Pilot study on STAMP-based hazard analysis for SMR I&C system: NuScale ECCS

Sung-Min Shin[a*], Seung Ki Shin[a], Jin Hee Park[a]
[a]Korea Atomic Energy Research Institute (KAERI), Daejeon, Republic of Korea
*Corresponding Author: kshpjk@kaeri.re.kr

Abstract: Small Modular Reactors (SMRs), currently under global development, strive to incorporate novel concepts and technologies. Despite advancements of SMR, there is a lack of empirical evidence from construction and operational cases, leaving potential unidentified hazards. The conventional fault tree(FT) framework, based on a binary classification of fail/success basic events, may be inadequate in capturing the potential hazards stemming from complex interactions between normal and abnormal operations of SMR in advance.
This study proposes an approach for hazard analysis of the SMR based on the STAMP(System Theoretic Accident Model and Processes). STAMP is basically a qualitative analysis approach. However, the STAMP not only considers the impact of system failures but also models the flow of reference signals related to decision-making elements, including mechanical and human factors. The model is utilized to identify hazardous situations (Unsafe Control Actions - UCAs) by listing instances where specific critical signals are not generated when required, generated unnecessarily, delayed, or disordered. After that, a series of scenarios are identified by reviewing the model to see if the UCAs can actually occur due to a specific cause.
This approach is useful in deriving potential hazard factors of SMR that have not yet been specified and can then be used complementarily with the analysis of fault trees. In this study, the process of this approach and the main results and insights derived from it are summarized.

Keywords: STAMP/STPA, Small Modular Reactor, NuScale, ECCS, Hazard

1. INTRODUCTION

Small Modular Reactors (SMRs) has novel concepts and technologies, such as multi-modules, automation of non-safety systems, simplification and passivisation of safety systems, and reduction in operational personnel compared to conventional large-scale nuclear power plants. However, there is a lack of empirical evidence from construction and operational cases, leaving potential unidentified hazards which can happen between mechanical elements, between mechanical elements and human operators, between human operators. Instrumentation and control (I&C) systems in nuclear power plants (NPPs) play a vital role in that they initiate safety functions by automatically generating control action (CA), in other word safety signals. In addition to the I&C system, there is, of course, another means to initiate safety functions: human operators. Currently, the reliability assessment process for human behavior during manual CA generation is conducted through the so-called human reliability analysis (HRA), which estimates the likelihood of failures in generating manual CAs by considering diverse performance shaping factors (PSFs) such as stress level and workload [1,2]. As a result of HRA, human error probability is derived. In addition to the PSFs currently applied in HRA, the condition of the I&C system itself at the moment of interaction with operators also needs to be considered because it affects not only the correctness of the relevant information required to make decisions but also the acquisition and transmission of manually generated CAs.

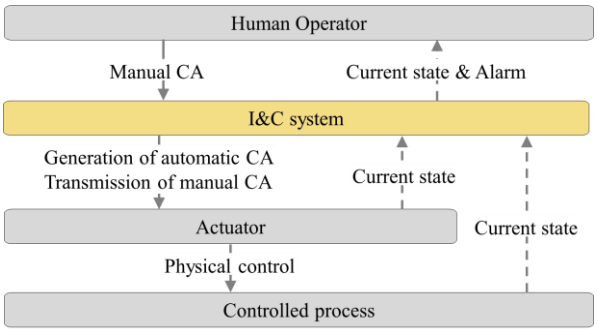

Figure 1. Interactions between an operator and the I&C system for CA generation

Figure 1 outlines the interactions when an I&C system and human operator are associated together in generating a CA. Based on Figure 1, the overall functions of the I&C system can be summarized as follows:

- Function-1) Obtaining the current state of the controlled process, generating an automatic CA based on it, and transmitting the CA to the actuator.\
- Function-2) Obtaining the current states of the controlled process and actuator, and transmitting them with relevant alarms to the human operator.
- Function-3) Acquiring a manual CA from the human operator and transmitting it to the actuator.

