Methodology for Selecting Periodic Safety Inspection Items to Reinforce the 2nd & 3rd Level of Defense-in-Depth

Jihan Lim*, Younwon Park, Hyungjin Kim, Seongsoo Choi
BEES Inc., Suite L508, 193 Munji-ro, Yuseong, Daejeon, 34051 Republic of Korea
**Corresponding Author: wib565@bees.pro*

1. Introduction

Defense-in-Depth (DID) concept is the basic principle of nuclear safety. The objectives and definitions of each 5 different DID levels are shown in Table I.

Table I: Definition of DID [1]

Levels	Objectives
1	Prevention of abnormal operation and failures
2	Control of abnormal operation and detection of failures
3	Control of accidents within the design basis
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents
5	Mitigation of radiological consequences of significant release of radioactive materials

The implementation of DID through the deterministic approach has been already incorporated into the design and operation. Domestic regulatory Periodic Safety Inspection (PSI) is being conducted by assuming that all Structures, Systems, and Components (SSCs) of nuclear power plants have the same importance in terms of safety and functional issues.

However, the use of probabilistic approach has not been fully explored. The probabilistic approach is mainly supported by Probabilistic Safety Analysis (PSA) that can provide useful insights and inputs for various areas for decision making on: (a) design and plant modifications, (b) optimization of plant operation and maintenance, (c) safety analysis and research programs, and (d) regulatory issues [2]. For this PSA to be used in the decision making process, a formal framework should be established depending on the purpose of its application.

Therefore, the objectives of this research were to replace the single line defense concept based regulatory PSI system to multi-level DID by developing methodology for selecting regulatory PSI items using Level 1 PSA.

2. Methodology

2.1 Development of New Methodology to link PSA and DID

When it comes to DID in ROP program, it is to note the review of selected definition of defence-in-depth provided by Per Hellstroem in "DID-PSA: Development of a Framework for Evaluation of the Defence-in-Depth with PSA [3]" and also the analysis by Hyung Jin Kim [4]. Their evaluation show that the ROP program, developed using risk insights of PSA results, is firmly based on the defence-in-depth whereas it was concluded by Hellstroem that the fundamental definition of DID from IAEA does not harmonize with results from PSA. The PSA is described, in general, by event trees starting from an initiating event. Before getting a specific PSA event tree to link with DID defined by IAEA, it would be necessary to associate them conceptually as described in Fig. 1.

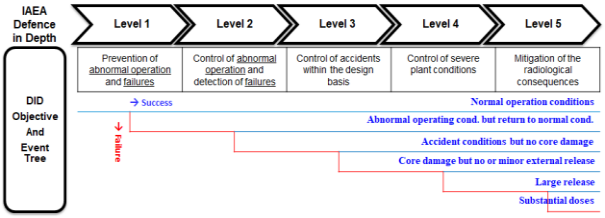

Fig. 1. Relationship between PSA and DID [3]

If prevention of abnormal operation could be ensured, then the level 1 of DID would be achieved. If it fails, the plant status would go over to level 2 of DID where control of abnormal operation or detection of failures are successfully done so that the plant could be back to normal situation and then the level 2 of DID would be achieved. In case level 2 of DID fails and an accident takes place, then the plant moves over to DID level 3. If the accident could be controlled within design basis, the DID level 3 would be achieved without core damage [3]. A deterministic approach to DID does not explicitly consider the frequencies of occurrence of an event nor does it include the probabilistic values of success in the subsequent provisions after an initiating event. To ensure the safety of plants, the three fundamental safety functions should be performed: (1) control of reactivity, (2) removal of heat from the core, and (3) confinement of radioactive materials. The level 1 PSA provides different scenarios and diverse event trees that can lead to core damage with a consideration of success or failure probabilities of each provision coming into play after an initiating event. The level 1 PSA can be associated with DID level 1-3 whereas DID level 4 can be linked with level 2 PSA that provides event trees for a given core damage under a severe accident condition as shown in the Fig. 2 [4].

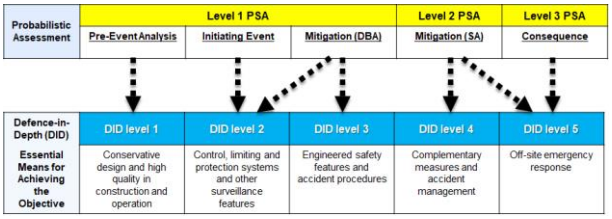

Fig. 2. Relationship between Level 1-3 PSA and DID Level 1-5

An appropriate number of initiating events for Level 1 PSA are determined from the evaluation of more than fifty pre-events that are considered in the design with occurrence frequency based on the event class. The event classes are provided in ANSI/ANS 51.1-1983 as plant conditions with five categories, from normal operations to unlikely events depending on frequency ranged from daily occurrence to 10-6 per reactor year, respectively. The normal operation pertaining to DID level 1 and plant condition 1 are not actually considered in the level 1 PSA. It means that level 1 PSA can be linked with DID level 2 and the above. The DID level 2 is composed of two pillars: the first is control of abnormal operation and the other is detection of failure. The periodic safety inspection program covers all SSCs of a plant to confirm the performance of SSCs and operators' capability so that the inspectors should review the operation records and observe specific functionality checks conducted during or after maintenance activities with equal importance. The investigation on this periodic safety inspection program done by Younwon Park et al. [5] shows that the major inspection activities are more or less focused on DID level 1 and 2 while the inspection items are not selected based on DID concept. For this periodic safety inspection program to be more balanced over DID level 1 to level 3, a systematic way of incorporating PSA insights into the program should be developed, in particular, to strengthen the inspection on DID level 3 related with mitigation systems.

