A preliminary study on STAMP/STPA application for potential hazard analysis and design requirement derivation of a control system in NPP

Sung-Min Shin[a*], Jinkyun Park [a], Seung-Cheol Jang[a], Jong-Gyun Choi[a]
[a]*Korea Atomic Energy Research Institute, 111 Daedeok-daero, 989beon-gil, Yuseong-gu, Daejeon, Republic of Korea 34057*
[*]*Corresponding author: smshin@kaeri.re.kr*

***Keywords :** Design requirement, Software, Safety analysis, STMAP, STPA

1. Introduction

With the digitalization of instrumentation and control (I&C) systems in nuclear power plants, their functionality has become increasingly software-dependent. These digital I&C(DI&C) systems, integrating software into their operations, engage in complex interactions with their surrounding elements, sometimes leading to unforeseen hazardous situations when design requirements are developed.

To ensure reliable performance, the derivation of design requirements considering potential hazard situations arising from interactions with software and surrounding elements becomes imperative. In this context, a method proposed by Professor Nancy Leveson from MIT, STAMP/STPA[1, 2], seems suitable for conducting hazardous analysis in the context of interactions among control system components.

In the field of nuclear power generation, the application of STAMP(Systems-Theoretic Accident Model and Processes)/STPA(System-Theoretic Process Analysis) to safety analysis for DI&C systems has gained significant attention, particularly with EPRI (Electric Power Research Institute) actively exploring its use[3]. In addition, the United States' nuclear regulatory authority, the NRC (Nuclear Regulatory Commission), has expressed its various potential including software analysis[4].

Therefore, this paper examines whether potential hazardous situations that are difficult to identify using existing risk analysis methods can be identified through STAMP/STPA, and whether design requirements can be derived based on the insights gained through this process, based on actual accident cases that occurred in nuclear power plants.

2. Methods and Case Study

This chapter describes the overview of STMAP/STPA and the accident case to be analyzed, and the process of applying STAMP/STPA to the accident case to analyze the loss scenario (cause - UCA- Hazard - loss) of the hazardous situation.

2.1 Over view of STAMP/STPA

STAMP is an accident and process model of a control system and is built based on a control loop consisting of the following elements.

- Controller: Decision-maker
  - Control algorithm: Controller's decision-making process
  - Process model: Controller's internal beliefs about the controlled process and it is used to make decisions and updated by feedback
- Controlled process: Object to be controlled
- Feedback: Information indicating the state of the controlled process
- Control action: Control signal issues by controller to control the controlled process

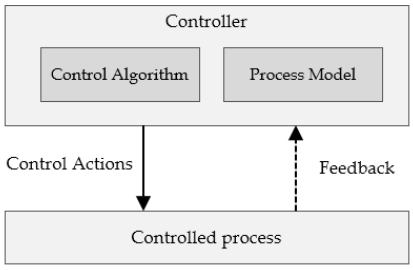

Fig. 1. Configuration of the control loop that makes up STAMP

In addition to the traditional logical analysis on component failure, STAMP focuses more on the interactions between system components. This approach provides an effective basis for comprehending the complex interactions among controllers and their surrounding components, aiding accident prevention and response efforts.

STPA is a hazard analysis technique based on STAMP that consists of four main steps below, like figure 2.

1) Define Purpose of the Analysis:
- Establish the boundaries of the system to be analyzed.
- Define concerns (losses and hazards) to be addressed. Here the system loss is an unplanned event that cannot be controlled anymore, and the system hazard is a system state or set of conditions

that can lead to system loss which can be controlled through design.

2) Model the Control Structure:
- This step is corresponding to the development of STAMP.
- Develop a comprehensive visual representation of the system to facilitate analysis; Identify controller, controlled process, feedback, control actions, and interactions between system components.

3) Identify Unsafe Control Actions(UCA):
- Analysis on control actions to identify potential UCAs that may lead to the hazards defined.

