http://dx.doi.org/10.5516/NET.04.2012.515

FAULT DETECTION COVERAGE QUANTIFICATION OF AUTOMATIC TEST FUNCTIONS OF DIGITAL I&C SYSTEM IN NPPS

JONG GYUN CHOI*, SEUNG JUN LEE, HYUN GOOK KANG, SEOP HUR, YOUNG JUN LEE, and SEUNG CHEOL JANG
Korea Atomic Energy Research Institute
1045 Daedeok-daero, Yuseong-gu, Daejeon, 305-353, Republic of Korea
*Corresponding author. E-mail : choijg@kaeri.re.kr

Invited September14, 2011
Received October 31, 2011
Accepted for Publication February 21, 2012

Analog instrument and control systems in nuclear power plants have recently been replaced with digital systems for safer and more efficient operation. Digital instrument and control systems have adopted various fault-tolerant techniques that help the system correctly and safely perform the specific required functions regardless of the presence of faults. Each fault-tolerant technique has a different inspection period, from real-time monitoring to monthly testing. The range covered by each fault-tolerant technique is also different. The digital instrument and control system, therefore, adopts multiple barriers consisting of various fault-tolerant techniques to increase the total fault detection coverage. Even though these fault-tolerant techniques are adopted to ensure and improve the safety of a system, their effects on the system safety have not yet been properly considered in most probabilistic safety analysis models. Therefore, it is necessary to develop an evaluation method that can describe these features of digital instrument and control systems.

Several issues must be considered in the fault coverage estimation of a digital instrument and control system, and two of these are addressed in this work. The first is to quantify the fault coverage of each fault-tolerant technique implemented in the system, and the second is to exclude the duplicated effect of fault-tolerant techniques implemented simultaneously at each level of the system's hierarchy, as a fault occurring in a system might be detected by one or more fault-tolerant techniques. For this work, a fault injection experiment was used to obtain the exact relations between faults and multiple barriers of fault-tolerant techniques. This experiment was applied to a bistable processor of a reactor protection system.

KEYWORDS : Fault-tolerant, Fault Detection Coverage, Fault Injection, Automatic Test

1. INTRODUCTION

Digital systems such as a programmable logic controller (PLC) or distributed control system (DCS) have been applied to non-safety systems of nuclear power plants (NPPs) due to difficulties in using analog systems. More recently, digital systems have also been applied to the safety systems of NPPs such as the reactor protection system (RPS). The RPS is a safety system that trips a reactor to prevent the development of an accident when the reactor deviates from normal operation. The first application of a digital RPS was at Kori unit 1 to resolve an obsolescence problem due to the accumulated years of operation. An Integrated Digital Protection System (IDiPS) RPS was developed in Korea [1-2] during the Korea Nuclear Instrumentation and Control System (KNICS) research and development project. The IDiPS RPS has four independent channels, where each channel consists of bistable processors (BP), coincidence processors (CP), an automatic test and interface processor (ATIP), a cabinet operator module (COM), and other hardware components, as shown in Fig. 1. For the platform of the IDiPS RPS, a safety PLC has been adopted. The PLC is composed of various modules such as a bus, power, processor, communication, and input/output modules.

To improve the reliability and availability of IDiPS RPS, various fault-tolerant techniques such as self-diagnostics of each module, a heartbeat check of the watchdog timer, and periodic automatic testing of the ATIP have been implemented in IDiPS RPS. For example, an automatic periodic test is periodically initiated by the ATIP without any human intervention. ATIP provides test inputs to the BP and CP, and automatically checks the test results received from the BP and CP during the automatic periodic test.

