Transactions of the Korean Nuclear Society Spring Meeting
Gwangju, Korea, May 30-31, 2013

Revisiting the Concept and Implementation of Defense-in-Depth

Young Sung Choi
Safety Policy Department, Korea Institute of Nuclear Safety
cys@kins.re.kr

1. Introduction

It is widely accepted that defense-in-depth (DID) has been the core of safety philosophy in nuclear safety regulation. Its concept has been developed and refined over many years to go beyond physical barriers and design practices. The historical development of the concept led to a general structure of four physical barriers and five successive levels of defense.

The accident at the Fukushima nuclear power plant (NPP) showed that multiple levels of defense could fail at the same time, demonstrated how these could work and how some were challenged, and gave the chance of the concept and implementation being improved.

This paper examines the traditional concept and implementation strategies of DID, identifies some weaknesses in that, and suggest some complements and new approach to improving the application of DID.

2. Descriptions of DID and Deficiencies at the Fukushima NPP

Since it is an effective safety strategy of high hazardous industry as well as nuclear industry, DID is described and explained in many literature. As far as nuclear safety is concerned, the followings should be referred to in order to understand the concept correctly:

- "[It] ensures that no single technical, human or organizational failure could lead to harmful effects" in the section, "Principle 8: Prevention of Accidents" in IAEA SF-1 [1],
- "Special attention has been paid to internal and external events that have the potential to adversely affect more than one barrier at once" in the section, "Requirement 13: Assessment of DID" in IAEA GSR Part 4 [2],
- "[If] a failure were to occur, it would be detected and compensated for or corrected by appropriate measures" in the section, "The concept of Defense in Depth" of IAEA SSR-2/1 [3],
- "Accident prevention is the first priority." in the section, "Strategy for DID" in IAEA INSAG-10 [4],
- "The ultimate purpose of DID is to compensate for uncertainty." in the chapter, "Treatment of Uncertainties" in NUREG-1860 [5], and
- "[The] application of defense-in-depth should be strengthened by formally establishing an appropriate level of defense-in-depth to address requirements for extended design-basis events." in U.S. NRC's NTTF Report [6].

Based on these basic but easy-to-overlook ideas, deficiencies of defenses at the Fukushima NPP can be found as briefed in Figure 1 even with only limited information currently available.

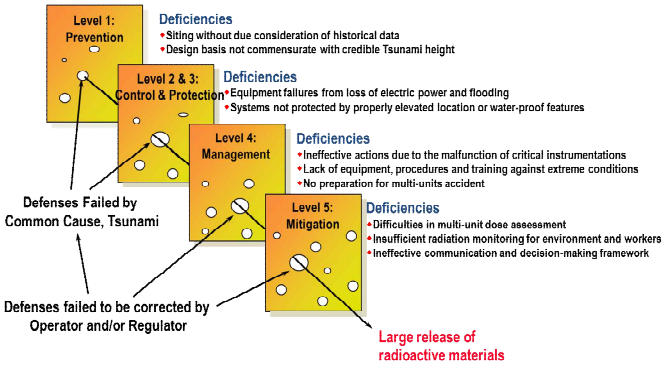

Figure 1. Deficiencies of defenses at the Fukushima accident

3. Complements to the DID Concept

For DID concept to be valid, several complements are needed on the basis of prominent lessons from the Fukushima.

First, provisions of DID have been well developed in detail against internally initiating events but they are less developed against external events. For example, the objective and essential means described in INSAG-10 [4] are not appropriate for flooding, wildfire, storm, sabotage, etc. Thus, additional protection measures in level 1 and 2 against external factors should be strengthened and implemented. The objective might include monitoring of and responding to natural phenomena and intentional acts; and the means might extend to defending guard such as tsunami wall, water-proof, fire suppression, security guards, etc.

Second, possible vulnerabilities in defenses are not detected or corrected by the concept itself but by the rigorous implementation of the concept in all safety related activities. Thus, detection and corrective action must be ensured by multiple levels of organizational controls/managements/oversights/peer-reviews as shown in Figure 2.

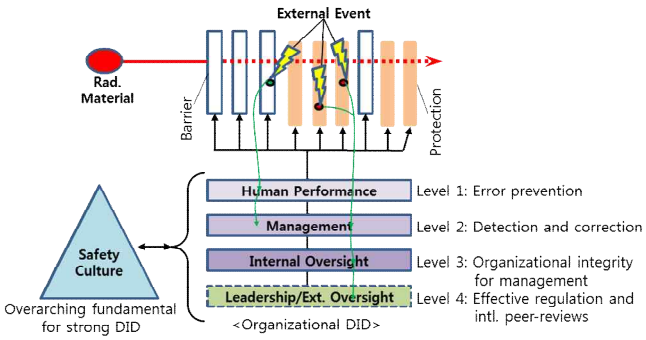

Figure 2. Application of DID concept to Organization

Third, multiple nature of DID may be misunderstood to excuse compromise in the absence of one level and subsequently bolster complacency. It should be enshrined that continuous improvements are needed to avoid concealment of dangerous defenses. Continuous improvements with best practices utilized should be embedded in the concept of DID or emphasized through upholding safety culture as a vital enabler of DID.