4) Identify Loss Scenarios:
- Explore the causal factors and conditions that can lead to UCA identified.

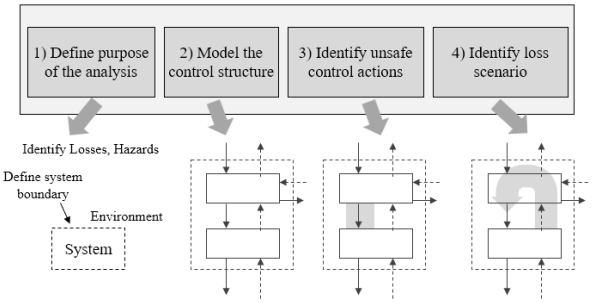

Fig. 2. 4 steps for STPA

Overall, STPA's 4 steps guide safety analysts in understanding the system's control structure, identifying potential hazards, and developing comprehensive loss scenarios(cause - UCA - hazard - loss). This approach emphasizes the causal relationships between control actions and potential accidents, providing valuable insights for enhancing system safety and preventing critical incidents.

2.2 Overview of an accident case to be analyzed [5]

In this study, the accident that occurred in Shin-Kori Unit 3 in 2018, automatic trip of reactor due to improper insertion of control rods, will be treated as an accident to be analyzed.

Nuclear power plants are required to test the operability of control element assemblies (CEAs) at three-month intervals using the following procedure. Refer to table I.

- Test sequence
  - Test from control group A to 5 in turn
- Test method for each control group (A, B, 1 and so on)
  - MCR operator selects the manual group (MG) mode and inserts all the control rods of the subgroup in 5 steps (1 step: 1.905 cm)
  - MCR operator selects manual individual (MI) mode, then the operator selects an individual control rod from the subgroup as well and insert/withdraw that control rod 2 steps.
  - After completing the test of every individual control rods in the subgroup in turn, select manual group(MG) mode and withdraw all control rods in the subgroup 5 step.

Table I: Problem Description

Control group		Subgroup	Number of individual CEA
Reactor trip[1)]	A	2	6, 8 ,10, 12
		3	7, 9, 11, 13
		16	62, 64, 66, 68
		17	63, 65, 67, 69
	B	8	30, 32, 34, 36
		9	31, 33, 35, 37
		11	42, 45, 48, 51
		12	43, 46, 49, 52
		13	44, 47, 50, 53
Reactor control[2)]	1	6	22, 24, 26, 28
		7	23, 25, 27, 29
	2	1	2, 3, 4, 5
		14	54, 56, 58, 60
		15	55, 57, 59, 61
	3	4	14, 15, 16, 17
		18	70, 71, 72, 73
		20	78, 79, 80, 81
	4	19	74, 75, 76, 77
		21	82, 83, 84, 85
	5	10	38, 39, 40, 41, 1
Partial steel[3)]	P	5	18, 19, 20, 21
		22	86, 88, 90, 92
		23	87, 89, 91, 93
Sum		23 subgroup	93 CEA

During the sequential test from subgroup 2 of control group trip A, according to the procedure, the actual insertion and withdrawal of the CEA was performed differently from the operator operation as follows.

First, all 4 CEAs (7, 9, 11, 13) of subgroup 3 were inserted in 5 steps, and then, during the testing of each individual CEA, not only one selected CEA but all CEAs in the same subgroup were inserted and withdrawn together (Figure 3).

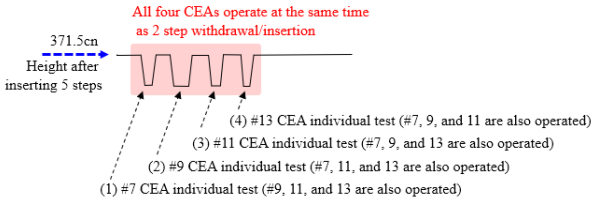

Fig. 3. Actual CEA locations under test for subgroup 3

Also, while testing subgroup 16, CEAs 64, 66, and 68 behaved incorrectly by continuously inserting regardless of whether they were inserted or withdrawn (Figure 4).

