# Effect Analysis of Digital I&C Systems on Plant Safety based on Fault-Tree Analysis

Seung Jun Lee and Wondea Jung
*Korea Atomic Energy Research Institute*
*1045 Daedeok-daero, Yuseong-gu, Daejeon, 305-353, Korea*
**Corresponding author: sjlee@kaeri.re.kr*

## 1. Introduction

Instrumentation and control (I&C) systems in nuclear power plants (NPPs) are important in the reliability analysis of an NPP. Operators in a plant are provided the plant information and perform the required controls through I&C systems. In addition, safety systems such as a reactor protection system (RPS) generate a reactor trip signal when the trip parameters are over the trip set points.

Recently, I&C systems have undergone digitalization. Deterioration and an inadequate supply of components of analog I&C systems have led to inefficient and costly maintenance. Moreover, since the fast evolution of digital technology has enabled more reliable functions to be designed for NPP safety, the transition from analog to digital has been accelerated. Owing to the distinguishable characteristics of digital I&C systems, a reliability analysis of digital systems has become an important element of a probabilistic safety assessment (PSA). Digital I&C systems have unique characteristics such as fault-tolerant techniques and software. However, these features have not been properly considered yet in most NPP PSA models [1-4].

The effect of digital I&C systems should be evaluated by comparing them to that of analog I&C systems. Before installing a digital I&C system, even though it is expected that the plant safety can be improved through the advantageous features of digital I&C systems, it should be validated whether the total NPP safety is better than analog systems or is the same at least. In this work, the fault-tree (FT) technique, which is most widely used in a PSA, was used to compare the effects of analog and digital I&C systems. From a case study, the results of plant safety were compared.

## 2. FT Models of Analog and Digital RPS

In this work, core damage frequency (CDF), which is one of the measures representing plant safety, was used for a comparison method. Partial fault tree models to evaluate the CDF were developed for analog and digital I&C systems for a case study. In these simple models, the top event is the CDF, which is estimated based on the reactor trip signal generation failure of an RPS.

For simplicity, the CDF of a plant with analog I&C systems is defined as Equation (1).

$$P(CDF)=F(IE) * P(RF) * P(MF) \qquad (1)$$

where
- *P(CDF):* probability of CDF
- *F(IE)*: Initiating event frequency
- *P(RF)*: Probability RPS failure (unavailability)
- *P(MF)*: Probability of manual backup failure

If a digital RPS is considered, other factors representing the characteristics of the digital RPS are as shown in Equation (2).

$$\begin{aligned}P(CDF)&=F(IE) * P(RF) * P(MF)\\ &=F(IE) * (P(HF)+ P(SF))*(1-P(FD))* P(MF) \qquad (2)\end{aligned}$$

where,
- *P(CDF):* Core damage frequency
- *F(IE)*: Frequency of an initiating event
- *P(RF)*: Probability RPS failure (unavailability)
- *P(MF)*: Probability of manual backup failure
- *P(HF)*: Hardware failure probability of RPS
- *P(SF)*: Software failure probability of RPS
- *P(FD)*: Failure detection probability of fault-tolerant techniques of RPS
- *P(MF)*: Probability of manual backup failure

Simple comparison FT models were developed with consideration of only one reactor trip parameter (pressurizer pressure high trip), as shown in Fig. 1.

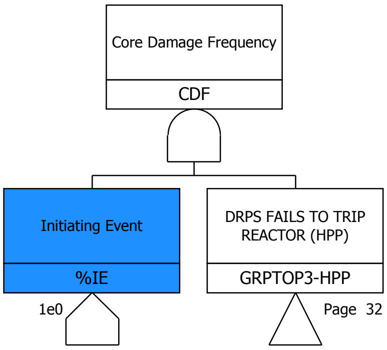


Fig. 1. Top event of the FT models.

The following assumptions were made for the digital RPS model to consider the characteristics of the digital RPS.

- Failure detection functions such as component self diagnostics, online status diagnostics, and automatic periodic testing were considered. From the experiment result using a fault injection technique, the total failure detection probability was evaluated at about 97% [1]. In this model, the failure detection probability was conservatively assumed as 90%.

- In addition to hardware failure probability, software failure probability was considered. It was assumed to be 1E-6.
- Common cause failures (CCFs) of RPS hardware and software were considered.
- Input and output modules were modeled with a card-level.
- In the case of failures of trip signal generation and a mechanical failure of trip circuit breakers, manual backup of the operators was considered.
- Except a part of the FT model related to digital systems, the other part is the same as that of an analog system.

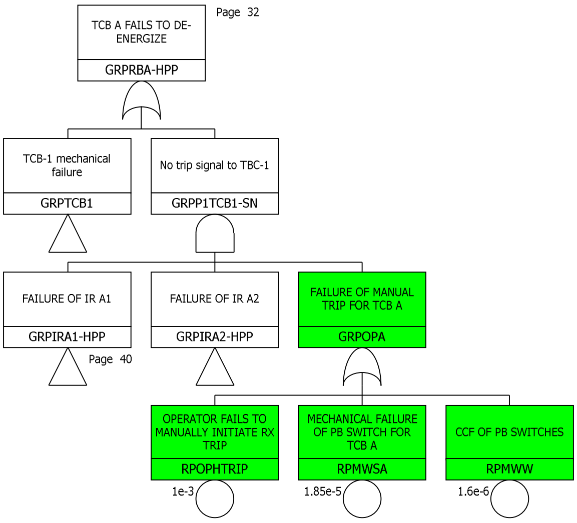


Fig. 2. Manual backup in case of trip signal generation failures.

