A preliminary study on application of STPA to Reactor Protection System for Defense-in-Depth and Diversity

Hyeongseok Eun [a,b*], Yoona Heo[c], Junbeom Yoo[c], Eunkyoung Jee[b], Jongmoon Baik[b], Sung-Min Shin[a], Joon-Ku Lee[a]
[a]*Korea Atomic Energy Research Institute, 989-111 Daedeokdaero, Yuseong-gu, Daejeon, Korea, 34057*
[b]*School of Computing, Korea Advanced Institute of Science and Technology (KAIST)*
[c]*Division of Computer Science and Engineering, Konkuk University, Korea*
[*]*Corresponding author: hseun@kaeri.re.kr*

1. Introduction

Instrumentation and control (I&C) systems in nuclear power plants (NPPs) have been gradually digitized with the advancement of digital technology with defense-in-depth and diversity (D3), leading to hardware and software complexity and technology diversification. As a result, I&C system failures are generally not caused by the failure of one component but by undesired interactions among several system elements. Traditional hazard analysis methods such as fault tree analysis (FTA), failure mode and effects analysis (FMEA), and hazard and operability analysis (HAZOP) have been widely applied to I&C system hazard analysis. However, traditional hazard analysis methods that analyze system components individually and in isolation are no longer sufficient [1]. System theoretic process analysis (STPA) is a hazard analysis technique based on systems engineering principles. The Nuclear Regulatory Commission (NRC) mentioned the recent use of STPA [2], and the NuScale small modular reactor (SMR) has verified the suitability of I&C design using STPA [3]. This study presents STPA results of the reactor protection system (RPS) function in the APR1400 I&C design with a D3 perspective.

2. Background

2.1 Overview of STPA

Systems theoretic accident model and processes (STAMP) is an accident model based on system and control theory, including more complex processes and unsafe interactions among system components. STPA is a hazard analysis technique based on STAMP. The basic steps in STPA are shown in Figure 1.

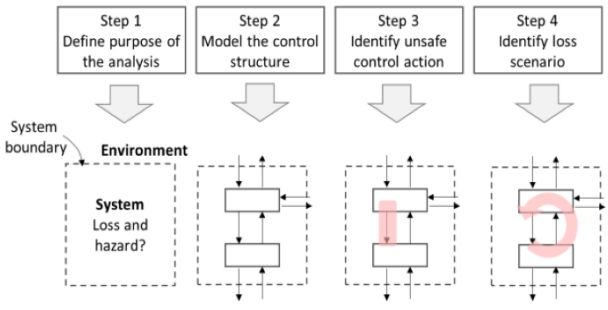

Figure 1. Overview of the STPA Method [4]

Using the causal factors identified through STAMP, STPA focuses on not only the individual components but also the entire accident process. STPA systematically analyzes areas not well represented in traditional hazard analysis methods and oversight processes (e.g., hazards associated with the maintenance and operation of safety systems, complex software interactions, and the identification of hazards associated with emergent properties).

2.2 Branch Technical Position (BTP) 7-19 and evaluation of STPA in NPP

Recently, the NRC published BTP 7-19, Revision 9 [5], which guides the evaluation of common cause failures (CCFs) in I&C systems and provides NRC staff with guidance for evaluating an applicant's assessment of the adequacy of D3 for a proposed I&C system. The revised BTP 7-19 states that the reviewer should consider whether the assessment demonstrates that the residual CCF is not risk-significant if the application includes a risk-informed approach. Furthermore, the applicant should assess the risk of CCF vulnerabilities using a risk-informed approach and apply design techniques, prevention measures, or mitigation measures commensurate with the risk significance of the postulated CCF.

NRC staff have recognized that STPA complements traditional hazard analysis methods [2]. NuScale SMR performed a hazard analysis on four safety systems utilizing STPA as a risk-informed approach, and NRC approved NuScale's final safety analysis report (FSAR), including the I&C STPA results.

2.3 Limitations of existing STPA application on RPS

Since the RPS is the most important safety system in NPPs, ensuring its safety has always been a major research topic in the nuclear industry [6]. However, few studies have been published on RPS although STPA studies for QIAS-P [7] and ESF-CCS [8] in I&C systems have been reported. Existing RPS studies [6,9] have not considered the diverse protection system (DPS) interconnection and related activities with a D3 perspective.

