pertaining to the catalog of subtasks. The feasibility of the proposed methodology was corroborated with a simple case study that contains one of the representative HFEs included in the progression of a multi-unit ELAP scenario followed by a MU-LOOP. Results demonstrated how the abovementioned HRA elements can be distinguished by using the proposed method.

Accordingly, it is expected that the STAMP/STPA could be a helpful tool for supporting MU-HRA. However, the proposed method may have its own limitations. First, large amount of resources may be required to explicitly visualize diverse and complicated interactions expected from many emergency response organizations through STAMP models via control loops. The case study was for one HFE (i.e. 1 MWe failure) in one scenario (i.e. MU-LOOP). Similar process may need to be performed for many HFEs and scenarios in the MU-PSA models. This alludes to the fact that HRA practitioners responsible for conducting MU-HRAs have to develop a lot of control loops with respect to one or more MCRs and the organizations belonging to the augmented ERO. Compared with the amount of resources required for conducting traditional HRA, it is evident that practitioners of MU-HRA are likely to feel a high burden.

Nonetheless, the catalog of UCAs with associated CAs/FBs could also support the determination of the third HRA element: context information to be collected for quantifying the HEP value of a given HFE. For the MU-HRAs consisting of many intertwined EROs, it is expected that the proposed method can be utilized for identifying and performing detailed analysis of the multi-unit accident HFEs. For this, it is necessary to further clarify its usefulness with more case studies that cover more complicated and realistic multi-unit accident scenarios. In this regard, the result of this study would be a good starting point for strengthening the proposed framework.

Acknowledgements

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) and by Nuclear Research & Development Program grants from the National Research Foundation of Korea (NRF), funded by the Korean government, Ministry of Science and ICT (Grant Code: RS-2022-00144175).

References

[1] Leveson, N. G., Thomas, J. P., 2018. STPA Handbook, MIT.
[2] Leveson, N. G., 2004. A new accident model for engineering safety systems, Safety Science, Volume 42, Issue 4, Pages 237-270.
[3] Jianbo, H., Lei, Z., and Shukui, X., 2018. Safety analysis of wheel brake system based on STAMP/STPA and Monte Carlo simulation, Journal of Systems Engineering and Electronics, Vol. 29, No. 6, pp.1327–1339, 2018.
[4] Shin, S., Lee, S., Shin, G., Jang, I., Park, J., 2021. STPA-based hazard and importance analysis on NPP safety I&C systems focusing on human–system interactions. Reliability Engineering and System Safety, 213, 107698. https://doi.org/10.1016/j.ress.2021.107698.
[5] Yamada, T., Sato, M., Kuranobu, R., Watanabe, R., Itoh, H., Shiokari, M., and Yuzui, T., 2022. Evaluation of effectiveness of the STAMP / STPA in risk analysis of autonomous ship systems, Journal of Physics, Ser. 2311, 012021. https://doi:10.1088/1742-6596/2311/1/012021.
[6] Bensaci, C., Zennir, Y., Pomorski, D., Innal, F., and Lundteigen, M.A., 2023. Collision hazard modeling and analysis in a multi-mobile robots system transportation task with STPA and SPN, Reliability Engineering and System Safety, 234, 109138. https://doi.org/10.1016/j.ress.2023.109138.
[7] Cheng, T., Utne, I.B., Wu, B., and Wu, Q., 2023. A novel system-theoretic approach for human-system collaboration safety: Case studies on two degrees of autonomy for autonomous ships, Reliability Engineering and System Safety, 237, 109388. https://doi.org/10.1016/j.ress.2023.109388.