A Study on the Implementation for Test Case of Digital Equipment using STPA

Hosun Ryu[a*], Min-Seok Kim[a], Dongil Lee[a]
[a]*KHNP, Central Research Institute, 70, 1312-gil, Yuseong-daero, Yuseong-gu, Daejeon, 34101, South Korea*
[*]*Corresponding author: hosunryu@khnp.co.kr*

1. Introduction

In the case of digital equipment, various functions are combined in the form of a combination of software and hardware. Therefore, it is difficult to verify the design/abnormal/failure of the digital equipment as a simple function-based inspection method. The more complex the system, the more difficult it is to test all the requirements.

However, safety-critical requirements must be tested. In this paper, we propose a method to derive test cases satisfying all safety requirements by using STPA (Systems Theoretic Process Analysis) risk analysis result as test input.

The STPA is a risk analysis method suitable for digital system. It is a model optimized for catching accidents caused by software errors and lack of safety constraints [1]. In addition, it is possible to derive the safety constraints associated with the interaction between systems in a software-driven system.

In this paper, we have developed a test case for the performance verification of the component cooling water (CCW) pump control facility among the digital facilities of the power plant. And it is applied to actual facilities to evaluate the possibility of utilization.

2. Generation of Test Case

The STPA is able to analyze how different combinations of processor Process Model Value (PMV) (system interactions) affect control behaviors. Therefore, it is applicable to software intensive system and digital system. In the STPA risk analysis process, the Process Model (PM) of the controller can be analyzed and the safety requirements can be derived.

However, since it is almost impossible to create a test case for all possible scenarios, we have created a test case that covers the safety critical scenario as much as possible. In this paper, we analyze the cases where CCW pump start command is provided and not provided [2].

2.1 System analysis and Hazard definition

The CCW is a system for removing heat from safety devices and some non-safety devices. The CCW consists of two divisions and consists of two pumps per division. The definition of Hazard for pump drive of CCW is shown in Table 1.

Table I: Defined Hazard

Hazard No	Description
H1	All pump stops during normal operation
H2	Pump operation less than 3(operation stop)
H3	All pump stops in abnormal operation
H4	All pump operation in abnormal operation

2.2 PMV and Context table

The control structure of the CCW pump is shown in Fig. 1. In Figure 1, the PMV of the plant is shown in Figure 2.

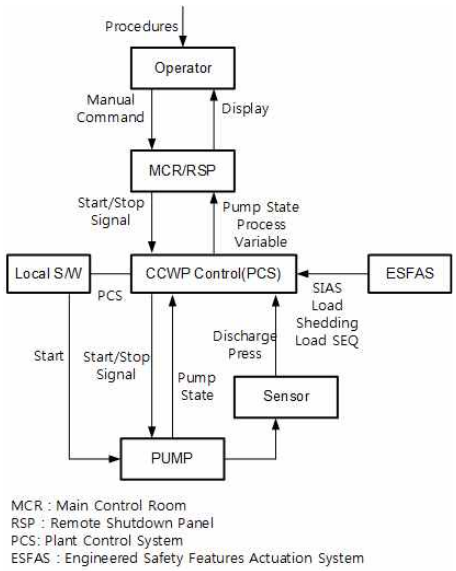

Fig. 1. Control Structure of CCW Pump

PMV No.	PMV	Status1	Status2	Status3	Description
PMV1	Operation Mode	기동/정지	정상	비상	
PMV2	HS-024C	Start	PCS		Local S/W
PMV3	HS-024A	Start	Stop	Auto	MCR
PMV4	HS-024B	Start	Stop	Auto	RSR
PMV5	Inoperable Detector	Yes	No		
PMV6	PP01B started	Yes (+65sec)	No		
PMV7	PP02B running state	Stop	Start (+65sec)	Start (+120sec)	
PMV8	PP01B Lead	Yes	No		
PMV9	PS-054	On	Off		Disch.Press.LO
PMV10	V/V102	Open	Close		TRN A&B Isolation V/V
PMV11	V/V104	Open	Close		TRN A&B Isolation V/V
PMV12	Load Shedding	On	Off		
PMV13	ESFAS-SIAS	On	Off		
PMV14	Load SEQ#6	On	Off		
PMV15	Elec.Protection	On	Off		
PMV16	SWGR HS	Close	Trip		
PMV17	Cell SW 33a	On	Off		BRK in Test Position

Fig. 2. Process Model Variables & Stat

Context table can be generated as follows according to the number of PMV status cases, and each context table for each control action is generated as shown in Fig. 3. The Fig.3 shows a part of the context table when the CCW Pump Start command is provided.

