한국압력기기공학회 논문집
제14권 제2호 2018년 12월 pp. 49-58

ISSN 1738-8333
http://dx.doi.org/10.20466/KPVP.2018.14.2.058

<연구논문>

A New Approach to Selection of Inspection Items using Risk Insight of Probabilistic Safety Assessment for Nuclear Power Plants

Younwon Park†, Hyungjin Kim*, Jihan Lim* and Seongsoo Choi*

(Received 1 November 2018, Revised 7 December 2018, Accepted 11 December 2018)

ABSTRACT

The regulatory periodic inspection program (PSI) conducted at every overhaul period is the most important process for confirming the safety of nuclear power plants. The PSI for operating nuclear power plants in Korea mainly consist of component level performance check that had been developed based on deterministic approach putting the same degree of importance to all the inspection items. This inspection methodology is likely to be effective for preoperational inspection. However, once the plant is put into service, the PSI must be focused on whether to minimize the risk of accident using defense-in-depth concept and risk insight. The incorporation of defense-in-depth concept and risk insight into the deterministic based safety inspection has not been well studied so far. In this study, two track approaches are proposed to make sure that core damage be avoided: one is to secure success path and the other to block the failure path in a specific event tree of PSA. The investigation shows how to select safety important components and how to set up inspection group to ensure that core damage would not occur for a given initiating event, which results in strengthening defense-in-depth level 3.

Key Words : Periodic Inspection, Defense in Depth, Risk-Informed Regulation, PSA, Initiating event

1. 서 론

The lessons learned from previous three major nuclear accidents, TMI, Chernobyl, and Fukushima showed the importance of defense-in-depth (DID) to minimize the consequences of nuclear disaster. The DID concept was introduced into nuclear power plant design in the early 1960 and has evolved as the lessons learned and operational experiences have been cumulated.

The International Atomic Energy Agency (IAEA) defined DID in Fundamental Safety Principles published in 2006 as the most important means for the prevention and mitigation of nuclear power plant accidents[1]. Recently, the IAEA investigation report on Fukushima Daiichi Accident indicated that DID was the most important factor in nuclear safety[2]. The concept of DID is to make sure multiple barriers to protect the public and environment from radioactive hazards, which consist of, in general, five levels: the first is to prevent deviations from normal operation and the failure of items important to safety, the second to detect and control deviations from normal operational states to prevent the anticipated operational occurrences, the third to mitigate the initiating events to be within design basis, the fourth to ensure the confinement for radioactive release to be as low as possible, and the fifth to protect the public and environment from the consequences of radioactive release by deploying emergency response[3][4]. The implementation of DID has been already incorporated into the design and operation through the deterministic approach while the use of probabilistic approach has not been fully explored.

The probabilistic approach is mainly supported by Probabilistic Safety Analysis (PSA) that can provide

† 책임저자, 회원, 비즈(주)
E-mail : jerom@bees.pro
TEL : (042)864-4781 FAX : (042)864-4789
* 비즈(주)

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(5). For this PSA to be used in the decision making process, a formal framework should be established depending on the purpose of its application.

In Korea, the first implementation of PSA had been done by regulatory recommendation provided in the Severe Accident Policy declared in August of 2001. As part of the PSA application, the Risk-Informed Safety Inspection and Risk-Informed, Performance Based Comprehensive Regulation Plan had been tried. The Korea Institute of Nuclear Safety (KINS) had also tried in 2006 to incorporate the PSA results into periodic inspection (PI) that has been conducted during every overhaul since early 1980 to ensure whether the NPP is in compliance with appropriate safety level as designed.

