Some Insights into Fault Detection Coverage of Digital I&C Systems

Man Cheol Kim[*]
Integrated Safety Assessment Division, KAERI, 1045 Daedeok-daero, Yuseong-gu, 305-353, Daejeon, Korea
[*]*Corresponding author: charleskim@kaeri.re.kr*

1. Introduction

Fault detection coverage is defined as the probability that a system detects an occurring fault in the system. After a sensitivity study on various important factor considered in the probabilistic safety assessment (PSA) of nuclear power plants (NPPs) with digital instrumentation and control (I&C) systems, Kang and Sung [1] identified the fault detection coverage of digital I&C systems as one of the most critical factors in the reliability and safety analysis of the digital I&C systems. Due to the importance of fault detection coverage of digital I&C systems in NPPs, there have been a lot of discussion on whether it is possible to determine a generic value of fault detection coverage or not. To get some insights into the fault detection coverage of digital I&C systems, an estimation of fault detection coverage of a digital system is performed.

2. Dependency of Fault Detection Coverage

Constantinescu [2] identified five factors affecting the fault detection coverage of digital systems. Smith et al.[3] also mentioned that a general mathematical expression for the system coverage can be expressed as a function of five factors. After the examination of the factors identified in the two literatures, the factors affecting the fault detection coverage of digital I&C systems are summarized into the following five factors, which are (1) fault type, (2) fault location, (3) fault occurrence time (4) fault duration, and (5) input/system state. The fact that the fault detection coverage is dependent on many factors means that the fault detection coverage cannot be easily specified unless those affecting factors are clearly specified.

3. Fault Injection Experiments

In an effort to get insights into the nature of fault detection coverage of digital I&C systems in NPPs, a n estimation on the fault detection coverage of an example digital system is performed.

One of the most widely used method for fault detection coverage estimation is the use of fault injection experiments. In fault injection experiments, faults are intentionally injection into the target digital system and the response of the target digital system is observed. Fig. 1 shows the fault injection experiment environment used in Korea Atomic Energy Research Institute (KAERI) for conducting researches on fault detection coverage estimation of digital I&C systems in NPPs.

Fig. 1. Fault injection experiment environment used in the fault detection coverage estimation

For the fault location, faults are injected only in the internal registers to limit the total number of fault injections in a reasonable number. Considering the fact that the general purpose registers are continuously overwritten, it can be assumed that the effect of permanent faults will be relatively more significant than that of transient faults. For this reason, we selected two most widely known permanent fault types, which are the stuck-at-0 faults and the stuck-at-1 faults. For the fault occurrence time, it is assumed that a fault occurs after the initialization procedure because in many process controllers the initialization procedure is executed only one time while the main() function is executed infinitely and therefore it is more feasible to assume that a fault occurs while executing the main() function is executed.

After the execution of the application software with an injected fault, the number of steps until the binary code arrives at the finishing point and the calculation results after injecting a fault in the target system are gathered as experimental data. If the number of steps to the finishing point exceeds a predefined number of steps, it is assumed that the target system falls into an infinite loop and therefore, if a watchdog timer is installed, the watchdog processor might reset the target system. For example, when a stuck-at-0 fault is injected into the 0-th bit of R0 register in the target processor, the calculation finished after the execution of 620 steps, instead of 621 steps of the execution without any injected fault, and the calculation result was different with the one without an injected fault. In a similar way, fault injection experiments to all 32 bits of R0 to R14 registers and the PC (program counter) register of the target processor were carried out. The total number of fault injection experiments was 512.

The effect of a fault is categorized into one of the three categories, (1) no effect, (2) infinite loop, and (3) wrong output. As mentioned above, it can be assumed that the watchdog timer can detect the occurrence of a fault in a digital system when the system falls into an infinite loop.

From the fault injection experiments, it was found that the faults injected into different registers produce different experimental results. (Fig. 2) For example, the 32 faults injected into the R0 register produce 21 no effect, 1 infinite loop, and 10 wrong result, while the 32 faults injected into the R1 register produce 26 no effect, 3 infinite loop, and 3 wrong result. This can be interpreted that the effect of an injected fault (and therefore the fault detection coverage of the target system) is dependent on the fault location. Therefore, it was confirmed that the fault location should be considered as an important factor in estimating the fault detection coverage of a digital system.