PMV	PMV1	PMV2	PMV3	PMV4	PMV7	PMV8	PMV9	PMV10	PMV11	PMV12	PMV13	PMV14
	Operation Mode	HS-02 4C	HS-02 4A	HS-02 4B	PP02B running state	PP01B Lead	PS-05 4	V/V10 2	V/V10 4	Load Sheddi ng	ESFAS -SIAS	Load SEQ#6
States1	Startup /Shutdown	Start	Start	Start	Stop	Yes	on	Open	Open	on	on	on
States2	Normal	PCS	Stop	Stop	Start (+65sec)	No	off	Close	Close	off	off	off
States3	Abnormal		Auto	Auto	Start (+120 sec)							

	PP01B START Command Provide												Analysis Results Hazardous?	
Row	PMV1	PMV2	PMV3	PMV4	PMV7	PMV8	PMV9	PMV10	PMV11	PMV12	PMV13	PMV14	H	
1	Abnormal	PCS	Auto	Auto	Stop	Yes	off	open	open	on	on	on		
2	Abnormal	PCS	Auto	Auto	Stop	Yes	off	open	open	off	on	off		
3	Abnormal	PCS	Auto	Auto	Stop	Yes	off	open	open	on	off	on		
4	Abnormal	PCS	Auto	Auto	Stop	No	off	open	open	on	on	on	H4	EDG 과부하
5	Abnormal	PCS	Auto	Auto	Stop	No	off	open	open	off	on	off		
6	Abnormal	PCS	Auto	Auto	Stop	No	off	open	open	on	off	on	H4	EDG 과부하
~ 생략														

Fig. 3. Process Model Variables & Status

3. Test and Result

3.1 Application test

The system configuration for the test is shown in Fig. 4. In order to verify the performance of the digital facility, the system developed by KHNP CRI was used for testing [3].

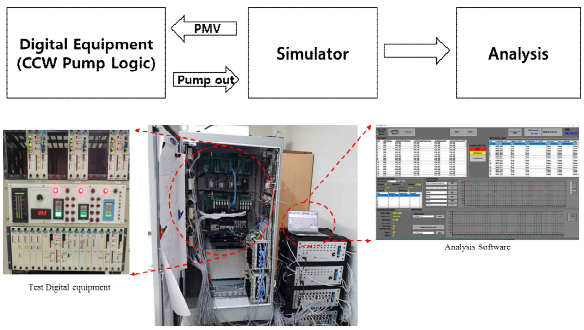

Fig. 4. Configuration of Test equipment

Once the test case is created, the PMV identified in STAP must be mapped 1:1 into the performance verification device input. First, the pump current status condition was created and then the test was performed. When testing the pump start command, the pump stop condition was set to the previous status and the test was performed.

3.2 Test result

The test results are presented in excel form as shown in Fig. 5. The PMV values are sequentially input to the PLC and Pass/Fail is evaluated by comparing the expected output with the output of the current PLC.

SignalType	Input	DO_00	DO_	DI_00	DI_01	DI_02	DI_03	DI_28	
NO	PartCheck	StartDelay	CLOSE_CMD	OPE	OPEN_LIGHT	INOPERABLE_LIGHT	PW_RE_LIGHT	CLOSE_LIGHT	CR1_ST	Pass/Fail
0	FALSE	300	FALSE	F	True	NA	False	True	True	
					True	NA	False	True	TRUE	Pass
1	FALSE	300	FALSE	F	False	NA	False	True	True	
					False	NA	False	True	TRUE	Pass
2	FALSE	300	FALSE		True	NA	False	False	True	
					True	NA	False	False	TRUE	Pass
3	FALSE	300	FALSE		False	NA	False	False	True	
					False	NA	False	False	TRUE	Pass
4	FALSE	300	FALSE		True	NA	True	True	True	
					True	NA	True	True	TRUE	Pass
5	FALSE	300	FALSE		False	NA	True	True	True	

Fig. 5. Test result reporting

As a result of the test, when the load shedding condition occurs, it was found that the pump stopped unconditionally. We were able to find a part of the risk analysis that was wrongly analyzed through this test.

Due to the nature of STPA analysis, analysis is performed at a higher level of the system.

Therefore, when the test is performed only with the corresponding PMV conditions in the actual PLC, it is analyzed that the output is differently derived from the state values of the input conditions that are not defined in the context table or the state values of the internal latches.

4. Conclusions

Through the test case test derived from the STPA technique, we were able to derive the missing safety constraint. In addition, errors in the STPA risk analysis process could be identified from the test results.

However, there was a difficulty in 1: 1 mapping of PMV condition derived from STPA risk analysis to actual PLC input. In the risk analysis process, the results are different according to the state values of the input conditions and the state values of the internal latches, which are not considered, and the 100% verification has not been performed.

Therefore, when deriving a test case using the STPA technique, the input condition and the internal memory status of the actual equipment should also be considered.

REFERENCES

[1] R.Torok, "Hazard Analysis Methods for Digital Insrumentation and Control Systems", EPRI TR-3002000509, 2013.

[2] H. T. Lim, H. S. Ryu, "A Study on the Application of STPA in Hazard Analysis of Nuclear Power Plant Control System", CICS'17 p. 392, 2018.

[3] H. Ryu, H. Kim, J. Kim and K. Lee, "Development of Control Verification Simulator for the Controller", CICS'18, pp. 259, 2018.