Method to Find Recovery Event Combinations in Probabilistic Safety Assessment

Woo Sik Jung [a*], Jeff Riley[b]
[a] *Sejong University, 209 Neungdong-Ro, Gwangjin-Gu, Seoul 143-747, South Korea*
[b]*Electric Power Research Institute, 3420 Hillview Avenue, Palo Alto, CA 94304, USA*
[*]*Corresponding author: woosjung@sejong.ac.kr*

1. Introduction

Probabilistic Safety Assessment (PSA) has developed over the last 35 years into a fairly standardized and rigorous activity that is used routinely by utilities that operate nuclear power plants. The continued development and application of this technology requires ongoing research activities to identify improved methods to more efficiently address known limitations in the methods, as well as incorporating new methods that take advantage of new and upcoming computational resources.

EPRI has several research activities that address PSA methods development in a variety of specific targeted areas, such as fire and seismic risk, human reliability, or component data collection. These research activities may develop mathematical methods, engineering analyses, and business processes.

The research activities of the project covered by this scope are directed toward the specific issues of implementing the methods and strategies on a computational platform, identifying the features and enhancements to EPRI tools that would be necessary to realize significant improvements to the risk assessments performed by the end user.

Fault tree analysis is extensively and successfully applied to the risk assessment of safety-critical systems such as nuclear, chemical and aerospace systems. The fault tree analysis is being used together with an event tree analysis in PSA of nuclear power plants. Fault tree solvers for a PSA are mostly based on the cutset-based algorithm. They generate minimal cut sets (MCSs) from a fault tree. The most popular fault tree solver in the PSA industry is FTREX.

During the course of this project, certain technical issues (see Sections 2 to 5) have been identified that need to be addressed regarding how minimal cut sets are generated and quantified. The objective of this scope of the work was to develop new methods or techniques to address these technical limitations.

2. Issues

In a PSA, minimal cut sets (MCSs) that reflect accident sequences of nuclear power plant are generated using fault tree and event tree logic. Minimal cut set is defined as a minimal set of component/equipment/ function failures that results in an undesired condition of a nuclear power plant such as core damage. A typical minimal cut set for core damage represents an accident sequence that consists of (1) an initiating event, (2) basic events (component failures of mitigation systems), and (3) recovery events (failures of operator actions). The recovery event is a human reliability analysis event (or HRA event) that the operator fails to restore one or more failed components in the minimal cut sets. The probability of recovery event is a human error probability (HEP).

Please note that current human reliability analysis (HRA) methods expect that the PSA analyst finds whole significant combinations of recovery events in minimal cut sets so that dependencies among recovery events in each minimal cut sets should be analyzed and evaluated. Nominally, the detection of recovery event combinations is done by setting all the HEPs to 1.0 and then solving the logic by FTREX, then extracting the minimal cut sets containing two or more recovery events. Here is a practical question "is there a better way to do this?" or "is there a way to get all of the combinations of recovery events that are significant without solving the entire fault tree or with efficiently solving the fault tree?".

2. Method to find recovery event combinations

Let us illustrate a fault tree that has recovery events.

$$\begin{aligned} CDF &= G1 + G4 \\ G1 &= G2 * G3 \\ G2 &= A * B + A * C + B * C \\ G3 &= H1 * H2 + H1 * H3 \\ G4 &= A * B * C * H2 * H3 \ . \end{aligned} \quad (1)$$

Here, $\{H1, H2, H3\}$ are recovery events, and $\{A, B, C\}$ are random failure events that require operator actions $\{H1, H2, H3\}$. In a real PSA fault tree for core damage, it is not easy to generate minimal cut sets after setting recovery event probabilities to the value 1.0. So, a new method is developed in this study. The developed method is as follows:

(Step 1)
Generate minimal cut sets after setting all the recovery events $\{H1, H2, H3\}$ to TRUE. Please note that the last cut set $\{A\ B\ C\ H2\ H3\}$ in Eq. (1) is subsumed into the other minimal cut sets.

$$CDF = A\ B + A\ C + B\ C\ . \quad (2)$$

(Step 2)
Develop mapping equations between events and minimal cut sets as

$$A = \%M1 + \%M2 + \%N$$
$$B = \%M1 + \%M3 + \%N \quad (3)$$
$$C = \%M2 + \%M3 + \%N\ .$$

Here, new initiating events $\{\%M1, \%M2, \%M3\}$ are introduced for indexing minimal cut sets, and $\%N$ is a dummy index for the minimal cut set(s) that is not in Eq. (2). Please note that the last cut set $\{A\ B\ C\ H2\ H3\}$ in Eq. (1) is subsumed into the other minimal cut sets in Eq. (2).

$$\%M1 = A\ B$$
$$\%M2 = A\ C \quad (4)$$
$$\%M3 = B\ C$$
$$\%N = \text{dummy initiator.}$$

Here, $\%N$ is a dummy initiator for cutsets such as $\{A\ B\ C\ H2\ H3\}$ that is subsumed in Eq. (2).