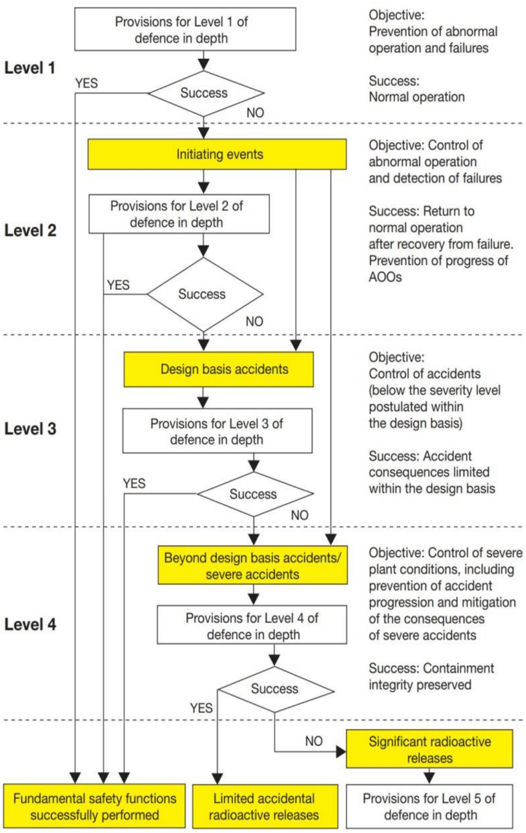

Fig. 1 Flow chart for defense in depth(3)

The motivation was that the PI, developed at the time when only 3 nuclear power plants, Kori unit 1 & 2 and Wolsong unit 1, were in operation, was too much relied upon strict deterministic approach. For this application, the results of PSA on Hanul unit 3 & 4 were used for updating and improving inspection items. The most contributing systems and components to core damage frequency (CDF) were selected and compared with the existing inspection items. This trial application of PSA into PI could enable the inspection program to be improved in a sense that some important items not covered in the existing inspection program were added in the inspection list. However, once the inspection item list modified, the PI has stayed depending on deterministic approach without utilizing any further PSA insights.

In this study, two track approaches are proposed using PSA to select safety important components and to set up inspection group to make sure that the core damage would not occur for a given initiating event: the one is to secure success path and the other to block the failure path in a specific event tree. This methodology could be used to supplement the current periodic safety inspection program using PSA insights that provide relative safety important systems and components to avoid core damage and it leads to strengthen DID level 3.

2. Review on the Nuclear Safety Inspection

2.1 Periodic Inspection Program in Korea

Regulatory inspection framework in Korea consists of three inspection programs: (1) preoperational inspection program conducted over construction phase, (2) periodic inspection program performed during every overhaul period of a nuclear power plant in operation, and (3) quality assurance inspection program for whole life span of a nuclear power plant. The objective of the preoperational inspection program is to make sure that the nuclear power plant is constructed and tested as designed so that all the systems and components should be subject to confirmation process through regulatory inspection program whatever their significance. Once the nuclear power plant is put into service, the appropriate level of safety for operation and licensee performance should be confirmed through periodic inspection program. The objective of this PI is defined in the Article 22 of Nuclear Safety Act that all nuclear power plants must be operated in compliance with the operating license so that the performance of each structure, system and component must exhibit the level of functionality identified through preoperational inspection program. periodic inspection program in Korea, therefore, has been developed to include all the structures, systems, and components (SSCs) as covered in the preoperational inspection program. The fundamental framework of periodic inspection program was developed in very early 1980s when there were only 3 nuclear power plants in operation, based on the idea that the activities of licensee and the performance of each SSC should be independently checked by regulatory inspectors. Historically, Korean nuclear power plants had been inspected until 2005 by two authorities: (1) nuclear safety authority and (2) electricity power generation authority. The first was by nature to cover mainly the primary side of a nuclear power plant and the other to cover the secondary side. These separate inspection programs from two different authorities were very much burdensome to licensee because those two inspection programs did not harmonize well. In 2005, it was decided by the government that those two split inspection programs should be merged and the authority on the secondary side of each nuclear power plant should be turned over to nuclear safety authority. The performance confirmation process for the secondary side should be then legally guaranteed by the law related to periodic inspection program at that time. That’s the reason why the periodic inspection program should include not only the safety related SSCs but also power conversion side that is not directly associated with nuclear safety matter. The periodic inspection program should include, therefore, all the SSCs regardless of safety significance and the inspection findings, whatever coming out of safety-related or non-safety-related, should be treated with almost the same level of importance. This is also a fundamental background that the periodic inspection program is considered as single front line basis rather than based on multi-layer defense-in-depth even though all the SSCs from normal operation and initiating events, to mitigating systems are covered.

