ASRAM2020-1069

Risk assessment of digital I&C system based on STPA and its implication for PSA

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

EXTENDED ABSTRACT

Keywords: Digital I&C, PSA, STPA, System theory

These days, digital features are being introduced to the I&C system in the existing nuclear power plants (NPPs) as well as the new design of NPPs worldwide. This shift involves new characteristics that were not present in existing analog I&C systems, such as software and network, which greatly complicate the interconnection between system components including human operators. On the other hand, the existing PSA consists of the event tree (ET) and fault tree (FT) framework, which is basically based on the concept of chain of events, in which the prior and post-relationship are clear between system components. Therefore, the complex interconnection of the DI&C system and the risk arising from it is difficult to clearly analyze under the PSA framework. In other words, risk characteristics of the DI&C system cannot fully be identified based on the FT framework only. To resolve this problem, this study analyzed the risks of the DI&C system based on system-theoretic process analysis (STPA) and sought to reflect the results in the PSA. 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 situation in APR-1400. In addition, the results of STPA are sought to be reflected in the PSA model.

The main characteristics of the STPA can be summarized in the following two: One is that 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 so-called emergent properties which can only be treated in their entirety. The other one is that STPA treats safety as a dynamic control problem rather than a failure prevention problem. During the analysis process, it develops a model called control structure in which generation and transmission of control signals between system components are indicated. Then it identifies whether some abnormal characteristic of these control signals leads to system hazards. Generally, STPA is conducted following the 4 steps shown in figure 1[1] and tasks required at each step can be summarized like table 1.

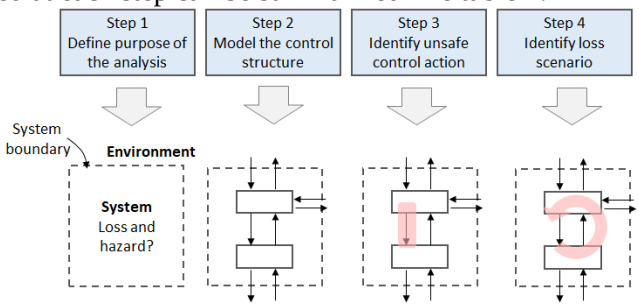

Figure 1 Analysis process of STPA

Table I Required tasks for each step

	Step 1	Step 2	Step 3	Step 4
Required tasks	Define system boundary, losses, and hazards	Indicate control signal generation and transmission process among system components	Identify system contextual information and control action failure mode (UCA type) and develop the UCA list based on them	Analysis of the causes of UCA and other causes of hazard and loss after the generation of normal control signals

To see the feasibility of STPA application to DI&C system, the above 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].

STEP 1. The target system boundary was set as follow: The automatic trip signal generation functions and related components of the reactor protection system (RPS) are included, and the possible manual trip approaches using reactor trip switch (RX-trip SWTC) in the 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 are included. The 4 manual trip approaches are based on the description in standard post-trip action (SPTA) document. The definition of sole loss is quite straightforward since this study is considering trip failure; [L1] Reactor trip failed in PZR low-pressure situation (less than 1810 psia). There are 5 hazards relating to the automatic and manual trip; [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.

STEP 2. Figure 2 shows the control structure developed [2, 3] in which control actions required for the automatic and manual trip are indicated, with the notation rule "name of control action/departure point/ (if there is) pass-through components /destination point". Although it is not given in this paper due to the paper restriction, the full scope control structure, in which all related components and feedbacks, also has been developed and utilized for step 4.