In current analyses of NPP I&C systems, Function-1 and Fuction-3 are analyzed in-depth in the form of fault trees, while Function-2 is not. Regarding I&C system Function-2, the safety analysis of human–system interaction—the transmission of feedback (FB) to human operators for manual CA generation—has not been faithfully examined. For a human operator to generate the appropriate manual CA, it is necessary to properly understand the current status of the controlled process. However, reliability analysis alone of I&C systems makes it difficult to fully analyze hazards that occur in human–system interactions caused by some problems in the I&C system. It should be clarified that safety analysis is different from reliability analysis; a system can be reliable but unsafe, or can be safe but unreliable [3]. Accordingly, proper safety analysis can only be performed by sufficiently considering the interactions between system components.
From a similar view, some research has raised concerns about the potential hazards caused by interactions between the I&C system and the controlled process or between I&C systems [4, 5]. In connection with this, system theory-based approaches have been suggested [3, 6–7] to capture the hazards in the interactions between system components. Among the various approaches [3, 8–10], System-Theoretic Accident Model and Processes (STAMP), which considers all the interactions between system components including machine and human, has been applied in practice to various fields including nuclear [8–12] industries.
In this study, the STAMP framework is applied to link the conditions of the SMR I&C system. In addition, a pilot study in conducted to analyze I&C system hazards from the perspective of FB transmission to human operators.

2. STAMP/STPA

As an accident and process model of a control systme, STAMP based on the system theory. The system theory is an approach that views systems as complex wholes whose properties and behaviors arise from the interactions and relationships among their components. It emphasizes understanding these interactions and the control loops within the system, rather than focusing solely on individual parts in isolation. The control loop in STAMP is consisting of the following elements.

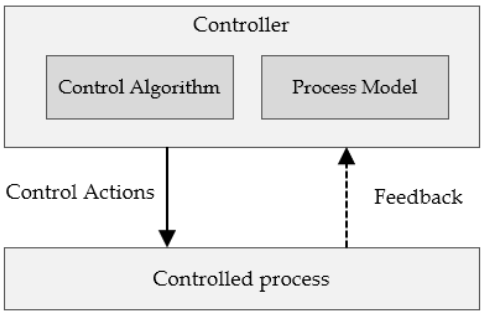

Figure 2. Configuration of the control loop that makes up STAMP

- 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

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

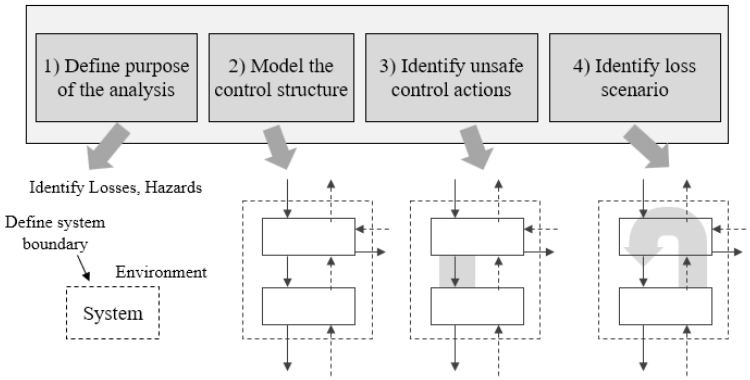

Figure 3. 4 steps for STPA

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.
   - The four criteria in Table 1 are commonly used to identify UCAs.
   - The risk of a system does not depend simply on the form in which the control is provided, but on the context, which refers to the environmental conditions of the system at the time the control is provided.
   - The context is closely related to the process model of the control entity, and the UCA is derived based on the context in which the control is given and the form in which it is provided.

Table 1. UCA types

UCA type	Description
Not providing causes hazard	Hazard occurs because <Controller> does not provide <Control Action>
Providing causes Hazard	Hazard occurs because <Controller> provides <Control Action>
Too late, too soon, out of order	Hazard occurs because <Controller> provides <Control Action> at the wrong time (too late, too soon, or out of order)
Stopped too soon, Applied too long	Hazard occurs because <Controller> provides <Control Action> but lasts too long or is stopped too soon.

4) Identify Loss Scenarios:
   - Explore the causal factors of loss
   - Loss scenarios can be derived based on the control structure, which can be categorized into two main types: (1) how risk factors such as incorrect feedback, inadequate requirements, design errors,

component failures, etc. can cause UCAs, (2) why the system may not function properly despite the correct control actions being provided.

