Application of STPA to Risk Analysis of Digital I&C System

Sung-Min Shin[a*], Sang Hun Lee[a], Seung Ki Shin[a], Inseok Jang[a]
[a] *Korea Atomic Energy Research Institute, 111 Daedeok-daero, 989beon-gil, Yuseong-gu, Daejeon, Republic of Korea 34057*

1. Introduction

Nowadays, most of the I&C systems in nuclear power plants (NPPs) are being digitalized. Although the changes caused by this shift should be assessed as a quantified form applicable to the PSA framework, there are some challenges: lack of failure data and new digital features difficult to express fault tree logic. Therefore, in this study, the applicability of another approach based on system-theoretic process analysis (STPA), a technique for identifying potential hazards, was investigated. Preliminary to consideration of PSA application, general STPA processes were followed with an example case that failure of reactor automatic and manual trip under pressurizer low-pressure condition. The STPA results themselves provided meaningful insights which were difficult to be checked from FT model analysis. As future work, it plans to seek ways to reflect the results from the STPA process in the PSA.

2. Overview of STPA

2.1 Key-features of STPA

STPA is based on system theory. The system theory focuses on the system taken as a whole, not on parts taken separately because it considers that some properties can only be treated adequately in their entirety. The before mentioned “some properties” can also be described as “emergent properties” that arise when system components interact with each other within all social and technical aspects. In brief, it can be represented by a sentence “the whole is greater than the sum of the parts”.

In STPA, safety is treated as a dynamic control problem rather than a failure prevention problem. It develops and utilizes a visual model called System-Theoretic Accident Model and Processes (STAMP) in which generation and transmission of control signals between system components are modeled. Then it identifies unsafe control action (UCA) leads to system hazards, arise from interactions between components even if the components have not failed, depending on various contexts.

2.1 Typical 4 Steps of STPA

Typical STPA can be conducted with the 4 steps shown in figure 1. In this paper, tasks required at each step are summarized as follow and a more detailed description can be found in the STPA handbooks [1].

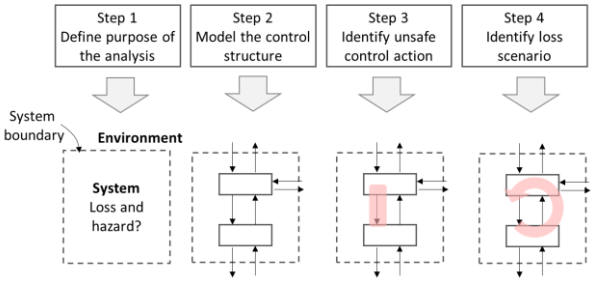

Figure 1 Typical 4 steps of STPA

Step 1 Define the purpose of the analysis
- Define system boundary
- Define system losses and hazards; Loss and hazard are a set of system conditions that are not uncontrollable and controllable, respectively.
- Correlation analysis between losses and hazards

Step 2 Model the control structure
- Model control signal generation and transmission process among system components

Step 3 Identify unsafe control action
- Identify the contextual information in which the system may be placed and control action failure mode (UCA type).
- UCA type and context are applied for each control signal and decided as UCA when system hazards occurred.

Step 4 Identify loss scenario
- Analysis of the causes of the selected UCA
- Analysis of the other causes of hazard and loss after the generation of normal control signals.

3. Application of STPA to DI&C system

To see the feasibility of this approach, the STPA procedure was applied to a case that automatic and manual trip failure in the pressurizer low-pressure (PZR Lo P) situation of APR-1400 [2, 3].

3.1 Define the purpose of the analysis

In this preliminary study, the target system boundary was set as follow: The automatic trip signal generation functions and related components of reactor protection system (RPS) and diverse protection system (DPS) other than PZR Lo P trip through the RPS are excluded, The possible manual trip approaches are manual trip using reactor trip switch (RX-trip SWTC) in safety console, the manual trip through information flat panel display (IFPD)-DPS trip function, the manual trip through IFPD-MG set disconnection, and manual trip

using reactor trip switch located in reactor trip switchgear system (RTSS) cabinet. The mentioned 4 manual trip approaches are based on the description in standard post-trip action (SPTA).

