Quantitative Effect Analysis of Input Diversities for ESF Component Actuation Signal

Hyun Gook Kang • Seung-Cheol Jang
Integrated Safety Assessment Team, Korea Atomic Energy Research Institute
P.O. Box 105, Yuseong, Daejeon, 305-600, Korea
hgkang@kaeri.re.kr

1. Introduction

In recent years many nuclear power plants have adopted modern digital I&C technologies since they are expected to significantly improve their performance and safety. OPR1000 in Korea (Korean standard nuclear power plant), typically Ulchin 5 & 6 nuclear units, have adopted safety-critical digital systems due to the functional advantages of smart digital systems and the obsolescence of the traditional analog components.

Recently, in Korea, there are several important industrial projects aiming at the development of digitalized safety-signal generation system for nuclear power plants. Among them, one of the most active research programs, Korean Nuclear I&C System (KNICS) project produced a new design of the engineered safety feature (ESF) component control system (CCS) based on newly developed microprocessor-based modules. Notable advances of this ESF-CCS design are active applications of new technologies: the in-module-test mechanism, the hot-standby redundancy, and the network communication technology for safety signal generation.

In this study, we performed sensitivity study to quantify the unavailability of newly developed ESF-CCS. And a sensitivity analysis on the effect of input diversities on the component actuation signal unavailability is investigated.

2. ESF Signal Generation: ESF-CCS, DPS & DMA

The ESF-CCS provides automatic manipulation of corresponding ESF components which consist of safety pumps and valves. The ESF-CCS includes input, processor, output and network modules. The processor modules in the ESF-CCS system can be categorized into two levels: Group controller and loop controller. A group controller performs auctioneering by using four channel outputs from the plant protection system (PPS). If a specific ESF signal is generated based on the auctioneering results, the group controller provides information to loop controllers. A loop controller which receives signal from the group controller generates control signals for the field components such as safety pumps and valves. As shown in Figure 1, there are three group controllers and up to twelve loop controllers in a division of KNICS ESF-CCS. Each loop controller has hot-standby backup.

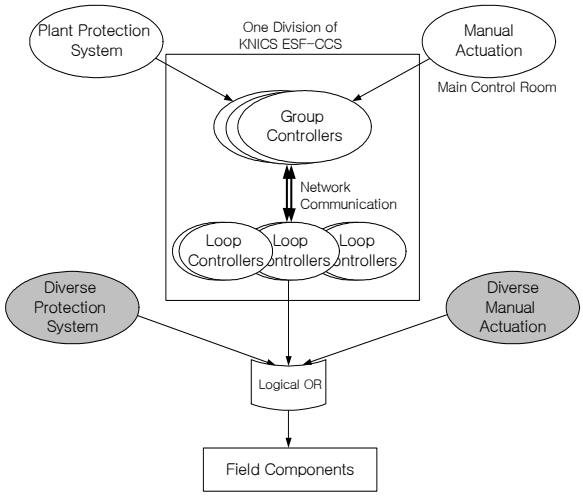

Figure 1. Conceptual layout and signal flow around KNICS ESF-CCS

There are two redundant input sources of the ESF-CCS: the PPS and an operator's manual actuation (MA). The group controllers' signals are processed in a loop controller based on two-out-of-three voting logic. When a loop controller receives more than two actuation signals, it generates the control signal. If the failure of a loop controller is detected by the group controller, the backup controller of corresponding group controller will take over the task.

In order to reduce the failure probability of field components' control signal, there are two more sources in addition to the ESF-CCS. Diverse protection system (DPS) is independent and separated system for automatic signal generation. Diverse manual actuation (DMA) provides a redundant mean for the operator in the main control room to access the field components via hard-wired path.