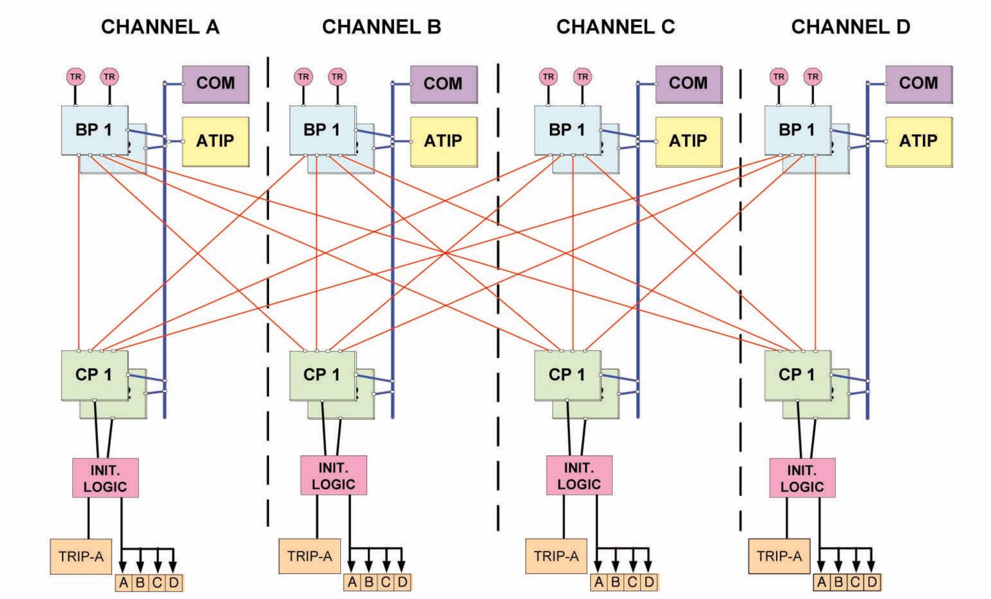


Fig. 1. Block Diagram of IDiPS RPS

Even though these fault-tolerant techniques are designed to ensure and improve the safety of the system, their effects have not yet been properly considered in probabilistic safety analysis (PSA) models. To include the effects of fault-tolerant techniques in the PSA model, some factors must be considered [3]:

- The fault-tolerant techniques implemented in the system can improve the system safety. A specific fault-tolerant technique, however, cannot detect and recover all possible faults that occur in the system, and can detect and recover only limited types of faults. It is therefore important to quantify the fault coverage of specific fault-tolerant techniques.
- It is important to exclude duplicated effects of fault-tolerant techniques since various fault-tolerant techniques such as component-level fault detection algorithms (e.g., memory checksum, illegal instruction detection of microprocessor), module-level self-diagnostics (e.g., loop back check of input and output modules), and system-level error detection mechanisms (e.g., on-line automatic periodic test of ATIP, heart beat check of watchdog timer) are implemented simultaneously at each level of the system's hierarchy.
- Each fault-tolerant technique has a different detection period. For example, a watchdog timer can detect faults in a few seconds when the faults halt the microprocessor. However, the detection period of the automatic periodic test is around a few hours.
- While some fault-tolerant techniques (e.g., watchdog timer) make the system automatically generate fail-safe signals for equipment controlled by the system to enter a safe state, some fault-tolerant techniques (e.g., automatic periodic test) simply provide an abnormal status warning to the system's human operators. In this case, the probability of human operators failing to detect and recover the warning should be considered.

This work is focused on the first and second issues. Specifically, a method to quantify the fault coverage with consideration of the duplicated effects of fault-tolerant techniques in IDiPS RPS is suggested using a fault injection experiment.

