STUDY ON INFLUENCE OF CCF MODELING IN IE FAULT TREES IN RISK MONITOR PSA MODEL OF NUCLEAR POWER PLANTS

Hu Yuehua[1], Yi Yan[2], Xu Yiquan[1], Wang Jie[1], Zhang Qinfang[1], Zhang Wuhang[1], Qian Yalana[1]

[1] *Shanghai Nuclear Engineering Research & Design Institute CO.LTD, Shanghai, China*
[2] *Nuclear and Radiation Safety Center, Beijing, China*

ABSTRACT

Abstract: In the risk monitor PSA model of nuclear power plant, the initiating event frequency of loss of support system should be calculated by the fault tree method, with the initiating event fault tree linked to the risk monitor model to generate frequency-type results. There are two ways to model the IE fault trees, one is the single multiplier method and the other is the frequency-based basic event method. This paper makes a comparative study of the advantages and disadvantages of these two methods when applied in risk monitors and their influence on configuration risk management. The study shows that although the single multiplier method can reflect the influence of common cause factors on the frequency of initiating events when a certain equipment fails, the modeling of common cause is too conservative, and it may produce unreasonable cut sets and risk views that are not in accordance with the actual nuclear power plant conditions, and the frequency-type basic event method cannot reflect the influence of common cause factors on IE frequency. This paper presents a new modeling method combining the above two methods, which can reflect the influence of common cause factors on IE frequency when an important component fails, and avoid unreasonable risk views caused by excessive amplification of common cause contributions.

Keywords: PSA, Risk Monitor, Initiating Event Fault Tree, Common Cause Failure, Nuclear Power Plants

I. INTRODUCTION

According to the group standard of Nuclear Power Plant Configuration Risk Management Peer Review Guide (T/CNSCPA 011-2023) [1] in China, the risk monitor model should properly consider how nuclear power plant configuration changes affect the frequency of initiating events (IEs). Typically, for the loss of support system, the frequency of initiating events should be calculated by fault tree method, and the support system initiating event fault trees should be linked to the risk monitor model, simultaneously the calculation core damage frequency (CDF) result should be frequency type.

At present, there are two common cause failure (CCF) modeling methods in IE fault tree in the industry, one is single multiplier method, and the other is frequency-based basic event method. In the practice of peer review of configuration risk management in nuclear power plants, it is found that these two methods are prone to exaggerate or weaken the influence of component common cause failure on the risk of nuclear power plants, thus forming a risk opinion inconsistent with many years of operation experience of nuclear power plants. In this paper, a new modeling method is proposed. The analysis results show that this method can effectively solve the above problems.

II. EXISTING IE FAULT TREE CCF MODELING METHODS

II.A. Single Multiplier Method

In the initiating event frequency calculation model, the main models adopt a modeling method similar to the fault tree models of the mitigation system, which only contain probabilistic basic events whose names are consistent with those of the mitigation system, while only one time factor is set as a frequency-type event to convert the result to a frequency. (Figure 1.)

The fault tree model of the modeling method is relatively simplified. Because the basic event types and names are the same with mitigating systems' model, the common cause group can be established to calculate the common cause failure. The IE and mitigation fault trees of the same system use the same basic event coding to facilitate correlation analysis.

For the systems with the number of sub-trains greater than or equal to 3 and the number of normally operating trains greater than or equal to 2, it is impossible to distinguish the equipment with initial failure and the trains that play a mitigating role through the model. In order to ensure that the contribution of random failure to the frequency of the initiating event is reasonable, the multiplier should be multiplied by the number of combinations. At present, there are two practices in the industry, taking the multi-Greek Letter method (MGL) and two-stage CCF as examples:

1) One practice is that The multiplier is directly taken as 365 (days) ;

$$CCF\ frequency = \beta \times Q \times 365 \quad (/reactor\ year) \tag{1}$$

Among them:

β is a CCF MGL parameter, β factor in the MGL method is a conditional probability that the common cause of a component failure will be shared by one or more additional components;

Q is the failure probability of equipment demand failure or the operation failure probability within 24 hours.

