Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 23-24, 2019

Perspective to the Safety Classification of Structures, Systems and Components on the Basis of Safety Function and Defence-in-Depth

Manwoong Kim*, Ki-Yeon Kwon
Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon 34142. Republic of KOREA
**Corresponding author: M.Kim@kins.re.kr*

1. Introduction

The objective of this study is to review the use of risk insights to the safety classification of SSCs as defined in 10 CFR 50.69 and SSG-30. This study also addresses some augmentations between the deterministic SSC classification system (safety related or non-safety related) and risk-informed categorization based on safety significance. This study also addresses regulatory perspectives to apply a way of the safety classification of SSCs according to their safety significance approach for ensuring the robustness of safety function and defence-in-depth (DiD) of nuclear power plant.

2. Technical Requirement of Safety Classification of SSCs

2.1 IAEA SSG-30 [1]

The functions required for fulfilling the main safety functions in all plant states, including modes of normal operation, should be categorized on the basis of their safety significance. The safety functions can be categorized on the basis of their safety significance approach that takes account of the following factors:

- The consequences of failure to perform the function;
- The frequency of occurrence of the postulated initiating event for which the function will be called upon;
- The significance of the contribution of the function in achieving either a controlled state or a safe state.

To ensure performing safety function appropriately, all SSCs should be identified and classified according to their safety significance to ensure plant states: (i) control of reactivity, (ii) removal of heat from the reactor and from the fuel store and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

Therefore, SSCs (including supporting SSCs) should initially be classified according to the severity of consequences of their failures so that they are designed to carry out identified functions as followings:

- Safety class 1: Any SSC whose failure would lead to consequences of 'high' severity.
- Safety class 2: Any SSC whose failure would lead to consequences of 'medium' severity.
- Safety class 3: Any SSC whose failure would lead to consequences of 'low' severity.

For most postulated initiating events (PIEs), a combination of both SSCs and their functions is implemented to decrease the frequency of occurrence of an accident and to make its consequences acceptable and also as low as practicable. Nevertheless, for a few initiating events, the implementation of safety functions to limit the consequences may not be necessary provided that the consequences are very low and that there is no need for any mitigation measures so that any SSCs should be classified appropriately in order to avoid an unacceptable impact from the failure of the function.

2.2 10 CFR 50 and Regulatory Guides of US NRC

The quality group classification system is established in 10 CFR 50.55a [2] incorporated by reference the criteria in Section III of the ASME Code, and Regulatory Guide 1.26 where provided for quality groups.

Thereafter, new requirements on the risk-informed categorization and treatment of structures, systems and components for nuclear power reactors was issued as 10 CFR50.69 [3]. There are two steps associated with the implementation of 10 CFR 50.69: the categorization of SSCs; and the application of special treatment requirements consistent with the safety significance of the equipment categorized. In order to implement the requirement in 10 CFR 50.69, Regulatory Guide (RG) 1.201 [4] specifies regulatory positions to determine the safety significance of SSCs and place them into the appropriate risk-informed safety class (RISC) categories. which incorporates both risk and traditional engineering insights. The process considers the safety functions of SSCs to include both the design-basis functions (derived from the safety-related definition) and functions credited for preventing and/or mitigating severe accidents.

Figure 1 shows the categorization process to identify safety-related SSCs and non-safety-related SSCs.

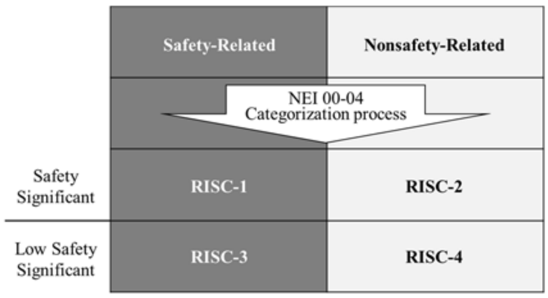


Figure 1 Risk Informed Safety Classifications (RISC)

It is noted that 10 CFR 50.69 does not replace the existing "safety-related" and "non-safety-related" categorizations. Rather, this requirement divides these categories into two subcategories, 'safety significant' and 'low safety significant'.

3. Categorization of Safety Function

3.1 IAEA SSG-30

All SSCs required to perform a function that is safety categorized should be identified and classified according to their safety significance to ensure safety stable states. SSCs (including supporting SSCs) that are designed to carry out identified functions should initially be assigned to the safety class corresponding to the safety category of the function to which they belong as shown in Table 1.