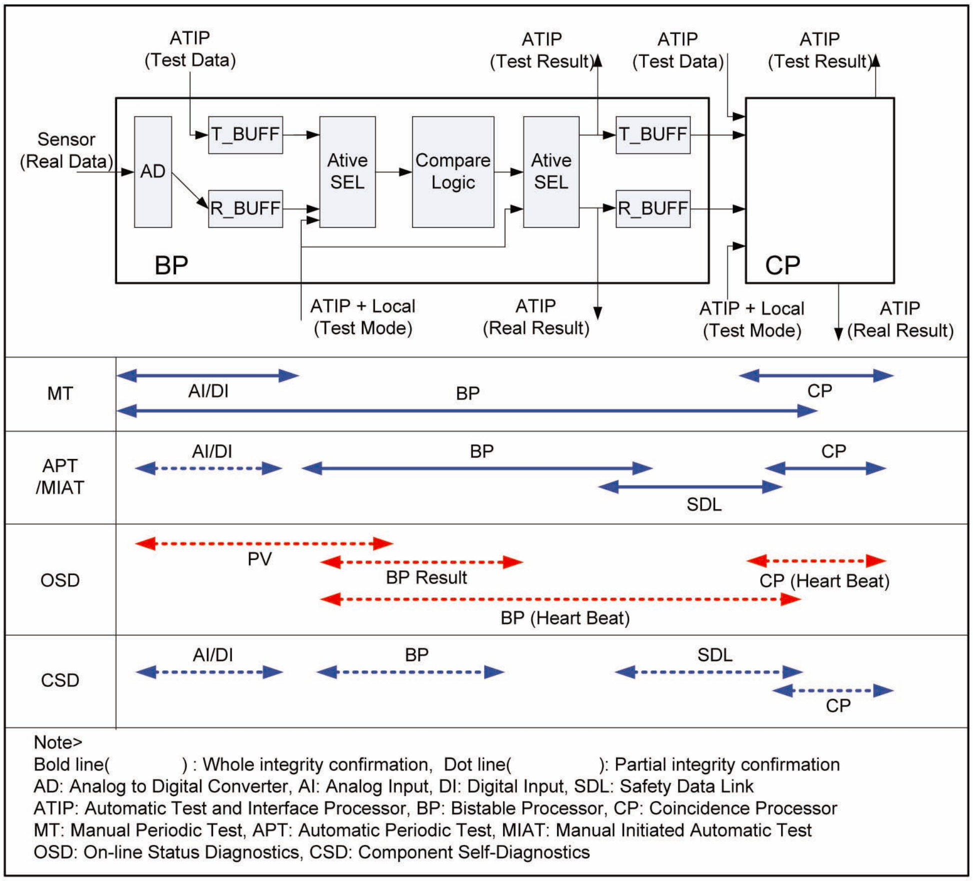
2. FAULT-TOLERANT DESIGN OF IDIPS RPS

IDiPS RPS tests can be classified into two categories, active tests and passive tests. Active tests consist of automatic periodic tests, manual initiated automatic tests, and manual tests [4]. An automatic periodic test is periodically initiated by the ATIP without any human intervention. A manually initiated automatic test is almost the same as an automatic periodic test except for the operator initiation and tested trip parameter selection. This test is performed by a human decision, if necessary. A manual test is generally performed once per month.

A passive test partially checks the system's integrity. This test consists of component self-diagnostics and on-line status diagnostics. Each test is overlapped so as not to leave any untested parts, as shown in Fig. 2.

2.1 Component Self-Diagnostics (CSD)

Each module of the PLC, such as the processor, analog



Note>
Bold line( ) : Whole integrity confirmation, Dot line( ): Partial integrity confirmation
AD: Analog to Digital Converter, AI: Analog Input, DI: Digital Input, SDL: Safety Data Link
ATIP: Automatic Test and Interface Processor, BP: Bistable Processor, CP: Coincidence Processor
MT: Manual Periodic Test, APT: Automatic Periodic Test, MIAT: Manual Initiated Automatic Test
OSD: On-line Status Diagnostics, CSD: Component Self-Diagnostics

Fig. 2. The Test Strategy of IDiPS RPS

input, and digital input/output module, has its own self-diagnostic algorithm. The processor module can detect a watchdog timeout error, execution cycle violation, and instruction operation code error. If the processor module detects an error, it stops the currently running applications. It does not, however, stop the applications in the case of a warning. Input and output modules carry out loopback monitoring functions to compare input/output signals with feedback signals. If there is a difference between these two signals, an error status is sent to the processor module. Each module also has light emitting diodes (LEDs) at the front panel to display its operation status. If the operation is faulty, the fault LED turns on.

2.2 On-line Status Diagnostics (OSD)

The on-line status diagnostics performed by the ATIP are passive in nature; that is, no active test signals are applied to the system. The ATIP receives all the statuses of the system via the network, such as the BP and CP statuses. This data is then analyzed to determine whether the system is operating properly. The analysis consists of the following:

- Channel-to-channel comparison of the input signals
- Setpoint checks to verify the proper setpoint settings
- Trip status check of BP and CP
- Heartbeat check of BP and CP

2.3 Automatic Periodic Test (APT)

An automatic periodic test performed by ATIP encompasses a BP logic test, CP logic test, data link test, and input/output module test, as shown in Fig. 3.

The test performs several tasks to ensure that the BP and CP logic is operating properly. First, a setpoint check is performed. This task reads trip and pre-trip setpoints of all process parameters from the BP, and compares them to the known setpoint. Second, an integrity check of the BP and CP is performed. This task produces the test commands and test data. The test data include the test start/stop, tested processor identification number, test step, and test scenario with test input. The BP and CP check the test command from the ATIP and perform a logic test and input/output module test using the test input from the ATIP. After finishing the specified test step, the BP and CP transmit the test results to the ATIP for every scan.

