A proposed approach for enhancing design safety assurance of future plants

[a*]Kju-Myeng Oh, [a]Sang-Kyu Ahn, [a]Chang-Ju Lee, [b]Inn Seock Kim
[a]*Korea Institute of Nuclear Safety, Gusung-dong Yusung-gu Daejeon, Korea, 305-338*
[b]*ISSA Technology, 21318 Seneca Drive, Germantown, MD 20876, USA*
[a*]Corresponding author: k313okm@kins.re.kr

1. Introduction

This paper provides various insights from a detailed review of deterministic approaches typically applied to ensure design safety of nuclear power plants (NPPs) and risk-informed approaches proposed to evaluate safety of advanced reactors such as Generation IV reactors. Also considered herein are the risk-informed safety analysis (RISA) methodology suggested by Westinghouse as a means to improve the conventional accident analysis, together with the Technology Neutral Framework recently suggested by the U.S. NRC for safety evaluation of future plants.

These insights from the comparative review of deterministic and risk-informed approaches could be used in further enhancing the methodology for design safety assurance of future plants.

2. Insights from deterministic and risk-informed approaches

2.1 Insights from deterministic approach [1]

A combination of the approaches to categorization of initiating events as provided in the ANSI 18.2-1973 and Regulatory Guide (RG) 1.70-1978 have been applied in the licensing and safety analysis of most existing NPPs up to now. However, an important drawback of these deterministic approaches is that safety arguments are made primarily on the basis of design basis accidents (DBAs) that were defined somewhat arbitrarily by combining initiating events with single failures and coincident occurrences such as a loss of offsite power.

For instance, RG 1.70-1978, RG 1.206-2006 and NUREG-0800-2007 Standard Review Plan 15.0 require that a step-by-step sequence of events, from event initiation to the final stabilized condition, be addressed for each initiating event with considerations of single active failures and operator errors. However, focus is still placed on the initiating events since no systematic method to identify the associated event sequences is provided.

ANSI/ANS-51.1-1983 touched upon several novel ideas, e.g. integration of dose consequence and the frequency with the initiating event combined with single or coincident occurrence. Also, this issue was further investigated by Westinghouse when developing the RISA approach with a pilot application to the loss of normal feedwater event [2].

Various key principles based on deterministic considerations, such as defense-in-depth, safety margin, redundancy, diversity and independence, have served the backbone of nuclear plant safety thus far. These key principles primarily intended to enhance plant performance against potential accidents are very useful concepts, and as a result, are expected to continue to play an important role in keeping the safety of future plants.

2.2 Insights from risk-informed approach [3]

There is an increasing interest in improving the deterministic approach by use of risk insights from a PSA. Our review of various risk-informed approaches (e.g., applied in evaluating design safety of MHGTR, PRISM and PBMR; and proposed for the Technology Neutral Framework by NRC) [4] indicates that the PSA technique is particularly useful in systematically identifying various event sequences in consideration of a combination of multiple failures consisting of independent failures, common-cause failures or human errors. As a result, the event sequences selected for the design basis events (DBAs) or licensing basis events (LBEs) would have a stronger basis than otherwise possible.

However, a deterministic process plays an important role even within the risk-informed frameworks (e.g., in determining success criteria or deciding upon the specific response of the plant in a given situation) and also the process for design safety assurance requires even wider techniques than the PSA. Also notable is that the PSA at design stage suffers considerable limitations because of: 1) lack of design and operational details in the pre-conceptual or conceptual design stage; 2) lack of relevant operating experience from which to derive a PSA database; 3) great uncertainties in sequence modeling for the reliability characteristics of novel safety features such as passive systems.

Therefore, an effective blend of deterministic and risk-informed approaches is needed to make a robust safety case for future nuclear power plants. An approach along this line is proposed later in the paper.

Actually, the risk-informed approach imposes a considerable challenge to the regulatory body especially because the acceptance criteria should be defined for the event sequence categories that are based on the quantitative frequencies of occurrence.

3. A new approach for design safety assurance of future plants [5]

3.1 Decision-making goals

In order to shed light on what kinds of decision making need to ensure design safety of future plants, a simplified logic tree was depicted as shown in Fig. 1 using a technique called goal-tree success-tree. The top goal of 'Adequate Requirement for Safety Assurance' can be satisfied if the three goals, i.e., 'Adequate Requirement for Event Selection', 'Adequate requirement for Event Analysis' and 'Adequate Establishment of Acceptance Criteria', are met. These goals constitute the essential

elements of the decision making needed, and the logic tree may be further developed for each goal.