The definition of loss in this study is quite straightforward; [L1] Reactor trip failed in PZR low-pressure situation (less than 1810 psia). There are 5 hazards which are related to the failure of the automatic manual trip to trip the reactor; [H1] Automatic trip failure through RPS, [H2] Manual trip failure through RX-trip SWTC, [H3] Manual trip failure through IFPD-DPS, [H4] Manual trip failure through IFPD-MG set, and [H5] Manual trip failure through RTSS cabinet trip SWTC. It leads to system loss when all hazards occur.

3.2 Model the control structure

A control structure shows functional relationships and interactions by modeling the system as a set of feedback control loops.

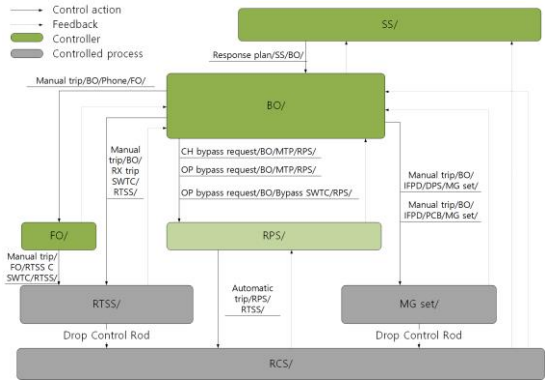

Figure 2 Control structure with control actions

Figure 2 shows the developed control structure in which only control actions required for the automatic and manual trip are indicated, with the notation rule "name of control action/departure point/ (if there is) passing points/destination point", because of paper restriction. Although it is not given in this paper, the full control structure with all full signals and all related components such as sensor and actuator has been developed and utilized for step 4 identification of loss scenario.

3.3 Identify unsafe control action

As the pre-process of UCA identification, contextual information in which the system be placed as tabulated and UCA types by which the control actions in figure 2 lead to the system hazards were outlined. Table I shows the tabulated contextual information. An assumption was made in this table which is that the order of the manual trip approach is followed based on the order of appearance in the SPTA document.

Table I System contextual information

Context ID	Description	RPS	RX trip switch	IFPD-DPS	IFPD-MG set	RTSS cabinet
CID 1	RPS Automatic trip is required when -PZR pressure is less than 1810 psia	O	N/A	N/A	N/A	N/A
CID 2	Manual trip within 3 minutes using RX trip switch is required when -PZR pressure is less than 1810 psia and -RPS automatic trip is failed	Fail	O	N/A	N/A	N/A
CID 3	Manual trip within 3 minutes using IFPD-DPS is required when -PZR pressure is less than 1810 psia and -RPS automatic trip is failed and -manual trip through RX trip switch is failed	Fail	Fail	O	N/A	N/A
CID 4	Manual trip within 3 minutes using IFPD-MG set is required when -PZR pressure is less than 1810 psia and -RPS automatic trip is failed and -manual trip through RX trip switch is failed and -manual trip through IFPD-DPS is failed	Fail	Fail	Fail	O	N/A
CID 5	Manual trip within 3 minutes using RTSS cabinet is required when -PZR pressure is less than 1810 psia and -RPS automatic trip is failed and -manual trip through RX trip switch is failed and -manual trip through IFPD-DPS is failed and -manual trip through IFPD-MG set is failed	Fail	Fail	Fail	Fail	O

Regarding the UCA types (A, B, C, and D), which were applied to each control action to see whether it affects system hazards, it is presented in Table II with the UCA list. The UCA list was developed based on the system contextual information and UCA type in table II.