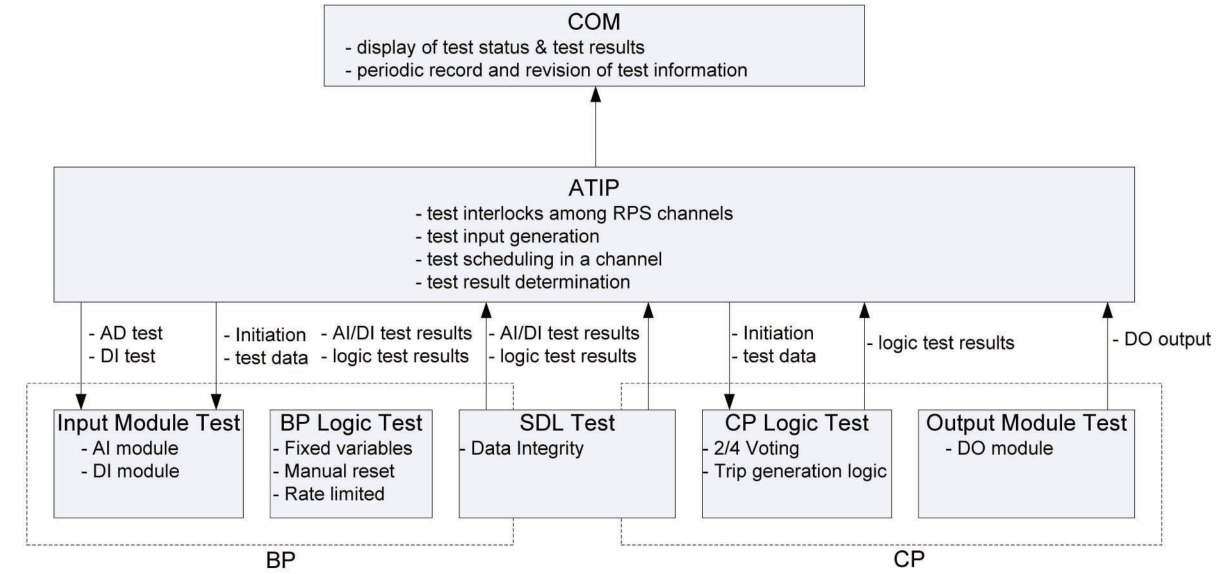


Fig. 3. The Functional Structure of the Automatic Periodic Test

Comparing the test results transmitted by the BP or CP with the expected test results, the task determines whether the test has been passed. If a discrepancy exists, the task annunciates a test failure and provides a message that describes the failure in more detail. The personnel can show the detailed test results via the COM display panel.

3. RELIABILITY MODEL OF FAULT-TOLERANT SYSTEM

When failures of the system are repairable, the unavailability is defined as [5]

Q(t) = the probability that the system is down at time t and unable to operate if called upon.

A simple representation for unavailability is the ratio of the expected value of the down time of the system to the sum of the expected values of up and down time given by

$$Q(t) = \frac{E[\text{Down Time}]}{E[\text{Up Time}] + E[\text{Down Time}]} = \frac{MTTR}{MTTF + MTTR}. \quad (1)$$

where MTTF is the mean time to failure and MTTR is the mean time to repair.

It is assumed that the repair restores the system to a state where the system is essentially as good as new. For repairable failures, two cases can be considered: (a) when failures are monitored, and (b) when failures are not detectable until a periodic surveillance test is performed. For the monitored case, the failure of the system is detected immediately by an alarm, annunciator, light, or some other signal. If the failure probability distribution of the system is an exponential distribution, the unavailability of the system is related to the frequency of failure and the average time needed to return the system to service [6] and is given by

$$Q_M = \frac{MTTR}{MTTF + MTTR} = \frac{T_D}{1/\lambda + T_D} = \frac{\lambda T_D}{1 + \lambda T_D} \cong \lambda T_D. \quad (2)$$

The quantity λ is the failure rate of the system and the quantity T_D is the average downtime to respond to the failure, repair the system, and return it to service. The approximation given by Eq. (2) is conservative and is within 10% accuracy for $\lambda T_D < 0.1$.

