On the Engineering Approach for Justifying Defense-in-Depth Principle in the Risk-Informed Integrated Decision-Making

Seung-Cheol Jang
Korea Atomic Energy Research Institute, Daedeok-Daero 989-111, Yuseong-Gu, Daejeon, 34057, Korea
Corresponding author: scjang@kaeri.re.kr

1. Introduction

In risk-informed decision-making (RIDM), licensing basis changes are expected to meet five principles as follows ([1],[2]).

① The change meets the current regulations.
② The change is consistent with the defense-in-depth(DiD) philosophy.
③ The change maintains sufficient safety margins.
④ The risk increases by the change are small and are consistent with the safety goal policy.
⑤ The impact of the change should be monitored using performance measurement strategies.

According to the principles above, the appropriate engineering analyses should be conducted to justify the proposed licensing basis change, including traditional and probabilistic analyses. Each of these principles should be considered in the risk-informed integrated decision-making process, as illustrated in Fig 1 [1].

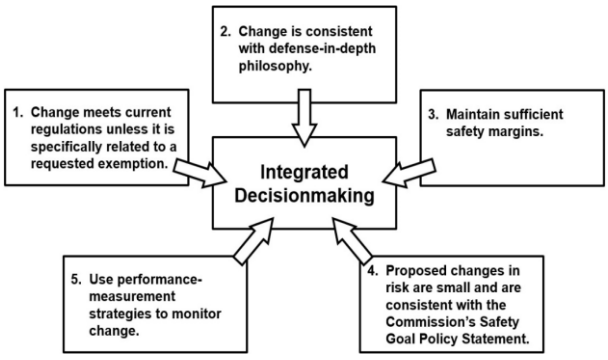

Fig. 1 Risk-informed integrated decision-making process [1]

This paper focuses on the engineering approach to justify the principle 2 (consistency with the DiD philosophy) in the risk-informed licensing basis changes. Note that the author does not take any position on the appropriateness of DiD philosophy itself, but rather explores an practical engineering approach to justify whether the change is consistent with the current DiD philosophy given in terms of traditional analysis. It can help risk-informed decision makers evaluate impact on the current DiD likely to result from the proposed licensing basis changes.

2. Current Domestic Regulatory Requirements for the Principle 2

The engineering evaluation should assess whether the proposed licensing basis changes are consistent with the DiD philosophy (Principle 2). Similar to NRC regulatory guide[1], the domestic regulatory positions for the principle 2 can be summarized as seven engineering elements ([2],[3]).

- DiD is an element of the safety philosophy that employs successive compensatory measures to prevent accident and mitigate damage if a malfunction or accident occurs at a nuclear facility
- Seven considerations that should be used to evaluate the impact of the design basis change on defense-in-depth:
  - ✓ Preserve a reasonable balance of accident prevention and accident mitigation
  - ✓ Preserve adequate capacity of design features without an overreliance on programmatic activities as compensatory measures
  - ✓ Preserve system redundancy, independence, and diversity commensurate with the expected frequency and consequences of challenges to the system, including consideration of uncertainty
  - ✓ Preserve adequate defense against potential Common Cause Failure(CCF)
  - ✓ Maintain multiple fission product barriers
  - ✓ Preserve sufficient defense against human errors
  - ✓ Maintain the intent of the general design criteria of nuclear facility.
- PSA information, such as quantitative risk measures such as core damage frequency (CDF) and large early release frequency (LERF), as well as contributors to accident sequences, can be utilized in assessing the impact of design basis changes on the DiD elements.

3. An Engineering Approach for Justifying the Principle 2

Defense-in-depth(DiD) is a key element of nuclear safety philosophy that provide multiple protective measures for accident prevention and accident mitigation, including multiple barriers to prevent external leakage of radioactive materials from nuclear power plants. Prior to discussing the engineering approach of the DiD principle for design basis changes, it need to note that DiD in nuclear power plant is implemented as four layers of defense that are a mixture of conceptual constructs and physical barriers, as in NRC RG1.173[1].

- Robust plant design to survive hazards and minimize challenges that could result in an event occurring,
- Prevention of a severe accident (core damage) if an event occurs,
- Containment of the source term if a severe accident occurs, and
- Protection of the public from release of radioactive material (e.g., through siting in low-population areas and the ability to shelter or evacuate people, is necessary).

In addition, K.F. Fleming, *et. al.*[4] outlined various definitions of the DiD principle of authoritative overseas regulators.

