# Fault tree modeling for dependency of human failure events in PSA

Ji Suk Kim [a], Sang Hoon Han [b], Man Cheol Kim [a*]
[a]*Department of Energy Engineering, Chung-Ang University, 84 Heukseok-ro, Dongjak-gu, Seoul, South Korea*
[b]*Korea Atomic Energy Research Institute, 989-111 Daedeok-daero, Yuseong-gu, Daejeon, 34057, South Korea*
[*]*Corresponding author: charleskim@cau.ac.kr*

## 1. Introduction

In probabilistic safety assessment (PSA), human failure events (HFEs) are modeled as basic events and are added to the fault trees of related systems, components, and functions. Human error probabilities are estimated with human reliability analysis (HRA) methods such as THERP, ASEP and HCR.[1]

There are pre-initiator human failure event and post-initiator human failure event as suggested by the HRA requirements of ASME PRA Standard [2] and NEI PRA Peer Review Guideline [3]. The former is a human error that may occur during routine actions and includes maintenance errors, testing errors and calibration errors. The latter includes human errors after an initiating event. ASME PRA Standard [2] and KAERI/TR-2961/2005 [1] also suggest that potential dependency among HFEs in a same accident scenario should be evaluated. This is because previous human failures event may affect subsequent HFEs.

Dependencies among HFEs are generally reflected in a PSA model using the post-processing of minimal cut sets. In this paper, we develop the fault tree modeling of human failure event dependencies using if-then-else (ITE). The basic idea was initially proposed by Korea Atomic Energy Research Institute (KAERI). We believe that this new method can supplement the limitations of the existing method using the post-processing of minimal cut sets.

## 2. Modeling of human failure events

There are three types of post-initiator HFEs: emergency actions, backup actions, and recovery actions [1]. Emergency actions are closely related to accident scenarios. In general, multiple actions can be represented as a single human failure event, indicating a failure of higher-level system or function. An example is the feed and bleed operation that includes the actions of starting safety injection and opening the pressurizer relief valves [4]. NUREG-1792 [4] recommends that HFEs be modeled in a location close to the relevant components, system, and function. The emergency actions are usually modeled at the top of a fault tree linked to an event tree branch. Backup actions are those operator actions for generating manual actuation signals when automatic actuation signals are not generated. These HFEs are modeled with AND logic with automatic signal generation functions. When manual operation of a standby system is required, it can be modeled with OR logic. An example of a recovery actions is the recovery of motor-operated valves in local. Depending on accident scenarios, whether the possibility of the recovery is reviewed and it is reflected through the post-processing of minimal cut sets.

If there is dependency among two or more HFEs in a minimal cut set, the human error probability of the subsequent events should be recalculated by reflecting the dependency. Post-processing is a method of replacing HFEs in a minimal cut set according to specified rules. New probabilities can be applied to the newly introduced HFEs. Post-processed minimal cut sets cannot be propagated to fault trees.

## 3. Fault tree modeling for dependency of human failure events

In this section, we introduce the ITE-based modeling method for dependent HFEs in a fault tree. This fault tree modeling method can be applied to the HFEs shown in Fig. 1. There are the post-initiator HFEs such as the emergency actions as mentioned in Section 2.

In Fig. 1, those events with ‘BE-’ represent the failure of component, system, or function and those event with ‘OP-’ represent HFEs. It is assumed that the subjects and sequences of HFEs and the dependency among the events have already been identified by reviewing accident sequences.

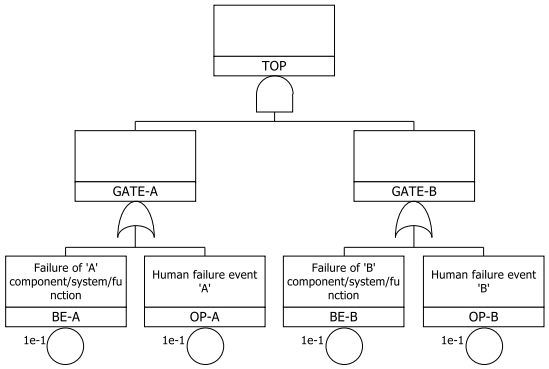


Fig. 1. An example of modeling of HFEs

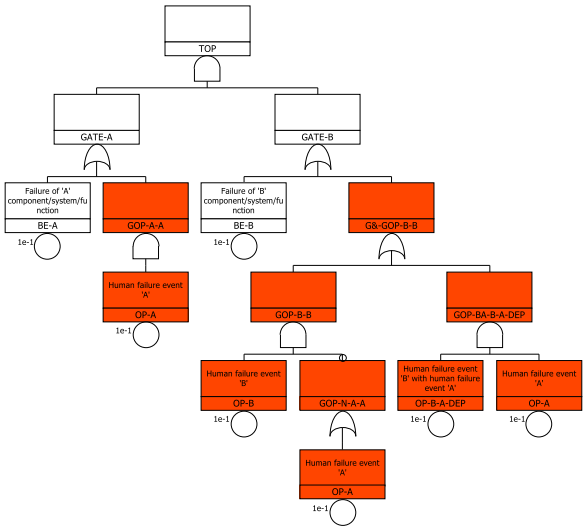


Fig. 2. ITE-based fault tree modeling of two HFEs and their dependency

The dependency of HFEs can be modeled using ITE as shown in Fig. 2. If there is not 'OP-A', 'OP-B' can be used as its original form. If there is 'OP-A', 'OP-B' is replaced with 'OP-B-A-DEP' to reflect the dependency between the two HFEs. The minimal cut sets derived from Fig. 2 is same as the result of post-processing as shown in Table I.

