Sensitivity Analysis of Unavailability of a Component in DPS with Various Fault-Tolerant Techniques

Bo Gyung Kim [a], Hyun Gook Kang [a,c,*], Hee-eun Kim [a], 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, Korea, 305-353*
[c]*Department of Nuclear Engineering, Khalifa University of Science, Technology & Research, Abu Dhabi, UAE*
[*]*Corresponding author: hyungook@kaist.ac.kr*

1. Introduction

With the improvement of digital technologies, digital protection system (DPS) has more multiple sophisticated fault-tolerant techniques (FTTs), in order to increase fault detection and to help the system safely perform the required functions in spite of the possible presence of faults. In the reliability evaluation of digital systems, fault-tolerant techniques (FTTs) and their fault coverage must be considered [1]. Fault detection coverage is crucial factor of FTT in reliability [2]. However, the fault detection coverage is not enough to reflect the effects of various FTTs in reliability model. Thus, integrated fault coverage is suggested to reflect characteristics of FTTs.

2. Model to estimate unavailability of a component in DPS with various FTTs

2.1Definitaion of integrated fault coverage

If a fault occurs in system, the fault can be detected by one or more FTTs. After the fault is detected, the fail-safe signal is generated by the relevant FTT or the human operator according to the type of FTT. The process of FTT can be defined as a process ranging from fault detection to the initiating of a fail-safe signal according to the type of FTT.

The integrated fault coverage is the probability that given the existence of faults in a component, one particular FTT will detect faults and make the system generate a fail-safe signal.

2.2 Unavailability Model

The unavailability caused by faults processed by one particular FTT (on-line FTT) can be quantified using the integrated fault coverage.

During the interval of MT, if faults occur, one particular FTT processes faults then the component in the system has downtime (shutdown). The detected problems in a component are maintained by the designated maintainers during repair duration. During unexpected repair, the related FTT does not detect faults.

Fig. 1 shows that the instantaneous unavailability caused by faults processed by on-line FTT in the MT interval.

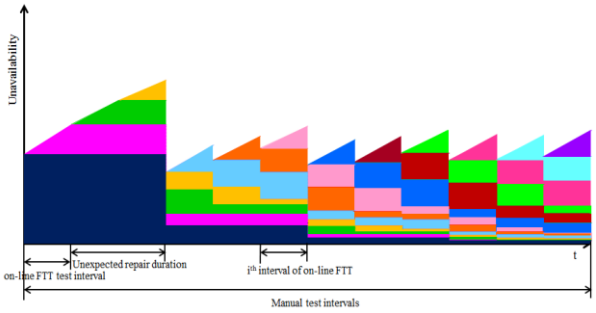

Fig. 1. Unavailability of a component in the MT intervals

During the FTT interval, the instantaneous unavailability for the FTT interval of operation in the MT interval can be increased by faults processed by related FTT. After the FTT processes faults at the 1st FTT operation, a probable downtime will occur at the end of the 1st FTT interval and remain until the end of 1st unexpected repair. The maintenance work performed on a component is not perfect. After the repair, the component can be still unavailable due to repair error.

The average unavailability between two MTs is the summation of the average unavailability according to FTTs and MT. Thus, the average unavailability between two MTs is the summation of average unavailability according to FTTs and MT in the MT interval

The MT detects faults that can be only detected by MT, but also detects faults that are processed by the on-line FTTs at the end of the MT interval. The MT always needs downtime during the test duration, and the periodic maintenance duration is added with the test duration when the component is repaired right after the detection of faults by the MT, in order to estimate the total downtime for periodic maintenance. Total probable downtime after the MT interval is the summation of MT duration and periodic maintenance duration.

The average unavailability between two refueling maintenances is the summation of the total average

unavailability according to FTTs and MT and total probable downtime after the MT interval.

3. Sensitivity Study of Unavailability According to the Failure of On-line FTTs

For estimating unavailability, the random hardware failure rate of a component is assumed $1.0\times10^{-6}/hr$. Human error levels of HFSSG process, MT, periodic maintenance, and unexpected repair are assumed 0.1%, 1%, 5%, and 5%. Downtime due to the MT is assumed 2 hours. Unexpected repairing time and periodic maintenance time are assumed 16 hours. All FTT component replacement intervals are assumed 3 years.

To ascertain the effects of failure of on-line FTTs on integrated fault coverage and unavailability, nine examples were selected, as shown in Table I.