Table 1 Relationship between Function and Severity of Consequence

Functions credited in the safety assessment	Severity of the consequences if the function is not performed		
	High	Medium	Low
Functions to reach a controlled state after anticipated operational occurrences	Safety category 1	Safety category 2	Safety category 3
Function to reach a controlled stated after design basis accidents	Safety category 1	Safety category 2	Safety category 3
Functions to reach and maintain a safe state	Safety category 2	Safety category 3	Safety category 3
Functions for the mitigation of consequences of design extension conditions	Safety category 2 or 3	Not categorized	Not categorized

Figure 2 shows that SSCs are implemented primarily to decrease the probability of an event and functions are implemented to make the consequences acceptable with regard to its probability as being classified 'high'. 'medium' and 'low' severity.

For most postulated initiating events (PIEs), the frequency of occurrence of an accident depends on the overall dependability of items of equipment, which itself is governed by their classification. As to grouping PIE and their associated transients. the most common approach is to group initiating events and their associated transients as indicated in Table 2 of IAEA SSG-2 [5].

As to the defence in depth (DiD) approach, it is generally divided into five levels. Table 3 summarizes the objectives of each level and the corresponding means that are essential for achieving them.

In order to identify the frequency criteria in Figure 1, Figure 3 shows an example of quantified frequency for each DiD level using the frequency criteria listed in Table 2.

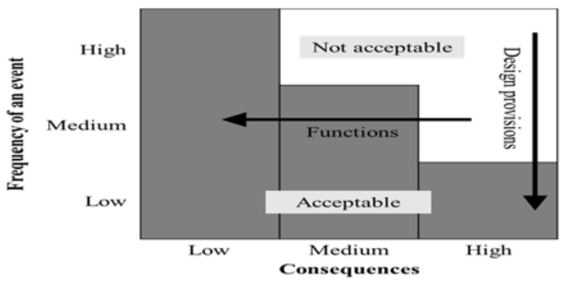


Figure 2 The basic concept of event frequency versus its consequences

Table 2 Subdivision of PIEs in IAEA SSG-2

Occurrence (1/reactor year)	Characteristic	Plant state	Terminology	Acceptance criteria
10^{-2}-1 (expected over the lifetime of the plant)	Expected	Anticipated operation occurrences	Anticipated transients, transients, frequent faults, incidents of moderate frequency, upset conditions, abnormal conditions	No additional fuel damage
10^{-4}-10^{-2} (chance greater than 1% over the lifetime of the plant)	Possible	Design basis accidents	Infrequent incidents, infrequent faults, limiting faults, emergency conditions	No radiological impact at all, or no radiological impact outside the exclusion area
10^{-6}-10^{-4} (chance less than 1% over the lifetime of the plant)	Unlikely	Beyond design basis accidents	Faulted conditions	Radiological consequences outside the exclusion area within limits
$<10^{-6}$ (very unlikely to occur)	Remote	Severe accidents	Faulted conditions	Emergency response needed

Table 3 Levels of DiD in IAEA SRS46

Levels of defense in depth	Objective	Essential means for achieving the objective
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 system 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

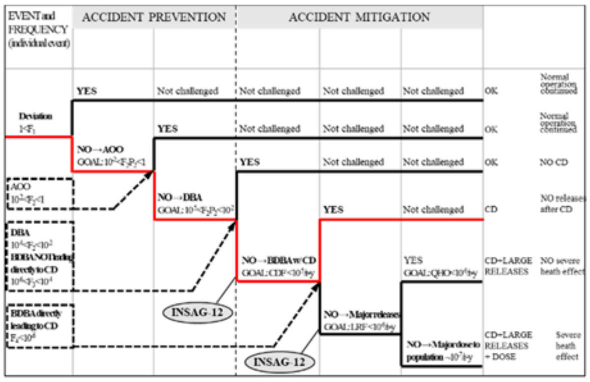


Figure 3 An example of quantified criteria of DID levels illustrated by the event tree technique

3.2 USNRC 10 CFR 50.69 and Regulatory Guide 1.201

The NRC developed regulatory requirements in 10CFR50.69 to determine the RISC categories in the basis of safety significance of SSCs so as to ensure their functionality during all plant states and accident conditions. Figure 4 provides a conceptual understanding of the new risk-informed SSC categorization scheme as followings:

RISC-1 SSCs are safety-related SSCs that the risk-informed categorization process determines to be significant contributors to plant safety.

RISC-2 SSCs are those that are defined as non-safety-related, although the risk-informed categorization process determines that they are significant contributors to plant safety on an individual basis. Hence RISC-2

SSCs is on the safety-significant functions for which credit is taken in the categorization process.

RISC-3 SSCs are defined as safety-related, although the risk-informed categorization process determines that they are not significant contributors to plant safety.

