Safety Measures Based on Defense-in-Depth for PHWR during Outage

Myung-Ki Kim, Sung-Yull Hong, Hae-cheol Oh, Bag-Soon Chung, Mi-Ro Seo, Myung-Suk Sung
Korea Electric Power Research Institute,103-16, Munji-Dong, Yusong-Gu, Taejon 305-380 Korea,
kimmk@kepri.re.kr

1. Introduction

The risk during outage should be properly managed and controlled since the nuclear operation experiences and researches have shown that its risk is in the same order of magnitude at power. Having some systems or components out of service during outage causes the potential for loss of safety functions that may prevent or mitigate the consequences of an event. The suitable outage schedule and strategies certainly enhances the safety during outage, so that plant safety assessment tool according to planned outage schedules becomes one of key elements in managing outage risk. It is well known that probabilistic safety assessment (PSA) is an effective tool for plant safety assessment, but during outage its limitation such as model quality, and phenomenal uncertainty prevent from application

Recently, ERPI has suggested an alternative method using defense-in-depth (DID) concept. It does not assess plant defense-in-depth itself, but assesses the plant safety in terms of level of defense-in-depth of major safety functions which are decay heat removal, inventory control, power availability, reactivity control, and containment. In order words, it assesses how many safety functions are available to maintain the plant safe.

In this paper, we propose the safety measures based on DID for pressurized heavy water reactor during outage, considering the relationship between PSA and DID and various defense-in-depth concepts.

2. Relationship between DID and PSA

There are two perceptions of DID in safety. One, structural model, is that DID is considered to be multiple and redundant measures to identify, prevent, and mitigation accident to such a degree that the design meets the safety objects. It is in general a view point of plant design. The other, rationalist model, is that its role schemes as compensation for inadequacies, incompleteness, and omission of risk analysis. It is a view point of risk informed regulation. For fullness of safety, two perceptions should be implemented in performing safety. That is, DID is interpreted by both traditional concept and as back up a quality of risk analysis. They complement each other, as shown in Fig. 1. We focus on DID measures, so that we consider the structural model as fundamental value, and the rationalist model as a subsidiary role, which is a case (a) in Fig. 1.

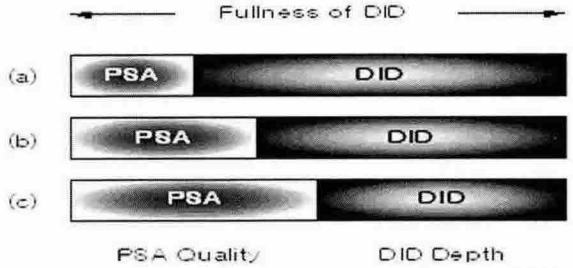


Figure 1. Fullness of safety from both PSA and DID.

From this view point, the relationship between DID and PSA as a risk analysis is shown in Fig. 2. For example, where the system configuration is changed by out of service of the systems and components during outage, tolerable margin on safety or relaxation of technical specifications estimated by PSA is related with DID as shown in Fig. 2.

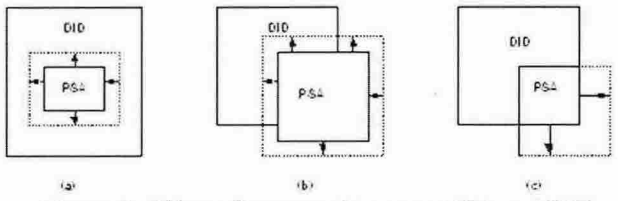
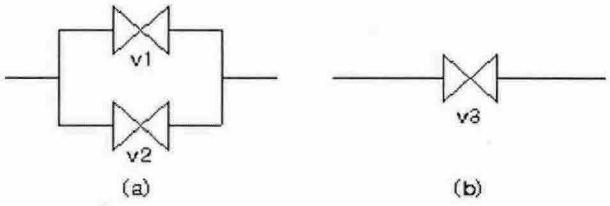


Figure 2. Effect of system change on PSA and DID.

