Approach to Modeling of Fault-Tolerant Techniques using Fault Tree

Bo Gyung Kim [a*], Seung Jun Lee [b], Hyun Gook Kang [a], Poong Hyun Seong [a,c]
[a]*Department of Nuclear and Quantum Engineering, KAIST, 373-1, Guseong-Dong, Yuseong-Gu, Daejeon, South Korea, 305-701*
[b]*Integrated Safety Assessment Division, Korea Atomic Energy Research Institute, 1045 Daedeok-daero, Yuseong, Daejeon, 305-353, Korea*
[c]*Department of Nuclear Engineering, Khalifa University of Science, Technology & Research, Abu Dhabi, UAE*

[*]Corresponding author: bogyungkim@kaist.ac.kr

1. Introduction

Recently, the reactor protection system (RPS) based analog I&C system in nuclear power plants (NPPs) has been replaced with digital based I&C system. Because of replacement with analog to digital system, the development of a methodology for the probabilistic safety assessment (PSA) of digital system is an important issue. The digital plant protection system (DPPS) has four identical safety channel cabinet, and it has diversity, dual/triple structure, and enhanced automatic system functions. Since the DPPS uses complex and heterogeneous components, the DPPS should have automatic system functions such as various fault tolerant techniques for high availability and reliability. Therefore, it is necessary to evaluate the relative effects of fault tolerant techniques in DPPS using PSA techniques such as fault tree analysis [1][2][3].

2. Fault Tolerant Techniques

In the reliability evaluation of digital system, the fault-tolerant techniques and their coverage must be considered. A fault is the source which has the potential of generating errors. Fault-tolerance is the system's capability to help the system perform correctly the specific required functions in spite of the presence of faults. In the fault-tolerance evaluation, fault detection coverage is a crucial factor. The fault detection coverage is a measure of the system's ability to perform fault detection, fault isolation, and fault recovery and it is mathematically defined as the conditionally probability that given the existence of a fault, the system detects and recovers.

$$C = \Pr(\text{fault detection} \mid \text{fault existence}) \quad (1)$$

If faults are not detected by a certain detection algorithm, the system could be in failure. A failure is when the delivered service deviates from the specified service. Therefore, evaluating the fault detection coverage of the fault-tolerant technique is very important for the safety analysis of digital systems [2].

The DPPS has more of various fault tolerant techniques. Table 1 shows the examples of fault tolerant techniques in DPPS [4].

Table I: Example of fault tolerant techniques in DPPS

Test Type	Test Kind	Function
Passive Testing	Self-diagnostics	-HW self-diagnostics -OS self-diagnostics -Support mean of surveillance Test
	On-line status diagnostics	-Status Comparison -Processor Integrity Monitoring -Support mean of surveillance Test
Active Testing	Automatic periodic test	-Protection logic test -I/O HW test -A mean of surveillance test
	Manual test	-I/O test -Protection path test -Protection logic test -Initiated circuits test -A mean of surveillance test

A fault occurred in a system might be detected by one or more fault tolerant techniques. Fig. 1 shows the relation between fault and fault tolerant techniques.

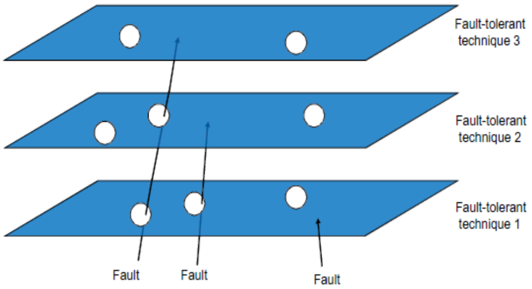
Fault-tolerant technique 3
Fault-tolerant technique 2
Fault-tolerant technique 1
Fault
Fault
Fault

Fig. 1. Faults and fault tolerant techniques. [2]

Some fault can be detected several fault tolerant techniques simultaneously or continuously. Fig.2 shows fault and fault tolerant techniques more effective. Fig. 1 and Fig. 2 show that the overall fault coverage of fault tolerant techniques implemented in system is not the simple summation of fault coverage of each fault tolerant techniques, but union set of faults which can be detected by each fault tolerant techniques [2].