For the system, which is not monitored but is periodically tested, no occurring failures are detectable until the test is performed. If the system is found to have failed through a surveillance test with intervals of T, the unavailability is given by

$$Q_T = \frac{\lambda T}{2} + \lambda T_R \cong \frac{\lambda T}{2}, T_R << T. \quad (3)$$

In Eq. (3), T_R is the average repair time obtained from the downtime consideration. For repairable failures, the unavailability is thus given by Q_M or Q_T depending on whether monitoring exists or periodic testing is performed with no monitoring between tests.

Digital systems have generally adopted both testing strategies simultaneously, as shown in Fig. 2. That is, various fault detection techniques are implemented in the system to monitor the system failure. In addition, a manual periodic test is performed once per month. In this case, fault-tolerant techniques and their fault coverage are crucial factors [7] in the evaluation of system unavailability. The fault detection coverage is a measure of the system's ability to detect faults, and is mathematically defined as the

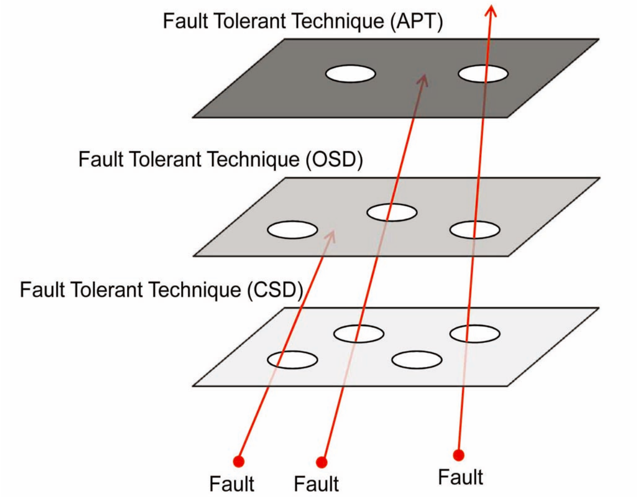

Fault Tolerant Technique (APT)
Fault Tolerant Technique (OSD)
Fault Tolerant Technique (CSD)
Fault
Fault
Fault

Fig. 4. Relation between Faults and Fault-tolerant Techniques

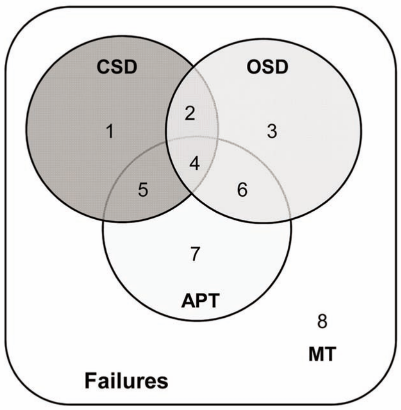


Fig. 5. Union set of Fault Coverage

conditional probability that the system detects an existing fault [8].

$$C = \Pr(\text{fault detected} \mid \text{fault existence}) \tag{4}$$

Each fault-tolerant technique has a different inspection period, from real-time monitoring to monthly testing. The range covered by each fault-tolerant technique is also different. The digital I&C systems, therefore, adopt multiple barriers consisting of various fault-tolerant techniques to increase the total fault detection rate, as shown in Fig. 4.

While some faults occurring in a system can be detected by one or more fault-tolerant techniques, some faults may not be detected by any fault-tolerant technique. The overall fault coverage of fault-tolerant techniques, therefore, is not the simple summation of fault coverage of each fault-tolerant technique, but a union set of the fault coverage of each fault-tolerant technique, as shown in Fig. 5.

In this case, the system unavailability can be obtained with a combination of Eqs. (2), (3), and (4) and is given by

$$Q = \sum_{i=1}^{6} \lambda_i T_R + \lambda_{APT}\left(\frac{T_{APT}}{2} + T_R\right) + \lambda_{MT}\left(\frac{T_{MT}}{2} + T_R\right) \tag{5}$$

The first term in Eq. (5) considers the failures detectable by CSD or OSD. The failures that are detectable by CSD and OSD have an instantaneous detection time because the time to detect a failure is 1 minute or less. The second term in Eq. (5) considers a failure detectable only by APT. The third term considers failures detected by the manual test. The failures that are detectable by APT and MT cannot be assumed to have an instantaneous detection time, because these tests have a periodic test interval of 8 hours and 1 month, respectively.

