U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Public Meeting on the Development of Regulatory Guide (RG) 1.174, Revision 3

May 23, 2016
One White Flint North, Room 3B-04
11555 Rockville Pike
Rockville, MD

Agenda

- Introduction
- Presentation on progress to date and meeting goals
- Discussion of revised guidance
- Meeting wrap-up
- Adjourn

Background

- SRM-SECY-11-0014 directed the staff to clarify defense-in-depth (DID) language in RG 1.174
- The staff issued draft guide (DG-1285) for public review and comment (May, 2012)
- Public comments were received, but not addressed
- Completion of effort delayed due to ongoing work related to Fukushima Near-Term Task Force Recommendation 1 and the Risk Management Regulatory Framework
- SRM-SECY-15-0168 directs staff to "…expeditiously complete the revision to Regulatory Guide 1.174 on defense in depth, in order to improve the clarity of the guidance…"

Background (continued)

- RG 1.174, Rev. 2:
  - Lists 7 elements (a.k.a. factors) for evaluating whether DID will be acceptably maintained following a proposed change to the licensing basis
  - No explanation of the seven factors is provided
  - No examples regarding how to use each factor
- DG-1285 (May, 2012):
  - Reorganized the 7 factors into a hierarchy: 2 high-level and 5 supporting
  - Provides narrative to explain the meaning of each factor
  - Provides examples to further explain the meaning of each factor

Public Comments from 2012

- Guidance not provided on how to assess impact on DID
- In general, three main types of comments:
  - Reorganization of the DID factors did not add clarity; introduced additional confusion
  - The examples used to illustrate the meaning of each DID factor are often confusing
    - Industry proposed to develop and provide different examples
  - Public expressed a desire to be more engaged

Current Approach

- Revert back to seven factors—i.e., no hierarchy
- Providing further clarity in the description of and narrative for each factor
- Provide one or more integrated examples—i.e., as opposed to examples for each factor—that show how a licensee might justify that a proposed change meets each of the seven factors

Goals for this Meeting

- Obtain feedback on the draft revision of Section 2.1 in DG-1285 related to:
  - Organization of the factors
  - Description of and narrative for each factor
  - Use of examples
    - One or more integrated examples to explain process of addressing all factors?
    - Multiple examples that further explain each factor?
    - Both?

Organization of the Factors

- The draft revision of Section 2.1 from DG-1285 reverts back to a list of seven factors with a narrative for each factor to explain the meaning—i.e. no hierarchy.

Organization of the Factors (continued)

	RG 1.174, Revision 2	Currently Proposed Version
1	A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.	Preserve a reasonable balance among the four layers of defense.
2	Over-reliance on programmatic activities as compensatory measures associated with the change in the LB is avoided.	Preserve adequate capability of design features without an over-reliance on programmatic activities as compensatory measures.
3	System redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties (e.g., no risk outliers).	Preserve sufficient system redundancy, independence, and diversity.
4	Defenses against potential common-cause failures are preserved, and the potential for the introduction of new common-cause failure mechanisms is assessed.	Preserve adequate defense against potential common-cause failures (CCF) and assess the potential for the introduction of new CCF mechanisms.
5	Independence of barriers is not degraded.	Maintain integrity of multiple fission product barriers.
6	Defenses against human errors are preserved.	Preserve sufficient defense against human errors.
7	The intent of the plant's design criteria is maintained.	Maintain the intent of the plant's design criteria.

Factor 1

Preserve a reasonable balance among the four layers of defense.

A reasonable balance of the four layers of defense—minimizing challenges to the plant, preventing any events from progressing to core damage, containing the radioactive source term, and emergency preparedness—helps to ensure an apportionment of the plant's capabilities between limiting disturbances to the plant and mitigating their consequences. "Reasonable balance" is not meant to imply an equal apportionment of capabilities. A reasonable balance is preserved if the proposed plant change does not significantly reduce the effectiveness of a layer that exists in the plant design before the proposed change. The NRC recognizes that there may be aspects of a plant's design that may cause one of the four layers to be adversely affected. For these situations, the balance between the other three layers becomes especially important when evaluating the impact of a proposed change to the LB and its impact on defense in depth.

Factor 2

Preserve adequate capability of design features without an over-reliance on programmatic activities as compensatory measures.

Programmatic activities are used to ensure safety functions; however, the regulations demonstrate a definite preference for engineered safety features to mitigate DBAs. The licensee should adhere to this preference and, therefore, should assess whether the proposed change would increase the need for programmatic activities to compensate for the lack of engineered features. If the change requires new or additional reliance on administrative controls, the licensee should justify that reliance on these measures is not excessive. Use of compensatory measures may be considered overreliance when a programmatic activity is substituted for an engineered means of performing a safety function, or failure of the programmatic activity could prevent an engineered safety feature from performing its intended function. Moreover, overreliance on a programmatic activity can potentially result in significant reduction in the effectiveness of one of the defense-in-depth layers that exists in the plant design before the proposed change, or it may lessen the effectiveness of one of the fission product barriers. The licensee should evaluate the impact to confirm that a reasonable balance of the defense-in-depth layers is preserved.

The NRC also recognizes that programmatic activities used as compensatory measures are sometimes associated with temporary conditions. A licensee may request a risk-informed change to the plant's licensing basis to permit occasional entry into conditions requiring compensatory measures. For such situations, the licensee should demonstrate that the plant condition requiring such compensatory measures would occur at a sufficiently low frequency

Factor 2 – Examples of Programs

- Nuclear power plant licensees implement a number of programs, such as:
  - Quality assurance
  - Testing and inspection
  - Maintenance
  - Control of transient combustible material
  - Foreign material exclusion
  - Containment cleanliness
  - Training

Factor 3

Preserve sufficient system redundancy, independence, and diversity.

