STPA-based Hazard Identification of Human Operator Interaction with Passive Safety Systems

Sung-Min Shin[1], Yochan Kim[1], Jinkyun Park[1], Jin Hee Park[1]

[1] *KAERI: 111 Daedeok-daero 989 beon-gil, Yuseong-gu, Daejeon, Republic of Korea 34057, smshin@kaeri.re.kr*
[1] *KAERI: 111 Daedeok-daero 989 beon-gil, Yuseong-gu, Daejeon, Republic of Korea 34057, yochankim@kaeri.re.kr*
[1] *KAERI: 111 Daedeok-daero 989 beon-gil, Yuseong-gu, Daejeon, Republic of Korea 34057, kshpjk@kaeri.re.kr*
[1] *KAERI: 111 Daedeok-daero 989 beon-gil, Yuseong-gu, Daejeon, Republic of Korea 34057, jhpark6@kaeri.re.kr*

EXTENDED ABSTRACT

To ensure protection under uncertain conditions, many advanced reactors are adopting the passive safety systems (PSSs) that are automatically actuated in the absence of operator input, following a deterministic set of conditions or elapsed time. However, this default-to-safe behavior introduces operational constraints. Once a PSS is actuated, significant downtime, resource consumption, and post-activation restoration procedures may be required before the plant can return to normal operation. As a result, designers incorporate mechanisms that allow operators to block or delay automatic activation of the PSS when it is confidently deemed unnecessary. NuScale, for instance, enables manual blocking of the Emergency Core Cooling System (ECCS), a gravity-driven feed-and-bleed cooling loop [1], contingent on verified safety conditions [2]. Although such capability grants operators strategic flexibility, allowing them to avoid unnecessary actuation of PSS, it also introduces a critical challenge to human operators: the potential for inappropriate manual inhibition of a vital safety function under misinterpreted or misleading indications.

This study employs System-Theoretic Accident Model and Processes (STAMP) and Systems-Theoretic Process Analysis (STPA) [3] to develop a set of loss scenarios, focusing specifically on manual actuations. In order to derive comprehensive results, an analysis model including all of human operator, system hardware, operator interfaces, environmental conditions, and procedural logic, that is, a control structure, is developed, and the interaction between them is closely examined to see if they can cause the loss scenarios. Furthermore, the analysis further considers how feedback mechanisms, procedural clarity, and interface design can be reinforced to support correct operator decisions. The results of this study support a dual objective: enhancing safety through systematic hazard identification and improving operational availability by avoiding unnecessary system actuations. With the aims above, referring to the NuScale ECCS, this study conducts STPA on the decision-making of the human operator regarding the blocking of PSS, which is supposed to be automatically started 8 hours after the reactor trip occurs. For reference, it was assumed that manual blocking may also be released before 8 hours after the trip. In the analysis process, the STPA tool TRACEIT developed by Korea Atomic Energy Research Institute (KAERI) in Korea was used [4].

STPA is a top-down hazard analysis method developed based on the STAMP. Unlike traditional failure-based approaches, STPA views safety as a control problem that causes unsafe interactions, making it particularly well-suited for analyzing complex systems that involve both automated elements and human. As shown in the figure 1, STPA consists of four major steps: 1) defining the purpose of the analysis, 2) modeling the control structure, 3) identifying unsafe control actions(UCAs), and 4) identifying loss scenarios. Each step builds upon the previous one, ultimately supporting the derivation of system-level safety constraints and guiding safer system design and operation.