RISC-4 SSCs are defined as non-safety-related, and that the risk-informed categorization process determines are not significant contributors to plant safety.

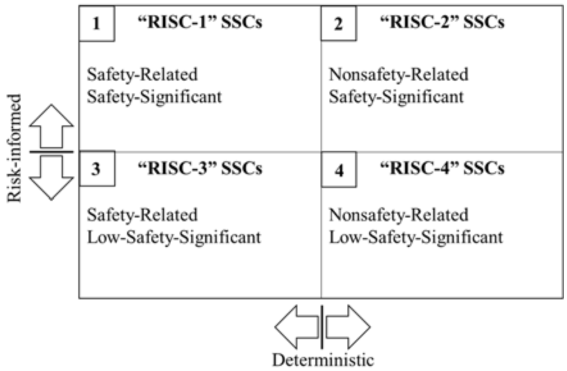


Figure 4 10CFR50.69 RISC Categories

4. Quantitative Results of Categorization Efforts

The following quantitative results were provided by the utilities that have implemented the risk-informed categorization process described in NEI 00-04: South Texas Project (STP) which involved 50 systems and 75,000 components. These results imply that 10 CFR 50.69 divides the existing "safety-related" and "non-safety-related" categorizations into two subcategories based on high or low safety significance.

4.1 Example of Reactor Coolant System Categorization

Figure 5 shows that after risk-informed categorization, only 66% of the safety-related SSCs remained safety significant, whereas 34% of those safety-related SSCs were categorized as low safety significant. The figure also shows that only 14% of the originally classified non-safety-related SSCs were subsequently categorized as safety significant.

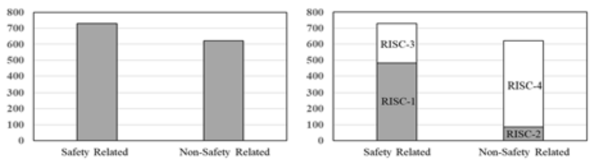


Figure 5 RCS SSCs Categorized Under 10CFR50.69

4.2 Example of Residual Heat Removal System Categorization

Figure 6 shows that after risk-informed categorization, only 36% of the safety-related SSCs were categorized as safety significant, whereas 64% of those safety elated SSCs were categorized as low safety significant. The figure also shows that only 20% of the originally classified non-safety-related SSCs were subsequently categorized as safety significant.

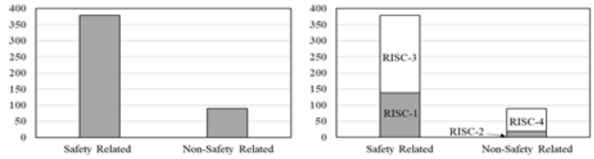


Figure 6 Residual Heat Removal SSCs Categorized Under 10CFR50.69

4.3 Summary of Categorization

Figure 7 shows that after risk-informed categorization, only 24% of the safety-related SSCs were categorized as safety significant, whereas 76% of those safety-related SSCs were categorized as low safety significant. The figure also shows that only 1% of the originally classified non-safety-related SSCs were subsequently categorized as safety significant.

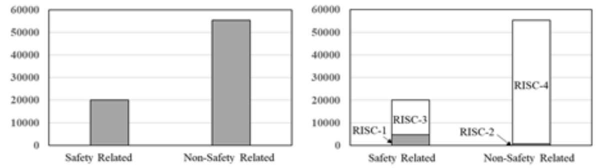


Figure 7 Scope of Components Categorized Under 10CFR50.69

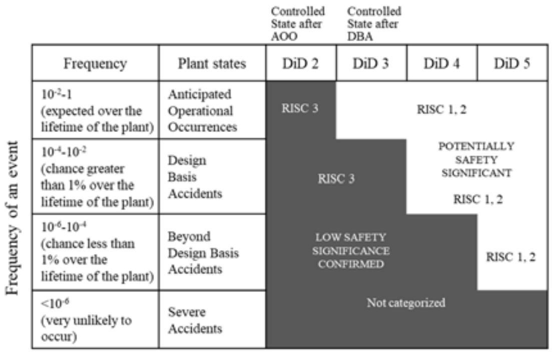
5. Challenges for Application and Implementation

5.1 Consequences acceptable with Defence-in-Depth

The initial assessment should consider both the level of defence-in-depth to the frequency of the events. Figure 8 is an example of such an assessment. This figure depicts the initiated anticipated operational occurrences considered in the licensee's safety analysis report (i.e., the events that were used to identify an SSC as safety-related) and considers the level of defence-in-depth available to prevent and mitigate accident conditions. For each active component/function categorized to identify the region in which the plant mitigation capability lies without credit for the function/SSC that has been proposed as low safety-significant, and without credit for any identical, redundant SSCs within the system that are also classified as low safety-significant. If the result is in the region entitled "Low Safety Significance Confirmed," then the low safety significance of the function/SSC has been confirmed. If the result is in the region entitled "Potentially Safety-significant," then the function/SSC should be classified as safety-significant. The basis of determining the safety level is the role of item in the three basic safety functions, and considering the consequences of failure to perform its functions, and the time or duration of the item to be put into operation after the postulated initially event.