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.

3. NUSCALE ECCS (Emergency Core Cooling System)

The ECCS provides a passive means of decay heat removal in the event of a loss of coolant accident (LOCA). The ECCS consists of two independent reactor vent valves and two independent reactor recirculation valves. All four valves are closed during normal operation. During ECCS operation, the reactor vent valves vent steam from the reactor pressure vessle (RPV) into the containment vessel (CNV) where the steam condenses and collects in the bottom of the containment. The reactor recirculation valves allow water to reenter the RPV and be naturally circulated through the core. When reactor coolant temperature is reduced to below the boiling point, core cooling continues via conduction through the CNV to the reactor pool. The cooling function of the ECCS is entirely passive[13]. ECCS is located at the end of the accident mitigation sequence following the occurrence of almost all initial events and has a very profound effect on the prevention of core damage in nuclear power plants. ECCS, which performs such an important function, can automatically actuated by module protection (MPS) that compares the value of the process variable with the value of the set point, by a timer that counts 8 hours after the trip, by another timer that counts 24 hours after the low voltage of the DC battery charger occurs, and can manually actuated by human operators.

Figure 4 is a control logical diagram based on information extracted from NuScale FSAR. These diagrams are commonly used to describe the functions of the I&C system. However, this format does not indicate what information the human operator receives, what cognitive model is formed, and what decision-making logic(control algorithm).