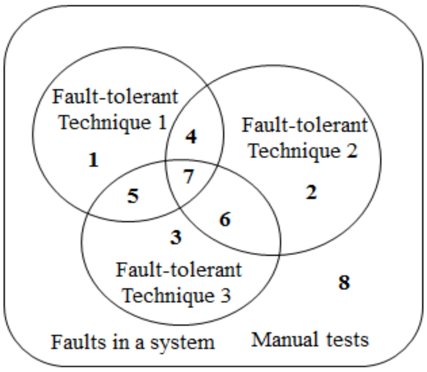
Fault-tolerant Technique 1
Fault-tolerant Technique 2
Fault-tolerant Technique 3
1
2
3
4
5
6
7
8
Faults in a system
Manual tests

Fig.2 Fault set diagram in a system [2]

3. Necessity of modeling of fault tolerant techniques using fault tree

The fault tree is currently used by the worldwide NPP PSA community [5]. The logical structure of the fault tree (FT) makes it easy for system design engineers to understand and it is the most familiar tool for safety analysis.

However, fault tolerant techniques except watchdog timer (WDT) are not reflected in fault tree methodology for PSA of digital systems since the fault coverage and the duplicated effects of fault-tolerant techniques are difficult to estimate.

If fault tolerant-techniques are modeled properly by FT, we can get more accurate and reliable system unavailability of digital I&C system than conventional PSA.

4. Considerations of modeling of fault tolerant techniques using fault tree

4.1 Fault coverage

We should consider the fault coverage for modeling of various effects of fault tolerant techniques using fault tree. Particularly, it is important to consider duplicated effect of fault tolerant techniques as shown in area 4-8 in Fig.2.

If we assume that every fault in a system can be detected all fault tolerant techniques, the basic event of detection failure disappears in fault tree. Therefore, we consider the relation between fault and fault coverage of fault tolerant techniques and reflect each area's fault coverage in fault tree.

Also, we should identify the reason of detect failure occurrence. The reason might be whether the fault cannot be detected because of coverage or the fault tolerant techniques have a problem. According to these reasons, fault tree modeling would be different.

4.2 Detection period

Each fault-tolerant technique has a different detection period. Thus, when duplicated effects of fault-tolerant techniques are considered, we should be careful to treat test time interval. An appropriate value for the time interval needs to be defined in consideration of the time intervals of the fault-tolerant techniques for the area in order to generate more accurate results [2]. When we construct the fault tree, we should consider the duplicated fault detected area's detection period reasonably.

4.3 Fault recovery

While some fault-tolerant techniques make the system automatically generate fail-safe signals for equipment controlled by the system to go to safe state, some fault-tolerant techniques just warn the abnormal situation to the system's human operators. In this case, the probability for human operators to fail to detect and recover the warning should be considered and reflected in fault tree modeling [2].

5. Conclusions

To use the digital system, it is necessary to improve the reliability and availability of a system through fault-tolerant techniques.

Various fault-tolerant techniques, which used in digital system in NPPs, should reflect in fault tree analysis for getting lower system unavailability and more reliable PSA.

When fault-tolerant techniques are modeled in fault tree, categorizing the module to detect by each fault tolerant techniques, fault coverage, detection period and the fault recovery should be considered.

Further work will concentrate on various aspects for fault tree modeling. We will find other important factors, and found a new theory to construct the fault tree model.

REFERENCES

[1] Jun Seok Lee, Man Cheol Kim, Poong Hyun Seong, Hyun Gook Kang, Seung Cheol Jang, Evaluation of error detection coverage and fault-tolerance of digital plant protection system in nuclear power plants, Annals of Nuclear Energy, Vol.33, p. 544-554, 2006.

[2] Seung Jun Lee, Jong Gyun Choi, Hyun Gook Kang, Seung-Cheol Jang, Reliability assessment method for NPP digital I&C systems considering the effect of automatic periodic tests, Annals of Nuclear Energy, Vol.37, p. 1527-1533, 2010.

[3] Suk Joon Kim, Poong Hyun Seong, Jun Seok Lee, Man Cheol Kim, Hyun Gook Kang, Seung Cheol Jang, A method for evaluating fault coverage using simulated fault injection for digitalized system in nuclear power plants, Reliability Engineering and System Safety, Vol.91, p.614-623, 2006.

[4] KAERI/RR-2914/2007, Development of the Digital Reactor Safety Systems, KAERI, 2007.

[5] Hyun Gook Kang, Seung-Cheol Jang, A Quantitative Study on Risk Issues in Safety Feature Control System Design in Digitalized Nuclear Power Plant, Journal of Nuclear Science and Technology, Vol.45, No.8, p.850-858, 2008.