Engineering assessment of the DiD elements is to make engineering interpretations, reviews, and judgments about the extent to which the the defined DiD elements are affected by design basis change. In general, there are two approaches that can be applied to the engineering assessment of the DiD principles: 1) the deterministic approach and 2) the risk-based approach. However, there are differences in interpretation of DiD concepts between structuralists who advocate application of deterministic approach and rationalists who assert risk-based approach[5]:

- Structralist's interpretation: DiD is embodied in the structure of regulations and in the design of the facilities built to comply with those regulations. The requirements for defense in depth are derived by repeated application of the question, “What if this barrier or safety feature fails?”
- Rationalist's interpretation: DiD is the aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression.

Differences in the scope and nature of DiD do not mean a standoff between the two groups, and the problem is that no group is providing the only means to determine whether the degree of DiD has been sufficiently secured. While the structuralist's interpretation of the DiD may dilute the benefits of regulation on the use of risk information, the rationalist's interpretation of the DiD may overlook the benefits from the experience of the structuralist[6]. Accordingly, NRC[5] adopted a pragmatic approach, which is key to:

- Apply the concept of defense in depth in the deterministic ('structuralist' or traditional) approach to the upper level,
- Apply a probabilistic ('rationalist' or 'risk-based') approach at the lower level, but return to the deterministic approach if the PSA model is incomplete.

This approach forms the basis for the implementation of the reactor monitoring process (ROP)[7]. First, in Fig 2, the uncertainty of PSA results increases from the left ('Initiating Event') to the right ('Risk'). From the structuralist's point of view, there are interim goals of upper level (rectangular with blue-dashed line in Fig. 2), such as core image frequency (CDF), large early release frequency (LERF), conditioned connection failure capability (CCFP), or FC (frequency-consequence) curve, which are considered to be a measure of balance between accident prevention and mitigation. However, for structuralists, the traditional DID interpretation perspective is practically maintained for lower levels (i.e., system and content performance, fission product transport, etc.) dealing with the issue of decision uncertainty.

On the other hand, from the rationalist's point of view, the interim safety target values are only one option that is not relevant to the DiD, and the rationalist's interest is in a lower level model (rectangular with red-dashed line in Fig. 2), such as the system model, containment performance model, and transportation model of radioactive materials, etc. From a rationalist's point of view, the DiD is generally a component of the PSA model, so it only needs to be used to address the issue of uncertainty in the lower level PSA model. It is clear that the extreme of rationalist interpretation lies not in 'risk-informed' but in 'risk-based'.

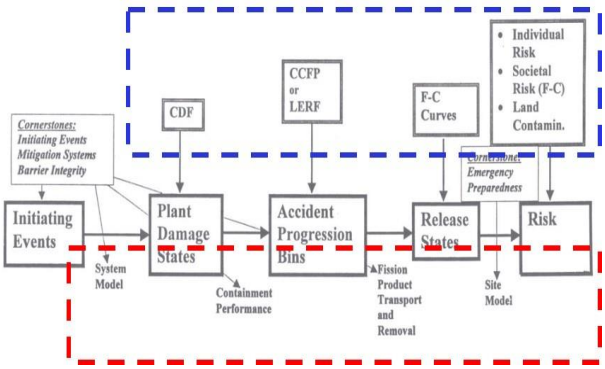

Fig. 2 Risk Measures for risk-informed decision-making[8]

The proposed pragmatic approach combines the concept of DiD into the concept of risk-informed regulation, as shown in Fig. 3, which is a combined approach of structuralist's and rationalist's DiD concepts. It is because each group's approach are incomplete in dealing with impact of design basis changes on DiD elements. For example, for the current safety impact assessment on smoke in the event of a fire, it is important to address the uncertainty of decision making according to the traditional prescriptive DiD measures, which is not covered by the fire PSA model. Examples of these can exist in many areas, including digital software, the effects of electromagnetic interference(EMI), and so on.

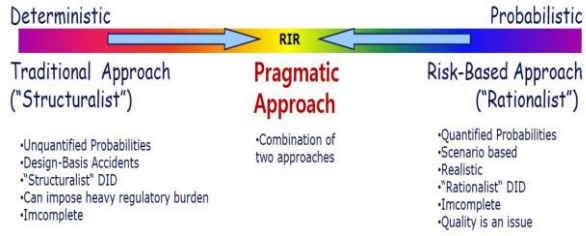

Fig. 3 A pragmatic approach in risk-informed regulation

Finally, in this paper, the analysis process is proposed as shown in Fig. 4 on the basis of a pragmatic approach to confirm the maintenance of the DiD principle on design basis changes.