In the i-SMR [10] and Generation IV SMRs, the STPA with a D3 perspective can be a new complement to regulatory activities for licensable digital I&C technologies. Therefore, this study conducts STPA

preliminary analysis reflecting the latest APR1400 RPS design by referring to the APR1400 design certification documents [11,12] for Shin-Hanul NPP units 1 and 2 FSAR [13] and Saeul NPP units 3 and 4 FSAR [14].

3. Methods and Results

We used the XSTAMPP program [15] to draw a control structure and identify unsafe control actions (UCAs). STPA involves four main steps [4]:

1) STEP 1 - Define the purpose of the analysis

In this study, the target I&C system is the RPS of the APR1400 NPPs for Shin-Hanul NPP units 1 and 2 and Saeul NPP units 3 and 4. The components of RPS, such as programmable logic controllers (PLCs) and distributed controller systems (DCSs), connected sensors, and actuators are also included to analyze the adequacy of D3. The control structure includes not only physical components, such as PLC and DCS, but also activities related to I&C, such as design, manufacturing, operation, quality assurance, and maintenance. Dealing with these activities is one of the advantages of STAMP[4].

Losses are typically defined by referring to STPA steps presented in the previous studies [16,17], while defined hazards are specific to RPS like the previous study's approach [18]. The connectivity between the defined losses and hazards is shown in Table I.

Table I: Losses and hazards focused on RPS

ID	Loss name
L-1	Loss of life; injury to people
L-2	Damage to environment (e.g. contamination, release)
L-3	Loss of power generation
L-4	Financial losses (e.g. repair)
L-5	Loss of reputation, goodwill, trust, investor confidence

ID	Hazard name	Links
H-1	Digital CCF occurrence	L-1,2,3
H-2	Human Error	L-1,2,3
H-3	False positive indication or alarm	L-3
H-4	False negative indication or alarm	L-1,2
H-5	Unexpected reactor trip	L-3,4,5
H-6	Failure of reactor trip	L-1,2,5
H-7	Time delay in signal processing	L-3
H-8	Abnormal fluctuation in input signal	L-3
H-9	Maintenance Error	L-1,2,3,4
H-10	Regulatory licensing basis violation	L-1,2,3,4,5