Table I: Comparison of the quantification results of ITE-based fault tree modeling and post-processing of minimal cut sets to reflect the dependency of two HFEs

| ITE-based fault tree modeling | | | Post-processing | | |
|---|---|---|---|---|---|
| Value | #BE1 | #BE2 | Value | #BE1 | #BE2 |
| 1E-02 | BE-A | BE-B | 1E-02 | BE-A | BE-B |
| 1E-02 | BE-B | OP-A | 1E-02 | BE-B | OP-A |
| 1E-02 | BE-A | OP-B | 1E-02 | BE-A | OP-B |
| 1E-02 | OP-A | OP-B-A-DEP | 1E-02 | OP-A | OP-B-A-DEP |

Fig. 3 shows the ITE-based fault tree modeling for the dependency among three HFEs. 'Gate-A' and 'Gate-B' is same as in Fig. 2. The result of quantification is in Table II.

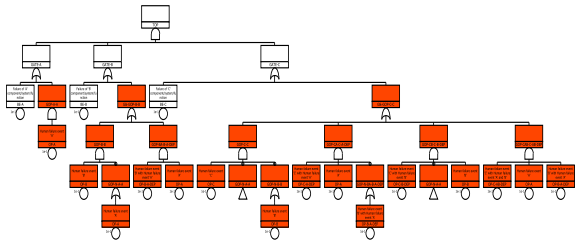

Fig. 3. ITE-based fault tree modeling of three HFEs and their dependency

Table II: Quantification result of ITE-based fault tree modeling to reflect the dependency of three HFEs

| Fault tree modeling | | | |
|---|---|---|---|
| Value | #Basic event 1 | #Basic event 2 | #Basic event 3 |
| 1.00E-03 | BE-A | BE-B | BE-C |
| 1.00E-03 | OP-A | BE-B | BE-C |
| 1.00E-03 | BE-A | OP-B | BE-C |
| 1.00E-03 | BE-A | BE-B | OP-C |
| 1.00E-03 | OP-A | BE-B | OP-C-A-DEP |
| 1.00E-03 | BE-A | OP-B | OP-C-B-DEP |
| 1.00E-03 | OP-A | OP-B-A-DEP | BE-C |
| 1.00E-03 | OP-A | OP-B-A-DEP | OP-C-AB-DEP |

By directly modeling the dependency of HFEs in a fault tree, it is possible to propagate the minimal cut sets to the fault tree. It facilitates the review of minimal cut sets. This method can be more generalized by using scripts such as the SIMA rule in AIMS-PSA. The dependencies of more than three HFEs can be easily reflected.

## 4. Conclusions and further work

It is important to properly consider the dependency among HFEs so that the impact of them are not underestimated. Reviewing minimal cut sets in PSA is also one of the important tasks to maintain the logical validity of PSA models. It may be easier to reflect the dependency of HFEs using post-processing, but the post-processing-based method makes it difficult to review minimal cut sets. If the dependency of HFEs is directly modeled in a fault tree using the ITE-based method, minimal cut sets can be propagated in fault trees, making it easier to review the minimal cut sets. In addition, the existing method cannot reflect the dependency of HFEs when minimal cut sets are cut off before being subject to post-processing. The ITE-based dependency modeling in fault trees would not inappropriately cut off such minimal cut sets because the minimal cut sets are identified after the dependency is applied in the logic of the fault tree.

The ITE-based dependency modeling in a fault tree described in this paper can be applied to the emergency actions shown in Fig. 1. Further work is needed on the method so that it can be generalized and applied to backup actions and recovery actions.

## REFERENCES

[1] W. D. Jung, D. I. Kang, J. W. Kim, "Development of A Standard Method for Human Reliability Analysis(HRA) of Nuclear Power Plants – Level 1 PSA Full Power Internal HRA - ", KAERI/TR-2961/2005, Korea Atomic Energy Research Institute, 2005.
[2] ASME, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications", ASME RA-S-2002, American Society of Mechanical Engineers, 2002.
[3] NEI, "Probabilistic Risk Assessment Peer Review Process Guidance", NEI 00-02, Nuclear Energy Institute, 2000.
[4] USNRC, "Good Practices for Implementing Human Reliability Analysis (HRA)", NUREG-1792, United States Nuclear Regulatory Commission, 2005.