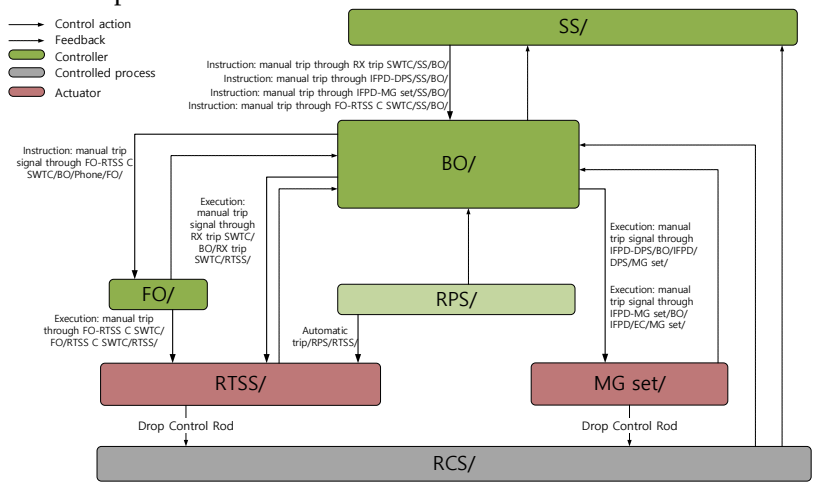

Figure 2 Control structure with control actions

STEP 3. As the pre-process of UCA identification, system contextual information and UCA types need to be defined. Table II shows the tabulated system contextual information. An assumption was made in this table which is that the order of the manual trip approach will be followed the order of appearance in the SPTA document. The UCA list was developed in the table III and the applied UCA types are directly given in the table.

Table II System contextual information

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

Table III UCA list

	ID	UCA type A	UCA type B	UCA type C
Reference control action		Not Provided, but needed	Provided, but inappropriate	Provided, but too late
Automatic trip/RPS/RTSS/	1	1A) RPS does not provide an automatic trip signal when CID1 [H1]	1B) RPS provides an inappropriate automatic trip signal when CID1: not satisfy 2/4 selective voting logic [H1]	
Instruction: manual trip through RX trip SWTC/SS/BO/	2	2A) SS does not provide instruction for trip through RX trip SWTC when CID2 [H2, H3, H4, H5]		2C) SS provides instruction for trip through RX trip SWTC too late when CID2 [H2, H3, H4, H5]
Execution: manual trip signal through RX trip SWTC/BO/RX trip SWTC/RTSS/	3		3B) BO provides an inappropriate manual trip signal through RX trip SWTC when CID2: activate just 1 switch or 2 sets of wrong switches [H2]	3C) BO provides manual trip signal too late when CID2: exceeds 2 minutes [H2, H3, H4, H5]
Instruction: manual trip through IFPD-DPS/SS/BO/	4	4A) SS does not provide instruction for trip through IFPD-DPS when CID3 [H3, H4, H5]		4C) SS provides instruction for the trip through IFPD-DPS too late when CID3 [H3, H4, H5]
Execution: manual trip signal through IFPD-DPS/BO/IFPD/DPS/MG set/	5		5B) BO provides an inappropriate manual trip signal through IFPD-DPS when CID3: activate either CH1 manual RX trip or CH2 manual RX trip [H3]	5C) BO provides the manual trip signal too late when CID3: exceeds 2 minutes [H3, H4, H5]
Instruction: manual trip through IFPD-MG set/SS/BO/	6	6A) SS does not provide instruction for trip through IFPD-MG set when CID4 [H4, H5]		6C) SS provides instruction for the trip through IFPD-MG set too late when CID4 [H4, H5]
Execution: manual trip signal through IFPD-MG set/BO/IFPD/EC/MG set/	7		7B) BO provides an inappropriate manual trip signal through IFPD-MG set when CID4: deactivate either PCB for MG set 1 or PCB for MG set 2 when CID4 [H4]	7C) BO provides the manual trip signal too late when CID4: exceeds 2 minutes [H4, H5]
Instruction: manual trip through FO-RTSS C SWTC/SS/BO/	8	8A) SS does not provide instruction for trip through FO-RTSS C SWTC when CID5 [H5]		8C) SS provides instruction for the trip through FO-RTSS C SWTC set too late when CID5 [H5]
Instruction: manual trip signal through FO-RTSS C SWTC/BO/Phone/FO/	9			9C) BO provides instruction for the manual trip too late when CID5: exceeds 2 minutes [H5]
Execution: manual trip through FO-RTSS C SWTC/FO/RTSS C SWTC/RTSS/	10		10B) FO provides an inappropriate manual trip signal through FO-RTSS C SWTC when CID5: activate just 1 switch or 2 sets of wrong switches [H5]	10C) FO provides the manual trip signal too late when CID5: exceeds 2 minutes [H5]