The failure rates of each area in Fig. 5 are represented using the failure rate of the system and the fault detection coverage of each area as follows:

$$\lambda_i = \lambda \cdot C_i \tag{6}$$

$$\lambda_{APT} = \lambda \cdot C_7 \tag{7}$$

$$\lambda_{MT} = \lambda\left(1 - \sum_{i}^{7} C_i\right) \tag{8}$$

where λ is the failure rate of the system and C_i is the fault detection coverage of a fault tolerant technique in area i.

4. FAULT INJECTION EXPERIMENT

In this work, a fault injection experiment was used to obtain the relations between faults and multiple barriers of fault-tolerant techniques implemented in IDiPS RPS. To identify the exact relation, it is best to inject all expected faults in the real IDiPS RPS environment. However, because of the system complexity, it is very difficult to identify and inject all of the fault modes. In addition, it is difficult to set up a real IDiPS RPS environment due to the experimental costs. Limited fault modes and fault location have therefore been selected in this experiment. The location for the fault injection is focused on only the memory, in which the trip logic of the BP is stored, and the type of injected faults are limited to stuck-at-zero and stuck-at-one faults. Only four representative fault-tolerant techniques in IDiPS RPS were considered in the experiments: self-diagnostics in the BP, status check of the BP by ATIP, heartbeat check of the BP by ATIP, and automatic testing of the BP by ATIP.

The experiment environment consists of a simplified BP, simplified ATIP, a computer for fault injection, and a computer for data acquisition and storage, as shown in Fig. 6. The faults can be injected into memory or registers

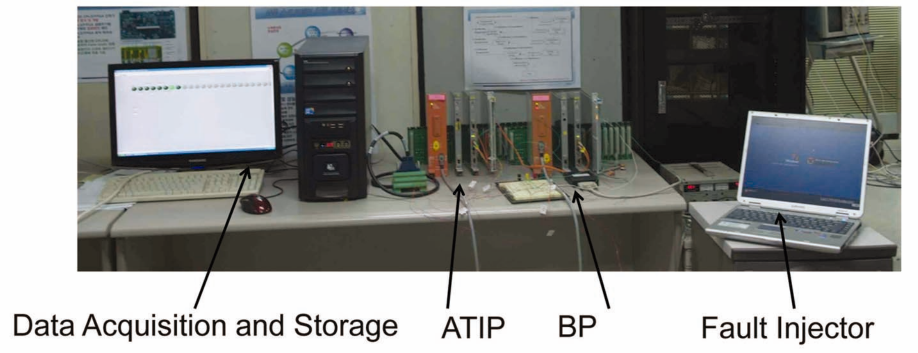


Fig. 6. Configuration of Fault Injection Experiment

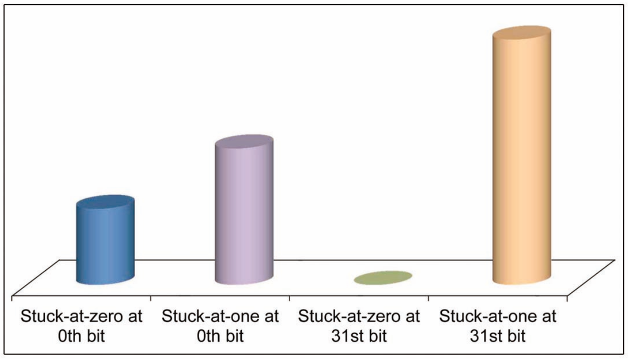


Fig. 7. Relative Spurious Trip Failure Frequency: Case (a)

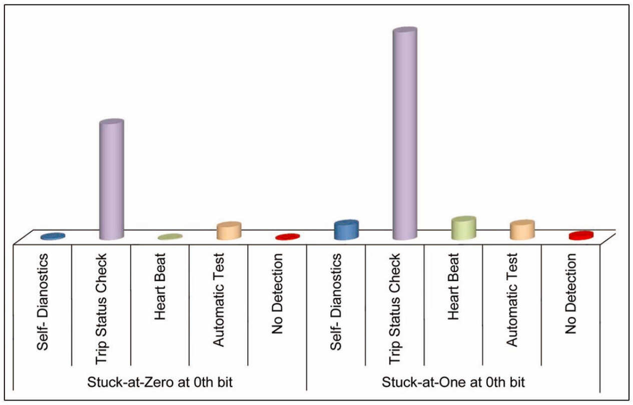


Fig. 8. Relative Failure Detection Coverage at 0th bit Faults: Case (a)

in the microprocessor in the BP by a fault injector, which is a software program specially designed for this experiment. The fault injector is based on a commercial emulation tool that provides basic capabilities such as read/write memory, read/write CPU register, single step and real time execution, and hardware breakpoints and trigger features. After a specific type of fault is injected, the results of the experiment are automatically stored in the data acquisition and storage computer in which the data acquisition program and hardware are installed.

