# Practical Application of PSA Model for the Evaluation of Defense in Depth

Ho Gon Lim [a], Jin Hee Park [a], Dong San Kim [a]
[a]*Korea Atomic Energy Research Institute., Division of Integrated Safety Assessment, 1045 Daedeuk-Daero, Yusung-Gu, Daejeon, The Republic of Korea*
[*]*Corresponding author: hglim@kaeri.re.kr*

## 1. Introduction

Since defense in depth (DID) has been accepted as fundamental concept of nuclear safety [1, 2], various studies have been performed to characterize the DID more objectively and quantitatively [3, 4, 5, 6, 7]. Recently, the methodology of Defense in depth (DID) characterization using PSA model has been proposed to avoid the subjectivity in the evaluation and also overcome the qualitative aspects of DID [8]. In this study, DID level 1 and 2 may correspond to initiating event (IE) in a PSA model, which means DID level 1 and 2 can be deducted from. Initiating event. However, the practical method how DID level 1 and 2 can be separated from IE was not given from the paper. This paper proposes the method how DID level 1 and 2 can be separated from IE in a PSA model.

Also, contrary to the DID level 1 and 2, DID level 3 need to be broken up to know the detailed DID structure from the accident sequence of level 1 PSA. This is due to the fact that most of safety resources of a nuclear power plant are assigned to DID level 3. Emergency Core Cooling System for Large LOCA is a good example of DID level 3. The detailed DID level 3 separation method is also proposed at the present paper.

## 2. PSA Application for DID Evaluation

In this section, methods of DID level 1 and 2 evaluation from IE and detailed DID level 3 substructure characterization from level 1 PSA model are presented.

### *2.1 Separation of DID 1 and 2 from IE of PSA model*

In most PSAs, a specific IE is a set of events that pose a similar threat to a NPP, and is treated as a simple event without considering causality between primitive cause and mitigation of the event, and an accident scenario is derived from it.

If the causal relationship according to the occurrence of the IE can be identified, the frequency of the initiating event can be evaluated using the fault tree (FT). In general, an IE caused by a failure of a system that supplies essential safety resources, such as electricity or cooling water, can be evaluated by a logical model such as a FT. The failure of the DID level 1 and 2 corresponds to (1) occurrence of an event causing abnormality and (2) failure to recover from an abnormal state. So it can be separated from a FT of IE by decomposing abnormal event and failure event of mitigation from the whole FT structure. The FT is basically a Boolean logic expression, and is usually expressed as the sum of product events called as the minimal cut set (MCS) through the simplification process of the Boolean expression using a computer program. For better understanding, consider a simple system that supplies a fluid as shown below.

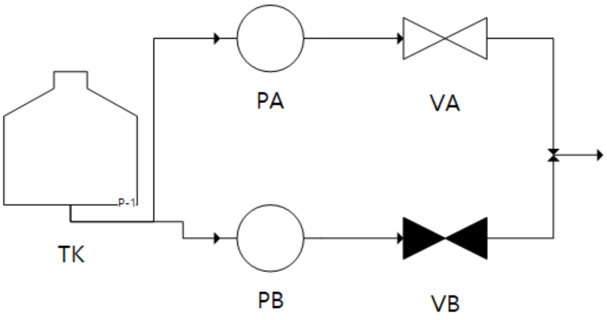

Fig. 1. Flow diagram of simple cooling fluid supply system.

A FT can be generated assuming only a single failure of each device in the figure above, and it can be expressed using Boolean expression as follows.

$$\begin{aligned} System\ failure &= TK + (PA + VA) \cdot (PB + VB) \\ &= TK + PA \cdot PB + PA \cdot VB + VA \cdot PB + VA \cdot VB \end{aligned}$$

In the figure above, assuming that the upper flow path supplies fluid during normal state and the lower flow path is on standby, the event that causes this system abnormality is the case where the events described as TK, PA, VA occur. If the flow path is working, it is possible to recover from these abnormal events.