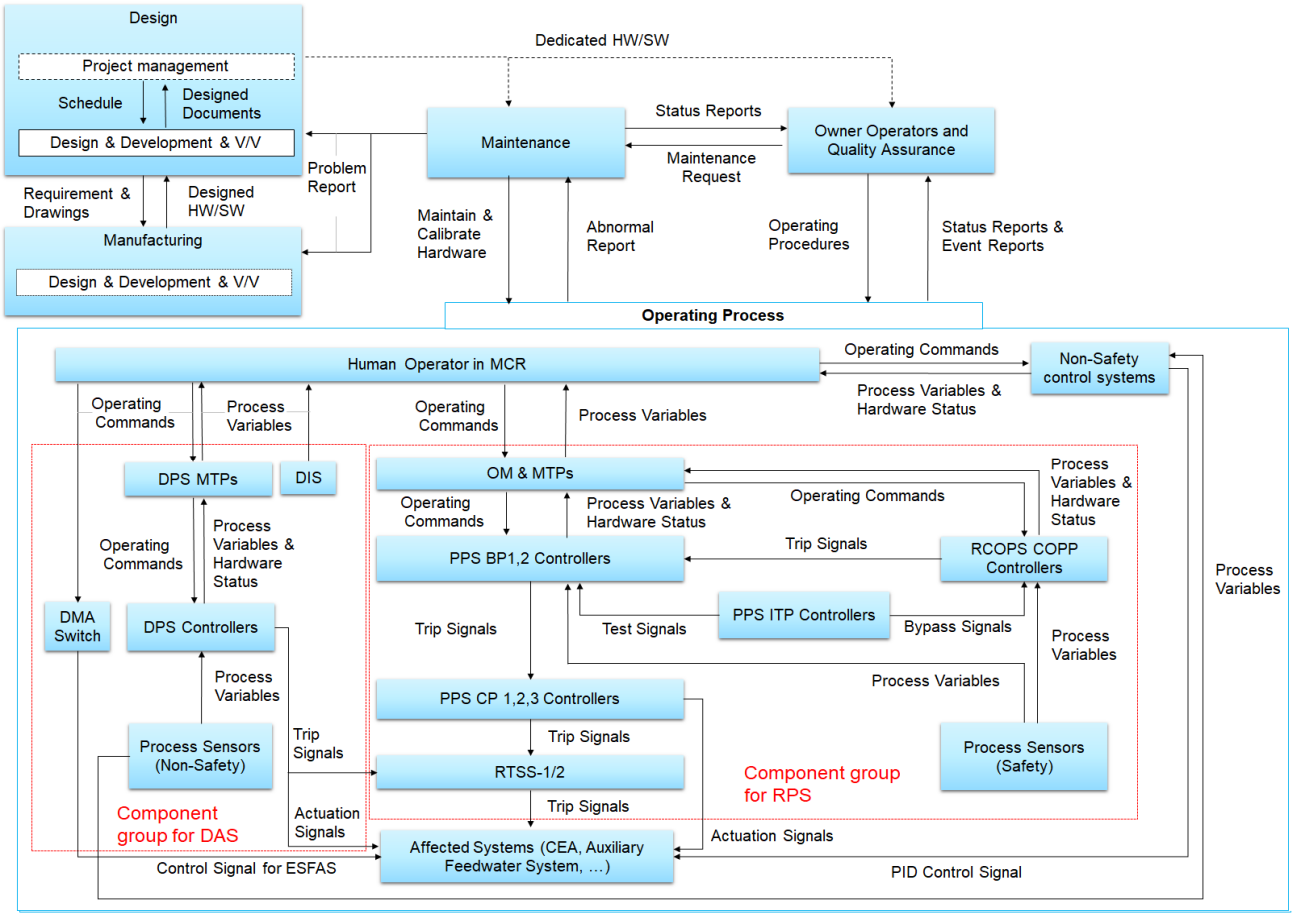

Figure 2. Control structure of APR1400 I&C system focused on RPS

Table II: UCAs related to setpoint modification

Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or Applied too long
Operating Commands (CA-7) (Source: OM/MTPs, Destination: BP1,2)	[UCA1.12] OM or MTP does not provide a setpoint modification (including manual setpoint reset) signal when the operator sends a request to change the setpoints.	[UCA1.13] OM or MTP provides an incorrect setpoint value when the operator requests to change the setpoints.	[UCA1.14] OM or MTP provides a setpoint modification signal too late when the operator sends a request to change the setpoints.	[UCA1.15] OM or MTP provides a setpoint change signal within an insufficient amount of time and the processor does not receive the signal.
Links	[H-5], [H-6]	[H-3], [H-8]	[H-6], [H-7]	[H-6]

Actual losses can occur as a combination of these hazards, so multiple failures should be considered.

2) STEP 2 - Model the control structure

A control structure has functional relationships and signal interactions. The control structure of the APR1400 I&C system focused on RPS is shown in Figure 2.

Figure 2 solely shows the control structure focused on RPS and does not include all the actual signal lines. In addition, some I&C subsystems unrelated to the RPS function are abstracted or grouped. Although we developed a detailed control structure showing subsystems and process instrument components, it is not provided in this paper due to space limitations and the need for design verification.

3) STEP 3 - Identify unsafe control action

In this step, we determine which control actions in the control structure lead to system hazards with unsatisfied safety constraints that can become UCAs. When defining a UCA, key considerations are the RPS-related system interactions included in the I&C, and the alternative signal flow with a D3 perspective, such as the DPS or the diverse manual actuation (DMA) switch. Table II and Figure 3 provide examples of how control action CA-7 links to multiple UCAs.

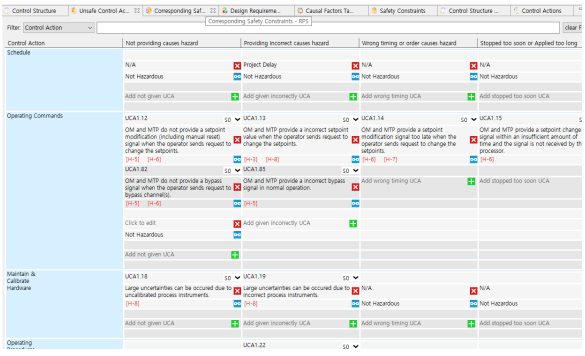

Figure 3. Identifying UCAs with XSTAMPP

In Table II, control action CA-7 is an operator command signal to change a setpoint value in the operator module (OM) or maintenance test panel (MTP). In some situations, this command signal should be applied to the PLC after the operator clicks the OM or MTP screen. If this signal is ended too early, there is a possibility that the signal will not reach the PLC. If then, the changing setpoint request is ignored, which may cause the H-6 (Failure of reactor trip). However, not all identified UCAs result in losses. The possibility of actually causing a loss is identified in the next steps.