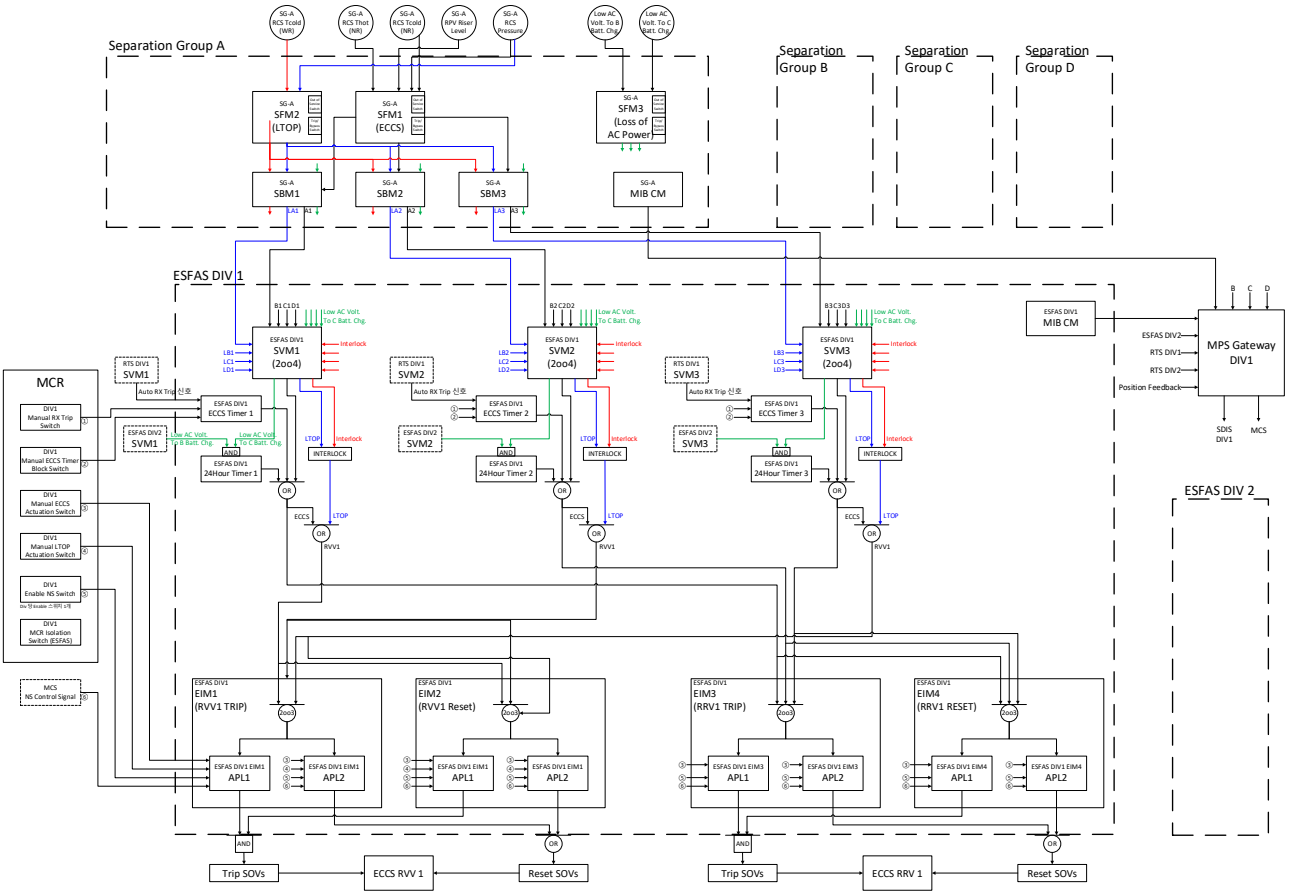

Figure 4. Control logic diagram for ECCS actuation

Figure 5 shows STAMP development for ECCS activation which include all the system components related ECCS actuation including human operator. The STAMP principle is to make a linkage between which signals update a process model of the controller (the human operator is one of the controllers) and which process model a control algorithm refers to. Naturally, the STAMP developed is encouraged to look at all the flow of signal generation/transmission/performance according to this principle. The model was made using TRACEIT, a STAMP/STPA tool developed by KAERI. TRACEIT focuses on the complex I&C analysis of NPP, so instead of expressing a signal as text on the feedback or control action line, the contents are computerized and all links between them are also made during the STAMP development procedure.