For example, if it is found that the emergency core cooling system (ECCS) pumps were LSS in the categorization process using risk information. In this case, the ECCS pumps have the function of providing coolant makeup to the RCS. This function is required either (a) as a large LOCA of DBAs in response to DID

3, or (b) as other transients and LOCAs where other coolant makeup systems are failed due to failures of ECCS pumps in response to DiD 4 and/or 5. Therefore, with failures of ECCS pumps exceeds 10^{-4} but less than 10^{-6} with having high consequence, pump should be categorized RISC 2 or 3. In case of large LOCA, ensuring the function of ECCP pumps to avoid high consequence, pump should be categorized RISC 2 or 3.



* Medium or low severity consequences are not expected to occur in the event of non-response of a dedicated function for the mitigation of design extension conditions.

Figure 8 Defence-in-depth Matrix

5.2 Practically elimination of current relevant requirements

In 10 CFR 50.69, safety-related components determined to be safety significant are categorized as RISC-1 and are treated no differently than they are exist rules. Non-safety-related components determined to be safety significant are known as RISC-2. Nevertheless, it is recognized that if current controls are not inadequate to ensure the safety of the SSCs, any additional treatment of RISC-2 is necessary to be applied. However, in case of RISC-3, these requirements eliminate a number of special treatment requirements for RISC-3 that the component will perform its safety function during design basis conditions. Therefore, 10CFR50.69 can eliminate the following "special treatment" requirements for applications that have been designated as RISC-3 as show in Table 4.

Table 4 Special Treatment Requirements That May Be Removed for Low Risk SSCs under 10CFR50.69

Maintenance Rule [10 CFR 50.65]
Environmental Qualification [10 CFR 50.49]
Seismic Qualification [Portions of Appendix A to 10 CFR Part
ASME XI repair & replacements, applicable portions, with limitations [10 CFR 50.55a(g)]
Applicable Portions of IEEE standards [10 CFR 50.55a(h)]
In-service Testing [10 CFR 50.55a(f)]
In-service Inspection [10 CFR 50.55a(g)]
Local Leak Rate Testing [10 CFR 50 Appendix J]
Quality Requirements [10 CFR 50 Appendix B]
Deficiency Reporting [10 CFR Part 21]
Event Reporting [10 CFR 50.55(e)]
Notification Requirements [10 CFR 50.72, 50.73]

6. Conclusions

This study provides perspectives on application of requirements on the risk-informed categorization and treatment of structures, systems and components for nuclear power reactors was issued as 10 CFR50.69.

The degree of relief that the NRC will accept under 10CFR50.69 (i.e., SSCs subject to relaxation of special treatment requirements) will be commensurate with the assurance provided by the evaluation.

The quantitative results from South Texas Project (STP) which have implemented the risk-informed categorization process described in NEI 00-04 in compliance with 10CFR50.69, these results show only 24% of the safety-related SSCs were categorized as safety significant, while 76% of those safety-related SSCs were categorized as low safety significant. Moreover, only 1% of the originally classified non-safety-related SSCs were subsequently categorized as safety significant.

Therefore, application of risk-informed categorization process of SSCs in SSG-30 and 10CFR50.69 allows opportunities not only for reduced regulatory burden on licensees and more efficient oversight processes for the regulator, but also enhancement of nuclear safety and operational flexibility, simplify work, reduce cost, and potentially shorten outage durations.

ACKNOWLEDGEMENTS

The authors of this paper would like to acknowledge former IAEA colleagues, Dr I. Kuzmina and Dr A. Lyubarskiy for providing reference information.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014)

[2] 10CFR50.55a, Codes and Standards, Office of the Federal Register, National Archives and Records Administration, U.S. Government Printing Office, Washington, DC.

[3] 10CFR50.69, Risk-Informed Categorization and Treatment of Structures, Systems and Components for Nuclear Power Reactors, Office of the Federal Register, National Archives and Records Administration, U.S. Government Printing Office, Washington, DC. (2004)

[4] Regulatory Guide 1.201, Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to Their Safety Significant, U.S. Government Printing Office, Washington, DC. (2006)

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2, IAEA, Vienna (2009)