The importance of system redundancy, independence and diversity is to ensure that the "safety functions" can be achieved. The safety functions are accomplished by the safety related structures, systems, and components those functions needed to shut down the reactor, remove the residual heat, and contain any radioactive material release[2]. 10 CFR Part 50, Appendix A, General Design Criteria discusses the need for system redundancy, independence and diversity specifically as a means to prevent a single failure; that is, the system safety function can be accomplished assuming a single failure[3]. Redundancy provides for duplicate equipment that enables the failure or unavailability of at least one set of equipment to be tolerated without loss of function. Independence among equipment implies that the redundant equipment are separate such that they do not rely on the same supports to function. It can sometimes be achieved by the use of physical separation or physical protection. Diversity is accomplished by having equipment that perform the same function rely on different attributes, such as different principles of operation, different physical variables, different conditions of operation, or production by different manufacturers.

A substantial reduction in the ability to accomplish a safety function is not consistent with the defense-in-depth philosophy. A safety function may be compromised if one of the plant features that provides for either system redundancy, independence, or diversity is defeated. This adverse impact could occur by the introduction of a new dependency that could potentially defeat the redundancy, independence or diversity of the affected equipment. That is, system redundancy, independence and diversity can be assumed to be sufficient if, given the proposed licensing change, the affected system safety function can be accomplished assuming a single failure.

The licensee should demonstrate that the proposed licensing change would not affect system redundancy, independence, or diversity of the affected equipment; that is, the affected system safety function can still be accomplished assuming a single failure.

Factor 3 – Footnotes

2. 10 CFR 50.2 defines safety-related as systems and components means those structures, systems and components that are relied upon to remain functional during and following design basis events to assure:

   (1) The integrity of the reactor coolant pressure boundary

   (2) The capability to shut down the reactor and maintain it in a safe shutdown condition; or

   (3) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in § 50.34(a)(1) or § 100.11 of this chapter, as applicable.

3. A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety function. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions. [10 CFR 50, Appendix A, General Design Criteria for Nuclear Power Plants, Definitions]

Factor 4

Preserve adequate defense against potential common-cause failures (CCF) and assess the potential for the introduction of new CCF mechanisms.

An important aspect of ensuring defense in depth is to guard against CCF. Failure of several devices or components to function may occur as a result of a single specific event or cause. Such failures may simultaneously affect several different items important to risk. The event or cause may be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human-induced event, or an unintended cascading effect from any other operation or failure within the plant. A CCF can result in the failure, degradation, or effectiveness of a defense-in-depth layer that exists in the plant design before the proposed change.

The licensee should evaluate the proposed change to determine whether it increases the potential for events or causes that would be a CCF. The licensee should also evaluate the proposed change to determine whether new CCF mechanisms could be introduced.

Factor 5

Maintain integrity of multiple fission product barriers.

In this context a fission product *barrier* is a physical structure between the source term and the public, which is intended to prevent a release of radionuclide material. This factor includes physical barriers (e.g., the reactor coolant system pressure boundary) and the systems and components that protect the integrity of physical barriers (e.g., emergency core cooling system). The effectiveness of barriers is reduced if multiple barriers can be defeated or degraded by a single event as a result of the proposed change.

To maintain the integrity of multiple barriers, the licensee should ensure that the change does not result in a new event or increase the likelihood of an existing event whose effects would disable multiple barriers that are relied upon to mitigate the consequences of the initiating event.

Factor 6

Preserve sufficient defense against human errors.

Human errors include (1) the failure of operators to perform the actions necessary to operate the plant or respond to off-normal conditions and accidents, (2) errors committed during test and maintenance, and (3) operators performing an incorrect action. The plant design and operation includes defenses to prevent the occurrence of such events and errors. These defenses generally involve the use of procedures, training, and human engineering. These defenses are preserved if the proposed plant change does not increase the potential for human errors that can lead directly to a beyond-design-basis event or affect the ability of operators to place the plant in a safe-shutdown condition or carry out emergency operating procedures correctly. Human errors can result in the degradation or failure of a system to perform its function, thereby significantly reducing the effectiveness of one of the defense-in-depth layers or one of the fission product barriers.

The licensee should assess whether the proposed change would create new operator actions, increase the burden on operators in responding to events, or increase the probability of existing operator errors. The licensee should consider whether the change creates new situations that are likely to cause errors, not only for operators, but for maintenance personnel and other plant staff.

Factor 7

Maintain the intent of the plant's design criteria.

The plant's design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for SSCs important to safety; that is, SSCs that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public. When evaluating the effect of the proposed change, the licensee should determine whether the plant's design criteria are affected.

The plant's design criteria define requirements that implement the defense-in-depth philosophy; as a consequence, a compromise to those design criteria can directly result in a significant reduction in the effectiveness of one of the defense-in-depth layers.

Use of Examples

- The purpose of an integrated example is to illustrate how an analyst might use the seven factors to evaluate the impact of the licensing basis change on DID
- Is the integrated example approach feasible?
- Should use multiple examples for each factor?
- A combination of these approaches?

Meeting Recap and Wrap up

- Next steps
- Public meetings
  - June (tentative)
  - August Workshop (tentative)
- Closing remarks
- Adjourn