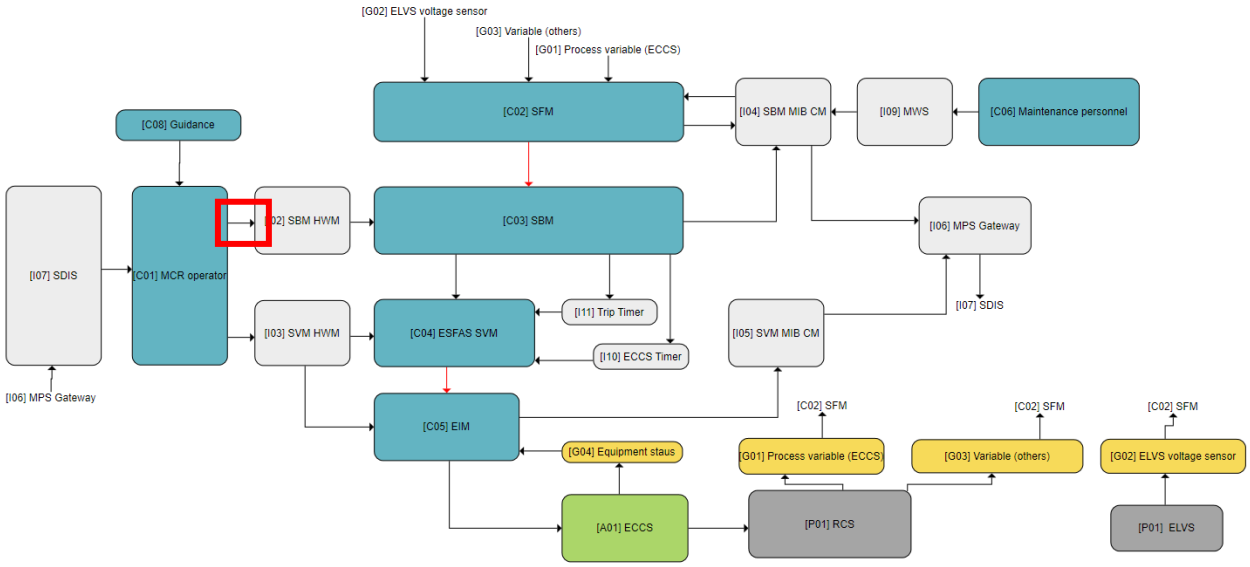

Figure 5. STAMP of ECCS actuation

Since the developed STAMP information is inherently computerized, it is possible to intensively review the generation/transmission/performance of signals related to a specific safety signal using this information. For example, if the entire signal flow is reconstructed focusing the "ECCS timer manual block" signal located in the red path in Figure 5, it is shown in Figure 6. For the implicit expression, both the relevant signal (SG) and process model (PM) are indicated by IDs and related information is collected and given in a separate table. For reference, "ECCS manual block" is a function that does not operate ECCS by manually blocking the ECCS timer if it is determined that there is no problem with criticality 8 hours after a trip that does not cause ECCS automatic operation occur.

Table 2. Signal table for ECCS actuation STAMP (Figure 6)

ID	Name	Remarks
PM01	Subcriticality	PM01 = SG44×(SG01+SG02+SG03+SG05)
PM02	Process variables exceed setpoint (ECCS)	PM02 = (SG01×SG07+SG02×SG09+SG03×SG10){1/3}
PM03	Process variables exceed setpoint (others)	PM03 = SG05×SG08
PM05	ELVS voltage condition	PM05 = SG04
PM06	SDB condition	PM06 = SG18
PM07	SFM N condition (Manaual input)	PM07 = +SG16
PM09	ECCS actuations and bypass (SG A/B/C/D)	PM09 = SG11+SG19+SG20
PM10	Elapsed time after trip	PM10 = SG31
PM11	Elapsed time after ELVS low V	PM11 = SG29
PM12	ECCS timer manual block	PM12 = SG37
PM13	ECCS auto actuations (SVM SD1/2/3)	PM13 = (SG28+SG27)+SG33+SG34
PM14	ECCS manual actuation (safety)	PM14 = SG38
PM15	ECCS manual actuation (NS)	PM15 = SG24×SG40
PM16	Current Module condition	PM16 = SG01+SG02+SG03+SG05

PM17	Time elapsed	PM17 = SG29+SG31
PM18	Automatic ECCS actuation status	PM18 = SG28+SG35
SG01	RPV riser level	
SG02	RCS temperature	
SG03	RCS pressure	
SG04	ELVS voltage	
SG05	Variables (others)	
SG07	Set point (RPV riser level)	
SG08	Set point (Others)	
SG09	Set point (RCS temperature)	
SG10	Set point (RCS pressure))	
SG11	ECCS actuation (SFM)	SG11** = PM02
SG12	Reactor Trip (SFM)	SG12** = PM03
SG13	Low ELVS voltage 24-hour timer ON	SG13** = PM05
SG16	SFM N Operate/OOS	
SG18	Alarm & not response (SDB failure detected by SFM)	
SG19	ECCS actuation (SBM)	SG19** = PM06×PM07
SG20	ECCS bypass (SBM)	SG20** = PM06×PM07
SG24	Enable NS	
SG27	Not response (SDB failure detected by SVM)	
SG28	ECCS actuation (SVM 2/4)	SG28** = PM09
SG29	Elapsed time after ELVS low V	SG13*
SG31	Elapsed time after trip	SG12*
SG33	ECCS actuation (8 hours later trip)	SG33** = PM10×!PM12
SG34	ECCS actuation (24 hours later ELVS low V)	SG34** = PM11
SG35	ECCS actuation (EIM)	SG35** = (PM13+PM14+PM15){1/3}
SG37	ECCS timer manual block	SG37** = PM01×PM17
SG38	ECCS manual actuation (safety)	SG38** = PM16×PM18
SG40	ECCS manual actuation (NS)	SG40** = PM16×PM18
SG44	Guidance (ECCS manual block or activation)	