In general, when the MCS is known from a FT of IE, MCS can be expressed by the following equation.

$$\boldsymbol{IE} = \sum_{i=1}^{n} \boldsymbol{A_i B_i} \tag{1}$$

Here, IE is an abbreviation for an initial event, and Ai and Bi correspond to an abnormal event and a recovery failure event, respectively. There are cases in which recovery of certain abnormal events is impossible, in which case Bi is “true” or 1. In the above example, if the tank is failed, there is no recovery function. In this case, the recovery failure event is 1. In Eq. (1), the failure of the first stage of DID can be expressed by the following Boolean equation.

$$d(1) = \sum_{i=1}^{n} A_i \qquad (2)$$

The failure probability of the DID level 1 can be obtained by calculating the probability of Eq. (2), and when the probability of an individual event is very small, it can be obtained as follows using the rare event approximation.

$$p(d(1)) = p\left(\sum_{i=1}^{n} A_i\right) \approx \sum_{i=1}^{n} p(A_i) \qquad (3)$$

In most cases, the probability of an anomalous event is not small and the number of anomalous events is quite large, so the rare event approximation cannot be used. Minimal cut upper bound can provide exact probability if it is assumed that the abnormal events are mutually exclusive in this case as follows

$$\mathrm{p}(d(1)) = p\left(\sum_{i=1}^{n} A_i\right) = 1 - \prod_{i=1}^{n}(1 - p(A_i)) \qquad (4)$$

According to Eq. (1), the evaluation of the DID level 2 can be obtained as follows by evaluating the failure probability of the DID level 2 and dividing it by the failure probability of the DID level 1 according to Eq. (3).

$$p(d(2)|d(1)) = \frac{p(d(1) \cdot d(2))}{p(d(1))} \qquad (5)$$

### *2.2 DID Level 3 Decomposition and Evaluation*

DID level 3 is a state in which, in response to an initial event, it performs the function to prevent the initial event from developing into a severe accident in which the nuclear fuel of the nuclear reactor is damaged. Most of the safety resources are allocated to this part in the design of the nuclear power plant, and the emergency cooling system and auxiliary water supply system for cooling the power plant are all safety systems designed to respond to these initial events.

In the design of a nuclear power plant, if a large number of safety resources are allocated and there are two or more detailed levels of DID within DID level 3, it is necessary to separate and evaluate the safety status of the NPP.

The entire role of each DID phase of a nuclear power plant is to maintain the plant's key safety functions. The main key safety functions of nuclear power plants include:

- Reactor Reactivity Control
- Reactor system pressure control
- Maintaining reactor system coolant inventory
- Reactor system heat removal
- containment pressure control

Failure of each DID level may cause an immediate failure of the above safety function for a specific period or may lead to a situation in which the safety function fails by transitioning the state. The failure of the 3rd level DID means that one or more of the safety functions have failed, and in order to increase the reliability of the 3rd level DID, it is common to have a redundant safety system in charge of the core safety function in general. .

When a specific initial event occurs and an accident progresses over time, the PSA models it using a logical event decomposition method called an event tree. In the event tree, the safety system necessary to maintain the safety function or the set of safety systems that perform safety functions according to the success or failure of human actions undergo changes over time, and can have multiple sets of safety systems.

For ease of understanding, suppose that two critical safety functions are required in a hypothetical power plant, and each of the two safety systems can perform the key safety functions. Let $S_{11}$ and $S_{12}$ denote the two safety systems in charge of the first safety function, and let $S_{21}$ and $S_{22}$ denote the two safety systems in charge of the second safety function. For a specific initial event, suppose that the safety system set ($S_{11}$, $S_{21}$) performed the safety function at the beginning of the event. After that, if $S_{11}$ fails and the set of safety systems is changed to ($S_{12}$, $S_{21}$), then $S_{21}$ fails and finally transitions to ($S_{12}$, $S_{22}$).

However, this detailed separation can over-express the DID levels when the number of core safety functions and safety systems increase, thereby distorting the qualitative properties of the DID steps. In addition to this, there are instances where certain critical safety functions may not be specifically required to achieve other safety functions. For example, when the boundary of the reactor coolant system is in intact, when heat removal from the reactor system is smoothly performed, safety functions such as pressure control and coolant inventory maintenance are not particularly required.

In order to overcome the difficulty of separating the DID level 3 in detail, and also to meet the design philosophy of the NPP in view of DID, a safety function that can perform multiple safety functions is selected, and the detailed defense in depth levels are separated based on this. This is the best way to evaluate a plant DID design philosophy.