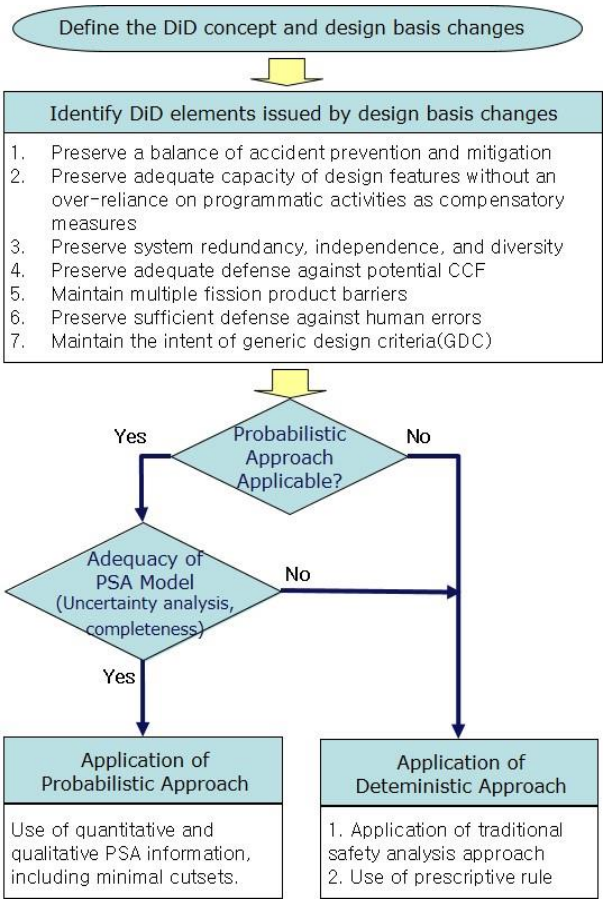

Fig. 4 A pragmatic analysis process for Principle 2 (consistency with DiD philosophy) of RIDM

4. Conclusions

This paper focuses on the engineering approach to justify the principle 2 (maintaining DiD philosophy) in the risk-informed licensing basis changes. Principle 2 is an area that should be addressed by a pragmatic approach, which combines traditional approaches and probabilistic ones. A pragmatic engineering procedure for principle 2 was proposed in the paper. The proposed procedure was applied to licensing basis changes of the surveillance test intervals for safety-related I&C systems in OPR-1000 reactors [8]. It can help risk-informed decision makers evaluate impact of design basis changes on the DiD elements.

ACKNOWLEDGEMENTS

This work was supported by the Nuclear Research & Development Program of the National Research Foundation of Korea grant, funded by Korean government, Ministry of Science and ICT.

REFERENCES

[1] U.S. NRC, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, Regulatory Guide 1.174, Rev.3, 2018.1.
[2] KINS, General Requirements of the Risk-Informed Application to Licensing Basis Changes for NPP, KINS Regulatory Guide 16.7, 2010.
[3] KINS, General Requirements of the Risk-Informed Application to Technical Specification Change for NPP, KINS Regulatory Guide 16.8, 2010.
[4] K.N. Fleming, F.A. Silady, A risk informed defense-in-depth framework for existing and advanced reactors, Reliability Engineering and System Safety, V.78, 2002, pp.205–225..
[5] U.S. NRC, The Role of Defense in Depth in a Risk-Informed Regulatory System, ACRS Letter from chairman Dana A. Powers to NRC chairman Shirley Ann Jackson, May 19, 1999.
[6] G.E. Apostolakis, "the Precautionary Principle and Defense in Depth," presented at the 2nd ILK Symposium, Munich, Oct. 28, 2003.
[7] J.N. Sorensen, G.E. Apostolakis, T.S. Kress and D.A., Powers, "On the Role of Defense in Depth in Risk-Informed Regulation," *Proceedings of PSA '99, International Topical Meeting on Probabilistic Safety Assessment*, Washington, DC, August 22 -26, 1999.
[8] S.C. Jang, *et. al*., Improvement of Risk-Informed Surveillance Test Interval for the safety-Related I&C System of Ulchin Units 3 and 4, KAERI/TR-4558/2012, 2012.