Transactions of the Korean Nuclear Society Spring Meeting
Chuncheon, Korea, May 25-26 2006

Defense-In-Depth Evaluation Model Development Procedure for Outage Risk Evaluation

Huichang Yang,a Ki Yong Kim,a Hae Cheol Oh,b Myung Ki Kim,b Sung Yull Hong,b
a Atomic Creative Technology Co., Ltd., 1688-5 Sinil-dong Daedeok-gu Daejeon 306-230, hcyang@enesys.co.kr
b Korea Electric Power Research Institute, Munji-dong Yuseong-gu Daejeon, Korea, 305-380

1. Introduction

Defense-in-depth evaluation method using safety function assessment trees (SFAT) is a complementary tool to evaluate the safety status of nuclear power during the plant outage operation. Based on the result from the deterministic safety analysis and engineering judgment, the defense-in-depth status can be categorized into 4 colors. This risk evaluation is based on the configurations during outage operation. To develop defense-in-depth evaluation model, the components and systems should perform key safety functions should be selected. The main safety function assessment logics and color assignment criteria should be developed. Based on the past experiences, the procedures for defense-in-depth model evaluation model using SFAT were established.

2. Model Development Procedures

For UCN 3&4, 8 safety functions for LP/SD operation were defined. Among safety functions, SFAT development for decay heat removal safety function was discussed in this paper as example. Also, 16 unique POSs for LP/SD operations were defined. The detailed system and component models were developed for the defense-in-depth status evaluation from the outage schedules.

2.1 Safety Function Definition

In the emergency operation procedures (EOP), critical safety functions were specified. In the functional recovery guidelines (FRG), such safety functions were listed exclusively. Based on these safety functions, the functions should be monitored during outage operations can be derived and defined. With a little modification on the original safety functions, the safety functions for UCN 3,4 were defined as followings;

1. Decay Heat Removal
2. Inventory Control
3. Reactivity Control
4. Containment Integrity
5. Spent Fuel Pool Cooling
6. Vital Electric Power AC
7. Vital Electric Power DC
8. Cooling Water

Above safety functions are for outage operations. For online operation, safety functions can be defined based on the procedures for online operation.

2.2 Plant Operating Status Definition

During the shutdown and outage operations, the physical status of RCS are changed from hot standby to defueled status. By classifying the similar status in terms of safety analysis, plant operating status (POS) can be defined in to several groups. During this process, the LP/SD PSA POS definition can be referred. Figure 1 is the example of POS determination for UCN 3&4.

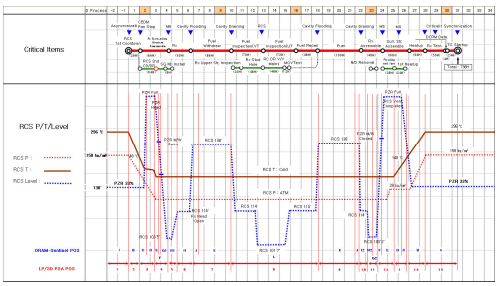

Figure 1. Plant Operating Status Determination Example

2.3 Filter Variable Determination

In SFAT methodology, SFATs which should be applied to a specific POS should be determines. From the process variables such as RCS temperature, level, pressure and operational modes, unique POS can be determined and to this specific POS, pre-defined SFATS should be applied for the evaluation. This is the role of filter variables. The existence of large vents in RCS, which makes the feed and bleed operation available, can be the good example of filter varialble.

2.4 SFAT Logic Development

To develop SFAT logic, many analysis results should b referred, and these safety analysis can b followings;

1. Technical Specification LCO conditions
2. Probabilistic Safety Assessment Success Criteria
3. Success Paths in EOP, AOP and FRG

Based on these safety analysis criteria, the condition blocks in SFATs can be defined and the colors for the end branch in SFAT can be determined.

Operational experiences of plant personnel should be reflected to the SFAT logics and color assignment rules.

Table 1 shows the general definition of color assignments and figure 2 should the general type of SFAT.