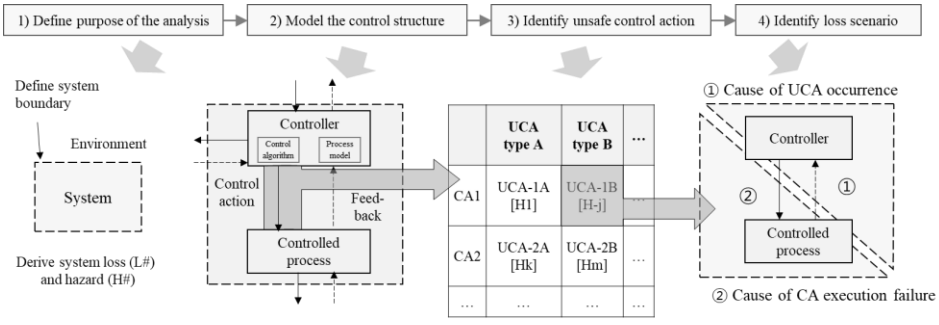

Figure 1 Overview of STPA

The first step of the STPA involves defining the losses and hazards associated with it, so , the potential losses and hazards were identified, as summarized in Figure 2.

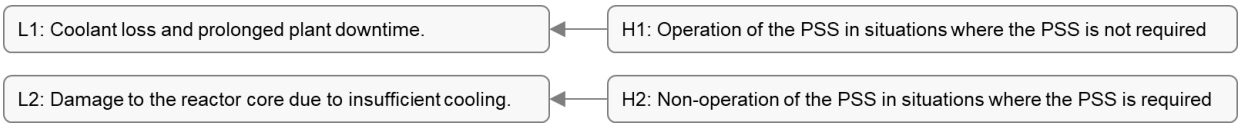

Figure 2. Losses and hazards

In Step 2 of STPA, a control structure is developed to capture how control actions (CAs) are issued and system components interact. Figure 3 illustrates the control structure developed, which depicts each system entity, the Feedbacks(FBs) each receives, and the associated Process Models (PMs) and CAs generated. The identifiers and name used in the Figure are summarized in Table 1. The interaction within this structure is illustrated focusing on CA1 (PSS Auto-actuation Blocking), which is issued by the [C1] Human Operator. The accurate generation of CA1 depends on the following Process Models: (PM1) Recognition of whether the plant is in a condition where PSS blocking is acceptable, (PM2) Evaluation of the operational availability of the PSS, considering testing, maintenance, or modification status, (PM3) Verification that the PSS has not already been actuated, (PM4) Monitoring the elapsed time since the last reactor trip, (PM5) Reference to up-to-date criteria and procedures for blocking, (PM6) Awareness of any external pressure influencing the blocking decision.