There are two types of failures in the BP: (a) spurious trip generation when a trip is not required, or (b) un-trip generation when a trip is required. If input signals from a sensor to the BP are controlled to stop the BP from generating a trip signal while injecting the fault into memory in the BP, a BP failure occurs when the BP generates a spurious trip signal. If input signals from a sensor to the BP are controlled to make the BP generate a trip signal while injecting the faults into memory in the BP, a BP failure occurs when the BP does not generate a trip signal.

Fig. 7 shows the relative frequency of a spurious trip when stuck-at faults are injected into each bit of memory in BP, and the input signals of the BP are controlled so as to not make the BP generate a trip signal.

Fig. 8 shows the relative failure detection rate when stuck-at faults are injected into the 0th bit of memory in the BP. When the BP generates a spurious trip signal due to the injected faults, the trip status check function of the ATIP has the highest detection coverage.

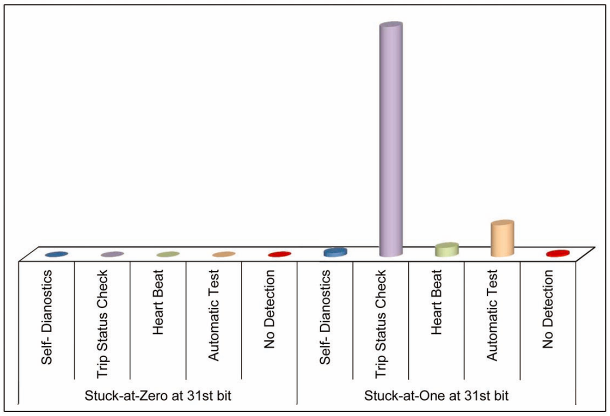


Fig. 9. Relative Failure Detection Coverage at 31st bit Faults: Case (a)

Fig. 9 shows the relative failure detection rate when stuck-at faults are injected into the 31st bit of memory in

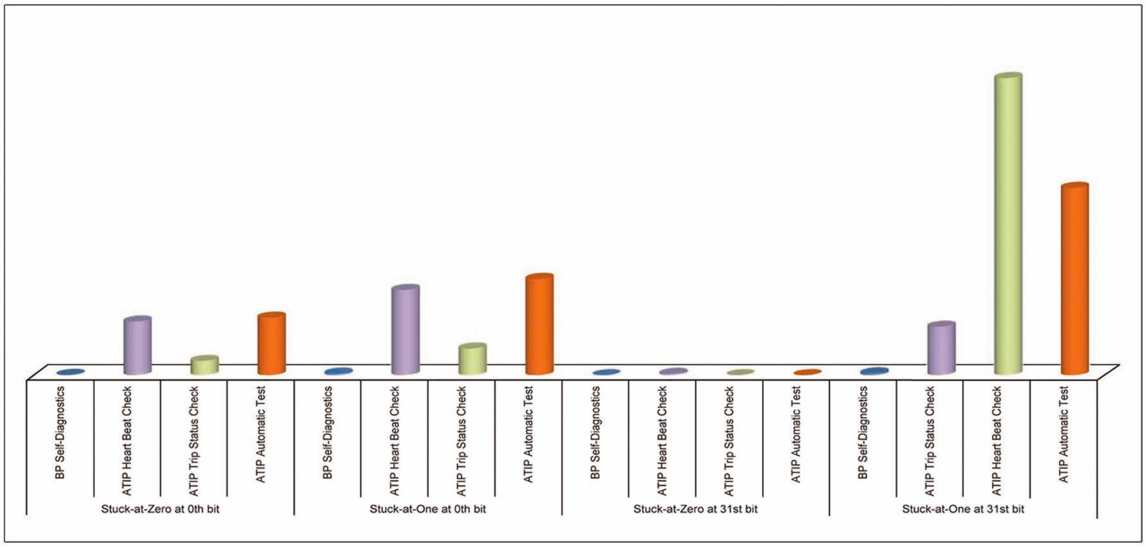


Fig. 10. Relative Fault Detection Coverage: Case (a)

the BP. When the BP generates a spurious trip signal due to injected faults, the trip status check function of the ATIP has the highest detection coverage. The detection coverage of a spurious trip failure due to stuck-at-zero faults injected into the 31st bit of memory is very low because the spurious trip frequency of the BP is very low, as shown in Fig. 7.