This triggered a deviation alarm between the individual control rods in subgroup 16, and the MCR operator attempted to withdraw control rod 64 for an additional 1step to resolve the deviation alarm, but the reactor shut down at August 21st 10:53:42 due to DNBR-Low signal as the three control rods, 64, 66 and 68, were inserted for 1 step.

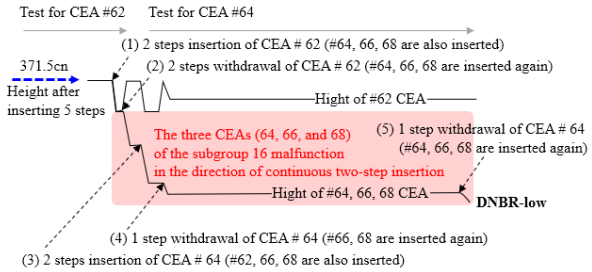

Fig. 4. Actual CEA locations under test for subgroup 16

In the process of investigating the cause of this incident, the NPP operator confirmed that the Maintenance & Test Pane (MTP) internal datalink server recorded a continuous abnormal status(Client missed reply timeout) from 29 June 2018 at 08:20. The operator confirmed that the datalink server had been inoperable since 30 June at 12:26.

2.3 STAMP/STPA Application to the Accident Case

In STPA step 1, the purpose of the analysis is defined. The boundary of the system is defined to include the elements involved in MG and MI, such as MCR operator, MTP, Logic Cabinet, Selecting Cabinet, Moving Cabinet, and Digital Rod Control System (DRCS) (Refer to figure 5). Then the system loss and hazard were briefly defined as follows.

- Loss 1: Loss of power generation (Unexpected reactor trip)
- Loss 2: Failure of operability test for control rod
- Hazard 1: DNBR margin is reduced

In STPA step 2, a control structure is developed. Figure 5 shows the control structure developed including the flow of control actions and feedbacks generated during operability test, and the control algorithm and process model inside each controller. Please note that the components having asterisk (*) in the figure are assumed due to the lack of information about the actual system design.

The signals (control actions and feedbacks) flow between system components during a test is as follows; The test mode (MG or MI), subgroup, and individual CEA information selected by the MCR operator according to the test procedure is transmitted to the Logic cabinet. The Logic cabinet then generates digitalized information of subgroup and individual CEA and sends them to the MTP, and the subgroup information is sent

