Transactions of the Korean Nuclear Society Autumn Meeting
Busan, Korea, October 27-28, 2005

Post Fire Safe Shutdown Analysis Using a Fault Tree Logic Model

Hyuntae Yim, *KMENT*, *hyuntaey@chol.com*
Junhyun Park, *KEPRI*, *junpark@kepri.re.kr*

1. Introduction

Every nuclear power plant should have its own fire hazard analysis including the fire safe shutdown analysis. A safe shutdown (SSD) analysis is performed to demonstrate the capability of the plant to safely shut down for a fire in any given area. The basic assumption is that there will be fire damage to all cables and equipment located within a common fire area. When evaluating the SSD capabilities of the plant, based on a review of the systems, equipment and cables within each fire area, it should be determined which shutdown paths are either unaffected or least impacted by a postulated fire within the fire area.

Instead of seeking a success path for safe shutdown given all cables and equipment damaged by a fire, there can be an alternative approach to determine the SSD capability: fault tree analysis. This paper introduces the methodology for fire SSD analysis using a fault tree logic model.

2. Methods and Results

In the fire SSD analysis using a fault tree logic model, (1) a fault tree having the top event, 'failure of SSD after a fire' is constructed and solved for the minimal cutsets representing the combinations of equipment failures leading to the failure of SSD, and then (2) combinations of equipments are compared with the list of damaged equipment to determine the capability of SSD.

2.1 Fault tree logic

For the purpose of deriving the combinations of equipment failures leading to the failure of SSD after a fire, a fault tree is constructed. Top event is defined as the failure of SSD after a fire. Beneath the top event failure logics are deductively developed for four kinds of SSD functions (reactivity control, pressure control, inventory control, decay heat removal). The first page is shown in Figure 1. Support functions like electric power and cooling, and the process monitoring for confirming the SSD functions running are included in the logic model as well. The fault tree logic is developed up to the component level. Specific considerations for each SSD function are described below.

For reactivity control function, boric acid injection by a charging pump and monitoring of subcriticality by source range and intermediate range nuclear instruments are needed. Boric acid tank and refueling water storage tank are available for boric acid source, and the level indications of the tanks are also needed.

For pressure control function, both increase and decrease of the primary pressure are required and monitoring of the primary pressure should be available. Pressure increase can be accomplished by either a charging pump or pressurizer heater, and pressure decrease by either a pressurizer PORV or pressurizer auxiliary spray.

For inventory control function, coolant makeup compensating the shrinkage of the coolant during cooldown is required and monitoring of the primary level should be available. Coolant makeup can be accomplished by a charging pump with water source of refueling water storage tank.

For decay heat removal function, both hot shutdown and cold shutdown should be considered. For hot shutdown, secondary heat removal using auxiliary feedwater system and atmospheric steam dump is required and monitoring of the cold leg and hot leg temperature and steam generator level should be available. One auxiliary feedwater pump is sufficient to supply the required flow to the steam generators and two condensate storage tanks are available for the water source. For cold shutdown, primary cooling by one train of residual heat removal system is required and monitoring of the cold leg and hot leg temperature should be available.

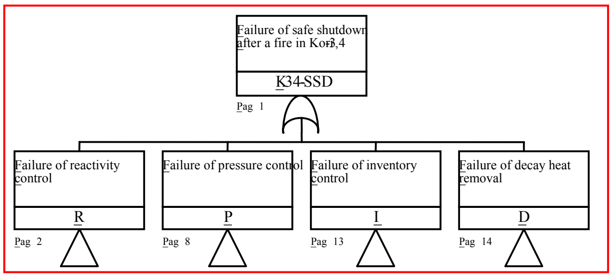

Figure 1. Fault tree for the failure of SSD after a fire(1st page)

2.2 Damaged equipment comparison

By deriving the minimal cutsets of the fault tree logic using Boolean algebra, we get the combinations of equipment failures leading to the failure of SSD. The combinations of equipment failures are compared with the list of damaged equipments to determine the capability of SSD. The list of damaged equipment is based on a review of the systems, equipment and cables within each fire area. Considering the large number of the combinations of equipments and the list of damaged equipments, Microsoft Excel macro function is used for comparison process rather than manual operation. There are three EXCEL sheets: 'LDE' (List of Damaged Equipment), 'COE' (Combination of Equipment), and 'RESULT'. Sheet 'LDE' contains the fire area code in the first row of each column, and the damaged equipment tag numbers in the second row and thereafter. Sheet 'COE' has the minimal cutset number in the first column of each row, and the equipment tag numbers comprising the corresponding minimal cutset in the second column and thereafter. Sheet 'RESULT' contains the results of the comparison process. Comparison process using Excel macro follows the sequences below.

① Compare the value of row 1, column B in sheet 'COE' with the value of each row of column A in sheet 'LDE' consecutively.
② If there is no identical value found in step ①, compare the value of row 1, column B in sheet 'COE' with the value of each row of column B, C, D, and thereafter in sheet 'LDE' consecutively.
③ If identical value is found in step ① or ②, remember the corresponding column in sheet 'LDE' and compare the value of row 1, column C in sheet 'COE' with the value of each row of the remembered column in sheet 'LDE' consecutively.
④ Compare the value of row 1, column C, D, E, and thereafter in sheet 'COE' with the value of each row of the remembered column in sheet 'LDE' consecutively.
⑤ If the 1^{st}, 2^{nd}, 3^{rd}, and thereafter remembered column in sheet 'LDE' has exact number of identical value as the number of columns of row 1 in sheet 'COE', write the value of the first row of those remembered column in row 1, column A, B, C, and thereafter of sheet 'RESULT'
⑥ If the 1^{st}, 2^{nd}, 3^{rd}, and thereafter remembered column in sheet 'LDE' has exact number of identical value as the number of columns of row 2, 3, 4, and thereafter in sheet 'COE', write the value of the first row of those remembered column in row 2, 3, 4, and thereafter, column A, B, C, and thereafter of sheet 'RESULT'

2.3 Results

As the results of the step ①～⑥ in section 2.2, sheet 'RESULT' shows the fire area codes in n-th row representing the failure of SSD given a fire in its area because that damaged equipments(LDE) by fire involve the n-th combination of equipments(COE) leading to the failure of SSD. After applying an appropriate filtering process to the 'RESULT' sheet, we can get SSD failure areas and the reasons for the failure of SSD in terms of damaged equipments by the fire in that area.

3. Conclusion

The methodology for fire SSD analysis using a fault tree logic model is found to very effective and valid in determining the SSD capability given a fire. But this approach cannot be solely applied to the SSD analysis. Rather, fault tree logic method can be applied to support the success path approach. Two approaches, fault tree method and success path method can assist each other complementarily in post fire safe shutdown analysis, making the result of the analysis more reliable and robust.

REFERENCES

[1] Fire Protection for Operating Nuclear Power Plants, Regulatory Guide 1.189, USNRC, Apr. 2001

[2] Guidance for Post Fire Safe Shutdown Analysis, NEI 00-01, Rev. D, NEI Circuit Failure Issues task Force, Oct. 2002

[3] Knowledge Base for Post Fire Safe Shutdown Analysis, Draft Report for Comment, NUREG-1778, USNRC, Jan. 2004

[4] Fire Hazard Analysis for Kori Nuclear Power Plant Unit 3&4, Draft for Comment, Korea Hydro and Nuclear Power, Co. 2005. 7