Quantification of Unavailability of Digital Plant Protection System with Various Fault Tolerant Techniques in Nuclear Power Plants

Bo Gyung Kim [a*], Hyun Gook Kang [a,c], Seung Jun Lee [b], Poong Hyun Seong [a]
[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

A digital plant protection system (DPPS) maintains safety by monitoring selected plant parameters, and initiating appropriate protective action when any parameter reaches to the set-point value. The protection system generates signal to actuate reactor trip whenever the process parameters exceed predefined limits. A DPPS is very important system to protect the core and the reactor coolant system. Therefore, it has various fault tolerant techniques to keep the system reliability and reactor safety. However, systematical frameworks or reasonable models to obtain the reliability of digital systems by considering the effects of fault tolerant techniques have not been proposed. [1][2][3].

2. Fault Tolerant Techniques

Fault-tolerance is the system's capability to help the system perform correctly the specific required functions in spite of the presence of faults. A fault occurred in a system might be detected by one or more fault tolerant techniques. Some fault can be detected several fault tolerant techniques simultaneously or continuously. Fig.1 shows fault and fault tolerant techniques more effective. Fig. 2 shows 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].

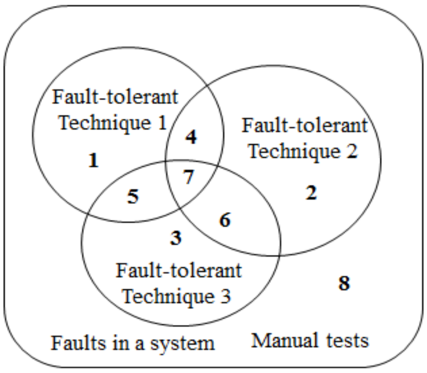
Fault-tolerant Technique 1
Fault-tolerant Technique 2
Fault-tolerant Technique 3
1
2
3
4
5
6
7
8
Faults in a system
Manual tests

Fig.1 Fault set diagram in a system [2]

3. Conventional system unavailability evaluation model based on the fault coverage quantification

Based on the fault detection rate estimated by experiment results, the unavailability of the target system can be calculated. We use the method in NUREG-0492 [4] to obtain the unavailability for repairable failures. Two types of repairable failures are considered in the method: (1) when failures are monitored and (2) when failures are not detectable until a periodic surveillance test is performed. For the monitored case, the unavailability q(t) quickly reaches a constant asymptotic value qM which is given by:

$$q_M = \frac{\lambda T_D}{1+\lambda T_D} \cong \lambda T_D \qquad (1)$$

The failure rate λ is the standby failure rate and the quantity T_D is the average on-line downtime obtained by statistically averaging the downtime distribution. The approximation given by Eq. (1) is conservative and is within 10% accuracy for $\lambda T_D < 0.1$.

For periodic tests performed at intervals of T, the unavailability rises from a low of q(t = 0) = 0 immediately after a test is performed to a high value of $q(t=T) = 1\text{-}e\text{-}\lambda T \approx \lambda T$ immediately before the next test is performed. Because the exponential can be approximated by a linear function (for $\lambda T < 0.1$ say) the average unavailability between tests is approximately $\lambda T/2$. If the component is found failed at surveillance test, then it will remain down during the necessary repair time. Considering this additional repair contribution, we have the following expression for the total average unavailability q_T for periodically tested components:

$$q_T = \lambda T/2 + \lambda T_R \qquad (2)$$

In Eq. (2), T_R is the average repair time obtained from downtime considerations.

If we assume that a system checks its availability through periodic fault-tolerant techniques and manual tests and that manual test detects all the faults which are not detected by other fault-tolerant techniques, then the unavailability of the system could be calculated using the following equation [5]:

$$Q = \sum_{i=1}^{n} \lambda_i \left(\frac{T_i}{2} + T_R\right) + \lambda_M \left(\frac{T_M}{2} + T_R\right) \qquad (3)$$

where, Q = system unavailability, n = number of areas, λ_i = failure rate for the portion detected by a fault-tolerant technique (or fault-tolerant techniques) in area i, λ_M = failure rate for the portion not detected by any fault-tolerant techniques, T_i = time interval of the fault-tolerant technique in area i, T_M = time interval of the manual test, and T_R = time required for maintenance.