Table 1. General Definition of Color Assignment

Color	Definition and Basis
Green	**Defense-in-depth is well maintained, or maximum, for the safety function.** **Insignificant Risk Increase.**
Yellow	**Defense-in-depth is degraded, but is adequate for the safety function.** **Usually the plant is in a technical specification LCO.** **Significant Risk Increase.**
Orange	**Defense-in-depth is marginal for the safety function. This color usually indicates multiple LCOs are in effect.** **Very Significant Risk Increase**
Red	**Defense-in-depth is extremely challenged for restoration of the safety function under some or all accident events. This configuration should not be entered into voluntarily. Additionally, a Technical Specification Violation results in a RED result.** **Unacceptable Risk Increase**

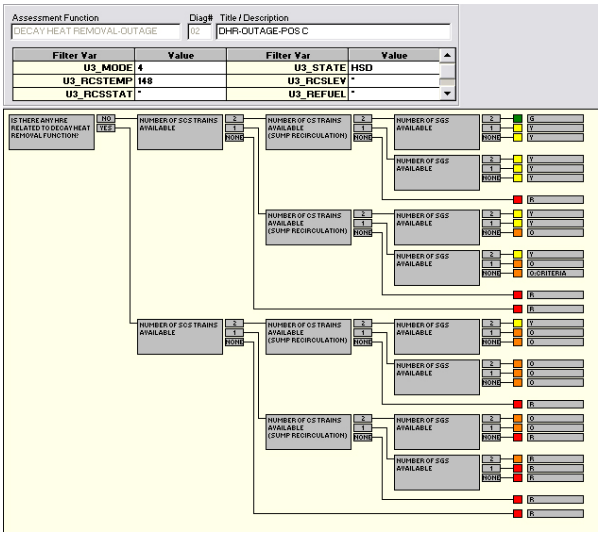

Figure 2. Example Decay Heat Removal SFAT

2.5 System Model Development

In each SFAT condition block, the questions about the availability of system, trains or components would be included. From the plant configuration database, the maintenance and test schedules will be linked to the evaluation model and from this, the availability of each system, train or component can be determined. The system models used in defense-in-depth evaluation model are purely dependency fault tree models. For developing system dependency fault tree model, the key components which are used during the shutdown and outage operation should be determined by referring the SSEL, EQ and FSAR. After determining the components, the mapping table which links the ERP ID and PCDB variable, should be developed. For ORAM-Sentinel, this table is called as 'translation matrix,' and for ORION, this table is called as 'mapping table.'

3. Conclusion

Safety function assessment trees are the main defense-in-depth evaluation method for low power and shutdown operation. With clearly defined safety functions and the methods which can evaluate the level of defense-in-depth according to maintenance schedules, low power and shutdown risk in nuclear power plant can be managed more easily and more objective way. Through this defense-in-depth evaluation and shutdown risk management, the overall safety of nuclear power plant can be enhanced.

By the mapping table, the schedules to be evaluated can be selected. The meaningless schedules, which does not impact the unavailability of system, should be excluded. Based on the color evaluation results, the maintenance schedules should be re-scheduled. Figure 3 shows the before and after risk evaluation results for the sample outage maintenance schedules.

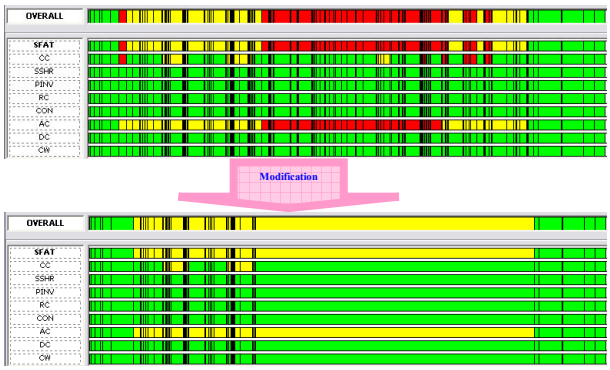

Figure 3. The maintenance schedule optimization using defense-in-depth evaluation model

REFERENCES

[1] U.S. NRC, "An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant-Specific Changes to the Current Licensing Basis ," Reg. Guide 1.174,, 1998.

[2] EPRI, "ORAM-Sentinel Development and ORAM Integration at Catawba and McGuire," EPRI TR-106802, 1998.

[3] NUMARC, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," NUMARC 93-01, 1996.

[4] NUMARC, "Guidelines for Industry Actions to Assess Shutdown Management," NUMARC 91-06, 1991.