2) Another practice is to increase the multiplier to consider the number of trains' combinations. For example, for the compressed air system with two trains operation and another two trains standby, the multiplier is 365 × 2 = 730.

$$CCF\ frequency = \beta \times Q \times 365 \times 2 \quad (/reactor\ year) \tag{2}$$

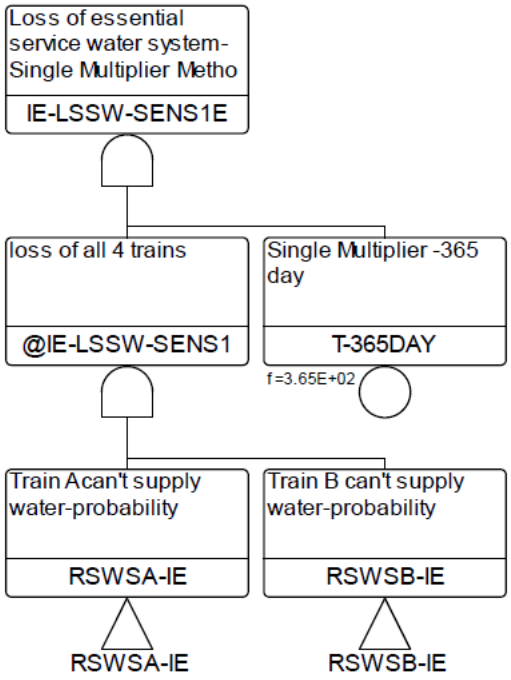

FIGURE 1. Example for Single Multiplier Method

These two practices consider the mission time of 1 year or several years for common cause failure, respectively. In particular, the second approach considers the mission time of several years, and overestimates the influence of common cause failure.

According to reference [2], in the risk monitor model, the common cause failure model may need to be improved so that it is able to take account of the reduction in redundancy when components are removed from service for maintenance and when failures have been identified.

In the risk monitor model, for two components considering the two-order common cause, when one component fails, Q = 1, according to the common cause processing method, the failure probability of another redundant component failure caused by the common cause will be replaced by the common cause parameter (such as β, which reflects the potential for a CCF to have occurred), and the quantitative results including CCF = β × 365 or CCF = β × 730 cutsets will appear. This kind of

cutsets further over-amplify the influence of common cause failure, and prone to inconsistent with the operation practice of nuclear power plants for many years.

Taking the component cooling water system and essential service water system of a nuclear power plant as an example, when the single multiplier method is used in the model, the risk monitor model results are shown in Table 1.

TABLE 1. Risk Assessment Example by Single Multiplier Method

Single Multiplier Method	CDF（/reactor year）	Risk Increase Factor	Risk Zone
If a component cooling water pump fails	3.42E-03	257	RED
If a service water pump fails	2.29E-03	172	RED

It can be seen from Table 1. that only one pump failure will cause the nuclear power plant to enter the risk unacceptable zone (RED zone) [3,4], which requires the measures such as shutdown the nuclear power plant being taken immediately. However, in this case, the technical specification of the nuclear power plant just requires that the faulty component should be restored to the operational state within 72 hours. The results of risk monitor are quite different with the requirements of technical specifications and nuclear power plant practice.

II.B. Frequency-type Basic Event Method

According to the industry standard 'ASME/ANS RA-Sb-2013' [5] HLR-IE-C10: If fault-tree modeling is used for initiating events, include all relevant event combinations in the IE fault tree models, such as the annual frequency of one component failure and the unavailability of other components (or failure during the repair time of the first component). In the IE fault tree model of this method, a frequency-based basic event is established for each component of the running train (the mission time is usually 1 year), while the remaining running trains or standby trains are probabilistic, and the mission time is 24 hours or the time required to repair the faulty train, i.e. the average maintenance time (MTTR), as shown in Fig. 2.

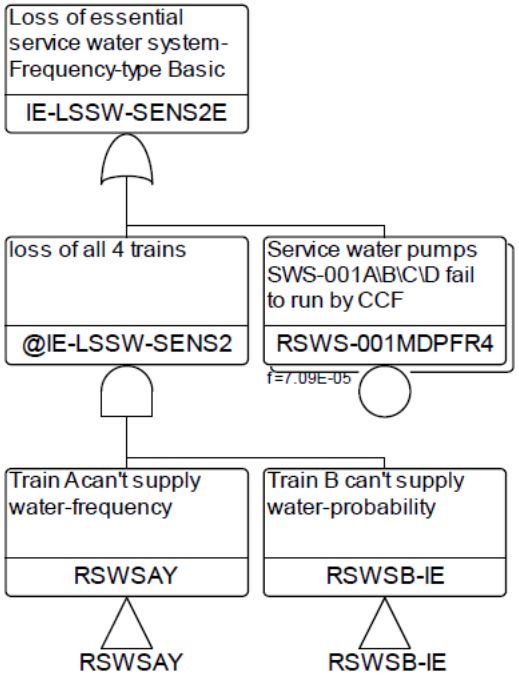

FIGURE 2. Example for Frequency-type Basic Event Method

The frequency of the IE fault tree top event is the sum of the frequencies of all frequency-type event groups, that is, only one frequency-type event is allowed in each cutset. Each cutset is composed of a frequency-type basic event and several probability-type basic events, and it is easy to distinguish the equipment with initial cause failure.