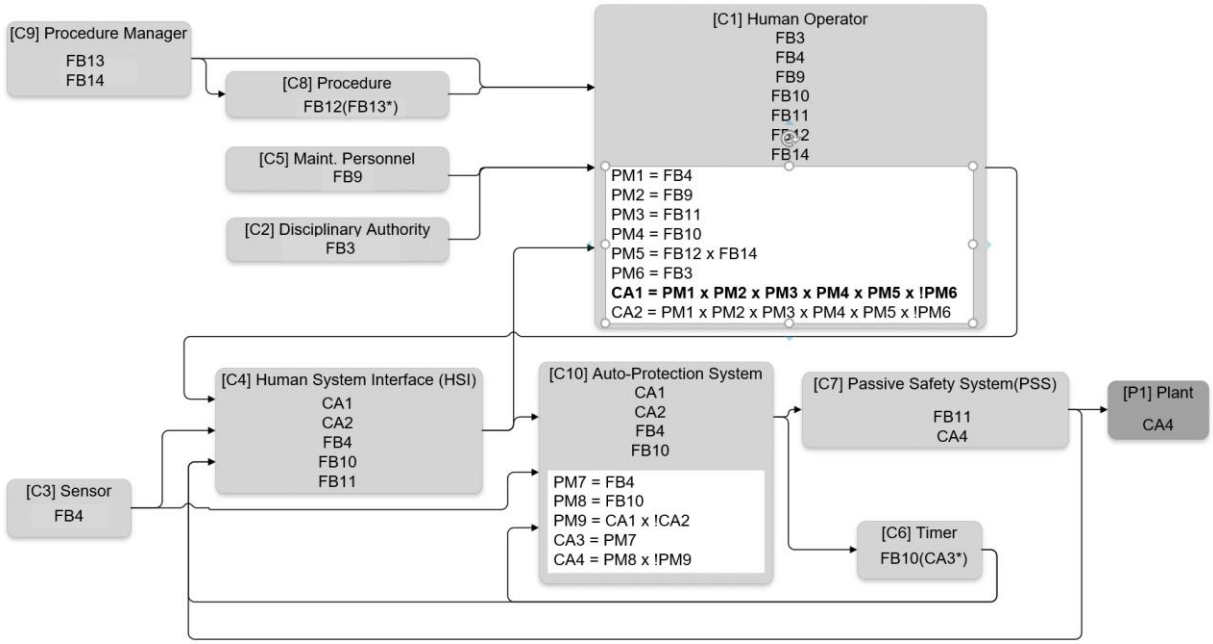

Figure 3. Control structure for PSS blocking and releasing

Table 1. Control actions, process model, and feedbacks in the control structure

Control action		Process model		Feedback	
ID	Name	ID	Name	ID	Name
CA1	PSS Auto-actuation Blocking	PM1	Current State of Plant	FB3	Pressure on a Certain Decision
CA2	Release PSS Auto-actuation Blocking	PM2	Availability of PSS	FB4	Plant Process Parameters
CA3	Trip Signal	PM3	Current PSS Operation	FB9	Notice of Test / Maintenance / Modification
CA4	Timer-induced PSS Auto-actuation	PM4	Elapsed Time Since Reactor Trip	FB10	Counting Time
		PM5	Up-to-date Procedure	FB11	Current Situation of the PSS
		PM6	Psychological Pressure on Mistake	FB12	Criteria of Manual Blocking/Releasing
		PM7	Parameter Exceeding Set Point	FB13	Modification on Procedure

PM8	Timer Elapsed Time	FB14	Notice/Training of Modification on Procedure
PM9	Manual Block Positive		

The formation of the above process models in the [C1] Human Operator depends on various feedbacks, as described below:

- PM1 (Current State of Plant) is updated by FB4 (Plant Process Parameters). This signal is generated by the [C3] Sensor and transmitted to the [C1] Human Operator through the [C4] HSI.
- PM2 (Availability of PSS) is updated by FB9 (Notice of Test/Maintenance/Modification). FB9 is generated by and transmitted from the [C5] Maintenance Personnel to the [C1] Human Operator. While this information could also be routed via the HSI, in this pilot study, direct delivery from [C5] Maintenance Personnel is assumed.
- PM3 (Current PSS Operator) is updated by FB11 (Current Situation of the PSS), and FB11 is transmitted from the front [C4] HSI, which is generated and transmitted from the [C7] PSS.
- PM4 (Elapsed Time Since Reactor Trip) is updated by FB10 (Counting Time). FB10 is transmitted through the [C4] HSI, which receives it from the [C6] Timer. In this context, CA3 (Trip Signal) is re-stated by [C6] Timer, and that CA3 was originally generated by the [C10] Auto-Protection System based on PM7 (Parameter Exceeding Set Point). PM7 is updated using FB4 (Plant Process Parameters), which originates from the [C3] Sensor and is transmitted to [C10] Auto-Protection System.
- PM5 (Up-to-data procedure) can be formed properly when both FB12 (Criteria of Manual Blocking/Releasing) and FB14 (Notice/Training of Modification on Procedure) are present. First, the FB12 (Criteria of Manual Blocking/Releasing) is re-stated FB13 (Modification on Procedure) in the front entity [C8] procedure, which means if there is a modification in the existing procedure, a new FB12 (Criteria of Manual Blocking/Releasing) may be formed accordingly. FB13 (Modification on Procedure) can be made by the front entity [C9] Procedure Manager). Meanwhile, as mentioned earlier, the PM5 (Up-to-data Procedure) of the [C1] Human Operator can be properly formed only when the FB14 (notification/training of modification on procedure) is given by the [C9] Procedure Manager.
- PM6 (Psychological Pressure on Mistake) can be formed by generating and giving FB3 (Pressure on a Certification Decision) from the front entity [C2] Discipline Authority.