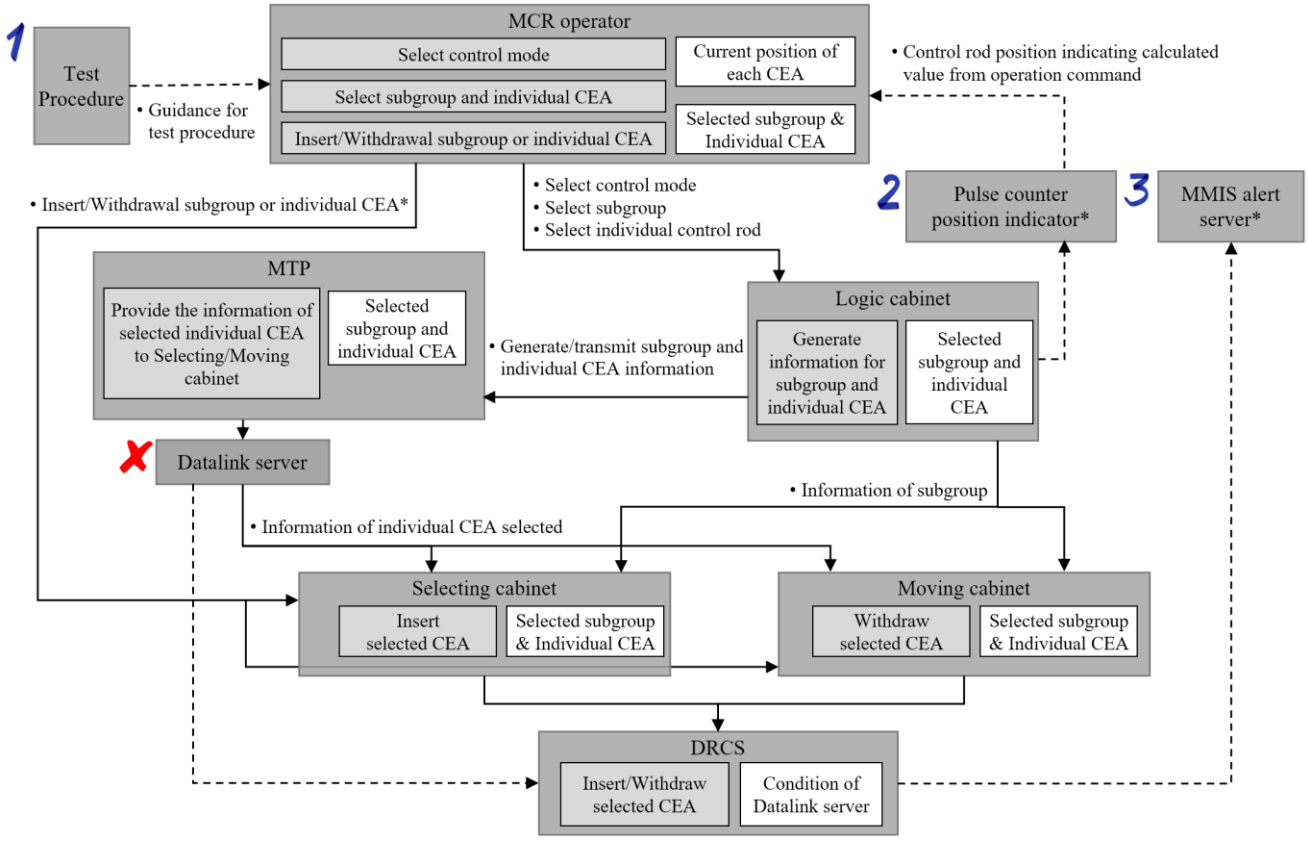

Fig. 5. Control structure of operability test for CEAs

directly to the Selecting/Moving cabinet. MTP transmits individual CEA information to the Selecting/Moving cabinet through the MTP datalink server based on the information received from the logic cabinet. In summary, subgroup information is transmitted directly from the Logic cabinet, and individual CEA information is transmitted via MTP to the Selecting/Moving cabinet. When the MCR operator operates the CEA, the CEA is inserted or withdrawn according to the information stored in Selecting/Moving cabinets.

STPA step 3 defines how the control actions in the control structure can go wrong and cause the hazard defined in STPA step 1. The following UCA is defined here; it is to focus on the control action for the final step deciding the movement of the CEA.

- (UCA1) MCR operator commands insert/withdraw subgroup or individual CEA when the given command and the actual movement may differ [Hazard 1].

Finally, in STPA step 4, the causes that can trigger the defined UCA are identified based on the control structure developed. Basically, any controller must have a correct perception of the current state of the object to be controlled, i.e. a correct process model, in order to generate the correct control actions. MCR operator has two process models "Current position of each CEA" and "Selected subgroup & individual CEA". If other controllers than MCR operators have the same or related process model, the process models' contents must consistency. In the control structure (Figure 5), the process model "Selected subgroup & individual CEA" is in the MCR operator and the Selecting/Moving cabinet. However, as in the accident case, the process models for the selected individual CEA may differ between the MCR operator and the Selecting/Moving cabinet. This is because the selected individual CEA information in the Selecting/Moving cabinet cannot be updated if the MTP's datalink server is unavailable.

