Coverage estimation of digital plant protection system in a nuclear power plant

Jun Seok Lee, Man Cheol Kim[(1)] and Poong Hyun Seong[(2)]
[(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
wahrheit@kaist.ac.kr, charleskim@kaist.ac.kr, phseong@kaist.ac.kr

1. Introduction

Due to the rapid development of digital technology, traditional 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 high design reliability compare to the conventional digital systems so that reliability assessment is very important.

In the reliability assessment of the digital system, error detection coverage of the system is one of the crucial factors. However, error detection coverage evaluation is very difficult because the system is very complex.

In this paper, simulation based fault injection technique on simplified processor is used to evaluate the error detection coverage of the system with high efficiency with low cost. And, the experiment results are compared in terms of the error detection coverage.

2. System overview

Fig. 1 shows schematic diagram of the DPPS. 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.

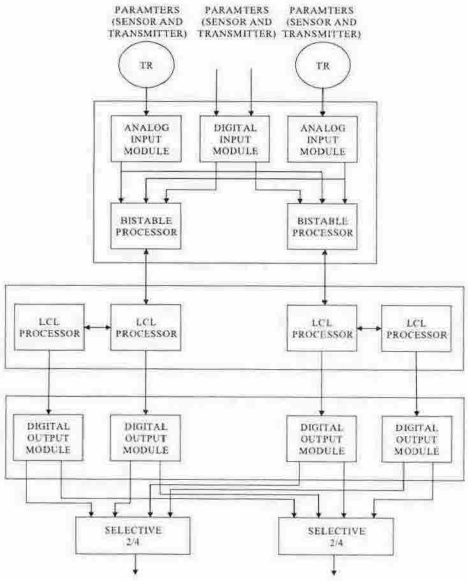

Fig. 0. Schematic diagram of DPPS

The LCL processor is selected as a target system. It 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 [1].

3. Fault injection and self checking

3.1 Fault Injection method

The permanent fault with stuck-at (0, 1) is selected as a possible fault. The permanent fault is related to irreversible physical defects in the circuit, so it remains indefinitely. [2]

3.2 Self checking and error detection

For the experiment, some error detection mechanisms are used to detect errors in the system. Heartbeat generation and watchdog timer, ROM checksum, RAM data verification, parity bit, register write and read, integration are selected as self checking methods of the system.

4. Fault injection experiments

The parameters of the experiment are summarized in Table 2. Error detection coverage is obtained from following representation.

•Error detection coverage of a component ($C_{d,comp}$)

$$C_{d,comp} = \sum \frac{N_{detected}}{N_{activated,comp}}$$

$N_{activated,comp}$: the number of activated errors of a component.

$N_{detected}$: the number of detected errors.

•Error detection coverage of the system ($C_{d,sys}$)

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	
Workload	2 out of 4 coincidence logic	
Fault location	CPU (Register, Control Unit), RAM, PROM	
Fault model	stuck-at (0, 1) fault	
Result analysis	Error detection coverage	

Table 2. Failure rate of each component [3]

	Failure Rate (failures/10^6Hours)
CPU	0.273680
RAM	0.144630
ROM	0.142336
I/O	0.0404

$$C_{d,sys} = \sum W_{comp} \cdot C_{d,comp} \quad \text{Where,} \quad W_{comp} = \frac{\lambda_{comp}}{\lambda_{total}}$$

$\square_{comp}$: failure rate of a component (failures/10^6Hours).
$\square_{total}$: failure rate of total components (failures/10^6Hours).
The failure rates are estimated by using the MIL-HDBK-217F

5. Results

From Fig. 2 to Fig. 3 shows error detection coverage of each component and the system depending on error detection method. In those graphs, the integration method has higher error detection coverage than any other methods. Parity bit has lowest error detection coverage among 6 methods. The integration method is combination of 3 error detection methods Heartbeat-Watchdog timer, ROM checksum and RAM data verification so that it is possible to detect errors in the system. But other methods are concentrated on only one component, so that it is possible to detect component errors, separately.

6. Summary and Conclusions

In this work, simplified LCL Processor in the DPPS is realized by C++ based hardware description language simulator system and stuck-at (0, 1) permanent faults are injected to the simulator. 6 error detection methods are used, heartbeat-watchdog timer, ROM checksum, RAM data verification, parity bit, register W/R and integration.

From the experiment results, we can obtain some conclusions as follows:

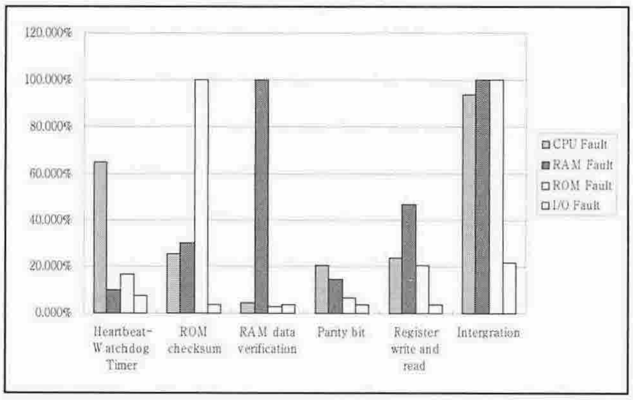

Fig. 0. Error detection coverage of each component

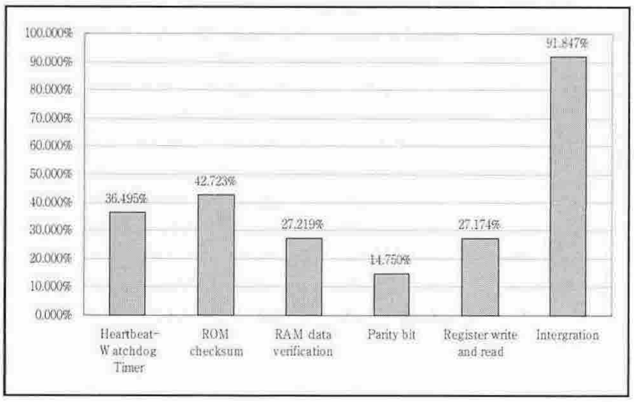

Fig. 0. Error detection coverage of the system

1. Detecting CPU errors are very difficult by direct access method such as parity bit or register W/R. If one error detection method can be used in the system, the heartbeat-watchdog timer is effective method to detect CPU errors.
2. Integration method has very high error detection coverage. Therefore, this method is suitable for error detection of the systems.

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 De-pendability Benchmarking Project (DBENCH), IST-2000-25245, July 2002.
[3] MIL-HDBK-217F, “Reliability Prediction of Elec-tronic Equipment”, Dec 2 1991.