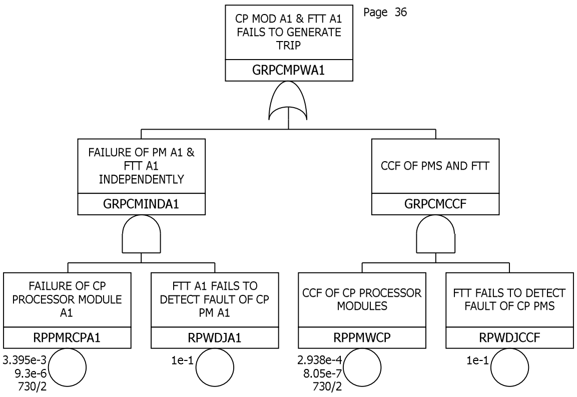

CP MOD A1 & FTT A1 FAILS TO GENERATE TRIP
Page 36
GRPCMPWA1
FAILURE OF PM A1 & FTT A1 INDEPENDENTLY
GRPCMINDA1
CCF OF PMS AND FTT
GRPCMCCF
FAILURE OF CP PROCESSOR MODULE A1
RPPMRCPA1
3.395e-3
9.3e-6
730/2
FTT A1 FAILS TO DETECT FAULT OF CP PM A1
RPWDJA1
1e-1
CCF OF CP PROCESSOR MODULES
RPPMWCP
2.938e-4
8.05e-7
730/2
FTT FAILS TO DETECT FAULT OF CP PMS
RPWDJCCF
1e-1

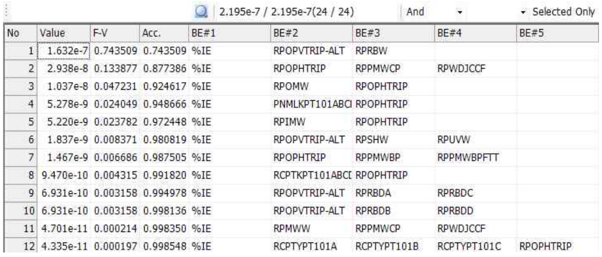
Fig. 3. A part of the digital RPS FT model

## 3. Results

In the evaluation results, the digital system showed a lower CDF than the analog system as follows:

- CDF of analog model: 1.743E-6
- CDF of digital model: 2.195E-7

When only a part of the trip signal generation is considered, the unavailability of a digital RPS is much less than that of an analog RPS. This is because the main contributors of the CDF are a failure of the sensors and trip circuit breakers, which occupy around 70%.



| No | Value | F-V | Acc. | BE#1 | BE#2 | BE#3 | BE#4 | BE#5 |
|---|---|---|---|---|---|---|---|---|
| 1 | 1.632e-7 | 0.743509 | 0.743509 | %IE | RPOPVTRIP-ALT | RPRBW | | |
| 2 | 2.938e-8 | 0.133877 | 0.877386 | %IE | RPOPHTRIP | RPPMWCP | RPWDJCCF | |
| 3 | 1.037e-8 | 0.047231 | 0.924617 | %IE | RPOMW | RPOPHTRIP | | |
| 4 | 5.278e-9 | 0.024049 | 0.948666 | %IE | PNMLKPT101ABCI | RPOPHTRIP | | |
| 5 | 5.220e-9 | 0.023782 | 0.972448 | %IE | RPIMW | RPOPHTRIP | | |
| 6 | 1.837e-9 | 0.008371 | 0.980819 | %IE | RPOPVTRIP-ALT | RPSHW | RPUVW | |
| 7 | 1.467e-9 | 0.006686 | 0.987505 | %IE | RPOPHTRIP | RPPMWBP | RPPMWBPFTT | |
| 8 | 9.470e-10 | 0.004315 | 0.991820 | %IE | RCPTKPT101ABCI | RPOPHTRIP | | |
| 9 | 6.931e-10 | 0.003158 | 0.994978 | %IE | RPOPVTRIP-ALT | RPRBDA | RPRBDC | |
| 10 | 6.931e-10 | 0.003158 | 0.998136 | %IE | RPOPVTRIP-ALT | RPRBDB | RPRBDD | |
| 11 | 4.701e-11 | 0.000214 | 0.998350 | %IE | RPMWW | RPPMWCP | RPWDJCCF | |
| 12 | 4.335e-11 | 0.000197 | 0.998548 | %IE | RCPTYPT101A | RCPTYPT101B | RCPTYPT101C | RPOPHTRIP |

Fig. 4. Minimal Cut-Set of the digital RPS FT model

## 4. Conclusions

In this work, the effect of a digital RPS was evaluated by comparing it to that of an analog RPS based on the FT models. In the evaluation results, it was observed that digital RPS has a positive effect on reducing the system unavailability. The analysis results can be used for the development of a guide for evaluating digital I&C systems and reliability requirements.

## REFERENCES

[1] S. J. Lee, J. G. Choi, H. G. Kang, 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, p. 1527-1533, 2010.

[2] H. G. Kang, M. C. Kim, S. J. Lee, H. J. Lee, H. S. Eom, J. G. Choi, and S. C. Jang, An overview of risk quantification issues of digitalized nuclear power plants using static fault tree, Nuclear Engineering and Technology, Vol. 41, p. 849-858, 2009.

[3] H. G. Kang and T. Sung, A quantitative study on important factors of the PSA of safety-critical digital systems, Nuclear Engineering and Technology, Vol. 33, p. 596-604, 2001.

[4] H. G. Kang, T. Sung, An analysis of safety-critical digital systems for risk-informed design, Reliability Engineering and System Safety, Vol. 78, p. 307-14, 2002.