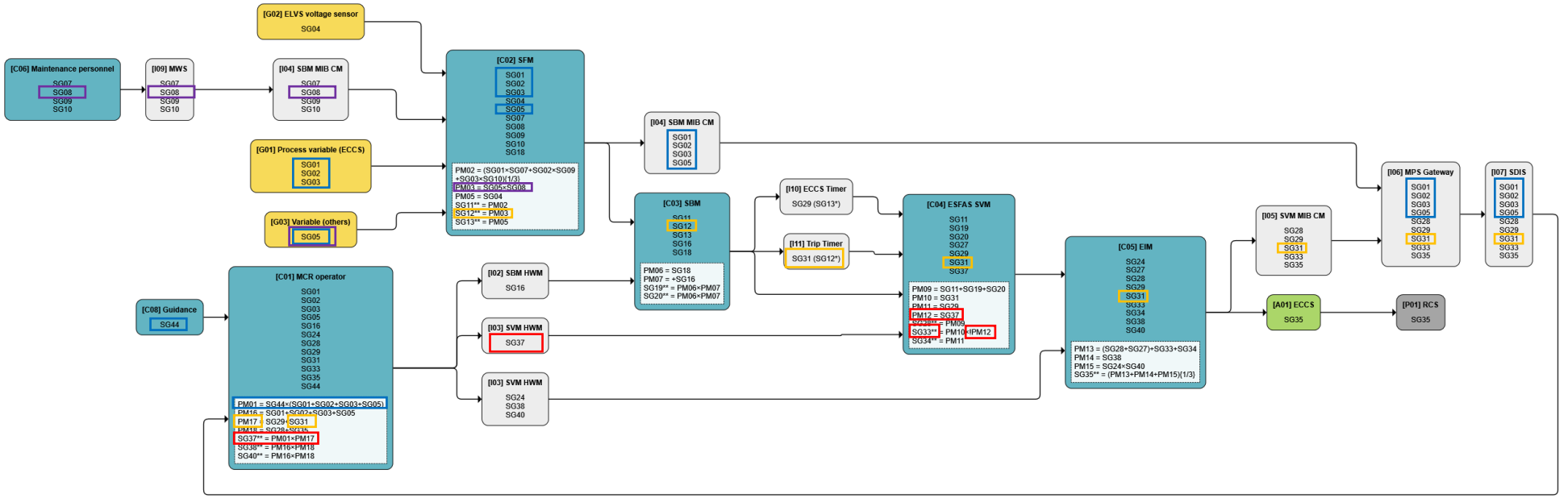

Figure 6. Reconstructed STAMP on "ECCS timer manual blal block"

Based on the STAMP information as shown in Figure 6, it is possible to reexamine whether the related factors are properly implemented. In particular, it is the unique strength of the STAMP model that forces a reviewer to examine the validity of the factors for forming the recognization (process model) and decision-making logic (control algorithm) of controllers.

The selected SG37 (ECCS temporal block) is generated only when PM01 and PM17 are present. First, PM01 is formed through SG44 and (SG01, SG02, SG03, or SG05). It was assumed that Criticality was judged as a result of monitoring these variables. For PM01, SG44 is given from the guidance of [C08]. Based on this, it is possible to reexamine whether SG44 provided in [C08] provides the correct guide to determine PM01 subcriticality according to the result of reviewing related variables.

SG01, SG02, SG03, and SG05 are then passed as is from [I07] SDIS, [I06] MPS Gatewary, [I04] SBM MIB CM, [C02] SFM, [G01] Process variable (ECCS) and [G03] Variable (others). It is possible to reexamine whether elements in the path through which the information is transmitted correctly generate the signal and transfer it without distortion at an appropriate timing.

Coming back to SG37, to create SG37, PM17 time elapsed, which also references SG31 Elapsed time after trip, is used to decide whether to create it. So, if we trace back SG31, it is passed as is through [I07] SDIS, [I06] MPS Gateway, [I05] SVM MIB CM, [C05] EIM, [C04] ESFAS SVM, [I11] Trip Timer, [C03] SBM. So, as above, we can reexamine the soundness of the elements in the transmission path. Furthermore, SG12 is determined by reference to PM03 in the [C02] SFM, which is formed by SG05 and SG08, i.e., it generates a trip signal by comparing the trip set point with the process variable. This can be reviewed to ensure that the trip set point, SG08, has been entered correctly by the [C06] Maintenance personnel and transmitted correctly by the [I09] MWS and [I04] SBM MIB CM. In addition, the sensor can be reviewed to see if the process variable was created correctly by [G03] Variable (others).

