An evaluation method of fault-tolerance for digital plant protection system in nuclear power plants

Jun Seok Lee, Man Cheol Kim[(1)], Poong Hyun Seong[(2)], Hyun Gook Kang and Seung Cheol Jang[(3)]
[(1)]*Center for Advanced Reactor Research*
[(2)]*Department of Nuclear and Quantum Engineering*
Korea Advanced Institute of Science and Technology
373-1, Guseong-dong Yuseong-gu, Daejeon, 305-701, Republic of Korea
[(3)]*Korea Atomic Energy Research Institute*
150 Deokjin-dong Yuseong-gu, Daejeon, 305-353, Republic of Korea
wahrheit@kaist.ac.kr, charleskim@kaist.ac.kr, phseong@kaist.ac.kr, hgkang@kaeri.re.kr, scjang@kaeri.re.kr

1. Introduction

In recent years, analog based nuclear power plant (NPP) safety related instrumentation and control (I&C) systems have been replaced to modern digital based I&C systems. NPP safety related I&C systems require very high design reliability compare to the conventional digital systems so that reliability assessment is very important.

In the reliability assessment of the digital system, fault tolerance evaluation is one of the crucial factors. However, the evaluation is very difficult because the digital system in NPP is very complex.

In this paper, the simulation based fault injection technique on simplified processor is used to evaluate the fault-tolerance of the digital plant protection system (DPPS) with high efficiency with low cost.

2. Target system

The DPPS supports plant safety by monitoring selected plant parameters, and initiating appropriate protection action when any parameter reaches a limiting safety system setting. It consists of analog input modules, bistable processors, LCL processors and digital output modules with selective 2 out of 4 logic modules.

In this paper, the LCL processor is selected as a target system. This processor is responsible for performing 2 out of 4 voting logic of the trip signals which is generated by the bistable processor. If more than 2 channels are in the trip state, the LCL will actuate the trip output. Fig. 1 shows the 2 out of 4 coincidence logic in the LCL processor.

3. Fault injection and self checking

3.1 Fault Injection

The permanent fault with stuck-at (0, 1) is selected as a possible fault in the system. The permanent fault is related to irreversible physical defects in the circuit, so it remains indefinitely. In the experiment, data modification method is used for the permanent fault effect.

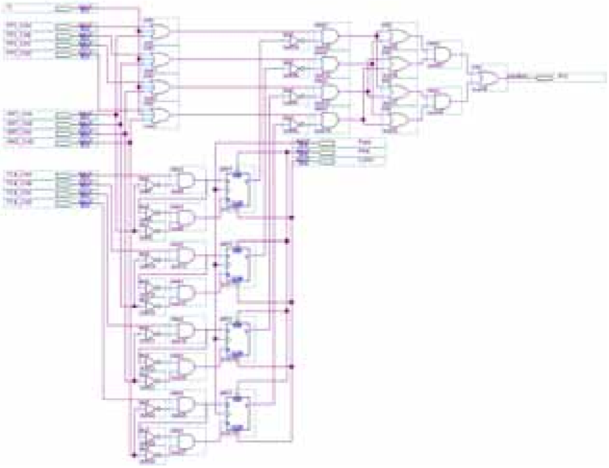


Fig. 1. 2 out of 4 coincidence logic in LCL processor

3.2 Self checking and error detection

For the experiment, 6 methods are used to detect errors in the system. Heartbeat-watchdog timer, ROM checksum, RAM data verification, parity bit, register write and read, integration are selected for error detection methods of the system.

4. Fault tolerant predicate block diagram

The experiment results are analyzed to evaluate fault-tolerant characteristics of the system. In order to abstract the behavior of the target system, a set of predicate block diagrams is used. Each predicate diagram could be summarized as follows:

- Not Activated Error: A fault cannot be activated as an error if the faulty location is not read by the specific input.
- Detected Error: An error can be detected by the error detection methods.
- Tolerated: If a fault is activated as an error, but that is not detected, and the procedure output is correct.
- Failure: The parser processes its input and assigns a wrong value to the output; no error is detected.

5. Experiment setup

Table 1. Experiment parameters

Number of faults	CPU	336
	RAM	1,050,608
	ROM	1,048,576
	I/O	64
	Total	2,099,584
Fault type	Permanent fault	
Fault location	CPU (Register, Control Unit), RAM, ROM	
Fault model	stuck-at (0, 1) fault	
Result analysis	Fault tolerant predicate block diagram	

The parameters of the experiment are summarized in Table 1. Fault tolerant predicate block diagram which is introduced in the previous section is used to analyze the simulation experiment result.

6. Results

Table 2 shows the result of the experiment. From the diagrams in the table, we conclude as following:

First, amount of program in the system is an important factor in the fault tolerance evaluation of the system. Program size of Integration method is larger than any other methods because of 3 error detection methods combination. From the experiment, not only high error detection coverage but also high percentage of activated errors can be obtained by using Integration method.

Second, detecting errors by CPU faults is very difficult by the direct-access methods such as Parity bit method or Register write and read method. If only one error detection method can be used in the system, the Heartbeat and watchdog timer is relatively effective error detection method for the CPU fault.

ACKNOWLEDGEMENT

This work is partly supported by the Korean Nuclear R&D Program.

REFERENCES

[1] Technical Manual for Digital Plant Protection System (DPPS) for Ulchin 5&6, Westinghouse electric company LLC, 2002.

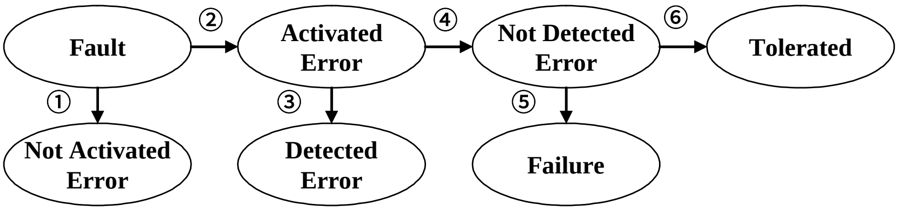
[2] Fault Representativeness, Deliverable ETDI2 of Dependability Benchmarking Project (DBENCH), IST-2000-25245, July 2002.

[3] Hyun Gook Kang and Tae Yong Sung, “An analysis of safety-critical digital systems for risk-informed design”, Reliability Engineering and System Safety, vol.78, no.3, pp. 307-314, 2002.

[4] M. Amendola, L. Impagliazzo, P. Marmo, and F. Poli, "Experimental Evaluation of Computer-Based Railway Control Systems", in Proceeding 27th Int. Symposium on Fault-Tolerant Computing (FTCS-27) Seattle, WA, USA, pp. 380-384, 1997

[5] J. Arlat, A. Costes, Y. Crouzet, J. Laprie, AND D. Powell, "Fault Injection and Dependability Evaluation of Fault-Tolerant Systems", IEEE Transactions on Computers, Vol. 42, No. 8, pp. 913-923, 1993

Table 2 Fault tolerant predicate block diagram



	①	②	③	④	⑤	⑥
Heartbeat-watchdog timer	78.157%	21.843%	33.291%	66.709%	97.094%	2.906%
ROM Checksum	71.792%	28.208%	26.344%	73.656%	98.311%	1.689%
RAM data verification	66.997%	33.003%	18.464%	81.536%	97.680%	2.320%
Parity bit	78.853%	21.147%	10.294%	89.706%	97.934%	2.066%
Register write and read	78.750%	21.250%	16.378%	83.622%	98.733%	1.267%
Integration	58.454%	41.546%	54.318%	45.682%	72.267%	27.733%