In Step 3 of the STPA process, unsafe control actions (UCAs) that may lead to hazards are identified for each relevant control action. This pilot study considers two types of UCAs—"Not providing causes a hazard" and "Providing causes a hazard"—while excluding timing- and duration-related UCAs. Accordingly, the UCAs identified are summarized in Figure 4.

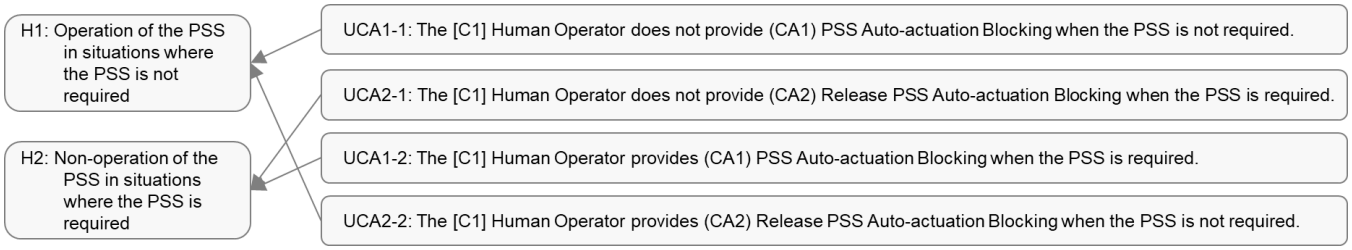

Figure 4. Unsafe control actions

In Step 4 of STPA, for each UCA identified in the previous step, potential generic causal factors were analyzed, and concrete loss scenarios (LSs) that could result from those causes were developed. These analyses help to understand how unsafe control actions could be triggered under specific system conditions, human errors, or process failures. Table 2 shows the loss scenario derived for UCA1-1 as an example among UCAs developed in STPA step 3. These scenarios provide actionable insights for developing effective safety constraints and mitigation strategies in later system design or operation phases.

Table 2. Loss scenarios related UCA1-1

ID	Cause	Loss Scenario
LS1	[CU1] Procedure change miscommunication	Due to a lack of awareness of procedure modifications, the operator is confused and does not block the PSS auto-actuation when the PSS is not required.
LS2	[CU2] Ambiguous/Deficient procedure	Due to the ambiguous/deficient procedure, the operator is confused and does not block the PSS auto-actuation when the PSS is not required.
LS3	[CU3] Faulty notice from Maintenance personnel	Due to a faulty notice from maintenance personnel, the operator thinks the PSS will not operate even without manual blocking and does not block the PSS auto-actuation when the PSS is not required.

LS4	[CU4] Pressure from the discipline authority	Due to pressure from the disciplinary authority to prioritize safety unconditionally, the operator does not block the PSS auto-actuation when the PSS is not required.
LS5	[CU5] Unsystematic HSI	Due to the unsystematic process-variable-related HSI, the operator is confused and does not block the PSS auto-actuation in time when the PSS is not required.
LS6	[CU5] Unsystematic HSI	Due to the unsystematic PSS-related HSI, the operator thinks the PSS is already blocked or actuated, so does not block the PSS auto-actuation when the PSS is not required.
LS7	[CU5] Unsystematic HSI	Due to the unsystematic timer-related HSI, the operator cannot be aware of the remaining time and does not block the PSS auto-actuation when the PSS is not required.
LS8	[CU6] Component failure	Due to the sensor failure, the operator cannot recognize the current state of plant and does not block the PSS auto-actuation in time when the PSS is not required.
LS9	[CU6] Component failure	Due to the timer failure, the operator cannot recognize the elapsed time and does not block the PSS auto-actuation in time when the PSS is not required.

Based on the loss scenarios identified in STPA Step 4, a set of countermeasures (CMs) was developed to mitigate the associated hazards and prevent the occurrence of unsafe control actions, as shown in the Table 3. These countermeasures were derived by analyzing the causal factors behind each loss scenario and proposing design, procedural, or operational improvements that could either eliminate the cause or reduce its impact, focusing on enhancing the accuracy and timeliness of information available to the [C1] Human Operator.