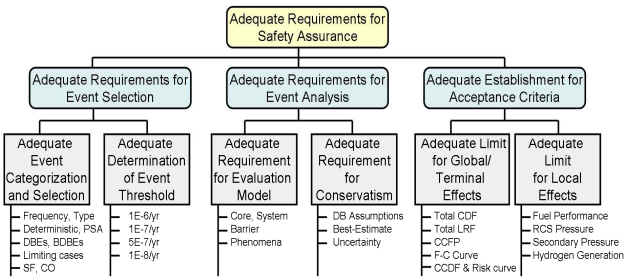

Fig. 1 Decision-making goals for design safety assurance of future plants

From this logic diagram, one can see that a comprehensive decision-making process is needed to ensure design safety of future plants.

3.2 A proposed process

As discussed earlier, an appropriate blend of the deterministic and risk-informed approaches should be developed to make a robust safety case for future plants as far as possible. An approach for design safety assurance of future plants is proposed herein which consists of the 9 steps as shown in Fig. 2.

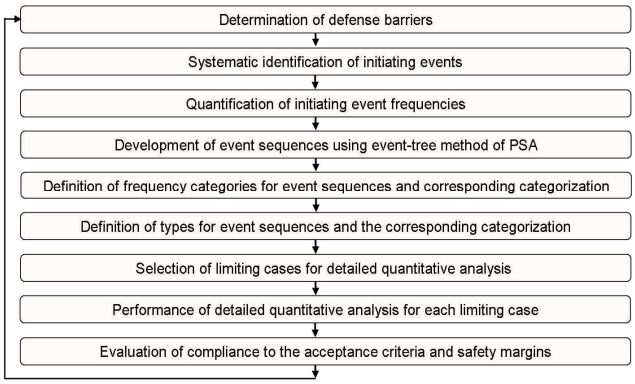

Fig. 2 A proposed process for design safety assurance of future plants

The deterministic safety principles such as defense-in-depth or safety margin should be properly incorporated in the process in order to prevent over-reliance on the PSA. These principles are taken into account particularly in connection with 'Determination of defense barriers' and 'Evaluation of compliance to the acceptance criteria and safety margins.'

The proposed approach primarily focuses on definition of event sequences, selection of limiting cases and their acceptance criteria, since these areas can be most benefited from a risk-informed approach. In this approach, event sequences are developed by constructing and solving event trees as typically done in a PSA. Frequency categories (e.g., anticipated operating occurrences, design basis events, and beyond-design basis events) covering a large spectrum of frequencies of occurrence need to be defined so that different acceptance criteria or evaluation methods can be established for each category.

As has been normally the case with deterministic approaches, events are also categorized in our approach not only by expected frequency of occurrence but also by type. The 7 types defined in RG 1.70 and RG 1.206 are utilized with some additional types like induced SGTR or containment bypass. Frequency categories can be selected from the event sequences leading to an end state of core damage or no core damage as identified in the PSA event trees, once the PSA is settled down following the iterative design process between the plant design and the evolving PSA.

Limiting cases can be determined by classifying each accident scenario according to frequency categories and the types and then selecting limiting cases within the event group after taking into account the occurrence of induced SGTR and containment bypass event. Some efforts are needed to select each limiting event in terms of dose consequences and on the basis of the most severe impact on plant parameters.

Detailed accident analysis (e.g. using thermal hydraulic codes) needs to be carried out for each limiting case.

Finally, the results should satisfy the relevant acceptance criteria. In a risk-informed approach, the design safety analysis may also have to meet the criteria on global effects of potential events (e.g., total core damage frequency, large release frequency, or containment failure probability, and frequency-consequence curve as well).

4. Concluding remarks

Based on the insights from a critical review of deterministic and risk-informed approaches, we have proposed a new approach for design safety assurance of advanced nuclear plants such as Generation IV reactors. This approach appropriately blends deterministic and risk-informed insights in that it is basically built upon key principles such as defense-in-depth or safety margin, and takes advantage of the event sequences from a PSA.

As the PSA, especially the design-specific PSA, is associated with considerable uncertainties and the process for design safety assurance requires even wider techniques than the PSA, the probabilistic approach should be prudently utilized only in a manner to complement, or overcome the weaknesses of, the traditional safety analysis methodology.

REFERENCES

[1] Sang Kyu Ahn, et al., Deterministic and risk-informed approaches for safety analysis of advanced reactors: Part I, Deterministic approaches, Reliability Engineering and System Safety Vol. 95(2010) 451-458
[2] WCAP-16084-NP, Development of risk-informed safety analysis approach and pilot application (2003)
[3] Inn Seock Kim, et al., Making a robust safety case for future nuclear plant designs, PSAM 10(2010)
[4] NUREG-1860, Feasibility study for a risk-informed and performance-based regulatory structure for future plant licensing (2007)
[5] Inn Seock Kim, et al., Deterministic and risk-informed approaches for safety analysis of advanced reactors: Part II, Risk-informed approaches, Reliability Engineering and System Safety Vol. 95(2010) 459-468