It was also confirmed that faults with different types produce different experimental results, even though the fault location is same. For example, when we compare the experimental results for the faults injected into R0 register, the stuck-at-0 faults produce 21 no effect, 1 infinite loop, and 10 wrong result, while the stuck-at-1 faults produce 0 no effect, 0 infinite loop, and 32 wrong result. This can be interpreted that the effect of an injected fault (and therefore the fault detection coverage of the target system) is dependent on the fault type. Therefore, the fault type should be considered as an important factor in estimating the fault detection coverage of a digital system.

For two factors, fault location and fault type, among the five factors described above, the dependency of the effect of a fault (and therefore the fault detection coverage of the target system) on the two factors are demonstrated through a fault injection experiment. In similar ways, the dependency of the effect of a fault (and therefore the fault detection coverage of the target system) on other factors can be demonstrated.

4. Conclusions

From the literature survey on fault detection algorithm and the estimation of the fault detection coverage of an example digital system with fault injection experiments, some insights related to the nature of the fault detection coverage could be found.

The first insight was the dependency of fault detection coverage on various factors including the target digital system. Five factors that should be considered for a quantitative estimation of the fault detection coverage of digital systems are identified based on previous researches. It means that each system has its own fault detection coverage, and therefore the generalized value of the fault detection coverage is not feasible.

The second insight is the importance of "no effect" faults. As can be seen in the experimental results, "no effect" (blue part in Fig.2) take a significant portion of the experimental results. The implication of this finding on the safety of the digital I&C systems in NPPs needs to be further investigated.

The identification of the dependencies of fault detection coverage on various factors and the insights from the experimental results are expected to contribute to practical estimation of the fault detection coverage of digital I&C systems in NPPs, as well as further researches on the fault detection coverage and fault injection experiments.

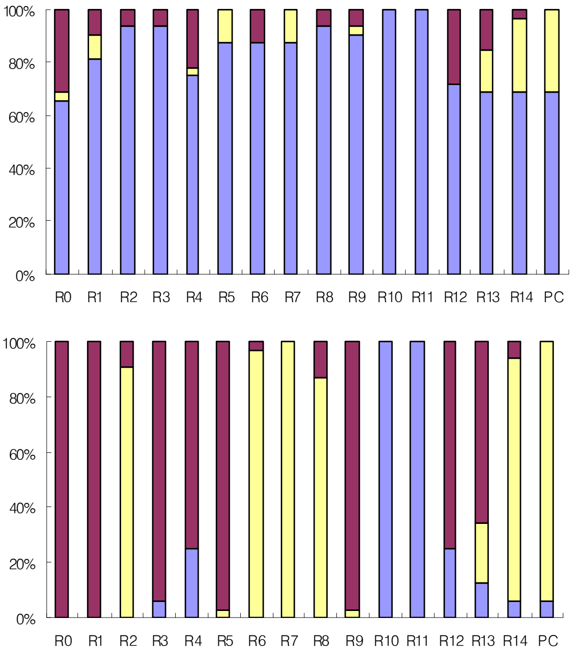

Fig. 2. Results of fault injection experiment for permanent stuck-at-0 and stuck-at-1 faults injected into the internal registers of the target processor

ACKNOWLEDGEMENT

This work was partly supported by Nuclear Research & Development Program of the National Research Foundation of Korea (NRF) grant funded by the Korean government (MEST). (grant code:2009-0078213)

REFERENCES

[1] H. G. Kang and T. Sung, An analysis of safety-critical digital systems for risk-informed design, Reliability Engineering and System Safety, Vol.78, p.307, 2002.

[2] C. Constantinescu, Experimental Evaluation of Error-Detection Mechanisms, IEEE Transaction on Reliability, Vol.52, p.53, 2003.

[3] D. T. Smith, B. W. Johnson, J. A. Profeta III, and D. G. Bozzolo, An analysis of safety-critical digital systems for risk-informed design, Proceedings of Annual Reliability and Maintainability Symposium, 1995