4) STEP 4 - Identify loss scenarios

We made a list of loss scenarios considering a combination of various casual factors (CFs) and we searched for plausible scenarios considering the DPS and DMA switch operations with a D3 perspective. We compared the listed plausible scenarios with published reactor trip cases [19,20] and expert experience to find several reasonable scenarios. Table III shows examples of causal factors related to maintenance activity.

Table III: Causal factor table for loss scenarios related to maintenance

Component	Unsafe Control Actions	Causal Factor
Maintenance	[UCA1.18] Large uncertainties can occur due to uncalibrated process instruments. [H-8]	Uncalibrated sensors are used during operation. [SC1.18]
	[UCA1.141] QA does not provide a maintenance request even if the hardware is abnormal. [H-3, H-9]	Abnormal hardware is used with false positive indication. [SC1.19]
	[UCA1.193] Spare sets of hardware or software with a design flaw (e.g., an internal digital fault) can be replaced at once during a maintenance period. [H-1, H-3]	Abnormal hardware is replaced with false positive indication. [SC-23, SC-187]

If UCA1.193 is triggered, a loss due to H-1 (Digital CCF occurrence) can occur. From a D3 perspective, corresponding safety constraints (SCs) 23 and 187 are not satisfied, which can cause problems in the entire I&C system due to H-1 (Digital CCF occurrence) or H-3 (False positive indication or alarm).

Table IV shows another identified loss scenario example related to UCA-105.

Table IV: Causal factor table for loss scenario related to RPS processor

Component	Unsafe Control Actions	Causal Factor
RPS processor	[UCA1.105] A processor provides process values and hardware status with inappropriate communication delays. [H-2, H-7]	Communication delay time related to CEA is not sufficient. [SC1.105]

In June 1998, Hanbit NPP unit 4 experienced a channel trip with reactor power cutback [20]. When the control element assemblies (CEAs) of regulating CEA group 4 and 5 dropped by reactor power cutback, an unexpected CEA out-of-sequence trip signal with a slight timing difference resulted in one channel trip. Loss scenario analysis of STPA predicts that this kind of signal transmission and timing difference can cause a risk. The current APR1400 design reflects an advanced scheme to prevent such events in operator procedures and RPS software.

Using XSTAMPP, we obtained the STPA report. Table V shows the analysis results.

Table V: Number of items for the STPA for RPS

Items	Number
Control Actions	34
UCA and Safety Constraints	94
Causal Factor Tables	39

After the preliminary STPA, we confirmed that performing STPA is a time-intensive process even for experts. The control structure had to be recursively modified to reflect the actual system at all STPA steps. STPA 3 and 4 took several times longer than expected because control structure components are often added or modified during this process. Design verification is also necessary to reflect actual system interactions. Therefore, we recommend performing STPA by a system manager directly in charge of the system. Moreover, when a non-manager safety analyst performs STPA, feedback from the system manager is essential. Because I&C involves many system interactions, it is expected to be time-consuming and challenging to derive UCAs and objectively estimate criteria for system experts.

4. Threat to validity

Due to resource limitations, this study does not consider cyber-attacks, which can cause simultaneous failures of multiple D3 levels, and engineered safety features actuation systems (ESFAS) function which is one of the important safety I&C systems. In addition, since the XSTAMPP 3.1.2 was developed before the STPA handbook [4] was published, some STPA steps in this study followed the old STPA style. Therefore, a revision of the XSTAMPP or a new STPA tool should be considered.

5. Conclusion

In this study, we conducted a preliminary STPA with a D3 perspective, which is hard to do with traditional hazard analysis methods. Analyzing the proposed control structure focused on RPS, we derived the UCAs and safety constraints causing failures of D3 levels. We found that STPA is a time-intensive process and that actual STPA application is likely even more time-consuming and challenging than the one shown in this preliminary study. Using the preliminary STPA results, we plan to conduct an integrated STPA application of the APR1400 I&C system, including the ESFAS function.