STEP 4. The possible loss scenarios are analyzed and some of them are given in Table IV. The analysis process, basically, is composed of two approaches; one is the analysis of causes of UCA developed in Table III, and another one is the analysis of causes of hazards occurrence due to other factors even though the correct control action has been generated. The UCA ID given in Table IV is a combination of the CA ID and the UCA type in Table III.

Table IV loss scenario analysis

	Causes of UCA			Causes of CA execution failure		Note
	Process model	Control algorithm	Physical failure of controller	Actuator/ Interface/ Medium	Contro-lled process	
UCA ID	Causes of incorrect recognition	Mistake or error on decision making		-	-	
1A	3/4 or more P-102 HW failure	RPS software fault	RPS HW failure	-	RTSS failure	
	3/4 or more P-102 miscalibration					
1B	3/4 or more P-102 HW failure					
	3/4 or more P-102 miscalibration					
2A	SS* and BO** are not aware of the situation to trip because of all feedbacks disabled.	SS thought that this is the situation not requiring manual trip.	SS's inappropri ate fitness for duty	-	-	* SS obtains Info. (Related feedbacks: WR PZR PR, NR PZR PR, RPS trip status, CH trip status) through IFPD and LPD. Example of cut-sets: IPS ** BO obtain Info. (same to the BO) through safety console and MTP in addition to IFPD and LPD. Example of cut-sets: SDN + NR PZR PR / P-199 / DPS / DCN / IPS / DCN / IFPD / BO / (Ch. X,Y) + WR PZR PR / P-102 / APC-S(P) / DIS / DIS FPD / BO / (Ch. A)
2C	It takes a long time for information gathering.	SS feels pressured and hesitates to trip the reactor				
		SS and BO do not know that there is 2 minutes of time constraint				
		It takes a long time for situation interpreting, and SS and BO are not aware of the passage of time.				
3B	-	BO misunderstands the set of channels for selective 2/4 trip.	BO's inappropri ate fitness for duty	RX trip SWTC failure	RTSS failure	
3C	-	It takes a long time for response planning or execution, and SS and BO are not aware of the passage of time.				

The risk of the DI&C system has been analyzed based on the STPA process. According to the STPA handbook, STPA results are used to derive safety constraints (SC) to prevent the occurrence of UCA. For example, the following safety constraint and measures to realize them can be developed based on the above analysis results.

SC. 1 The operators clearly recognize the situation in which a manual trip is required.

- If the RPS fails, the alarm must be provided.
- In the event of RPS failure, reliable relevant signals are trained and provided to the operators.
- If ordinary information acquisition interfaces such as LDP and IFPD fail, an alarm is provided for recognition.

SC. 2 The operators shall make a trip decision and complete it within 2 minutes.

- The required and remaining time for trip completion is provided for each expected situation.
- Eliminate the psychological factors that pressure the trip not to be carried out.
- Supporting methods are provided to complete the trip quickly.

STPA results may also be reflected in the PSA model. The following methods can be considered.

- Sensitivity analysis can be performed by converting STPA results to some FT logics or BEs and reflect them in existing DI&C FT. The extreme value, 0 or 1 can be applied to them because there is no exact value. If some of the factors are judged to be major factors affecting risk, we can consider

specific countermeasures for them. A similar study can be referring to the HAZCADS project being performed in EPRI [4].

- The results of STPA can provide information on what circumstance the operator may be placed in accident progress, and how such a situation may occur. This information can be used as input data for the evaluation of HEP under the digital environment.

On the basis of example case analysis, the DI&C STPA is thought to be able to systematically provide information on various DI&C system failures in assessing human error probabilities, and information on how complex components, such as software or network, affect system failures.

Acknowledgements

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.