Anyhow, the issue of graded approach based on risk importance has long been the key concern to KINS that is responsible for periodic inspection program. KINS tried to improve this PI program taking into account the risk insights provided by PSA results that was submitted to regulatory body from 2003 per the recommendation of Severe Accident Policy. In 2006, a primitive risk-informed inspection model was applied for Hanul unit 3 during overhaul period in parallel with the existing periodic inspection program. The outcomes

Table 1 Items subject to regulatory inspection of domestic nuclear power plants

Inspection target facilities	The num. of items	The num. of detailed items
1. Nuclear reactor (including fuels)	6	20
2. Nuclear reactor coolant system facility	6	20
3. Instrumentation and control system facilities	11	22
4. Nuclear fuel material handling and storage facilities	2	6
5. Radioactive waste disposal facilities	5	26
6. Radiation control facilities	7	16
7. Reactor containment facilities	6	19
8. Reactor safety system facilities	5	14
9. Power supply system facilities	17	54
10. Power conversion system facilities	10	36
11. Other facilities pertaining to the safety of a nuclear reactor	20	73
12. Technical Operation	5	16
Sum	100	322

of this trial application were just incorporated into revision of periodic inspection program by adding some specific SSC items relatively important to safety that had not been included in the previous periodic inspection program. Unfortunately, this pilot application of risk insights into periodic inspection program could not be extended over the other nuclear power plants because of the rigidity of legal system. Then the periodic inspection program remains yet as old fashioned firmly based on the initial deterministic framework that does neither have enough consideration of PSA insights nor defense-in-depth concept as shown in table 1[(6)].

2.2 ROP Inspection Program in USA

The power reactor inspection program of USA has been developed based upon Reactor Oversight Program (ROP) implemented since April of 2000 with the objective that provide tools for inspecting and assessing licensee performance and enforcing NRC requirements in a manner that was more risk-informed, objective, predictable, and understandable than previous oversight process[(7)]. The regulatory framework for ROP consists of three key strategic performance areas: reactor safety, radiation safety, and safeguards. These three key areas are supported by seven cornerstones to define specific elements of different defense-in-depth: initiating events, mitigating systems, barrier integrity, emergency preparedness, public radiation safety, occupational radiation safety, and security as shown in Fig. 2. Each cornerstone contains inspection procedures and performance indicators to ensure that their objectives are being met.

The major ROP programs can be implemented through risk-informed baseline inspection program and performance indicators. The baseline inspection program is to define the minimum level of inspection for each plant regardless of its performance. The performance indicators provide licensee's performance and rationale to conduct the supplemental inspection program in case the predetermined performance indicator thresholds are exceeded. The baseline inspection program has been developed using a risk-informed approach to determine a comprehensive list of inspection areas, called inspectable areas, within each cornerstone[(7)].

The inspectable areas are selected based on their risk significance derived from consideration of probabilistic risk analysis insights, operational experiences, deterministic analysis insights, and regulatory requirements. Forty one inspectable areas are provided in "Technical Basis for Inspection Program[(7)]" determined based on the reasons that: (1) the area is linked to the NRC's mission, (2) the inspectable area involves a key attribute to a cornerstone of safety, and (3) risk information justifies including the area in the baseline inspection program. In addition to the inspectable areas identified for many of the key attributes of each cornerstone of safety, the baseline inspection program also consists of inspection activities such as: (1) performance indicator verification, (2) problem identification and resolution, (3) event follow-up, and (4) plant status. Under the inspectable areas, how to conduct each specific inspection activity is provided in the Inspection Manuals[(8)] and Inspection Procedures[(9)].

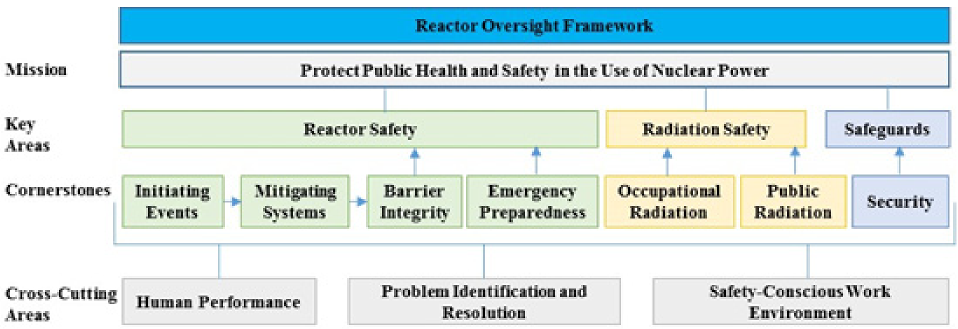

Fig. 2 Framework of reactor oversight program(4)

3. New Approach to incorporate PSA insights and DID concept into PI

3.1 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[7]" and also the analysis by Hyung Jin Kim[6]. 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. 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[7].

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. 4[6].