Because different types of basic events for different trains are used in this method, it is impossible to directly establish a common cause group, and additional CCF basic events need to be established. Taken the MGL method and two-order CCF as an example, the value of the common cause basic event $f_{CCF} = \beta \times \lambda \times T$ (where λ is the hourly running failure rate, T generally takes 8760 hours) is modeled as an independent frequency basic event. Therefore, in the application of risk monitor model, when a component is set to fail, the fault tree model cannot easily and intuitively reflect the change of the IE frequency caused by the common cause failure of the component.

Similarly, taking the component cooling water system and the essential service water system of a nuclear power plant as an example, the risk monitor model results are shown in Table 2 when the frequency-type basic event method is used in the model.

TABLE 2. Risk Assessment Example by Frequency-type Basic Event Method

Frequency-type Basic Event Method	CDF（/reactor year）	Risk Increase Factor	Risk Zone
If a component cooling water pump fails	1.57E-04	14.40	YELLOW
If a service water pump fails	4.81E-05	4.41	YELLOW

It can be seen from Table 2 that a pump failure will cause the nuclear power plant to enter the configuration risk management area (YELLOW area) [2, 3], which represent acceptable risk increases, provided that actions are taken to address non-quantifiable factors and establish risk-management actions that are appropriate to the configuration. Therefore, such configurations should not be treated as unsafe conditions to be avoided in all circumstances. The risk assessment results meet the requirements of the technical specifications and are in good agreement with the operation practice of the nuclear power plant. However, since the influence of CCF upon equipment failure only considers the increase in the failure probability of the mitigation system, without taking into account its impact on the CCF frequency of initiating events, the results tend to be overly optimistic

III. NEW INTEGRATION MODELING METHOD

According to the definition of common cause failure factor in NUREG/CR-5485[6], common cause failure factor is the conditional probability that a component failure will be shared by one or more additional components, indicating that the common cause parameter is a probabilistic parameter and has nothing to do with time duration.

Taking the common cause failure of two components of the same type in the IE fault tree as an example, if the MGL method is used to calculate the common cause failure probability, the common cause operation failure probability of the two components is:

$$\text{CCF frequency} = \beta \times Q = \beta \times \lambda \times T \text{ (/reactor year)} \quad (3)$$

Among them.

λ is the failure rate per hour.

β is a two-order common cause failure factor.

T = 8760h.

In the risk monitor model, the common cause failure probability after the failure of the operating equipment (i.e., Q = 1) should be :

$$CCF = \beta \times Q = \beta \quad (4)$$

It can be seen that in the risk monitor model, the failure of a component has a great influence on the frequency of initiating events, and it is easy to overestimate the influence of common cause failure on the risk of nuclear power plants.

In addition, according to the common cause failure data collection and statistical method given in Reference [7], in general, the common cause failure mainly refers to the failure of two or more similar components in the same system due to the same cause and failure mode within a selected period of time. In Reference [8], it is considered that the common cause failure should be considered when the standby or redundant equipment fails before the damaged equipment is repaired. Therefore, when calculating the IE frequency of the loss of the support system caused by the common cause, the time window is generally taken as the average maintenance time (MTTR) or 24 hours of the corresponding equipment. If the mission time of the common cause failure is taken as 1 year, it is too conservative and does not conform to the actual operation experience of the nuclear power plant. Only when the first failed component is repaired, the failure of the second same component due to the same cause and failure mode should be considered as the common cause of the initiating event. If the first failure component has been repaired before the second failure, even if the failure cause is a common cause factor, it does not cause the initiating event of loss of the support system.

The reference [8] also provides a recommended method for using the common cause parameters in the IE fault trees: one is to screen and remove the common cause events that do not cause the initiating event, and the other is to correct the common cause parameter. However, in the actual implementation process, both methods are difficult. The first method is limited to the difficulty of obtaining the details of the events collected in the CCF database, and the second method is limited to the difficulty of evaluating the selection method and rationality of the correction factor.

