Application of STPA Technique to Software Hazard Analysis for Nuclear Safety I&C System

Park Chan-Mo*, Moon Kwon-Ki, Choe Chang-hui, Jeong Soo-hyun
KEPCO E&C, Inc., 989-111, Daedeok-daero, Yuseong-gu, Daejeon, 34057, Korea
**Corresponding author: chanmo.park@kepco-enc.com*

1. Introduction

Current hazard analysis techniques start from a completed system design and assume that accidents are caused by component failures. Because the primary cause of accidents in the old systems was derived from component failure, the hazard analysis techniques (FMEA, FTA, HAZOP, and etc.) and safety design techniques focused on identifying critical components and either preventing their failure or providing redundancy to mitigate the effects of their failure.

The STPA (System-Theoritic Process Analysis) approaches in a different way compared to them traditional hazard analysis techniques as mentioned above. Generally, software failures do not result from random component failures but from lack of or flawed requirements. Deriving safety requirements and imposing those on software requirements will assure safety of software.

It is believed that the application of STPA to software hazard analysis can reduce efforts for software hazard analysis and for maintaining consistency of software hazard analysis with software changes. For this purpose, it is needed to identify safety related requirements at early phase of software life cycle.

In this paper, it will be presented that safety related requirements of simplified QIAS-P (Qualified Indication and Alarm System-P) can be derived by using STPA in the software hazard analysis.

2. Simplified QIAS-P

According to [1] and [2], simplified QIAS-P system provides indication for AMI (Accident Monitoring Instrumentation) variables for an operator in MCR (Main Control Room) to take specific planned manually-controlled actions for which no automatic control is provided and that are required for safety systems to perform their safety-related functions as assumed in the plant Accident Analysis Licensing Basis and to mitigate the consequences of an AOO (Anticipated Operational Occurrence).

The following variables are assumed as AMI Variables, called Type A parameters:

- Logarithmic Power (ENFMS)
- Pressurizer Pressure and Water Level (PZR)
- Steam Generator Pressure and Water Level (SG)
- Hot and Cold Leg Temperature (RCS)
- RCS Temperature Saturation Margin and Alarm*
- CET Temperature Saturation Margin and Alarm*

* The variable is calculated by PM.

Simplified QIAS-P system consists of Type A OM (Operator's Module) and PM (Processor Module) as shown in Figure 1. The PM converts analog signal to digital, calculates temperature saturation margin of RCS and CETs (Core Exit Temperature), and sends a current plant status of the AMI variables. The Type A OM indicates the current plant status received from PM.

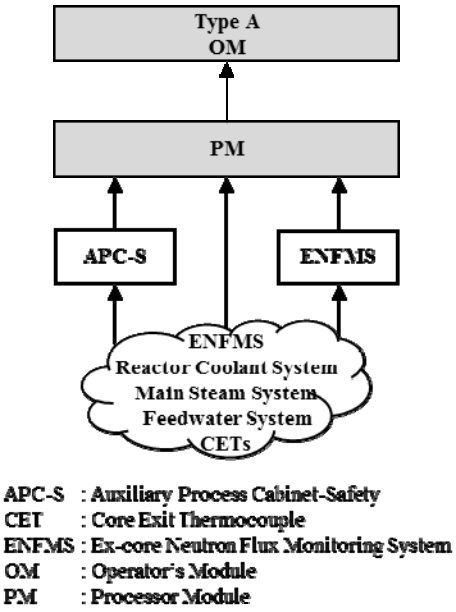

Figure 1. Simplified QIAS-P

3. STPA (System-Theoretic Process Analysis)

The STPA [3] is a hazard analysis technique and uses the STAMP (System-Theoritic Accident Model and Processes) [4] as accident model and process model. An accident is an event that results in a loss and a hazard is a system state that will lead to an accident.

In the STAMP, control process is modeled as a control structure as shown in Figure 2. In the control structure, a controller has process models, which are the states of the process, and control algorithms that determine control actions under the process model. The controller has two communication channels of control and feedback for the control actions with a controlled process.

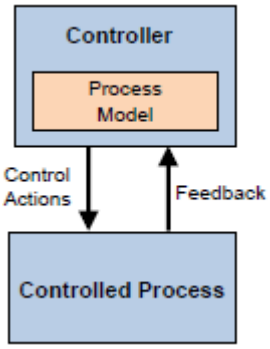

Figure 2. Control Structure Diagram.

The STPA consists of two-step process. The first step, based on STAMP, is to model the control process and to identify unsafe control actions which lead to accidents. The second step is to identify causal factors and causal scenarios of each unsafe control action using guide words in Figure 3.

The STPA process is as follows:

Step 1

1) Define system accidents and hazards.
2) Draw control structure for system
3) Identify UCAs (unsafe control actions)

Step 2

4) Identify causal factors and create scenarios

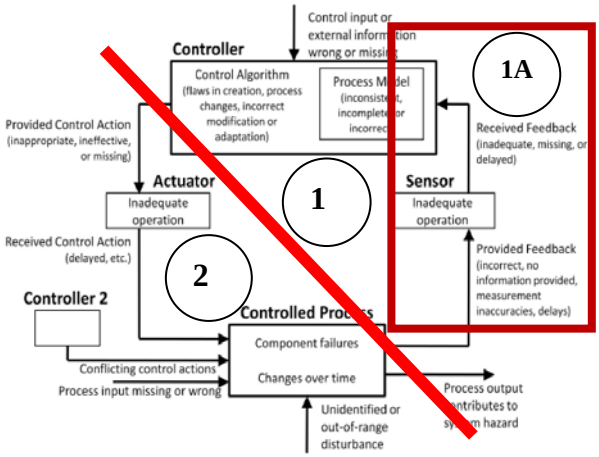

Figure 3. Guide Words for Causal Factors

4. Software Hazard Analysis based on STPA

XSTAMPP (An eXtensible STAMP Platform for Safety Engineering) tool [5] is used to make use of STPA methodologies easier.