Probabilities/frequencies of the new initiating events are

$$P(\%M1) = P(A\ B)$$
$$P(\%M2) = P(A\ C) \quad (5)$$
$$P(\%M3) = P(B\ C)$$
$$P(\%N) = Max\big(P(\%M1), P(\%M2), P(\%M3)\big)\ .$$

As shown in Eqs. (2) to (4), basic event A is in the two minimal cut sets $\{\%M1, \%M2\}$, basic event B is in the two minimal cut sets $\{\%M1, \%M3\}$, and basic event C is also in the two minimal cut sets $\{\%M2, \%M3\}$.

(Step 3)

Replace events $\{A, B, C\}$ in a fault tree with mapping in Eq. (4). That is, events $\{A, B, C\}$ become gates in a new fault tree.

$$CDF = G1 + G4$$
$$G1 = G2 * G3$$
$$G2 = A * B + A * C + B * C$$
$$G3 = H1 * H2 + H1 * H3 \quad (6)$$
$$G4 = A * B * C * H2 * H3$$
$$A = \%M1 + \%M2 + \%N$$
$$B = \%M1 + \%M3 + \%N$$
$$C = \%M2 + \%M3 + \%N\ .$$

(Step 4)

Generate minimal cut sets. If this fault tree is solved, generated minimal cut sets are

$$CDF = (\%M1 + \%M2 + \%M3 + \%N)$$
$$(H1H2 + H1\ H3) + \%N\ H2\ H3\ . \quad (7)$$

If the fault tree is so complex that it cannot be solved, individual minimal cut sets for each member of $\{\%M1, \%M2, \%M3\}$ are generated by turning off all the other cutset initiators. For example, if the fault tree is solved for $\%M1$ after setting $\{\%M2, \%M3, \%N\}$ to FALSE, the final minimal cut sets are

$$CDF = \%M1\ (H1H2 + H1H3)\ . \quad (8)$$

Similarly, if the fault tree is solved for $\{\%M1, \%M2\}$ after setting $\{\%M3, \%N\}$ to FALSE, the final minimal cut sets are

$$CDF = (\%M1 + \%M2)\ (H1H2 + H1H3) \quad (9)$$

If the fault tree is solved for $\%N$ after setting $\{\%M1, \%M2, \%M3\}$ to FALSE, the final minimal cut sets are

$$CDF = \%N(H1H2 + H1H3 + H2H3) \quad (10)$$

Please note that there is no way to get part of minimal cut sets by turning off/on the events in the original fault tree. If the minimal cut sets are calculated after setting events except for $\{A, B, C\}$ in $\{\%M1, \%M2\}$ to FALSE, the minimal cut set of $\{\%M3\}$ is additionally calculated. Due to this side effect, there is no way to get the minimal cut sets in Eq. (9) with the original fault tree in Eq. (1). It shows the strength of this method.

3. Conclusions

As explained in the previous Sections, the developed method is very flexible and very effective in order to generate the combinations of recovery events and fire failure events in the minimal cut sets. The strengths of the developed method are summarized as

1. By turning on all the cutset initiators $\{\%M1, \%M2, \%M3, \%N\}$, all the possible minimal cut sets can be calculated easier than with the original fault tree. It is accomplished by the fact that the number of events in the minimal cut sets are significantly reduced by using cutset initiators instead of random failure events.
2. By turning on a few chosen cutset initiators and turning off the other cutset initiators, minimal cut sets of the selected cutset initiator(s) can be easily calculated. As explained in the previous Sections, there is no way to calculate these minimal cut sets by turning off/on the random failure events in the original fault tree.
3. It is easy to implement the developed method into any fault tree solver by appending mapping equations between random failure events and minimal cut sets to the given fault tree, and selectively turning off/on the cutset initiators

REFERENCES

[1] W. S. Jung, Development of algorithms to detect recovery event combinations and fire failure event combinations in MCSs, White Paper, Sejong University, December 31, 2015.