In case of OPR-1000 power reactor in Korea, fifteen initiating events are selected from the evaluation of pre-event analyses. The first step is, therefore, to select an initiating event that is contributing the most to plant core damage frequency. That is station blackout (SBO) for Hanul units 3 & 4. Once an initiating event is selected, the core damage can be avoided by two ways: the first is to secure all the success paths and the other is to block all the failure paths in the event tree. For a given SBO in Fig. 3, the event tree shows that the first is more effective than the others because the first needs only four headings whereas the other requires to handle more than 10 headings. To secure the success paths, the success criteria should be defined using relevant design information, such as P&IDs (piping and instrument drawings), logic diagrams, and so on. Based on the success criteria, the associated SSCs and their subjugated specific components must be identified and listed. Whether the items to be inspected are identified in an appropriate way can be confirmed using PSA results in that for a given heading, minimal cut sets should be analyzed to determine relevant basic events. These basic events provide the information of all the specific items to be included in the given heading to be successful. So, the selection of inspection items for a given heading based on the success paths can be verified by PSA evaluation.

2.2 Case Study for Application of New Methodology

As a case study for application of this methodology, station blackout is selected. As shown in Fig. 3, PSA event tree for SBO consists of 15 headings that stretch out over 34 scenarios of which 22 paths are with core damage and 12 without core damage. After successful reactor trip, the first heading, indicated as AFT, is to deliver aux. feedwater using turbine driven pump. The success criteria can be set up using P&ID as shown in Fig. 4.

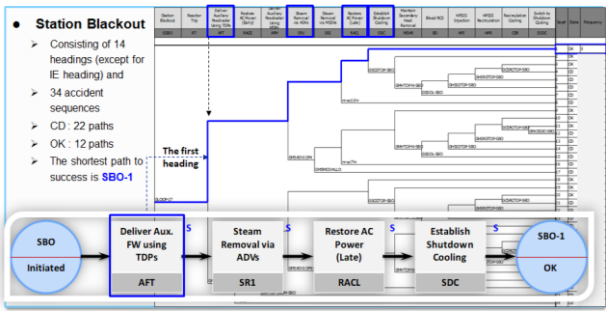

Fig. 3. Evaluation of the Event Tree for Station Blackout Initiating Event

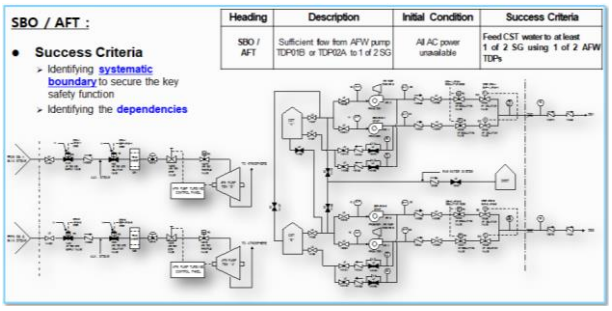

Fig. 4. Determination of Success Criteria for AFT heading

As shown in Fig. 4, at least one aux. feedwater turbine driven pump, its associated steam and water line including also the associated components of support systems must be selected. The detailed components are listed in Fig. 5.

Then, the analyses of minimal cut sets for AFT should be done to extract basic events and to finally determine whether the above process is appropriate in inspection item selection using AIMS-PSA/FTREX developed by KAERI. In the analyses, the cutoff value was set by 10-7 to limit the number of basic events. As

shown in Fig. 6, the most limiting basic event can be extracted from this analysis.