Table II UCA list

	ID	A	B	C	D
Control action		Not Provided, but needed	Provided, but not needed	Provided, but incorrect intensity	Provided, but incorrect timing
Automatic trip/ RPS/RTSS/	1	RPS does not provide automatic trip signal when CID1 [H1]		RPS provides automatic trip signal with incorrect intensity when CID1 [H1]	
Manual trip/BO/RX trip SWTC/RTSS/	2	BO does not provide manual trip when CID2 [H2]		BO provides manual trip with incorrect intensity (1 or wrong 2 switches) when CID2 [H2]	BO provides manual trip loo late (exceeds 3 minutes) when CID 2[H2]
Manual trip/ BO/IFPD/DPS/MG set/	3	BO does not provide manual trip when CID3 [H3]		BO provides manual trip with incorrect intensity when CID3 [H3]	BO provides manual trip loo late (exceeds 3 minutes) when CID3 [H3]
Manual trip/ BO/IFPD/PCB/MG set/	4	BO does not provide manual trip when CID4 [H4]		BO provides manual trip with incorrect intensity when CID4 [H4]	BO provides manual trip (exceeds 3 minutes) loo late when CID4 [H4]
Manual trip/ BO/Phone/FO/	5	BO does not request manual trip when CID 5 [H5]			BO requests manual trip too late (exceeds 3 minutes) when CID 5 [H5]
Manual trip/FO/RTSS C SWTC/RTSS/	6	FO does not provide manual trip when CID 5 [H5]			FO provides manual trip too late (exceeds 3 minutes) when CID 5 [H5]
CH bypass request/BO/MTP/RPS/	7		BO provide CH bypass request (all CH) when CID1 & bypass function enabled [H1]		
OP bypass request/ BO/MTP/RPS/	8		BO provide OP bypass request when CID1 & bypass function enabled & bypass permissive [H1]		
OP bypass request/ BO/Bypass SWTC/RPS/	9		BO provide OP bypass request when CID1 & bypass function enabled & bypass permissive [H1]		
Response plan/SS/BO/	10	SS does not provide response plan when CID2 [H2]			SS provides response plan too late when CID2 [H2]
Response plan/SS/BO/	11	SS does not provide response plan when CID3 [H3]			SS provides response plan too late when CID3 [H3]
Response plan/SS/BO/	12	SS does not provide response plan when CID4 [H4]			SS provides response plan too late when CID4 [H4]
Response plan/SS/BO/	13	SS does not provide response plan when CID5 [H5]			SS provides response plan too late when CID5 [H5]