As described above, the heat removal function of a nuclear reactor system can generally comprehensively support pressure control and coolant inventory maintenance, so by setting this function as a central function, the following method can be used to evaluate the three-level detailed DID. .

-Level 3 of detailed DID first layer: failure of the first reactor heat removal system or complete failure of other key safety function maintenance systems (failure to complete possible systems)
- Level 3 detailed DID 2nd layer: failure of the second reactor heat removal system or complete failure of other critical safety function maintenance systems

Subsequent detailed steps are repeated in the same manner as above. In the case of a standard light water reactor represented by OPR-1000 in Korea, it has an auxiliary water supply system and an feed and bleed operation system as a representative reactor heat removal system. In this case, DID level 3 can consist of up to two detailed sublevels. To illustrate the decomposition method of DID level 3 using the PSA model, DID level 3 is subdivided into detailed DID levels for the initial event that causes the shutdown of the power plant called as general transient event. The figure below shows the event tree for transient events used in the PSA model.

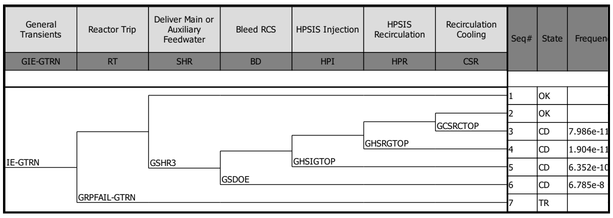

Fig. 2. General transient event tree used in a PSA model.

The failure of the first layer of DID level 3 is a failure of the first reactor heat removal system or a complete failure of the key safety function maintenance system. It is established when Auxiliary Feedwater (secondary side auxiliary water supply) fails. If this is expressed as a event tree of defense-in-depth, it is expressed as shown in the figure below.

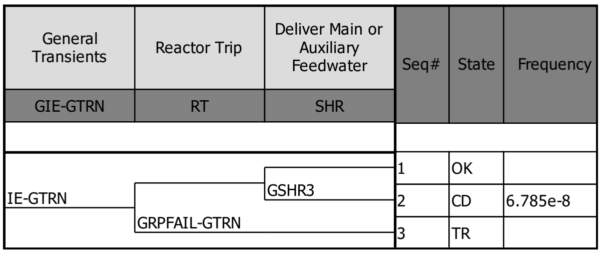

Fig. 3. DID 3.1 event tree for General transient event

Through the above process, DID level 3 can be divided into first and second layers, each can be evaluated, and the reliability of each can be quantitatively calculated through Eq. (3) of previous study [8].

## 3. Conclusions

A practical evaluation method for DID 1 and 2 from IE in a PSA model and decomposition of detailed DID 3 was proposed in this paper. IE using FT approach can be used to generate DID level 1 and 2 using proposed method. Detailed DID level 3 decomposition is necessary to understand the detailed structure of DID level 3 because most of safety resource in a NPP design is assigned to DID level 3.

By using the present method, DID strength and the steps can be effectively calculated and be used to know the effect of issues or design modification in a currently operating NPP. Also, this method can be used to confirm the safety of new design NPP.

## REFERENCES

[1] USNRC, Historical Review and Observations of Defense-in-Depth, NUREG/KM-0009, Washington, DC, March 2016
[2] Defense in depth in Nuclear Safety, INSAG-10, IAEA, Vienna
[3] A Framework for Using Risk Insights in Integrated Risk-Informed Decision-Making, EPRI, February, 2019
[4] The Link between the Defense-in-Depth Concept and Extended PSA, Technical report ASAMPSA_E / WP30 / D30.7/2017-31 volume 4
[5] Swedish Radiation Safety Authority, SSM, “DID-PSA: Development of a Framework for Evaluation of the Defense-in-Depth with PSA,” January 2015
[6] Fleming, K.N., and Silady, F.A., “A Risk Informed Defense-in-Depth Framework for Existing and Advanced Reactors,” Reliability Engineering & System Safety, Volume 78, issue 3, December 2002, Pages 205-225.
[7] Cindy Williams et al, Integrating quantitative defense-in-depth metrics into new reactor designs,” NED 2018
[8] H. G, Lim, Quantification of Defense in Depth using Risk model, Transactions of the Korean Nuclear Society Spring Meeting Jeju, Korea, May 13-14, 2021