Application of STPA Methodology to Safety Analysis of Operation Automation System of Nuclear Power Plant Using Artificial Intelligence Technology

Kee-Choon Kwon*, Jang-Yeol Kim, Seo Ryong Koo
Korea Atomic Energy Research Institute, 989-111 Daedeok-daero, Yuseong-gu, Daejeon, 34057, Republic of Korea
**Corresponding author: kckwon@kaeri.re.kr*

1. Introduction

We are developing a nuclear power plant startup/shutdown operation automation system using artificial intelligence technology. Safety analysis of system and artificial intelligence software is not performed properly. One of the reasons is that the safety analysis methodology is still not well organized because the safety analysis approach to artificial intelligence system and software is different from the existing software. System-Theoretical Process Analysis (STPA) is a relatively new safety analysis technique proposed by MIT's professor Nancy Leveson based on an extended model of accident causes [1]. STPA advantages over traditional hazard/risk analyses are as follows:

- Very complex systems can be analyzed, and unlike traditional hazard analysis methods, STPA can start with an early concept analysis and help identify safety requirements and constraints.
- STPA includes software and human operators in the analysis, ensuring that the hazard analysis includes all potential causal factors in losses.

Many evaluations and comparisons of STPA have been made for traditional hazard analysis methods such as Fault Tree Analysis(FTA), Failure Mode and Effect Critical Analysis(FMECA), Event Tree Analysis(ETA), and Hazard and Operability(HAZOP). In all of these evaluations, STPA not only found all the causal scenarios found in traditional analyses, but it also identified many more, often software-related and non-failure scenarios that the traditional methods did not found. Figure 1 shows the steps in the basic STPA [2]. This new approach, STPA, was viewed as a pilot application of the plant startup and shutdown operation automation system.

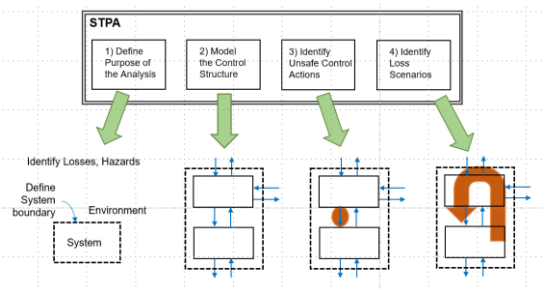

Figure 1. Overview of the basic STPA method [2].

2. Startup and shutdown operation automation system of nuclear power plant

The automation strategy of the nuclear power plant startup and shutdown operation automation system using artificial intelligence technology is to establish a rule-based expert system based on the operating procedures of the plant, and implement the parts that can be operated differently depending on the operator in the section of the expert system using deep learning. In this paper, the development of the expert system is not dealt with simply by the execution of the conditional statement, and the operation automation section, which depends on the operator's experience, is to be implemented with deep learning.

To implement plant startup and shutdown automation using deep learning, prototype which is utilized the compact nuclear simulator that modeling a three-loop pressurized water reactor was used in terms of the data availability aspects and development of the control systems.

The automation section, which is implemented by the deep learning proposed in this study, is the section where the pressurizer bubbles are generated within the hot shutdown operation zone from the cold shutdown. There are many operable operating variables in the pressurizer air bubbles, and various changes in pressure and temperature control can be made depending on the operator. Therefore, optimized operation can be obtained through deep learning.

The rule-based expert system of the operation procedure basically operates automatic operation for startup and shutdown of the plant, and automated operation is performed according to the judgment of the proposed circular neural network-based artificial intelligence framework in areas that require the operator's individual operation experience, such as the generation and operation of the plant air bubbles. Circular neural network-based artificial intelligence framework is basically applied with the Recurrent Neural Network (RNN) model as it can be more efficient as the structure of the circulation neural network becomes larger and wider. In this study, a three-layer Stack-RNN model was constructed and a fully connected model was connected at the last stage. The circulatory neural network is composed of Long Short-term Memory (LSTM) cells to be effective in time series analysis by reflecting the characteristics of plant startup and shutdown operation [3]. The proposed startup and shutdown operation automation system architecture is shown in Figure 2.

