Fault Tree Model of Human Error Based on Error-Forcing Contexts

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

1. Introduction

In the safety-critical systems such as nuclear power plants, the safety-feature actuation is fully automated. In emergency case, the human operator could also play the role of a backup for automated systems. That is, the failure of safety-feature-actuation signal generation implies the concurrent failure of automated systems and that of manual actuation. The human operator's manual actuation failure is largely affected by error-forcing contexts (EFC). The failures of sensors and automated systems are most important ones [1].

The sensors, the automated actuation system and the human operators are correlated in a complex manner and hard to develop a proper model. In this paper, we will explain the condition-based human reliability assessment (CBHRA) method in order to treat these complicated conditions in a practical way. In this study, we apply the CBHRA method to the manual actuation of safety features such as reactor trip and safety injection in Korean Standard Nuclear Power Plants.

2. Condition-Based HRA

The unsafe action (UA) of human operator is affected by EFCs including the unavailability of information sources. In the PSA accident scenario (L), for sensors (S) and automatic systems (A), in consideration that the failure of automatic system implies the failure of safety signal generation and the loss of alarms, the signal generation failure probability (F) is calculated as:

$$F = \sum_i \sum_j P(UA \mid A_i, S_j) P(A_i \mid L, S_j) P(S_j \mid L)$$
$$= \sum_i \sum_j P(UA \mid A_i, S_j) P(A_i \mid L, S_j) P(S_j)$$

The relationship among human operators, automatic systems, and instrumentation sensors is illustrated in Figure 1. Based on fault tree method, in order to take in the human error probability (HEP) issue with conditional events in a more effective manner, we propose following steps for CBHRA:

(1) Conducting an investigation into possible EFCs

(2) Selecting important EFCs

(3) Developing a set of conditions in consideration of selected EFCs

(4) Estimating the HEP for each condition

(5) Constructing fault tree model with flag events (FE) which represent the developed condition set

(6) Obtaining minimal cut sets (MCS) by solving the fault tree

(7) Conducting the conditioning process with the FEs

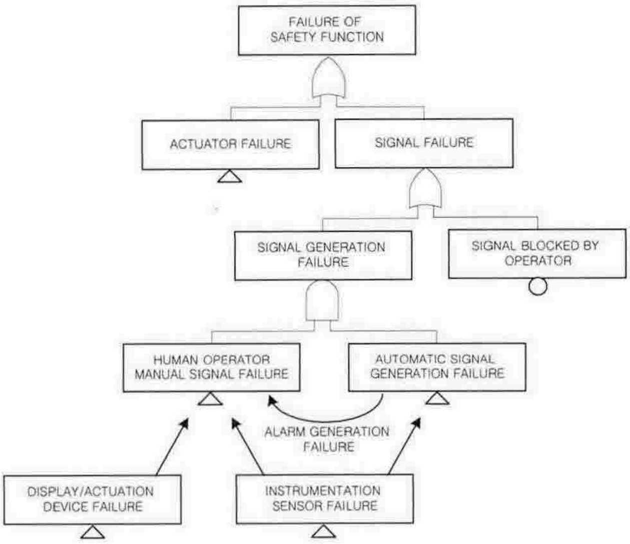
FAILURE OF SAFETY FUNCTION
ACTUATOR FAILURE
SIGNAL FAILURE
SIGNAL GENERATION FAILURE
SIGNAL BLOCKED BY OPERATOR
HUMAN OPERATOR MANUAL SIGNAL FAILURE
AUTOMATIC SIGNAL GENERATION FAILURE
ALARM GENERATION FAILURE
DISPLAY/ACTUATION DEVICE FAILURE
INSTRUMENTATION SENSOR FAILURE

Figure 1. The schematic of the concept of the safety function failure mechanism

Figure 2 shows a typical fault tree for the CBHRA with the FEs and the corresponding HEPs based on the concept in Figure 1. For the error of omission (EOO), we set the value of a proper FLAG at logical true and those of the other FLAGs at false. This process results in selecting one MCS for each MCS group and eliminating the other MCSs.

On the other hand, for the error of commission (EOC), in order to distinguish the groups, the investigation into the event of 'signal generation success' is necessary. Generally, when a negation gate is used in the fault tree model, it is very hard to obtain corresponding MCSs because usual software packages require many resources and long time to solve the negation logics. Therefore, for the practical use, the model of single EOC event is preferable than the model of multiple EOC events. It is the reason that the fault tree in Figure 2 contains single EOC event. In addition to that, the probability of 'signal generation success' event could be assumed to be unit when the automated signal processing channels are highly reliable.