Table 3. Countermeasures

ID	Countermeasure	Related Loss Scenario
CM1	If a PSS-related procedure needs to be changed, the procedure manager shall be evaluated by the operator for the impact of the change and shall proceed with the change reflecting the evaluation results.	LS1
CM2	Decide whether blocking should be irreversible or reversible; If irreversible, provide support to make an accurate decision closer to the decision deadline. If reversible with no limit on the number of reversals, it should be possible to support the operator's decision-making under all possible conditions clearly.	LS2
CM3	Decision on manual blocking is made regardless of the maintenance situation. However, if blocking has not been made or a previously made blocking is released, obtain maintenance information at that point and check whether the PSS will be operated normally after the timer has elapsed.	LS3
CM4	In order to exclude conflicts of interest, even if the PSS is operated, it should be designed not to have a significant adverse effect on the subsequent nuclear power plant operation rate.	LS4
CM5	Introduces agents to support efficient and clear decision-making of the operator, and forces the operator to leave a basis for decision-making.	LS4
CM6	If an operator makes a decision in accordance with the established decision-making system, legal protections are prepared to avoid unreasonable censures based on a result, and a safety culture is formed that focuses on identifying systemic faults that the operator was forced to make that decision.	LS4
CM7	The remaining time between the automatic operation of the PSS after the trip is visually indicated along with whether manual blocking is currently active, and an audible alarm is provided every 20 minutes from 1 hour remains.	LS6, LS7, LS9
CM8	All process variables related to PSS manual blocking are collected so that they can be identified on one page clearly, and the tendency over time is provided together to help judgment, and manual blocking and release according to decision-making are also accessible on the page.	LS5

This study has explored STPA-based hazard identification of human operator interaction with the PSS. The loss scenarios derived from the analysis demonstrate the potential to proactively identify specific human errors, taking into account the system context, including scenario, plant state, and assigned tasks. The insights we can get from the countermeasures can be effectively utilized to inform design improvements that enhance system safety and support more robust operator decision-making in complex and uncertain situations. Based on the above analysis process and results, STPA is expected to be used very effectively to preemptively analyze the hazards of safety systems involving complex interactions and derive measures to improve them. However, the control structure covered in the example analysis deals with the elements to be considered in practice, but it is difficult to guarantee that it deals with all the perfect sets and models the actual interactions between elements. Therefore, adding additional elements or specific interaction information as needed will provide additional practical insights.

The approach of this paper has the potential to further identify potential risks that have not been identified in existing probabilistic safety assessment (PSA). Accordingly, the additional identified risk factors can be reflected as basic events in the existing PSA model [5], and if the impact is significant, it is necessary to find a way to implement the relevant countermeasure

practically. In addition, the contents derived through example analysis are planned to be used as base data for deriving general requirements to be considered from the perspective of PSS design.

ACKNOWLEDGMENTS

This work was supported by and Innovative Small Modular Reactor Development Agency grant funded by the Korean Government (MSIT) (No. RS-2023-00258118).

REFERENCES

[1] NuScale, NuScale US460 Plant Standard Design Approval Application Ch.6 Engineered Safety Features (FSAR Revision 1), 2023 (https://www.nrc.gov/docs/ML2330/ML23304A345.pdf)
[2] NuScale, NuScale US460 Plant Standard Design Approval Application Ch.7 Instrumentation and Controls (FSAR Revision 1), 2023 (https://www.nrc.gov/docs/ML2330/ML23304A348.pdf)
[3] Leveson, N. G., & Thomas, J. P. "STPA Handbook." Massachusetts Institute of Technology, 2018.
[4] Shin, S., Kang, S. W., & Park, J. “From visual representation to signal flow connection: A new modeling approach for STAMP.” Nuclear Engineering and Technology, 57(8), 2025.
[5] Electric Power Research Institute (EPRI), HAZCADS: Hazard and Consequence Analysis for Digital Systems, 2023