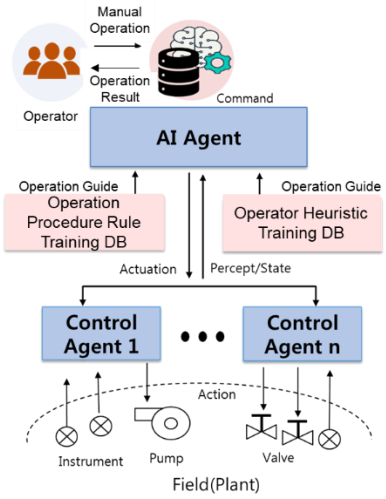

Figure 2. Startup and shutdown operation automation system architecture [3].

3. Application of STPA

We applied the STPA method to the plant startup and shutdown operation automation system which is using AI technology as following processes.

3.1 Step 1: Define purpose of the analysis

Defining the purpose of the analysis is the first step with any analysis aim to prevent? In other words, to identify losses and hazards. Will STPA be applied only to traditional safety goals like preventing loss of human life or will it be applied more broadly to security, privacy, performance and other system properties? What is the system to be analyzed and what is the system boundaries? These and other fundamental questions are addressed here. This analysis using STPA is aimed at identifying the hazards to prevent the startup and shutdown operation automation system of nuclear power plants using artificial intelligence techniques. First, in the identifying loss step, define loss as shown in Table 1.

Table 1. Defined losses and hazards

Loss	Hazards
L-1 People injured or killed	H-1 Release of radioactive materials H-2 Reactor temperature too high
L-2 Environment contaminated	H-1 Release of radioactive materials
L-3 Equipment damage (Economic loss)	H-3 Equipment operated beyond limits H-4 Reactor shut down H-5 AI Software failure
L-4 Loss of electric power generation	H-4 Reactor shut down H-5 AI Software failure

Once losses have been defined, and systems and system boundaries have been identified, the next step is to identify the system conditions that will result in loss in the worst-case environmental conditions, thereby identifying the system-level hazard. Hazards and related losses are shown in Table 2. It is simple to identify the system-level constraints (simply reversing the conditions) that should be implemented when the system-level hazard is identified.

Table 2. Hazards and related losses

Hazard	Related Losses
H-1 Release of radioactive materials	L-1, L-2
H-2 Reactor temperature too high	L-1, L-2, L-3, L-4
H-3 Equipment operated beyond limits	L-3, L-4
H-4 Reactor shut down	L-4
H-5 AI Software failure	L-3, L-4

3.2 Step 2: Build system model-control structure

The second step is to build a model of a system called a hierarchical control structure. The hierarchical control structure models the system as a set of feedback control loops to capture functional relationships and interactions. The control structure usually starts at a very abstract level and is refined repeatedly to capture more detailed information about the system. This step does not change regardless of whether STPA applies to safety, security, privacy, or other attributes. The control structure derived by applying STPA to the startup and shutdown operation automation system is shown in Figure 3.

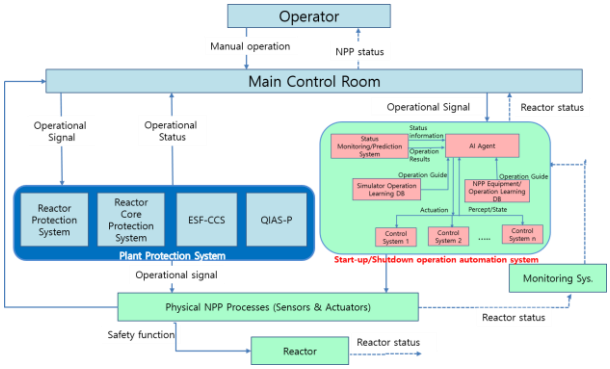

Figure 3. Control structure for startup and shutdown operation automation system

3.3 Step 3: Identify unsafe control action

The third step is to analyze the control measures of the control structure to examine how they can lead to the loss defined in the first step. These unsafe control actions (UCA) are used to create functional requirements and constraints for the system. Here, as a way to ensure system safety when using AI software, which is our concern, we derive UCA by deepening depth only for “AI Software Failure.” A part of the UCA derived by applying STPA to this system is shown in the third column of Table 3.