4.1 Define System Accidents and Hazards

Accidents and hazards of the QIAS-P are defined as follows:

Accident: People injured or killed [A-1]
Hazard: Core melting [H-1]

4.2 Draw Control Structure

Simplified QIAS-P does not have any automated controller to make control actions, and thus an operator plays the role of the controller that has control algorithms and process model. The control structure of QIAS-P is shown in Figure 4.

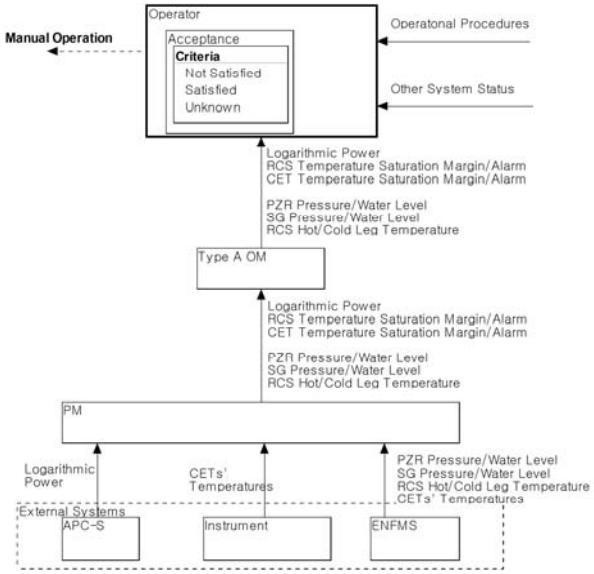

Figure 4. Control Structure Diagram for QIAS-P

4.3 Identify Unsafe Control Actions

Identified UCAs are shown in Table 1.

Table 1. Unsafe Control Actions for QIAS-P

Control Action	Not providing causes hazard	Providing causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long
Manual Operation	UCA1.1 Manual Operation not provided when the current plant status satisfies the acceptance criteria. [H-1]	UCA1.2 Manual Operation is provided when the current plant status does not satisfy the acceptance criteria. [H-1]	UCA1.3 Manual Operation is provided too early when the current plant status satisfies the acceptance criteria. [H-1]	N/A
	N/A	UCA1.5 Manual Operation is provided when the current plant status is unknown. [H-1]	UCA1.4 Manual Operation is provided too late when the current plant status satisfies the acceptance criteria. [H-1]	N/A

UCAs are identified by the following four categories:

1) A required control action to maintain safety is not provided.
2) An incorrect or unsafe control action is provided that induces a loss.

3) A potentially correct or adequate control action is provided too early, too late, or out of sequence.
4) A correct control action is stopped too soon.

4.4 Identify Causal Factors and Casual Scenarios

From unsafe control actions, causal scenarios and casual factors for Type A OM and PM were identified as Tables 2 and 3.

Since QIAS-P does not have any control actions, we used the guide words for causal factors (Figure 3, 1A) to identify causal factors.

Table 2. Causal Scenarios for Type A OM

Casual factor	UCA	Scenario	SR*
The current plant status not received by Type A OM	UCA1.1, UCA1.2, UCA1.3, UCA1.5	the current plant status not received by Type A OM; Type A OM display previous status satisfies the acceptance criteria.	S-1
The current plant status late received by Type A OM	UCA1.4	Type A OM received late	S-2

* Safety Requirement

Table 3. Causal Scenarios for PM

Casual factor	UCA	Scenario	SR*
The current plant status not received by PM	UCA1.1, UCA1.2, UCA1.3, UCA1.5	the current plant status not received by PM	S-3 S-4
The current plant status late. received by PM, PM sends the plant status late	UCA1.4	PM received late. PM sends late.	S-5 S-6

* Safety Requirement

4.5 Derive Safety Requirements

From causal scenarios in the Tables 2 and 3, safety requirements were derived as follows:

[S-1] Type A OM shall display variables missing from PM in different color or with symbol.
[S-2] Type A OM shall receive the current plant status every X milliseconds periodically.
[S-3] PM shall maintain missing plant status from external systems.
[S-4] PM shall send the current plant status including missing status to Type A OM.
[S-5] PM shall receive the current plant status at X milliseconds periodically.
[S-6] PM shall send the current plant status to Type A OM at X milliseconds periodically.

5. Conclusions

With the STPA technique, we identified the system accident and the hazard, drew control structure, identified unsafe control actions, and identified casual scenarios.

Through these processes, safety requirements could be developed from causal scenarios which were derived from unsafe control actions.

These requirements can be imposed upon software requirements as safety requirements. Succeeding hazard analyses will verify and validate correct implementation of these safety requirements.

Therefore, software hazard analysis using the STPA technique at early stage can reduce efforts for assuring software safety and maintaining consistency of the hazard analysis with software changes. Also, it can be extended to other nuclear safety I&C systems.

REFERENCES

[1] RG 1.97, Rev.04, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants”, 2006.
[2] IEEE Std. 497-2002, “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations”.
[3] Ishimatsu, T., Leveson, N. G., Thomas, J., Katahira, M., Miyamoto, Y., and Nakao, H., “Modeling and Hazard Analysis Using STPA”, International Association for the Advancement of Space Safety, 2010.
[4] Levesson, Lancy G., “A New Accident Model for Engineering Safer Systems”, Safety Science, Vol. 42, No. 4, pp. 2377-270, 2004.
[5] XSTAMPP, https://sourceforge.net/projects/stampp.