An appropriate number of initiating events for Level

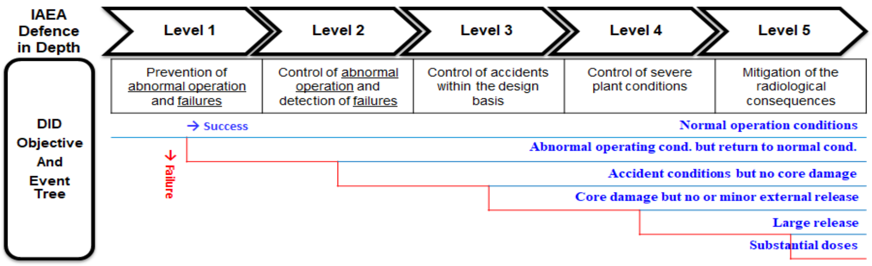

Fig. 3 Relationship between PSA and DID(7)

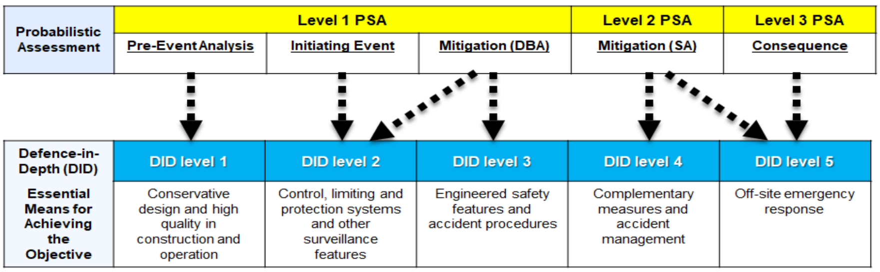

Fig. 4 Relationship between level 1-3 PSA and DID level 1-5

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. As described in the above Table 1, the periodic 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 inspection program done by Younwon Park et al.[12] 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 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. 5, 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.

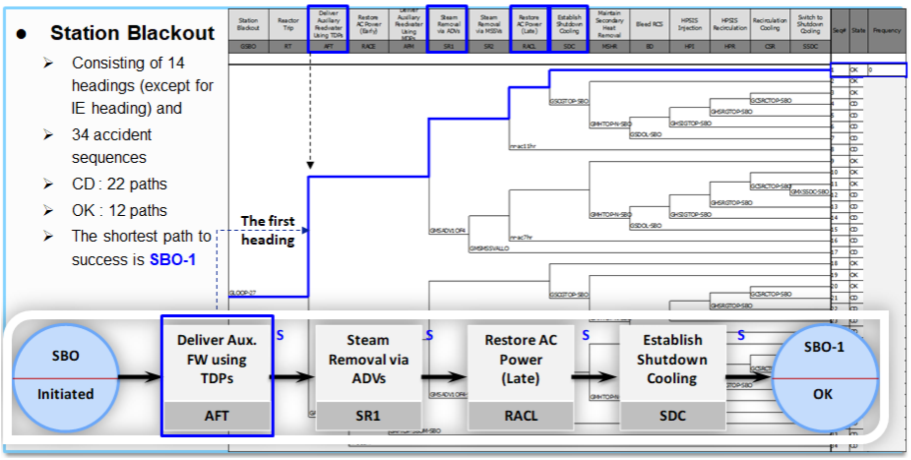

Fig. 5 Evaluation of the event tree for station blackout initiating event

3.2 Case Study for Application of New Methodology

As a case study for application of this methodology, station blackout is selected. As shown in Fig. 5, 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. 6.

As shown in Fig. 6, 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. 7.

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. 8, the most limiting basic event can be extracted from this analysis.

The key inspection items can be obtained from the very contributing basic events from minimal cutsets in Fig. 8. As shown in Fig. 9, the inspection items obtained from PSA minimal cut set evaluation are identical to those of Fig. 7 obtained from success path approach.