Reference [9] also suggests that it is necessary to correct the common cause parameters used in the initiating event fault tree. It is recommended to use the Bayesian updating method, but it is also necessary to correct the independent failure rate. The method proposed in this paper is also difficult in engineering application, especially when the IE fault trees need to interlink with the event trees and mitigation fault trees, because a basic event can't exist in different CCF groups simultaneously.

Therefore, according to the common cause failure analysis mechanism of IE fault tree in the above risk monitor model, a new integration modeling method is constructed. On the premise of using the existing common cause database, the above two methods in section 2 are combined, that is, one part adopts the single multiplier method, and the same basic events as those in the mitigation system fault trees are adopted in the IE fault trees, and the CCF groups are established to consider the common cause failure. The multiplier can be taken as the allowed maintenance time required by the technical specification, MTTR or mission time of level 1 PSA (usually 1 day). The other part adopts the frequency-based basic event method, in this part, the frequency-based basic events are established for the initial cause sub-train, and their frequencies are calculated by (365-the number of days corresponding to the multiplier)×failure rate per hour × 24. The same probability-based basic events as the mitigation system fault trees are established for the remaining sub-trains, without using additional CCF basic events but using the same CCF groups as those established in the mitigating system fault trees. The two parts are connected by OR gate to construct an IE fault tree, which can be interlinked with the corresponding event tree and mitigation fault trees, as shown in Figure 3.

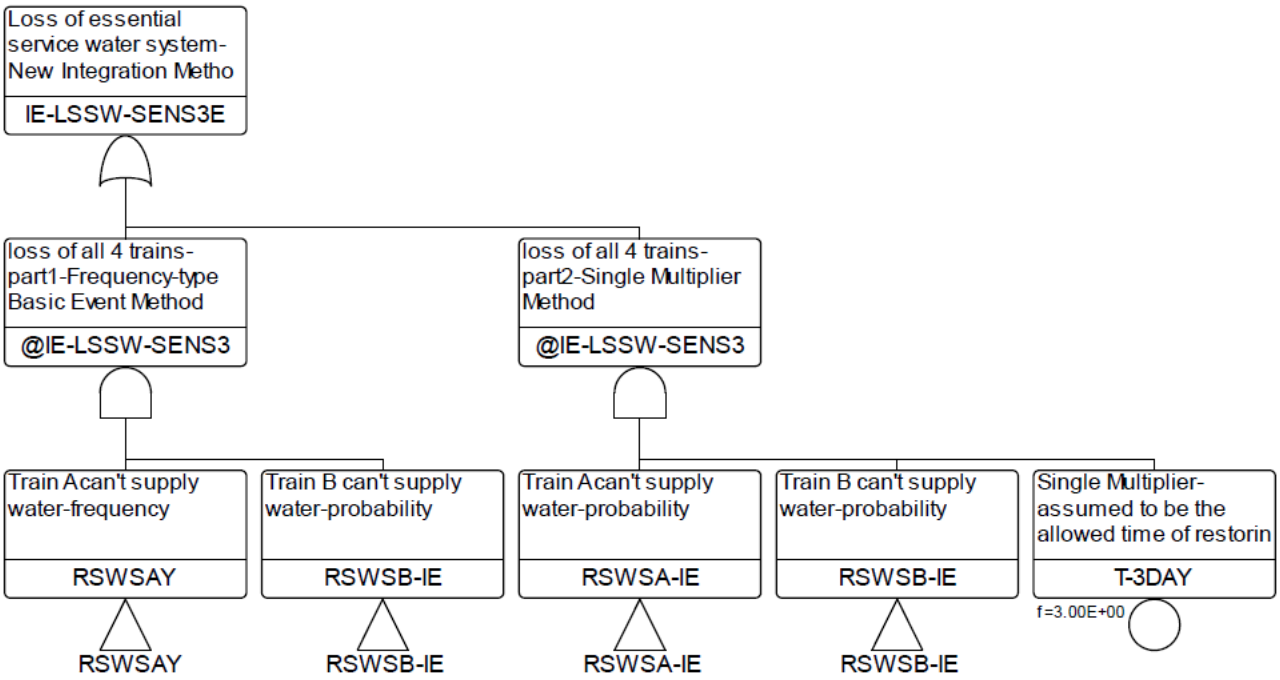

FIGURE 3. Example for New Integration Method

This modeling method matches the mechanism of common cause failure analysis, and can reflect the influence of common cause factors on the IE frequency change caused by the CCF in the IE fault tree after the failure of a component. It also avoids overestimating CCF influence and provides risk insights more consistent with nuclear power plant operational practices.