Case (a) is that the tolerable margin obtained from PSA information fully satisfy all DID requirements. Case (b) is that it partially satisfies DID requirements while partially do not. Case (a) is that it does not satisfy all of them. In other words, both PSA and DID analyses are needed in some cases, and in others do not.

Consider the importance of valves in Figure 3, where reliability of valve 1 and 2 are the same, and valve 3 is twice as reliable as valve 1. From the PSA view point, the reliability of the system (a) is the same as that of the system (b). But from DID view point, the system (a) is more safe than the system (b) because the system (a) has a redundant structure system. It means that PSA does not supply information on system structure such as system redundancy in some cases. Consequently, PSA and DID are complementary each other, so that two measures are involved in evaluating safety.



3. DID Measures

In order to develop the new safety assessment measures based on DID, which should be easily quantified and implemented to assess plant safety status during outage, we firstly review the several concepts of defense in depths referred in IAEA safety series, risk-informed regulation, NUMARC 91-06, and ERPI ORAM documents. Next, we develop DID measures considering each DID characteristics.

Firstly, the concept of defense in depth is stated in INSAG-3 as "All safety activities, whether organizational, behavioral or equipment related, are subject to layers of overlapping provisions, ..., This idea of multiple levels of protection is the central feature of defense in depth..." This concept extended to incorporating PSA and severe accident management in INSAG-12. The means of defense in depth are both 5 levels of defense and multiple barriers. The implementation of defense in depth consists of several means such as deterministic design, PSA, enhancement of safety, accident control, management of severe accident, and so on. IAEA DID concept is traditional and well balanced. Diversity, independence, PSA and severe accident management are key elements in DID implementation.

Risk-informed regulation requires the impact of the proposed licensing basis is consistent with the defense-in-depth philosophy. It says that the defense-in-depth philosophy is maintained if the followings are met: 1) a balance of prevention and prevention 2) avoidance of over-reliance on programmatic activities 3) system redundancy, independence, and diversity 4) defenses against potential common cause failures 5) independence of barriers 6) defenses against human errors, and 7) maintenance of general design criteria.

NUMARC 91-06 deals with managing risk during shutdown, and it says that defense in depth is 1) providing SSC to ensure bask up key safety function using redundant, alternative or diverse methods, and 2) planning outage activities in a manner that optimizes safety system availability.

According to NUMARC 91-06, EPRI has developed assessment tool (ORAM) of management of outage with safety function assessment tree (SFAT) and plant transient assessment tree (PTAT).

From these DID concepts, we developed safety measures based on DID with following characteristics;

- Evaluation of safety status by SFAT
- Back up for SFAT with PSA
- Obtaining key safety functions from emergency procedures, operation procedures, technical specifications, and operation and maintenance experiences
- Evaluating diversity of key safety functions as a target of safety evaluation
- Establishment of contingency plan where excessive degradation of safety functions
- Considerations of Common cause failure, human error in contingency plan
- 4 colored codes, "Red", "Orange", "Yellow", "Green" for rating safety status, and 'RED' being out of technical specifications

4. Conclusions

In this paper, from relationship between DID and PSA we shows they are complementary in safety analysis, so that they all should be performed to evaluate plant safety. Next, we propose a safety measures based on DID for rating safety status during outage of PHWR considering several concepts of defense in depths.

References

[1] J.N. Sorensen, etc., "On the Role of Defense in Depth in Risk-Informed Regulation," PSA '99, 1999
[2] International Nuclear Safety Advisory Group, "Defense in depth in nuclear safety," INSAG-10, International Atomic Energy Agency, Vienna, Austria, 1996
[3] International Nuclear Safety Advisory Group, "Basic Safety Principles for Nuclear Power Plants," INSAG-12, International Atomic Energy Agency, Vienna, Austria, 1999
[4] U. S. Nuclear Regulatory Commission, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis," Regulatory Guide 1.174, June 1998
[5] Electric Power Research Institute, "ORAM-Sentinel User's Manual," TR-107018, Sep. 1997
[6] INPO, "Guidelines for the management of planned Outages at Nuclear Power Station," April 1997
[7] NUMARC, "Guidelines for Industry Actions to Assess Shutdown Management," Dec. 1991