3.4 Step 4: Identifies the reasons why unsafe control might occur

The fourth step explains why unsafe controls occur in the system. Scenarios are created to explain:
- How incorrect feedback, inadequate requirements, design errors, component errors, and other factors can cause unsafe controls and ultimately lead to loss.
- Safe control measures provided, but improperly executed, ultimately resulting in loss.

Use these results to create additional safety requirements, identify mitigation methods, guide the architecture, and determine design recommendations and new designs. The safety requirements derived from the STPA process activities summarized in Table 3[4,5].

4. Conclusion

The safety analysis of the plant startup and shutdown operation automation system, which includes artificial intelligence software, has not yet been developed with a systematic approach. We have applied STPA to derived a system-level construct of AI software failure, which is our concern. When this system-level component is redefined as a system safety requirement. The suggested system safety requirements are computer and software redundancy, thorough and sufficient planning, testing, and commissioning of AI software, robust system design, etc. This will contribute to improving the safety level of the system.

Acknowledgement

This work, described herein, is being performed for "Development and Operation of ICT-based Nuclear Energy Safety Validation System" as a part of the Korea Atomic Energy Research Institute (KAERI) projects and funded by Ministry of Science and ICT since on January the 1st, 2019. (No. 524320-19). Also this work was supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry, & Energy (MOTIE) (No. 20171510102040).

REFERENCES

[1] Nancy Leveson, Engineering a Safer World, The MIT Press, Cambridge, 2011.
[2] Nancy Leveson and John Thomas, STPA Handbook, March 2018.
[3] Seo Ryong Koo, Hyeonmin Kim, GeonPil Choi, and Jung Taek Kim, "Development of AI Framework Based on RNN for Startup and Shutdown Operation of Nuclear Power Plant," Journal of Institute of Control, Robotics and Systems, Vol. 25(9), pp. 789~794, 2019.
[4] John Thomas, Francisco Luiz de Lemos, and Nancy Leveson, NRC-HQ-11-6-04-0060, "Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants," Nov. 2012.
[5] Osiris Valdez Banda and Sirpa Kannos, Hazard Analysis Process for Autonomous Vessels.

Table 3. The safety requirements derived from the STPA process

Hazard	Safety control	Potentially Unsafe Control Actions	Redefining of the safety control
H-5 AI Software failure	-Computer and software redundancy	-Computer breaks down and there is no computer and software redundancy	-Computer and software redundancy ensure availability of the functions at all times
		-Secondary computer does not take over in case of a failure	-Secondary computer take over in case of a failure
	-Through planning, testing, and commissioning of AI software	-Through planning, testing, and commissioning of AI are not done	-Through and sufficient planning, testing, and commissioning of AI software ensure that the software is robust and free of errors
		-Insufficient planning, testing, and commissioning of AI	
	-Robust system design	-Without robust system design it is not possible to detect and cope with poor and/or missing data	-Robust system design should be able to isolate failures in the system and allow for the rest of the system to continue operating
		-Single point failure takes the whole system down	
	-Appropriate system (software) design and maintenance processes	-User requirements are not known or taken into account and the final product is not the expected	-Ensure that the system meets customer's expectations -Provide good documentation -AI software verified properly -Configuration management is working properly
		-System requirements are not clear for the developers and do not cover relevant issues potential causes	
		-System design does not meet expectations	
		-System implementation does not meet expectations	
		-Software is not verified properly	
		-Configuration management is not working properly	
	-AI software learning data	-Insufficient software learning data	-Sufficient software learning data are required -No error in learning data
		-Error in learning data	
	-When AI SW Failure, transform from automatic operation to manual operation	-Transform from automatic operation to manual operation is not working	-Transform from automatic operation to manual operation should be work
		-Stop automatic operation	