Similarly, taking the component cooling water system and the essential service water system of a nuclear power plant as examples, the risk monitor model results are shown in Table 3 when the new integration modeling method is used in the

model. Since it considers both the impact of equipment failure on the increased probability of mitigation system failure caused by CCF and the impact on the increased frequency of initiating events caused by CCF, the results show a slight increase compared with Table 2.

It can be seen from Table 3 that a pump failure will cause the nuclear power plant to enter the risk management zone (YELLOW zone) [3, 4], which requires the nuclear power plant to control risks, measures should be taken to minimize the duration of YELLOW work windows or compensatory actions are put in place to reduce plant risk (reduced, yet adequate defense-in-depth). The risk assessment results meet the requirements of the technical specifications and are in good agreement with the operation practice of the nuclear power plant.

Comparing with Table 2, it can be seen that the Risk Increase Factor of the new integration method is slightly larger, which more appropriately reflects the influence of common cause failure on the risk of nuclear power plants, while avoiding the excessive amplification of influence on the risk of nuclear power plants.

TABLE 3. Risk Assessment Example by New Integration Method

New Integration Method	CDF（/reactor year）	Risk Increase Factor	Risk Zone
If a component cooling water pump fails	1.84E-04	17.52	YELLOW
If a service water pump fails	6.71E-05	6.39	YELLOW

IV. CONCLUSIONS

To address the challenge of how the risk monitor model of nuclear power plant can better reflect the influence of common cause failure of components on the risk of nuclear power plant, two IE fault tree modeling methods in the current industry are summarized in this paper. A comparative analysis of advantages and disadvantages in the application of risk monitor model are made, and the advantages of the two methods are integrated to propose a new integration modeling method. The examples show that the new integration modeling method can properly reflect the influence of common cause failure on the risk of nuclear power plant and avoid the excessive amplification of CCF influence on the risk of nuclear power plant. The application of new integration modeling method can provide an important reference for the implementation of configuration risk management of nuclear power plants.

ACKNOWLEDGMENTS

During the process of writing this paper, assistance was received from several colleagues such as Zhan Wenhui and He Jiandong. Moreover, in the peer review of configuration risk management, its application was recognized by many peers including Chu Yongyue from the Nuclear and Radiation Safety Center. Here, I would like to express my special gratitude.

REFERENCES

[1] Nuclear power plant configuration risk management peer assessment, T / CNSCPA 011-2023 [S], Beijing, China Nuclear Safety and Environmental Culture Promotion Association, 2023 : 15-16.

[2] RISK MONITORS - The State of the Art in their Development and Use at Nuclear Power Plants, NEA/CSNI/R(2004)20 [M], France, NUCLEAR ENERGY AGENCY COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS, 2004.

[3] Technical Policy for Configuration Risk Management of Nuclear Power Plants (Trial), *National Nuclear Safety Administration* [2019] No.262 [S], Beijing, National Nuclear Safety Administration (2019).

[4] T.Morgan, Applications of Colors as Risk Metrics – Background and Effective Practices, 2018 Configuration Risk Management Forum Research Task, 3002012995[M], California, Electrical Power Research Institute, Sep.2018.

[5] ASME/ANS RA- Sb-2013, Addenda to ASME/ANS Ra -S - 2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications [S], New York, The American Society of Mechanical Engineers, Sep. 2013.

[6] A.Mosleh, et al. Guidelines on modeling common-cause failures in probabilistic risk assessment, NUREG/CR-5485[M], Washington DC, United States Nuclear Regulatory Commission, June 1998.

[7] M.Marshall. et al. Common-Cause Failure Parameter Estimations， NUREG/CR-5497[M]， Washington DC, Idaho 1National Engineering and Environmental Laboratory， 1998: 1-2.

[8] K. Canavan, et al. Support System Initiating Events: Identification and Quantification Guideline, EPRI-1013490[M], California, Electrical Power Research Institute, 2006:5-8.
[9] J. Julius, et al. Support System Initiating Events Identification and Quantification Guideline, EPRI-1016741[M], California, Electrical Power Research Institute, 2008:2-14, 15.