A Study on the Applicability of STPA Method to Digital I&C Design Assessment with regard to Safety Requirements

Seung Ki Shin *, Sung-Min Shin, Sang Hun Lee, Inseok Jang
Korea Atomic Energy Research Institute, 111 Daedeok-daero 989beon-gil, Yuseong-gu, Daejeon 34057, Republic of Korea
**Corresponding author: skshin@kaeri.re.kr*

1. Introduction

In the early design stage of a nuclear facility, specific safety functions are identified to achieve its safety goals such as control of reactivity, cooling of fuel elements, etc., and accordingly, safety systems are designed to automatically perform the safety functions. Safety systems should be designed in accordance with various regulatory requirements, and also it should be shown that the design of safety systems complies with the design criteria considered necessary to ensure high functional reliability.

As digital technologies are adopted in design of instrumentation and control (I&C) systems, the failure mechanisms of I&C systems becomes more diverse and complicated compared to analog-based systems. In this regard, it is necessary to carefully consider an effective way rather than conventional methods to assess the design of digital I&C systems with regard to reliability in licensing process.

System-theoretic process analysis (STPA) method is a relatively new hazard analysis technique based on an extended model of accident causation [1]. In this study, it is investigated how to utilize the STPA method when evaluating the safety design of digital I&C systems according to associated regulatory guidance.

2. Guidance on Safety Design Assessment

IEEE Std. 603 [2] establishes minimum functional and design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems. It provides various design requirements for safety systems such as single-failure criterion, independence, and reliability.

According to IEEE Std. 603, for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design should be performed in order to confirm that such goals have been achieved. The guidance for qualitative and quantitative reliability analysis is provided in IEEE Std. 352 [3] and IEEE Std. 577 [4]. The qualitative reliability analysis is performed to assess conformance of safety systems to applicable design criteria such as single-failure criterion, independence, and channel integrity. Failure modes and effects analysis (FMEA), fault tree analysis, and reliability block diagrams are introduced as qualitative analysis methods in IEEE Std. 352. The quantitative reliability analysis is performed to establish initial periodic testing intervals for safety equipment and to provide a means for evaluating operational performance against requirements. The mathematical modeling methods for reliability and availability estimation is introduced in IEEE Std. 352.

In addition, according to IEEE Std. 603, an engineering evaluation for software common cause failures (CCFs) of digital safety systems should be performed including use of manual action and non-safety systems, or components (or both) to provide means to accomplish the function that would otherwise be defeated by the CCF. Diversity and defense-in-depth (D3) analysis should be performed to evaluate the digital I&C design against potential software CCFs of safety systems in accordance with NUREG-0800 Branch Technical Position 7-19 [5] and NUREG/CR-6303 [6].

The conventional approaches for safety design assessment works for systems where coupling and interactions among components are relatively simple. However, for digital systems with more complicated interactions each other, it would be better to utilize an appropriate method to support the conventional methods.

3. System-Theoretic Process Analysis

The STPA is a hazard analysis method that is part of a relatively new set of safety engineering methods rooted in the theory of Systems-Theoretic Accident Model and Process (STAMP). In addition to component failures, STPA assumes that accidents can also be caused by unsafe interactions of system components, none of which may have failed. The system is treated as a whole, not as the sum of its parts. The basic STPA method has four steps as shown in Fig. 1.

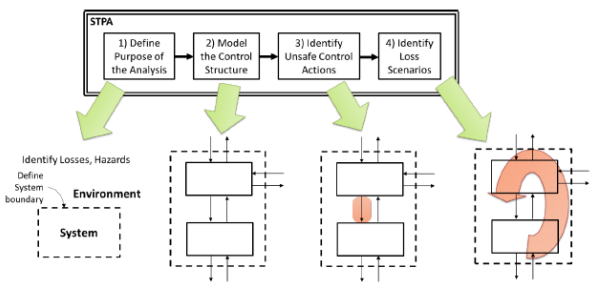

Fig. 1. Overview of the basic STPA method.

The first step is to define purpose of the analysis. In this step, losses, system-level hazard, and system-level constraints are identified.

The second step is to build a model of the system called a control structure. A control structure captures functional relationships and interactions by modeling the system as a set of feedback control loops.

The third step is to analyze control actions in the control structure to examine how they could lead to the losses defined in the first step. These *unsafe control actions* are used to create functional requirements and constraints for the safety.

The fourth step is to identify the reasons why unsafe control might occur in the system. Scenarios are created to explain (1) how incorrect feedback, inadequate requirements, design errors, component failures, and other factors could cause unsafe control actions and ultimately lead to losses, and (2) how safe control actions might be provided but not followed or executed properly, leading to a loss.

Among various advantages of the STPA over traditional hazard/risk analysis techniques represented in the STPA handbook [1], the main advantages for utilizing it in safety design assessment of digital I&C systems are as follows.

- STPA can be started in early concept analysis to assist in identifying safety requirements and constraints. These can then be used to design safety into the system architecture, eliminating the costly rework involved when design flaws are identified late in development or during operations.
- STPA includes software and human operators in the analysis, ensuring that the hazard analysis includes all potential causal factors in losses.
- STPA can be easily integrated into system engineering process.

4. Applicability of STPA to Safety Design Assessments of Digital I&C Systems

In this section, it is investigated how the STPA method can be utilized in safety design assessment of digital I&C systems according to the regulatory licensing requirements described in Section 2.