ACKNOWLEDGMENTS

This work was supported by the Nuclear Safety Research Program through the Regulatory Research Management Agency of SMRS (RMAS) and the Nuclear Safety and Security Commission (NSSC) of the Republic of Korea (No. 2024-00509643), and the National Research Foundation of Korea (NRF) funded by the Korea Government (Ministry of Science and ICT) (NRF-2020M2D7A1079181).

REFERENCES

[1] J. Berger, R. Tiusanen, H. Kothalawala and A. Pakonen, "Applying Priority-Informed STPA to a Nuclear I&C System," 2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA), Padova, Italy, pp. 1-7, 2024.

[2] U.S. Nuclear Regulatory Commission, "Guidance for Addressing Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems," NEI 20-07.

[3] P. Butchart, "Use of STPA in the Development of a Reactor Protection System at NuScale Power," NuScale, 2020 STAMP Workshop, virtual workshop July 20 to August.7, 2020.

[4] N. Leveson, and J. Thomas, "STPA Handbook," MIT Partnership for Systems Approaches to Safety and Security, 2018.

[5] U.S. Nuclear Regulatory Commission, "Branch Technical Position Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," BTP-7-19, Revision 9.

[6] C. Liu, Z. Chen, Z. Wu, H. Liu, and X. Yang, "Research and Application of STPA to Digital Reactor Shutdown System in NPP for System Safety Analysis," Nuclear Power Engineering, 2015, 36(S2): 157-161.

[7] C. Park, K. Moon, C. Choi, and S. Jeong, "Application of STPA Technique to Software Hazard Analysis for Nuclear Safety I&C System," Transactions of the Korean Nuclear Society Autumn Meeting, Gyeongju, Korea, October 26-27, 2017.
[8] D. Lee, J. Lee, S. Cheon, and J. Yoo, "Application of System Theoretic Process Analysis to Engineered Safety Features-Component Control System," in Proc. Of the 37th Enlarged Halden Programme Group (EHPG) meeting, Gol, Norway, 2013.
[9] S. Jung, Y. Heo, and J. Yoo, "A formal approach to support the identification of unsafe control actions of STPA for nuclear protection systems," Nuclear Engineering and Technology, volume 54, issue 5, May 2022, pages 1635-1643.
[10] H. Kang, B. Lee, S. Lim, "Light water SMR development status in Korea," Nuclear Engineering and Design, volume 419, 2024.
[11] Korea Electric Power Corporation and Korea Hydro & Nuclear Power Co. Ltd., "Safety I&C System," APR1400-Z-J-NR-14001-NP, Rev.3, 2018.
[12] Korea Electric Power Corporation and Korea Hydro & Nuclear Power Co. Ltd., "APR1400 Design Control Document Tier 1," APR1400-K-X-IT-14001-NP, Rev.3, 2018.
[13] Korea Hydro & Nuclear Power Co., Ltd., "Final Safety Analysis Report for Shin-Hanul Units 1&2", Rev.2, 2018.
[14] Korea Hydro & Nuclear Power Co., Ltd., "Final Safety Analysis Report for Shin-Kori Units 5&6", Rev.1, 2022.
[15] A. Abdulkhaleq and S. Wagner, “XSTAMPP 2.0: New Improvements to XSTAMPP Including CAST Accident Analysis and an Extended Approach to STPA,” 2016 STAMP Conference at MIT, 2016.
[16] S. Birla, “Identifying Hazards in a System Design,” http://www.nrc.gov/docs/ML2327/ML23272A033.pdf, (accessed April. 11, 2025).
[17] T. John, “Introduction to STPA,” http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/JThomas-STPA-Introduction.pdf, (accessed April. 11, 2025).
[18] E. Chen, H. Bao, T. Shorthill, H. Zhang and T. Dinh. “Systems-theoretic Hazard Analysis of Digital Human-System Interface Relevant to Reactor Trip,” ArXiv abs/2209.05480, 2022.
[19] Operational Performance Information System for Nuclear Power Plant [OPIS], http://opis.kins.re.kr, (accessed March. 13, 2025).
[20] W. In, “Feasibility Study for Core Protection Calculator Development,” KAERI/RR-2369/2003.