4. Balance between Prevention and Mitigation

Reducing the frequency of initiating events and their resulting events is viewed as a preventive measure and helping to cope with its consequences is seen as mitigation as shown in Figure 3. Usually, prevention measures are emphasized first and then mitigation measures come to deal with the remaining sequence of low frequency. Since a given component, procedure or resource may serve for both prevention and mitigation, comprehensive analysis such as probabilistic safety analysis (PSA) would be necessary to find the balance between them.

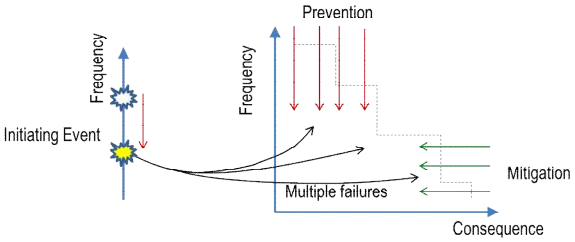

Figure 3. Prevention and Mitigation on Frequency-Consequence (F-C) Curve

Fukushima accident showed that sole dependence on mitigation strategy could not guarantee sufficient defenses against a rare-yet-credible event which has a potential for cliff-edge effects. This can be shown graphically in Figure 4.

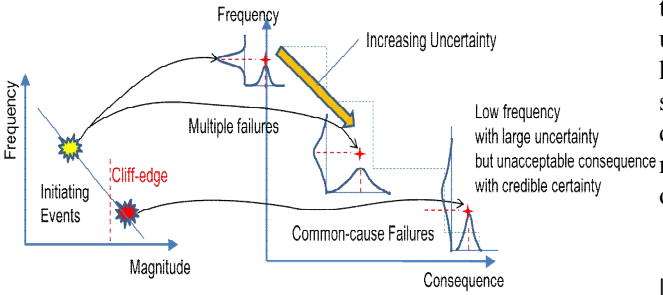

Figure 4. The implication of a rare-yet-credible event with a potential for cliff-edge effects

Although it might be said that mitigation was successful based on the fact of no acute radiological effects on human health and the expectation of no chronic ones, we must acknowledge that less rigorous application of DID was made to a number of areas. Lessons continue to emerge in a wide variety of areas such as:

- Stringent approach to external events, particularly with cliff-edge effects on multiple units,
- Multi-purpose, multi-applicable and high-reliable mobile equipment for control, cooling and containment over a wide range of events,
- Extension of consideration to cooling spent fuel pool (preserving the integrity of dry cask of spent fuel and protecting radwaste storage facility),
- A preplanned hierarchy of command and control and decision-making with clear transition points,
- Technically sound and practical procedures, guidelines, emergency plan, and
- Decision-maker, plant operators and supporting staff with competences and protective equipment.

At this point, there is a question arising, is a new defense-in-width concept necessary? An application of DID to a variety of events, equipment, procedures, resources, facilities, etc. as wide as possible can be the last but not least prominent way of dealing with the unexpected.

5. Conclusions

The philosophy of the multiple layers of protection of the defense-in-depth worked well at Fukushima in response to some of the challenges – safety systems successfully responded to the initial earthquake that surely challenged the Design Basis. However the subsequent tsunami, with its maximum wave height greater than the design basis, invalidated all layers of the Fukushima NPP. This raises the question on which of the philosophy or the implementation of DID fell short at Fukushima.

This paper suggests several complements necessary to the concept of DID and new application practice in a wide variety of safety related objectives/areas/events. Since its conception, DID appears to have been successfully applied to the design and operation but less to the site, external events, resource requirements, the unexpected impacts of organization, etc. Thus, the horizontal as well as vertical application of DID is suggested. Here, the latter application means repeated questions of "What if this fails?" and the former one means the application of DID to all the applicable objectives, which can be a real defense-in-width.

REFERENCES

[1] IAEA, Fundamental Safety Principles, SF-1, 2006
[2] IAEA, Safety Assessment for Facilities and Activities, GSR Part 4, 2009
[3] IAEA, Safety of Nuclear Power Plants: Design, SSr-2/1, 2012
[4] IAEA, Defense in Depth in Nuclear Safety, INSAG-10, 1996
[5] U.S. NRC, Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing, NUREG-1860, 2007
[6] U.S. NRC, Recommendations for Enhancing Reactor Safety in the 21st Century, 2011