Table III Loss scenario analysis

Hazard	CA ID	UCA ID	Causes of UCA			Causes of CA execution failure		Note
			Process model	Control algorithm	Physical failure of controller	Actuator/Interface/Medium	Controlled process	
H1	1	1A	P-102 HW failure	RPS software fault	RPS HW failure		RTSS failure	
			P-102 miscalibration					
		1C	Partial failure leads to wrong 2/4 selective trip logic for TCB					
	7	7B		BO thinks it's okay to bypass all RPS channels and omits CH bypass reset.		N/A	N/A	Given condition: bypass function is enabled.
	8	8B		BO omits OP bypass reset.		N/A	N/A	Given condition: bypass function is enabled & bypass permissive signal on
	9	9B		BO omits OP bypass reset.		N/A	N/A	Same to above
H2	2	2A	BO is not aware of the situation to trip because of failure combination of components that disable all feedback paths. (Related feedbacks: WR PZR PR, NR PZR PR, RPS trip status) Examples: P-101 & P-102 & P-199 & RPS (or SDN) - many combination can be found FT modelling or some other approaches			RX trip SWTC failure	RTSS failure	It makes sense only if SS is also not aware of the situation.
			BO is not aware of IFPD and LPD failure so does not approach to information of safety console and MTP. Examples of IFPD and LDP failure: IPS, DCN					
		2C		BO thinks single switch works for trip.				
				BO misunderstands the set of channels for selective 2/4 trip.				
		2D		BO hesitates to trip.				
				BO is not aware of the passage of time.				
	10	10A	SS is not aware of the situation to trip because of failure combination of components that disable all feedback paths. (Related feedbacks: WR PZR PR, NR PZR PR, RPS trip status) Examples: P-101 & P-102 & P-199 & RPS (or SDN)					It makes sense only if BO is also not aware of the situation.
			SS is not aware of IFPD and LPD failure so does not ask to BO to check the information of safety console and MTP. Examples of IFPD and LDP failure: IPS, DCN					
		10D		SS feels pressured and hesitates to trip the reactor.				
				SS does not know that he/she has to decide whether to trip in three minutes.				
				SS is not aware of the passage of time.				
H3	3	3A	BO is not aware of the situation that manual trip should be attempted again because of failure combination of components that disable all feedback paths. (Related feedbacks: Log power, Linear power, RTSS open status, CEA floor indicator) Examples: ENFMS & DCN & RTSS(or one of ITP, SDN, MTP	BO does not think that he/she should confirm success of manual trip via RX trip SWTC.		IFPD failure	MG set failure	It makes sense only if SS is also not aware of the situation.
		3C		BO thinks single DPS trip actuation works for reactor trip.		DPS failure		
		3D	3 minutes have elapsed due to the time-consuming during the past process.					
	11	11A	SS is not aware of the situation that manual trip should be attempted again because of failure combination of components that disable all feedback paths. (Related feedbacks: Log power, Linear power, RTSS open status, CEA floor indicator) Examples: ENFMS & DCN & RTSS(or one of ITP, SDN, MTP	SS does not think that he/she should confirm success of manual trip via RX trip SWTC.				It makes sense only if BO is also not aware of the situation.
		11D	3 minutes have elapsed due to the time-consuming during the past process.					
H4	4	4A	Same to 3A			IFPD failure	MG set failure	It makes sense only if SS is also not aware of the situation.
		4C		BO thinks single MG set disconnection works for reactor trip.		PCB failure		
		4D	Same to 3D					
	12	12A	Same to 11A					
		12D	Same to 11D					
H5	5	5A	Same to 3A			Phone failure	FO does not response	It makes sense only if SS is also not aware of the situation.
		5D	Same to 3D					
	6	6A	FO is not aware of the situation to trip because of Phone failure			RTSS C SWTC failure	RTSS failure	
		6D	Same to 3D					
	13	13A	Same to 11A					
		13D	Same to 11D					

3.4 Identify loss scenario

In the STPA 4, the possible loss scenarios are analyzed like Table III. The analysis process, basically, was composed of two approaches; one is the analysis of causes of UCA developed in Table II, and another one is the analysis of causes of hazards occurrence due to other factors even though the correct control action has been generated.

4. Concluding Remarks

Overall, the assessment of digital I&C risks based on STPA enables a more specific practical analysis of the system hazardous status. In more detail, it has the following advantages like:

- The complex characteristics of the system can be flexibly expressed. Especially digital system-specific risk information in the human-machine interface (HMI) can be provided. It is believed that risk information could be used to evaluate a more accurate human error probability (HEP) in the digital environment.
- It can be clearly identified that how the software and network, the representative new features entailed in the digitalization of I&C, are linked for both automatic and manual generation of a specific safety signal.

Based on the contents presented in this paper, we would like to conduct the following studies in the future.

- The original purpose of the STPA is to reduce the system risk by suggesting safety constraints and by enforcing the safety constraints through a proper system modification. Correspondingly, safety constraints related to digital I&C functions can be developed and enforced. For example, a manual trip should be done within 3 minutes in the example situation (UCA 2D, 10D, 3D, 11D, 4D, 12D, 5D, 6D, and 13D). However, it can take 3 minutes or more for operators to figure out the situation. In such a case, a safety constraint like “operators should make a trip decision within 3 minutes” may be presented. In order to enforce this constraint, the elapsed time after the occurrence of the PZR Lo P signal can be given.
- Currently, the safety assessment of NPPs is being carried out in accordance with the PSA framework. Therefore, it is necessary to explore how to quantify, or at least apply, the results obtained from STPA for the purpose of application to PSA models. Studies that reflecting the results from the STPA method in the PSA are currently being actively conducted in ERPI [4].

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] KHNP, Final Safety Analysis Report for Shin-Kori 3/4 Chapter 7. 2009.
[3] KHNP, Design Control Document Tier 2, Chapter 7, 2018.
[4] M. Gibson, Hazards and Consequences Analysis for Digital Systems, 2018.