And the failure rates of each area are represented using the failure rate of the system and the fault detection coverage of each area.

$$\lambda_i = \lambda \cdot C_i \qquad (4)$$

$$\lambda_M = \lambda \left(1 - \sum_{i=1}^{n} C_i\right) \qquad (5)$$

where, λ = failure rate of the system, C_i = fault detection coverage of a fault-tolerant technique (or fault-tolerant techniques) in area i.

For example, if a system checks its availability through three kinds of periodic fault-tolerant techniques and manual tests, then the faults in the system are covered by eight areas as shown in Fig. 1. The faults in the areas 1–3 are detected by the only one fault-tolerant technique. The faults in the areas 4–7 are detected by two or more fault-tolerant techniques. The other faults in the area 8 represent the faults which are not detected by any fault-tolerant techniques but detected by only manual tests. The overall unavailability of the system is calculated by summation of the unavailability of each area (areas 1–8) as shown in Eq. (3) [2].

4. Considerations of effects of fault tolerant techniques

4.1 Detection Failure

Previous studies consider that the detection failure is the probability of undetected coverage of fault tolerant techniques and they consider the undetected coverage is a constant. But as time goes on the undetected coverage can be changed because the test input component or test result judgment such as ATIP can be failed. Sometimes different algorithms of fault tolerant techniques can make interference. In this case, the fault tolerant technique cannot operate correctly.

4.2 Recovery Process

The recovery process is very important process in fault tolerant techniques. While some fault-tolerant techniques (e.g., watchdog timer) make the system automatically generate fail-safe signals for equipment controlled by the system to go to safe state, some fault-tolerant techniques (e.g., automatic periodic test) 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 and the probability for system to fail to recovery should be considered.

4.3 System Design

There are four redundant channels in DPPS with a selective 2-out-of-4 (selective 2oo4) logic configuration to perform automatic safe shutdown of the plant whenever a deviation of process parameter is detected. During periodic tests or corrective maintenance for a component of DPPS, the associated channel or process parameters are bypassed by setting a 2-out-of-3 (2oo3) logic operation. The DPPS can fail due to sudden failure in the normal state (2oo4) or sudden failure in the bypassed state (2oo3). Sudden failure can be common cause failure (CCF), combination of modules failure, design limits and so on.

5. Conclusions

Modern nuclear power plants use a complex DPPS for safety. Whenever a process parameter exceeds a limit, the plant protection system immediately generates a signal for safe shutdown of the reactor. For maintaining the reliability, the DPPS has various fault tolerant techniques. Various fault-tolerant techniques, which used in digital system in NPPs, should be quantified their effects in digital system to get more accurate reliability and availability. There are the considerations of the effect of fault tolerant techniques in digital I&C system to reflect in Markov or fault tree model for evaluating unavailability of DPPS. Further work will concentrate on various aspects for evaluating unavailability. We will find other important factors, and found a new theory to construct the model for unavailability of DPPS.

REFERENCES

[1] M. Khalaquzzaman, “Reliability and Cost Modeling for Periodically Repairable Components/System in NPPs with Consideration of Maintenance Human Errors”, Ph. D. Dissertation, KAIST, 2011.

[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] Wvsely, W.E., et al., Fault Tree Handbook, NUREG-0492, US Nuclear Regulatory Commission, 1981.

[5] Park, J.H., Lee, D.Y., Kim, C.H., Development of KNICS RPS prototype. In: Proceeding of ISOFIC-2005 November 1–4. Tongyeong, Korea, 2005.