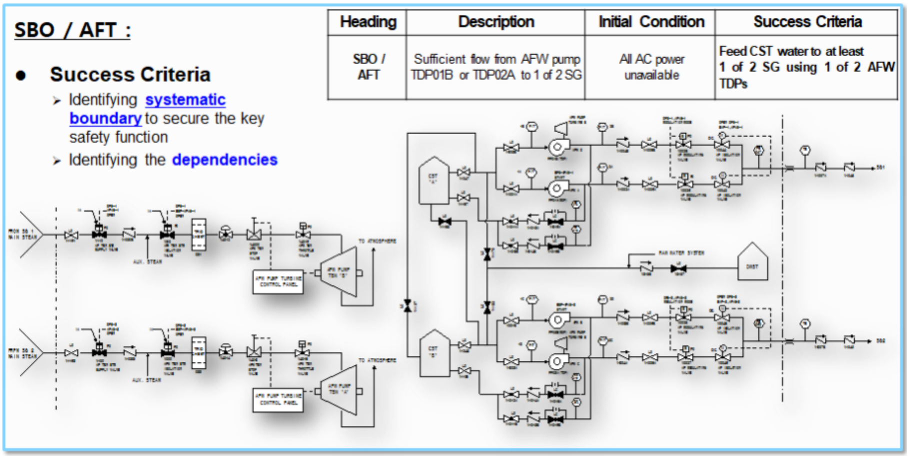

Fig. 6 Determination of success criteria for AFT heading

SBO / AFT :

- **Areas to be inspected**
  1. **AFW TDP**
  2. **Feed water Line**
  3. **Steam Line**
  4. **Dependencies**

SSC		Dependency	Category
3. Steam Line	V009	ESF-AFAS-2	TBN STM Isolation V/V
	V010	ESF-AFAS-1	TBN STM Isolation V/V
	V017		TBN Stop V/V
	V018		TBN Stop V/V
	V019		Throttle V/V
	V020		Throttle V/V
	…	…	…

SSC		Dependency	Category
1. AFW TDP	01B	125V DC01B EPS-AFAS-1, B	Control Power AFAS
	02A	125V DC 01A EPS-AFAS-2, A	Control Power AFAS
2. AF Modulating Valves	V035	125V DC 12-MC01A EPS-AFAS-1, A	Control Power AFAS
	V036	125V DC 01B EPS-AFAS-1, A	Control Power AFAS
	V037	125V DC 01A EPS-AFAS-2, A	Control Power AFAS
	V038	125V DC 12-MC01B EPS-AFAS-2, A	Control Power AFAS
	…	…	…
2. AF Isolation Valves	V043	480V MCC 11-MC08A EPS-AFAS-1, A, CH. A	Control Power AFAS / Cycling
	V044	125V DC 01C EPS-AFAS-1, B, CH. C	Control Power AFAS / Cycling
	V045	125V DC 01D EPS-AFAS-2, B, CH. D	Control Power AFAS / Cycling
	V046	480V MCC 11-MC08B EPS-AFAS-2, A, CH. B	Control Power AFAS / Cycling
	…	…	…