The impact of a failure of these components cannot be completely excluded, no matter how reliable the components are. Therefore, even if a failure of these components occurs, it can be prevented from causing a UCA if the relevant controller is aware of the occurrence or impact of such a failure. Referring back to the control structure (figure 5), some functions to detect such failure have been implemented, but they are not sufficient for the MCR operator to actually recognize them.

- The Pulse counter position indicator does not show the actual position of the CEA, but rather a computational representation of the position of the CAE that will be moved by the generated command.
- DRCS had the capability to detect a failure of the MTP datalink server, but the detecting information was designed to be transmitted to the MMIS alert server but not to the MCR operators.

Therefore, the loss scenario for UCA1 can be described as follows.

- MTP datalink server failure – UCA1 (MCR operator commands insert/withdraw subgroup or individual CEA when the given command and the actual movement may differ) – Hazard 1 (DNBR margin is reduced) – Loss 1&2 (Loss of power generation & Failure of operability test for control rod)

On the other hand, from the perspective of deriving design requirements, these loss scenarios can be generalized again as follows.

- Failure of system components - Generation (or non-generation) of control action in situations where the same or related process models are inconsistent between multiple controllers – Deviation from steady state – Loss of power or failure of operability test for control load

To prevent the above-generalized loss scenario, the following design requirements can be derived on the entire system.

- The system should be designed to eliminate inconsistency in the same or related process model between the controllers, and if inevitable, MCR operator (or other controller deciding the movement of the CEA) should able to recognize and cope with the inconsistency.

Given this design requirement, the system analyzed as an incident case would have implemented at least one of the following features (see Figure 5 for the number below).

1. The test procedure guides the MCR operator to intuitively check the control rod position or to recognize the abnormal condition of the DRCS through the related variables.
2. The pulse counter position indicator provides information to recognize whether the actual control rod position is abnormal (the existing pulse counter does not provide the actual control rod position information)
3. The MMIS alert server transmits the stored datalink server failure status to the MCR operator.

3. Discussion & Conclusion

In fact, the three features for satisfying the design requirements described above were also mentioned in the Nuclear Accident Failure Investigation Report [5] for the accident. This paper may seem to have reconstructed the process of drawing such conclusions according to the STPA. However, the failure of the data link server is not the only one that can cause such a situation. Redefining the accident process as a general scenario, and deriving and presenting general design requirements to prevent it, can contribute to the safer implementation of the analyzed system and other systems in NPPs. Although this paper focused on analyzing specific UCA, it is believed that additional general design requirements can be derived by analyzing additional potential UCAs and loss scenarios. However, this would require more detailed information on the signaling of the I&C system in question (some of the configurations and signaling between them in Figure 5 are assumed).

In addition, the same system may have different control structures depending on the mode in which it operates (only MG and MI modes are discussed in this paper, while the system operates in MS (manual sequential), AS (Auto sequential), and SB (Standby) modes). Therefore, further analysis of the signal transmission in other modes is necessary.
Therefore, more detailed information on the above will be confirmed in the future, and additional design requirements will be derived considering them.

ACKNOWLEDGEMENT

This work was supported by the Korea Foundation Of Nuclear Safety (KoFONS) of the Republic of Korea funded by the Nuclear Safety and Security Commission(No. 2106005).

REFERENCES

[1] Leveson NG, Thomas JP. STPA handbook. MIT; 2018.
[2] Leveson NG. Engineering a safer world: systems thinking applied to safety. The MIT Press; 2011.
[3] Wheeler T, Clark A, Williams A, Muna A, Dawson L, Geddes B, Blanchard D. Hazards and consequences analysis for digital systems. EPRI Technical Report; 2018. Dec.
[4]J. Thomas, Investigation of the use of System-Theoretic Process Analysis at the NRC, 2021 (https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML22272A315)
[5] KINS, 신고리 3 호기 제어봉집합체 시험 중 부적절한 제어봉 삽입에 의한 원자로 자동정지, 2018