The BP does not create a spurious trip signal if the BP halts due to an injected fault at the un-trip level. In this case, the BP cannot generate a trip signal even if the input signals approach the trip level. That is, the BP will be in a failed state if the input signals approach the trip level, even though the BP is not in a failed state at the current input signals of the un-trip level. Fig. 10 shows the relative fault detection coverage that includes these cases.

5. CONCLUSIONS AND FURTHER STUDIES

New NPPs have adapted digital I&C systems in which there are multiple barriers consisting of various fault-tolerant techniques to help the system safely perform the specific required functions in spite of the presence of faults. Even though these fault-tolerant techniques are adopted to ensure and improve the safety of the system, their effects have not yet been properly considered in most PSA models. The PSA model without consideration of the effects of fault-tolerance techniques results in underestimation of the system safety. The PSA model should also consider duplicated effects of various fault-tolerant techniques in the system; otherwise it results in overestimation of the system safety.

Therefore, it is necessary to develop an evaluation method that can describe these features of digital I&C systems. Several issues must be considered in the fault coverage estimation of a digital I&C system, and two of these issues were addressed in this work. The first is to quantify the fault coverage of each fault-tolerant technique, and the second is to exclude the duplicated effect of fault-tolerant techniques.

In this work, an unavailability model that considers the overall fault coverage of various fault-tolerant techniques has been developed. This unavailability can be used in the PSA model as a basic event that represents a system adopting various fault-tolerant techniques. In addition, a fault injection experiment was performed to obtain the overall fault coverage in the unavailability model. These experimental results were utilized to assess the correct unavailability and not overestimate the system safety in the PSA model.

A fault injection experiment for only a spurious trip generation case was also presented in this work. A fault injection experiment for un-trip generation is currently being performed. The unavailability estimation of the BP will be performed after the fault injection experiment is finished.

ACKNOWLEDGMENT

This work has been carried out under the Nuclear R&D Program supported by the Ministry of Education, Science and Technology (MEST) (Grant code: 2011-0001904).

REFERENCES

[1] Kee. C. Kwon and M. S. LEE, "Technical Review on the Localized Digital Instrumentation and Control Systems," *Nuclear Engineering and Technology*, Vol. 41, No. 4, pp. 447-454 (2009).

[2] J. H. Park, D. Y. Lee, and C. H. Kim, "Development of

KNICS RPS Prototype," Proceedings of ISOFIC 2005: *International Symposium on the future I&C for NPPs*, Tongyeong, Gyeongnam, Korea, Nov. 1-4, 2005.

[3] S. J. Lee, J. G. Choi, H. G. Kang, and S. C. Jang, "Reliability Assessment Method for NPP Digital I&C Systems Considering the Effect of Automatic Periodic Tests," *Annals of Nuclear Energy*, Vol.37, No. 11, pp. 1527-1533 (2010).

[4] S. Hur, D. H Kim, and I. K. Hwang, "A New Automatic Periodic Test Method for the Digital Reactor Protection System," *6th American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies*, Knoxville, Tennessee, USA, Apr. 5-9, 2009.

[5] W. E. Vesely, F. F. Goldberg, N.H. Roberts, and D. F. Haasl, "Fault Tree Handbook," NUREG-0492, U.S. Nuclear Regulatory Commission (1981).

[6] J. W. Hickman, et al, "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," NUREG/CR-2300, U.S. Nuclear Regulatory Commission (1983).

[7] H. G. Kang, "An Overview of Risk quantification Issues of Digitalized Nuclear Power Plants Using Static Fault Trees," *Nuclear Engineering and Technology*, Vol. 41, pp. 849-858 (2009).

[8] J. B. Dugan, K. S. Ttrivedi, "Coverage Modeling for Dependability Analysis of Fault-Tolerant Systems," *IEEE Transactions on Computer*, Vol. 38, No. 6, pp. 77-87 (1989).