Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, November 2-3, 2006

A New Methodology of Fault Trees Construction for Low Power and Shutdown PSA using Fault Trees for Full Power PSA

Jin-Hee Park[a] Ho-Gon LIm[a] Seung-Cheol Jang[a]
[a]*Korea Atomic Energy Research Institute P. O. Box 105, Yusung, 305-606, Taejeon, Korea Phone: +82-42-868-8297*
Fax: +82-42-868-8256
E-mail:jhpark@kaeri.re.kr

1. Introduction

To assess the risk in LPSD (Low Power & Shutdown) operation, the whole duration of LPSD must be divided into several POS (Plant Operational States) in which various system configurations of NPP in LPSD operations could be taken into account. It is assumed for LPSD PSA that the plant configuration and Thermal/Hydraulic conditions are identical in a POS. For a realistic risk calculation, the POSs needed for the LPSD PSA model may be increased to reach almost 20 POSs [1]. It means that there should be lots of ET/FT (event tree/fault tree) for the construction of LPSD PSA model. This approach requires large resources of manpower and time. Also, even if the LPSD PSA model is constructed in spite of large resource consumption, it can be difficult to maintain the LPSD PSA model for the plant modification and the overhaul plan.

To overcome these difficulties, this paper proposes the easy method to develop the LPSD PSA model. While maintaining the original structure of the FT for full power PSA, the simple modifications from full power FT model to the LPSD FT model using several methods are the key factors of the present study. By doing so, the full power and low power PSA model could be maintained consistently at the same time.

2. Methodology

2.1 Use of condition gate

A Condition Gate (CG) function is applied frequently when a system operation mode change would be needed in a FT model. For an example, if a system has a two functions like a running and a standby condition, the CG could be applied to remove the useless function in FT model. In a Boolean expression, the CG can be written as follows:

$$S = a + bc \quad (1)$$

$$S(a \to \pi) = \pi + bc = bc \quad (2) \text{ (Set 'True")}$$

$$\backslash S(b \to \Omega) = a + \Omega c = a + c \quad (3) \text{ (Set 'False")}$$

2.2 Alternative FT structure for the change of overhaul plan

A system can be in various operation conditions such as a running, a standby, and a maintenance in LPSD period. Therefore, a FT structure used in the LPSD model should have the features to represent various configuration changes. In general, the FT used in the full power FT model usually describes the standby state of a system since the most of the safety systems are in the standby state at full power operation. For an example, shutdown cooling system is normally in standby state while one train of this system is in the running state at LPSD period.

To model alternative state of a system with a FT, we used flag option with a condition gate function. Let the fault tree describing standby state of a system be $S(\vec{E}_d, \vec{E}_s)$ where $\vec{E}_d$ and $\vec{E}_s$ represent a vector of demand failures and standby failures of a system respectively. With a Boolean expression, the fault tree representing alternative condition of a system can be written as follows:

$$S_{LPSD} = S(\vec{E}_D, \vec{E}_R)F_S + S(E_D = \vec{0}, E_R)\overline{F_S} \quad (4)$$

The F_S means a flag option that a system is in standby state. If F_S is set to 1(Set 'True" in FT logic), Eq. (4) represent a fault tree of a system in standby state. On the contrary, if F_S is set to 0(Set 'False" in FT logic), Eq. (4) represent a fault tree of a system in running state. Eq. (4) can be illustrated with the following figure 1. The meaning of the notation used in figure 1 is shown in Table 1

2.3 Substitution of a gate or basic event

When a system FT used in full power PSA model is converted to LPSD PSA model, substitution of a gate or basic event into a new gate or basic event is needed. Typically, this corresponds to the instrument and control signal modeling. During a normal operation of the NPP, the safety systems or components receive actuation signal from the plant control system under an accident condition. If there is some fault in the signal transfer to the safety systems or components, these systems will not be properly operated. Therefore, the fault trees of these systems and component should consider the signal transfer failures. However, the plant control systems in LPSD period are bypassed to prevent malfunctions and operator must actuate the signal manually.

In this case, the part of fault tree representing signal transfer failures should be eliminated and then replaced with the event of operator error to actuate the signal. To solve this problem, there can be several approaches without the modification of the original fault tree.