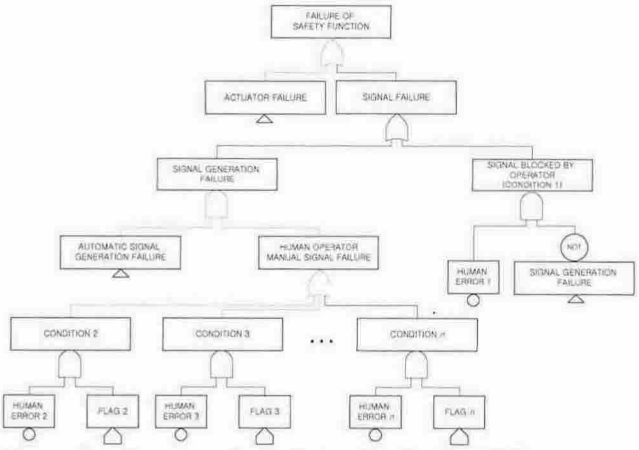
FAILURE OF SAFETY FUNCTION
ACTUATOR FAILURE
SIGNAL FAILURE
SIGNAL GENERATION FAILURE
SIGNAL BLOCKED BY OPERATOR (CONDITION 1)
AUTOMATIC SIGNAL GENERATION FAILURE
HUMAN OPERATOR MANUAL SIGNAL FAILURE
HUMAN ERROR 1
NOT
SIGNAL GENERATION FAILURE
CONDITION 2
CONDITION 3
. . .
CONDITION n
HUMAN ERROR 2
FLAG 2
HUMAN ERROR 3
FLAG 3
HUMAN ERROR n
FLAG n

Figure 2. An example fault tree for the CBHRA

3. Application of CBHRA to KSNPP Safety Signal Generation

In this study, two kinds of target safety signals are considered: Reactor trip signal and engineered-safety-feature (ESF) actuation signals which are the most important signals considered in the safety assessment of the KSNPP. The effective categorization of EFCs into several condition groups is the key of successful modeling. If we consider every status of the signal processing system or instrumentation channels, there will be too many conditions to be modeled in the fault tree. In consideration of availability of indications (sensors) and alarms, we categorized EFCs.

There are two cases for grouping: Single-parameter safety signals and multiple-parameter safety signals. As a typical single-parameter safety signal, we consider the auxiliary-feed-water-actuation signal (AFAS). With several assumptions, its EFCs are categorized into three groups. The reactor trip signal in the case of small LOCA is considered for representing the multiple-parameter safety signal and its EFCs are categorized into five groups.

We conducted interviews with three HRA experts in order to estimate the operator's time consumption due to the unavailability of information for each condition group. The EOC probability ('Human Error 1' event) in Figure 2 is not considered in this study. Based on the experts' opinion, the HEPs of manual safety signal actuation are determined using the performance curve of the THERP methodology [2]. In order to see the effect of the HEP variation, we also performed sensitivity study. From the conventional case to the 10% of conventional available time case, totally seven cases are inspected. The results are graphically illustrated as in Figure 3 and 4.

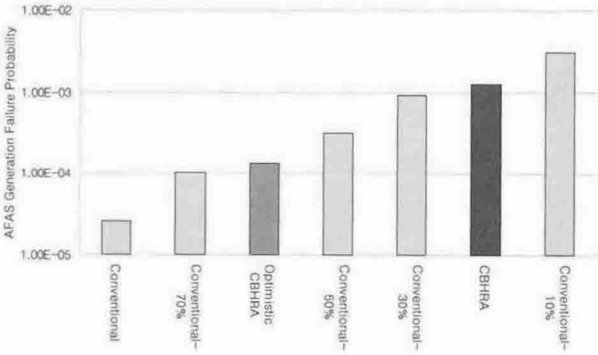

Figure 3. The AFAS generation failure probability

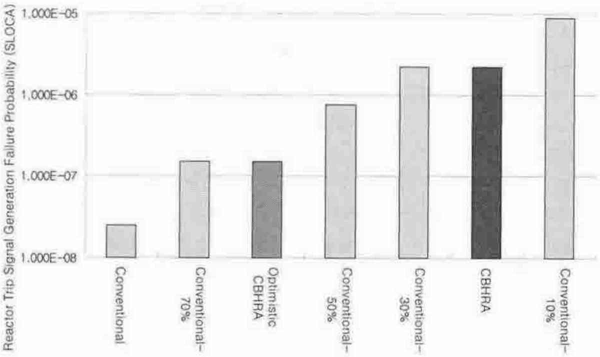

Figure 4. The reactor trip signal generation failure probability in the case of small LOCA

4. Conclusion

In this paper, we propose the CBHRA method in order to treat complicated conditions of human error in a practical way. We also compare the results of CBHRA with those of the conventional models. They show the difference up to hundred times. Based on the result of this study, the necessity of the CBHRA application to the single-parameter safety signal should be emphasized. Even in the case of multiple-parameter safety signal, the EFC of human error should also be carefully investigated.

The analysis on the effect of human error estimation to the plant risk is recommended as a further study.

Acknowledgement

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

REFERENCES

[1] H.G. Kang, et al., "Analysis on Manual Actuation Failure and Risk Effect," Proceeding of NPIC&HMIT 2004, Columbus, Ohio, September, 2004.

[2] Swain, A.D., Guttmann, H.E, 1983. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278.