3. Fault-Tree Model Development and Quantification

The assumptions used in the model can be summarized as follows:

- Generally, the fault coverage of processor-to-processor (PTP) monitoring is much higher than that of watchdog timer (WDT) monitoring because the PTP monitoring method usually adopts much more sophisticated algorithms [1]. Since the coverage of WDT monitoring

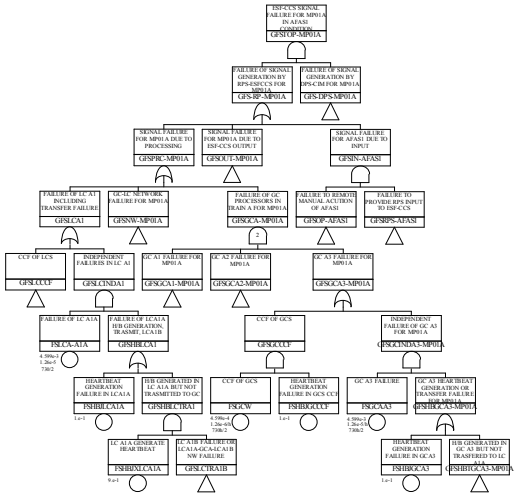

Figure 2. Typical top logic of the developed fault tree

could be assumed as around 0.5 [2], we assumed that the PTP monitoring coverage to be 0.9.

- We ignore the probability of software failure in the controllers.
- If a failure of network communication occurs, a controller is assumed to fail to detect the failure of other controller(s). The loop controllers are assumed to fail when they lose communication with the group controllers.
- We assume that the components are tested at least once per month and ignore the effect of automatic tests.
- Once the operator fails to initiate the signal (MA failure), we do not give credit to the DMA.

The top event of the developed model is the failure actuation signal for field component. Figure 2 shows one of the developed fault tree. The fault tree is constructed and the minimal cutsets are determined by using the KIRAP, an integrated safety assessment software package developed at KAERI. For the newly developed digital modules by the KNICS, we use their failure probability data in a KNICS design document [3]. For the conventional analog equipment and sensors, the generic data updated by KAERI [4] is used.

We performed sensitivity study for quantifying the effect of two kinds of input diversities: manual actuation method diversity and automated system diversity. The results are summarized in Table 1. The failure probability of MA and DMA are assumed to be 0.05 and 0.1, respectively. Gray-colored cell indicates the case of no input redundancy.

Usually, the order of magnitude of the failure probability of active components such as pumps and valves is 1.0E-3. The quantification results show that the failure probabilities of the safety signals are quite high in the case of no input redundancy. With input diversity, the actuation signal failure probabilities become low. The difference between the best signal unavailability and worst one is very severe (around 500 times).

The result implies that the careful design of input diversity is very important. If the operators manipulate field components directly and they are well trained for this task, the risk from signal failure could be reduced effectively.

Table 1. The quantification results

ESF signal	SIAS	AFAS-1
DPS	X	O
Input sensor(s)	Pressurizer pressure Containment pressure	Steam generator level
Signal Unavailability (w/o MA, DMA)	4.78E-3	1.17E-4
Signal Unavailability (w/ MA, w/oDMA)	2.34E-3	7.95E-5
Signal Unavailability (w/ MA, DMA)	3.49E-4	9.71E-6

5. Conclusion

Based on fault-tree models developed to assess the failure probability of the ESF component actuation, we performed quantitative analysis on the effect of input diversities. Without input diversities, the results show that the failure probability of signal generation is too high to use in safety-critical application in nuclear plants. The application of diversity in the automatic signal generation system and that in the access path of human operators effectively improves the signal failure probability.

Acknowledgement

This work has been carried out under the Nuclear R&D Program supported by MOST

REFERENCES

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

[2] Kim, S.J., Seong, P.H. Lee, J.S., Kim, M.C., Kang, H.G. & Jang, S.C., A method for evaluating fault coverage using simulated fault injection for digitalized systems in nuclear power plants , *Reliability Engineering and System Safety* 91(5): 614-623, 2006.

[3] Choi, J.K. et al., 2004, *RPS unavailability analysis*, KNICS-RPS-AR103. Rev. 02, Korea Atomic Energy Research Institute.

[4] Min, K.R. et al. 2002, *Reliability Study: KSNPP Reactor Protection System*, KAERI/TR-2164/02, Korea Atomic Energy Research Institute.