Quantification of Defense in Depth using Risk model

Ho Gon Lim [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 considered as the qualitative aspects of nuclear safety, it is treated such as checklist of important DID elements of nuclear system or questionnaire are given to check the integrity of the DID structure. Recently, DID is no longer treated as pure qualitative manner. Instead, some aspects of DID is quantitatively measured to obtain more general and objective result for the DID strength of a nuclear power plant (NPP). [1, 2]

This paper proposes a new framework and measures to quantify DID of NPP based on the IAEA conceptual DID structure [3] and risk model in terms of probabilistic safety assessment (PSA).

2. DID structure modeling

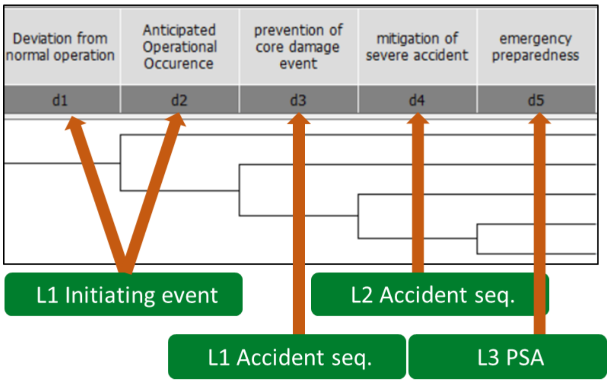
2.1 Conceptual DID structure

First conceptual DID structure is mainly focused on the physical structure of radiological material not to release to environment such as fuel cladding, reactor coolant system, and containment. In this study, more general concept of DID described in INSAG-10 [3] is used to model the DID structure. Table 1 shows the five sequential stages of DID described in INSAG-10

Levels of defense in depth	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

2.2 Translation of DID into PSA model

Most of DID levels can be expressed with PSA model. For example, the DID level 1 and 2 of INSAG-10 is corresponding on the initiating event of a PSA model. Figure 1 shows each correspondence of DID level with PSA model.



3. Quantification of DID model

3.1 DID event tree quantification

As is not similar with PSA model quantification, DID model should be quantified sequentially from the level 1 to level 5 to evaluate each DID level failure frequency. This is due to the dependency of each DID level. At the level i of DID the failure event is expressed with the following Eq. (1)

$$Df_i = \cap_{j=1}^{i} d(j) \quad (1)$$

where Df_i is the successive failure event from level 1 to level i of DID failure event and *d(j)* is the failure event of level *j* DID.
Since each DID level has dependency on the previous DID level, the failure probability of Df_i is expressed as follows :

$$p(Df_i) = p\big(d(1)\big) \cdot p\big(d(2)\big|d(1)\big) \cdots p\big(d(i)\big| \cap_{j=1}^{i-1} d(j)\big) \quad (2)$$

Where the last term of Eq. (2) is the probability of DID level i considering the dependency with DID levels from 1 to i-1. Since each DID level failure probability has dependency on other DID level, its quantification can be accomplished by the calculation of sequential failure probabilities as follows:

$$p\big(d(i)\big| \cap_{j=1}^{i-1} d(j)\big) = \frac{p(Df_i)}{p(Df_{i-1})} \quad (3)$$

3.2 DID measure development

To evaluate the various aspects of DID, it needs to make quantification measures using the DID model. For a given initiating event, DID toughness can be defined as follows :

$$DID\ \ Toughness = \left(\prod_{j=1}^{n} p(Df_j\right)^{-1} \quad (4)$$

Where $p(Df_i)$ is bounded by a prescribed value to consider the conservatism of the DID barrier. 10^{-3} is the one of the recommended value for the lower bound.

Since DID has a qualitative characteristic in essence, the number of total failure of DID level for a given initiating event is an important parameter. In the DID model, it can be obtained by tagging the heading of DID event tree.

For the total DID strength cumulative failure frequency may be an important measure to evaluate the DID strength of an NPP as follows :

$$TDf = \sum_{j=1}^{m} p(Df_5^j) \quad (5)$$

Finally, to evaluate the dependency on human event of the DID level, the following program dependency measure can be used.

$$PD = \frac{p(Df_i|\forall Hep, Hep = 0)}{p(Df_i)} \quad (6)$$

Additional DID measures can be developed to evaluate various aspects of DID. For example, the common cause failure (CCF) is a very important aspects of DID which has not yet developed in this paper

3. Conclusions

As decision making methodology for the safety of NPP has been moved toward risk-informed manner, the role of risk in the decision making process increase its area. The DID quantification using risk model is one example of such trend. DID quantification method using PSA model was proposed in this paper based on conceptual 5 level DID structure. Also, several DID measures was developed to evaluation the various aspects of DID strength. Real pilot study using NPP PSA model will help the applicability of the proposed method including further improvement of the method.

REFERENCES

[1] A Framework for Using Risk Insights in Integrated Risk-Informed Decision-Making, EPRI, February, 2019
[2] Swedish Radiation Safety Authority, SSM, "DID-PSA: Development of a Framework for Evaluation of the Defense-in-Depth with PSA," January 2015
[3] Defense in depth in Nuclear Safety, INSAG-10, IAEA, Vienna