4.1 Use of STPA in Qualitative and Quantitative Reliability Analysis

As described in Section 2, the reliability analyses of digital safety I&C systems should be carried out in qualitative and quantitative manners. The potential failure modes of each component and their effects on safety of the whole system can be scrutinized through the FMEA method. However, the FMEA focuses on the independent failure of each hardware component, thus it is difficult to figure out the potential system failure caused by multiple components' failures or a software related failure using the FMEA. In this regard, the STPA can be utilized to address those failures as it finds all the causal scenarios leading to an identified loss. The STPA considers the system behavior as a whole and unsafe interactions of components not failed can be captured as a loss scenario, whereas conventional methods such as the FMEA and fault tree analysis begin with decomposing a system into individual components. Therefore, it can be expected that the STPA identifies causal scenarios of system failures that traditional methods cannot find.

In addition, the control structure built in the second step of the STPA can be utilized as one of resources for human reliability analysis (HRA). Figure 2 shows an example of control structure in a very abstract level modeled to analyze digital I&C systems of APR-1400 using the STPA [7] and it is iteratively refined to capture more detail about the system. In the detailed level of control structure, the signal interfaces between systems or components including the list of control and feedback signals are described including human operators. Therefore, from the information contained in the control structure, it can be easily found which feedback signals are credible given that a certain component has failed. Similarly, the credible transmission path of a control signal from human operators can be discriminated in the control structure. It is expected that this kind of information can give an important basis for the HRA or human performance assessment.

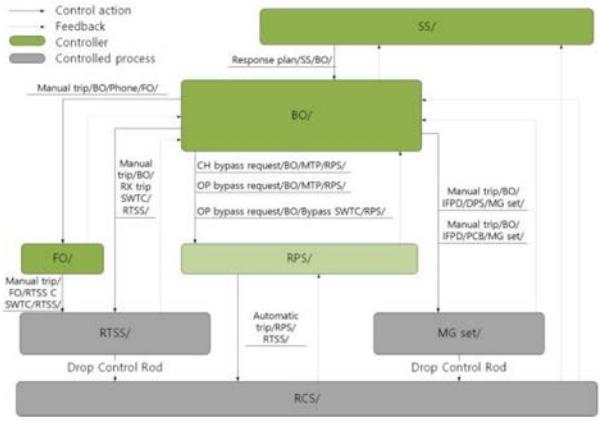

Fig. 2. An example of control structure modeled for digital I&C systems [7].

4.2 Use of STPA in D3 Analysis

As described in Section 2, the D3 analysis should be performed to identify the potential vulnerabilities to a software CCF and verify whether the required safety functions of safety systems can be substituted by other systems unaffected by the CCF when any design basis event occurs concurrently with the CCF. It is very clear that the control structure of STPA is useful for D3 analysis. For example, the guideline 9 of D3 analysis in NUREG/CR-6303 is about output signals and it should

be demonstrated that, in cases where a block has more than one output signal, no output signal is significantly influenced by any credible change or failure of equipment to which any other output signal is connected. To confirm this guideline, the signal interfaces between blocks should be identified first and the control structure of STPA can be utilized for this work. In addition, the control structure can be used as an important schematic diagram to check the compliance with other guidelines such as diversity among echelons of defense, plant monitoring, and manual operator action.

5. Summary and Conclusion

Safety I&C systems should be designed to be highly reliable to achieve the required safety functions and to satisfy various safety design criteria necessary to ensure high functional reliability. In the licensing process, it is required to assess the design of I&C systems whether various safety requirements are met in I&C design using appropriate analysis approaches. As digital technologies are adopted in designing I&C systems, the signal interactions among components and the failure mechanisms become more complicated compared to analog-based systems. Therefore, to overcome the limitations of conventional approaches for safety design assessment of digital I&C systems, it is required to utilize an appropriate method to support the conventional methods. In this regard, we investigated the applicability of the STPA that is a hazard analysis method rooted in the theory of STAMP. In conclusion, it is expected that the STPA method can be utilized effectively with conventional methods for safety design assessments such as qualitative and quantitative reliability analysis and D3 analysis. In addition, a well-modeled control structure is very useful for design assessment of digital I&C systems in many ways.

ACKNOWLEDGEMENT

This work was supported by the National Research Foundation of South Korea Grant funded by the Korean Government (MSIP) (No.2017M2A8A4015291).

REFERENCES

[1] N. G. Leveson and J. P. Thomas, STPA handbook, 2018
[2] IEEE Power & Energy Society, IEEE Std 603-2009, IEEE Standard Criteria for Safety Systems for
Nuclear Power Generating Stations, 2009.
[3] IEEE Power Engineering Society, IEEE Std 352-1987, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems, 1987.
[4] IEEE Power Engineering Society, IEEE Std 577-2004, IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities, 2004.
[5] USNRC, NUREG-0800, Branch Technical Position 7-19, Revision 6, Guidance for Evaluation of Diversity and Defense-in-Depth in Digital computer-Based Instrumentation and Control Systems, 2012.
[6] USNRC, NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, 1994.
[7] S. M. Shin et al., Application of STPA to Risk Analysis of Digital I&C System, Transactions of the Korean Nuclear Society Autumn Meeting, 2020.