4. CONCLUSION AND DISCUSSION

In this paper, the authors develop a STAMP model of ECCS automatic/manual signal generation applied to NuScale as an example to systematically examine the hazards that may occur in complex interactions between system components including human operators, and examine how the model can be analyzed from the perspective of hazard analysis. STAMP is considered to be very useful for reviewing hazards from a holistic perspective by logically representing the interactions between complex I&C system components, including human factors, in a single model which was difficult to do so in FMEA and FTA. Also, the signal flow can eventually be interpreted as the effect of the failure, so it may be possible to convert the model to FT later. Such an approach would greatly increase the efficiency of creating FTs for I&C systems.
The hazard analysis of the completed STAMP model can be reviewed more systematically through STPA. In this study, we plan to perform STPA on several safety signal generators in NuScale, including the ECCS actuation signal. The insights gained from this process will be utilized as input to the design of the i-SMR currently under development in Korea.

Acknowledgements

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

References

[1] A. Kolaczkowski, J. Forester, E. Lois, and S. Cooper, "Good Practices for Implementing Human Reliability Analysis", U.S. Nucl. Regulatory Commission, Washington DC, USA, NUREG-1792, Apr. 2005.
[2] Y.C. Kim, J.W. Kim, J.k. Park, C.S. Choi, and H.E. Kim,An HRA Method for Digital Main Control Rooms ― Part II: Estimating the Failure Probability Due to Cognitive Error," Korea At. Energy Research Inst., Daejeon, Republic of Korea, Tech. Rep. KAERI/TR-8065/2020, Sep. 2020.
[3] N. G. Leveson, Engineering a safer world: systems thinking applied to safety. Cambridge, MA, USA: MIT Press, Jan. 2011.
[4] T. Aldemir, D. W. Miller, M. P. Stovsky, J. Kirschenbaum, P. Bucci, A. W. Fentiman, and L. T. Mangan, "Current state of reliability modeling methodologies for digital systems and their acceptance criteria for nuclear power plant assessments," U.S. Nucl. Regulatory Commission, Washington DC, USA, Tech. Rep. NUREG/CR-6901, Feb. 2006.
[5] T. Aldemir, M. P. Stovsky, J. Kirschenbaum, D. Mandelli, P. Bucci, L. A. Mangan, D. W. Miller, X. Sun, E. Ekici, S. Guarro, M. Yau, B. Johnson, C. Elks, and S. A. Arndt, "Dynamic reliability modeling of digital instrumentation and control systems for nuclear reactor probabilistic risk assessments," U.S. Nucl. Regulatory Commission, Washington DC, USA, Tech. Rep. NUREG/CR-6942, Oct. 2007.
[6] J. Rasmussen, "Risk management in a dynamic society: a modelling problem," Saf. Sci., vol. 27, no. 2, pp. 183-213, Dec. 1997, doi: 10.1016/S0925-7535(97)00052-0.
[7] E. Hollnagel, Barriers and accident prevention. Aldershot, UK: Ashgate, 2004.
[8] J. Thomas, F.L. Lemons, N. Leveson, "Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants", Res. Rep. : NRC-HQ-11-6-04-0060, Nov. 2012
[9] B. Geddes, M. Bailey, L. Freil, J. Thomas, B. Antoine, N. Geddes, D. Blanchard, and N. Thuy, "Hazard Analysis Methods for Digital Instrumentation and Control Systems", EPRI technical report, Jun. 2013.
[10] T. Wheeler, A. Clark, A. Williams, A. Muna, L. Dawson, B. Geddes, and D. Blanchard, "Hazards and Consequences Analysis for Digital Systems", EPRI technical report, Dec. 2018.
[11] "An Integrated Risk Assessment Process for Digital Instrumentation and Control Upgrades of Nuclear Power Plants, DOE, INL/EXT-19-55219"
[12] S.H. Lee, S.-M. Shin, J.S. Hwang, J.K. Park, "Operational Vulnerability Identification Procedure for Nuclear Facilities using STAMP/STPA", IEEE access, vol.8 99. 166034-166046, 2020
[13] NuScale Final Safety Analysis Report, Revision 0, Chapter 1, 2022