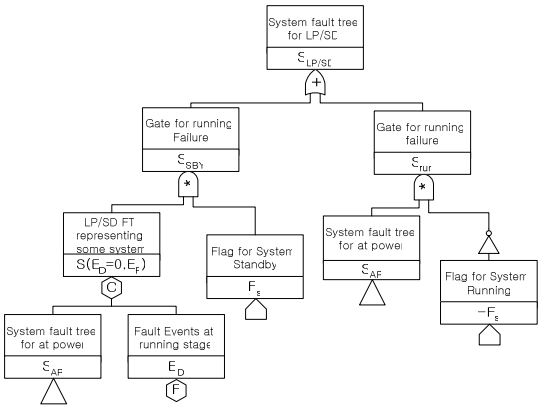

Figure 1 the structure of FT in LPSD PSA

Table 1 meaning of the symbols used in figure 1

symbols	meaning
+	OR operation
*	AND operation
C	CONDITION operation
	HOUSE event
F	FALSE events Gate
	Transfer gate

We introduce this method by expressing fault tree with Boolean function as follows. Let the original fault tree be S as follows:

$$S(G) = A + B \cdot G \quad (5)$$

Where A is a failure event set independent on the signal failures and B is a set of events with which signal failure event, G can make the system be failed. The fault tree that should be obtained from the original fault tree can be written as follows:

$$S_{LPSD} = A + B \cdot O \quad (6)$$

Where event "O" represent the event of operator error

Using Eq. 5 with some conditioning, Eq. 6 can be written as follows:

$$S_{LPSD} = S(\pi) + S(\Omega) \cdot O \quad (7)$$

The proof of Eq. 7 can be easily done by inserting Eq. 5 into Eq. 7 as follows

$$S(\pi) + S(\Omega) \cdot O = A + (A + B) \cdot O = A + B \cdot O \quad (8)$$

Another method is to replace old fault tree with a new one by using the configuration order in project files. In the project, all files associated with the one-top model are included in the project. The order of the files determines the replacement order. Since the current KIRAP cannot handle the former method, we used latter methods for the substitution function

2.4 Dual FT generation for the verification of the one-top model

The present study proposed a new method of one-top fault tree using above mentioned methods. However, the one-top model should be refined by reviewing and debugging the fault tree. For the purpose of reviewing, the current KIRAP [2] can generate a fault tree which all flag and conditions are merged into the structure. After all conditions and flags are merged into the FT structure, it is possible to investigate that all conditions and flag are properly functioned on the FT of full power PSA.

3. Results and Discussion

Using the method described in section 2, we constructed one-top FT for the POS 3 which is a part of the LPSD period. Figure 2 shows the overall results of the POS 3. Although the method for the construction of the one-top FT has been developed and the one-top FT structure was completed, the data used in the model such as human error probability is being under development. So, the numerical value described in the figure does not represent the final quantification results.

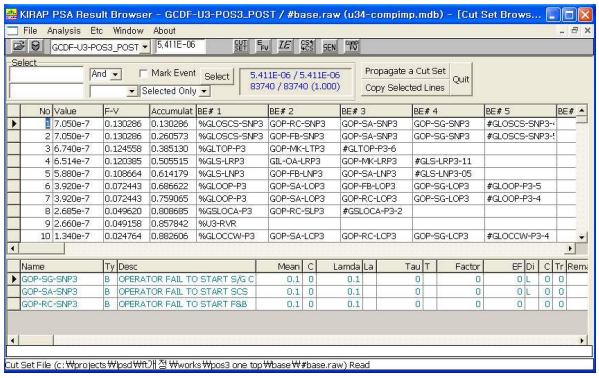

Figure 2 Quantification result of POS 3

4. Conclusion

The present study proposed a new method of constructing of one-top FT for LPSD PSA. New method use the FT used in the full power FT without any modification. By the new methods, the FT for the LPSD PSA can be easily constructed from the FT of the full power PSA. Also, the new method enables that the consistency between full power PSA and LPSD PSA are always maintained.

Based on the new method, we constructed one-top FT for POS 3 which is a part of LPSD period of OPR-1000 for the first time. From this application, we confirmed that the new method was adequately adapted and can be easily applied to LPSD PSA.

ACKNOWLEDGMENTS

This work has been carried out under the Nuclear long term R&D Program sponsored by the Korea Ministry of Science and Technology.

REFERENCES

[1] KHNP, 2002, Probabilistic Safety Assessment for Young Gwang 5&6: Low Power and Shutdown Analysis

[2] Han S. H., 1990, PC-workstation based level 1 PRA code package-KIRAP, Reliab Eng Syst Safety 30:313–22.