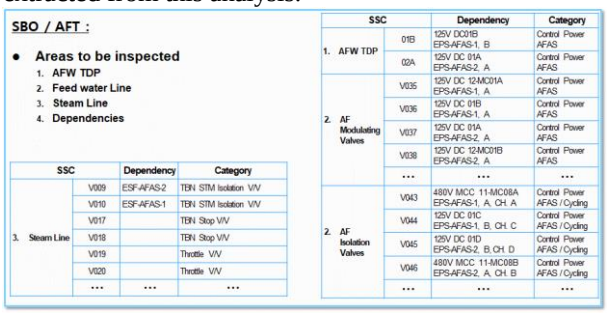

Fig. 5. Inspection Items Selected for AFT Heading

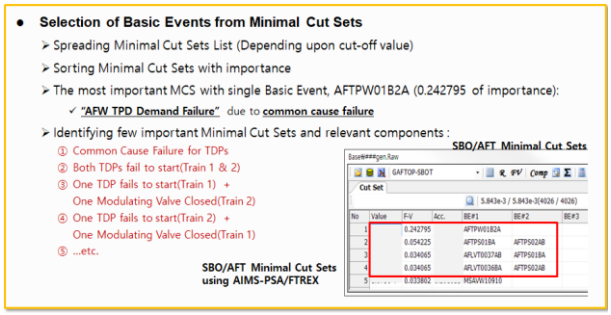

Fig. 6. Basic Event List Obtained from PSA Cut Set Evaluation

The key inspection items can be obtained from the very contributing basic events in Fig. 6. As shown in Fig. 7, the inspection items obtained from PSA minimal cut set evaluation are identical to those of Fig. 5 obtained from success path approach. Once an initiating event occurs, the subsequent headings, by nature, belong to mitigating systems and DID level 3. Using this methodology, a success path to avoid core damage can be secured and the associated inspection items can be selected. The advantage of this method is that the relevant inspection items can be determined using PSA approach for a given initiating event, which eventually strengthen the DID level 3 in a systematic way.

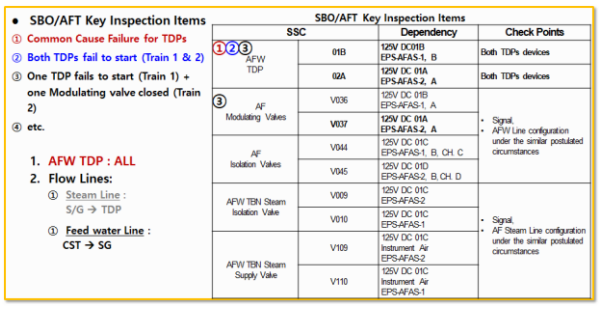

Fig. 7. Inspection Items Obtained from Minimal Cut Set Evaluation for AFT

3. Conclusions

The periodic safety inspection program conducted at every overhaul period is the most important program for confirming the safety of operating nuclear power plants in Korea. This inspection program was developed in early 1980 based on deterministic approach with the objective that nuclear power plant must be operated in compliance with the operating license so that the performance of each structure, system and component must exhibit the level of performance identified through preoperational inspection program. The periodic safety inspection program should include, therefore, not only the safety related SSCs but also power conversion side that is not directly associated with nuclear safety. The inspection findings, whatever coming out of safety-related or non-safety-related, should be treated with almost same level of importance.

This inspection program is likely to be effective for preoperational inspection because each functionality of the plant structures, systems and components should be verified to make sure that the plant is ready to operate. However, once the plant is put into service the regulatory safety inspection must be focused on whether to minimize the risk of accident using defense-in-depth concept and risk insight obtained from probabilistic safety analysis.

Actually, the incorporation of DID concept and risk insight into deterministic based safety inspection has not been well studied so far since the regulatory safety inspection was developed depending on each country's specific regulation. In this study, two track approaches are proposed: the one is to secure success path and the other to block the failure path in a specific event tree. For a given nuclear power plant, there are in general 15 events that give rise to about 30 scenarios and some of them lead to core damage. Each of 15 events consists of specific headings such as high pressure safety injection, low pressure safety injection, steam dump to atmosphere, etc. The investigation shows how to select safety important components and how to set up inspection group to make sure that the core damage would not occur for a given initiating event. Station blackout (SBO) was selected as an initiating event for a case study because SBO is the most contributing initiating event to core damage in case of Hanul units 3&4. The inspection items were determined through success path approach and the results were compared with the components selected from the basic events of minimal cut sets for the same heading of PSA event tree. The inspection items obtained from PSA minimal cut set evaluation are identical to those from success path approach. Once an initiating event occurs, the subsequent headings, by nature, belong to mitigating systems and DID level 3. Using this methodology, a success path to avoid core damage can be secured and the associated inspection items can be selected. The advantage of this method is that the relevant inspection items can be determined using PSA approach for a given initiating event, which eventually strengthen the DID level 3 in a systematic way.

Acknowledgments

This work was supported by the Nuclear Safety Research Program through the Korea Foundation of Nuclear Safety (KoFONS), granted financial resource from the Nuclear Safety and Security Commission (NSSC), Republic of Korea. (No. 1603012)

REFERENCES

[1] No. SF-1, 'Fundamental Safety Principles', IAEA, 2006.
[2] IAEA, "Development and Application of Level 1 PSA for Nuclear Power Plants", Safety Standards Series SSG-3, 2010.
[3] USNRC, "Technical Basis for Inspection Program", Inspection Manual Chapter 0308 Attachment 2, 2018.
[4] Hyung Jin Kim et al., "Review of the Regulatory Periodic Inspection System from the Viewpoint of Defence-in-Depth in Nuclear Safety", to be published in Nuclear Energy Technology in 2018.
[5] Younwon Park et al., "Development of Defence-in-Depth based Periodic Safety Inspection Incorporating Probabilistic Safety Assessment", N-STAR-16NS12-07, 2016.