Table I: Description of examples

Examples	Description
$f_{CSD}=f_{ATIP}=1$	FTT A, B, and C are failed.
$f_{CSD}=1$	FTT A is failed.
$f_{ATIP}=1$	FTT B and C are failed.
High level of f_{CSD}, f_{ATIP}	FTT A, B, and C have high level of failure probability.
Intermediated level of f_{CSD}, f_{ATIP}	FTT A, B, and C have intermediated level of failure probability.
Low level of f_{CSD}, f_{ATIP}	FTT A, B, and C have low level of failure probability.
$f_{CSD}=0$	FTT A never fails.
$f_{ATIP}=0$	FTT B and C never fail.
$f_{CSD}=f_{ATIP}=0$	FTT A, B, and C never fail.

If a system checks its availability through three kinds of on-line FTTs (FTT A, B, and C) and MT, than the faults in the system, 4 kinds of integrated fault coverage can be estimated. Fig. 2 shows the integrated fault coverage according to the failure of on-line FTTs. Fig. 2 shows the change of integrated fault coverage according to the failure of FTTs.

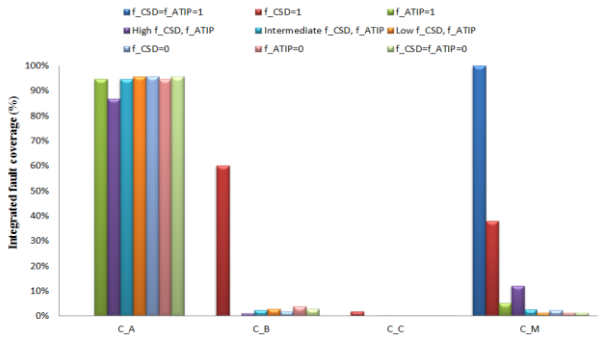

Fig. 2. Integrated fault coverage

A failure of FTT A is related to the component self-diagnostics (CSD) component failure. A failure of FTT B and C is related to the automatic test and interface processor (ATIP) hardware failure. A range of failure rate level of CSD and ATIP make change integrated fault coverage of on-line FTTs and MT.

The average unavailability between the two refueling maintenances, according to the failure of FTT, is shown in Fig. 3. The unavailability can be changed, if the fault-tolerant techniques fail, as can be seen in Fig. 3.

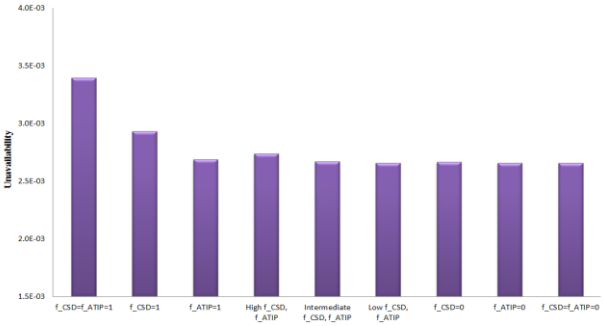

Fig. 3. The average unavailability between two refueling maintenances

When on-line FTTs never fail, the unavailability becomes the lowest value. Even though on-line FTTs have high failure probabilities, the average unavailability when FTT A, B, and C have a high failure probability is 19.4% less than the average unavailability when FTT A, B, and C are failed. The average unavailability when the level of on-line FTTs is high is 3.1% larger than the average unavailability when all on-line FTTs never fail.

4. Conclusions

The proposed model is useful in quantitatively analyzing the effects of FTTs. From the sensitivity study, the average unavailability between refueling maintenance can be seen to strongly depend on the integrated fault coverage of the MT.

Even though the level of failure of on-line FTTs is high, the unavailability decreased extremely. From this result, even if on-line FTTs are not safety-critical component, the unavailability can decrease highly. Also, the failure of on-line FTTs should not be ignored in reliability. Besides, the failure of FTT A has more effect on the average unavailability than the failure of FTT B and C. Therefore, to improve system reliability, it is effective to reduce the CSD component failure probability. If the CSD component and ATIP failure probabilities cannot easily be reduced, the FTT component replacement period needs to be short. Even if the level of failure of on-line FTTs is high, on-line FTTs can reduce the unavailability.

REFERENCES

[1] Kang et al., 2009. An overview of risk quantification issues of digitalized nuclear power plants using static fault tree. Nucl. Eng. Technol. 41, 849–858.
[2] Lee et al., 2010, Reliability assessment method for NPP digital I&C systems considering the effect of automatic periodic tests. Ann. Nucl. Energy 37, 1527-1533.