Fig. 7 Inspection items selected for AFT heading

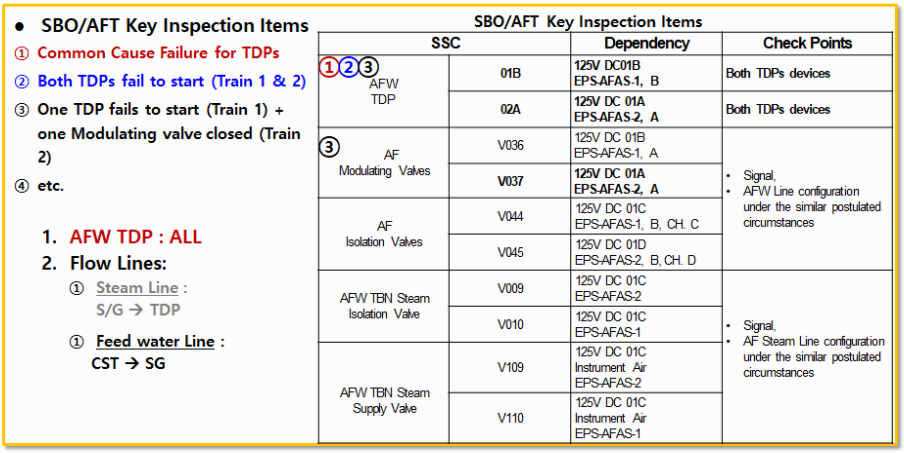

Fig. 8 Basic event list obtained from PSA cut set evaluation

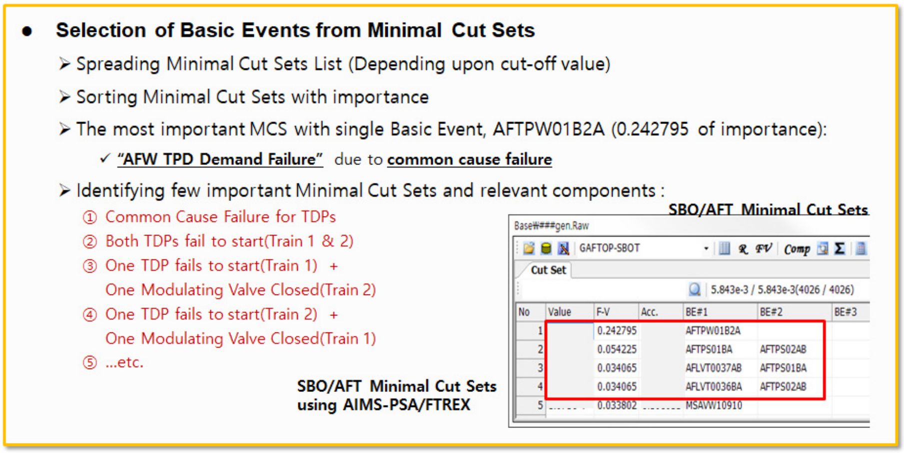

Fig. 9 Inspection items obtained from minimal cut set evaluation for AFT

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.

4. Conclusion

The periodic safety inspection program has been developed based on deterministic approach with the objective that nuclear power plant must be operated in compliance with the licensed conditions as confirmed through preoperational inspection program. The periodic inspection program should include, therefore, not only the safety related SSCs but also power conversion side that is not directly associated with nuclear safety. Therefore, 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. In this study, two track approaches are proposed using PSA: 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 initiating 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 OPR-1000. The inspection items were determined through success path approach and its 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. This methodology proposed in this investigation could be used to supplement the current periodic safety inspection program based on the deterministic approach by providing relative safety important systems and components to avoid core damage frequency. After Fukushima accident, design extension conditions should be considered to improve safety of nuclear power plants. As safety confirmatory process, the periodic safety inspection should by nature cover newly added safety systems and components to cope with design extension conditions. As further study is necessary to exploit the full PSA considering design extension conditions, this methodology should be also investigated more to accommodate such new conditions.

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) IAEA, 2016, "Fundamental Safety Principles", International Atomic Energy Agency, Vienna, *Safety Fundamentals No. SF-1*.

(2) IAEA, 2015, "The Fukushima Daiichi Accident", International Atomic Energy Agency, Vienna, *GC(59)/14*.

(3) IAEA, 2005, "Assessment of Defence in Depth for Nuclear Power Plants", International Atomic Energy Agency, *Safety Report Series No. 46*.

(4) IAEA, 2016, "Safety of Nuclear Power Plants: Design", International Atomic Energy Agency, Vienna, *Specific Safety Requirements No. SSR-2/1 (Rev.1)*.

(5) IAEA, 2010, "Development and Application of Level 1 PSA for Nuclear Power Plants", International Atomic Energy Agency, Vienna, *Specific Safety Guide No. SSG-3*.

(6) Lim, J., Kim, H. and Park, Y., 2018, "Review of the Regulatory periodic inspection System from the Viewpoint of Defence-in-Depth in Nuclear Safety", *Nucl. Eng. Tech.*, No. 50, pp. 997-1005.

(7) USNRC, 2018, "Technical Basis for Inspection Program", Attachment 2, U.S. Nuclear Regulatory Commission, Washington, DC, *Inspection Manual Chapter 0308*.

(8) USNRC, 2018, USNRC Inspection Manual Chapters, https://www.nrc.gov/reading-rm/doc-collections/insp-manual/manual-chapter/.

(9) USNRC, 2018, USNRC Inspection Procedures,

https://www.nrc.gov/reading-rm/doc-collections/insp-manual/inspection-procedure/.
(10) Park, Y., Park, H., Park, H., Lim, J., Park, J., An, H., Lee, Y., Lee, B., Lee, U. and Ham, J., 2016, "Development of Defence-in-Depth based periodic safety inspection Incorporating Probabilistic Safety Assessment", *N-STAR-16NS12-07.*
(11) USNRC, 2014, "Reactor Oversight Process Basis Document", U.S. Nuclear Regulatory Commission, Washington, DC, *Inspection Manual Chapter 0308.*
(12) Per Hellstroem, 2015, "DID-PSA: Development of a Framework for Evaluation of the Defence-in-Depth with PSA", Swedish Radiation Safety Authority, Katrineholm, 2015:04