Revised Draft of Section 2.1 from DG-1285

## 2.1 Evaluation of Defense-in-Depth Attributes and Safety Margins

One aspect of the engineering evaluation is to show that the proposed change does not compromise the fundamental safety principles on which the plant design was based. Design-basis accidents (DBAs) play a central role in the design of nuclear power plants. DBAs are a combination of postulated challenges and failure events against which plants are designed to ensure adequate and safe plant response. During the design process, plant response and associated safety margins are evaluated using assumptions of physical properties and operating characteristics that are intended to be conservative. National standards and other considerations such as defense-in-depth attributes and the single-failure criterion constitute additional engineering considerations that also influence plant design and operation. The licensee's proposed LB change may affect margins and defenses incorporated into the current plant design and operation; therefore, the licensee should reevaluate these items to support a requested LB change. As part of this evaluation, the impact of the proposed LB change on the functional capability, reliability, and availability of affected equipment should be determined. The plant's LB identified in the FSAR is the reference point for judging whether a proposed change adversely affects safety margins or defense-in-depth. Sections 2.1.1 and 2.1.2 below provide guidance on assessing whether implementation of the proposed change maintains adequate safety margins and consistency with the defense-in-depth philosophy.

### 2.1.1 *Defense-in-Depth*

The engineering evaluation should evaluate whether the impact of the proposed LB change is consistent with the defense-in-depth philosophy. In this regard, the intent of this key principle of risk-informed decision-making is to ensure that any impact of the proposed LB change on defense-in-depth is fully understood and addressed and that the philosophy of defense-in-depth is maintained; not to prevent changes in the way defense-in-depth is achieved. The licensee must fully understand how the change will impact the design, operation and maintenance of the plant, both from risk and traditional engineering perspectives.

This section provides some background on the defense-in-depth philosophy. Next is discussion of seven key factors that may be used to evaluate the impact of a proposed change on defense-in-depth. One or more examples are provided to help illustrate what is meant by each factor. Finally, this section provides guidance on a process for evaluating the seven key factors, including an integrated example.

#### 2.1.1.1 Background

Defense-in-depth is an element of the NRC's safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility[1]. The defense-in-depth philosophy has traditionally been applied in reactor design and operation to provide multiple means to accomplish safety functions and prevent the release of radioactive material. It has been and continues to be an effective way to account for uncertainties in equipment and human performance and, in particular, to account for the potential for unknown and unforeseen failure mechanisms or phenomena, which (because they are unknown or unforeseen) may not be reflected in either the PRA or traditional engineering analyses.

[1] Staff Requirements Memorandum (SRM) - SECY-98-0144, "White Paper on Risk-Informed and Performance-Based Regulation," March 1, 1999, (Agencywide Document Access and Management System (ADAMS) accession number ML003753601).

For the purposes of this RG, it is useful to consider the following layers of defense (successive measures) when evaluating the impact of the proposed licensing basis change on defense-in-depth:

- Robust plant design to survive hazards and minimize challenges that could result in an event occurring;
- Prevention of a severe accident (core damage) should an event occur;
- Containment of the source term should a severe accident occur; and,
- Protection of the public from any releases of radioactive material (through, e.g., siting in low population areas and the ability to shelter or evacuate people if necessary).

2.1.1.2 Key Factors for Evaluating the Impact of LB Changes on Defense-in-depth

Any one or more of the layers of defense discussed above may be adversely impacted by a proposed change to a plant's licensing basis. The NRC has identified seven factors that should be used to assess the impact of the change on defense-in-depth. These are discussed in detail below. Guidance on how to apply these factors is discussed in more detail in section 2.1.1.3.

The NRC finds it acceptable for a licensee to use the following seven key factors to evaluate whether a proposed change to the LB maintains the philosophy of defense-in-depth.

1. Preserve a reasonable balance among the layers of defense.

a. Guidance

*A propose change should not* significantly reduce the effectiveness of a layer of defense that exists in the plant design before the proposed change.

*The evaluation of the proposed change should* consider insights based on traditional engineering approaches; insights from risk assessments may be used to support engineering insights, but not be the only justification for meeting this factor.

b. Discussion

A reasonable balance of the 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. The term *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 layers to be adversely affected. For these situations, the balance among 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.

If a comprehensive risk analysis is done, it can provide insights into whether the balance among the layers of defense remains appropriate to ensure protection of public health and safety. Such a risk analysis would not only include the likelihood of challenges to the plant (i.e., initiating event frequencies) from various hazards, but would include estimates of core damage frequency, containment response and, in some cases, dose estimates to the public. It would include implementation of the emergency plan and estimate the effectiveness of actions such as sheltering in place or evacuation.

Note that the risk acceptance guidelines in this RG are based on the surrogates for the Commission's quantitative health objectives, CDF and LERF. These risk metrics, developed as part of the risk assessment, can help inform the licensee's assessment of the relative balance between the second and third layers of defense.

However, to address the unknown and unforeseen failure mechanisms or phenomena, the licensee's evaluation of this factor of defense-in-depth should also address insights based on traditional engineering approaches. Results of the risk assessment may be used to support the conclusion but should not be the only justification for meeting this factor. The licensee should consider the impact of the proposed change on each of the layers of defense:

– <u>Robust plant design to survive hazards and minimize challenges that could result in an event occurring</u> - the change should not significantly increase the likelihood of initiating events or create new significant initiating events;

– <u>Prevention of a severe accident (core damage) should an event occur</u> - the change should maintain the availability and reliability of SSCs that provide the safety functions that prevent plant challenges from progressing to core damage;

– <u>Containment of the source term should a severe accident occur</u> - the change should maintain the containment and SSCs that support that barrier, such as containment fan coolers and sprays; and,

– <u>Protection of the public from any releases of radioactive material</u> - the change should not reduce the effectiveness of the EP program, including the ability to detect and measure releases of radioactivity, to notify offsite agencies and the public, to shelter or evacuate the public as necessary

c. Examples

[Under development]

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

a. Guidance

*A proposed change should not* significantly reduce the reliability and availability of design features to perform their safety functions.

*The evaluation of the proposed change should demonstrate that the change does not* result in the overreliance of programmatic activities to compensate for a proposed reduction in the capability of engineered safety features.

b. Discussion

Nuclear power plant licensees implement a number of programs, including, for example, programs for quality assurance, testing and inspection, maintenance, control of transient combustible material, foreign material exclusion, containment cleanliness, training, and so forth. In some cases, activities taken as part of these programs are used to ensure safety functions; for example, reactor vessel inspections that provide assurance that reactor vessel failure is unlikely.

A proposed change that does not affect how safety functions are performed or reduce the reliability or availability of the SSCs that perform those functions would meet this defense-in-depth factor. However, a licensee could contemplate a change where a reduction in the capability of those SSCs is compensated in some manner by reliance on plant programs. In such a case, the licensee 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 such programs, the licensee should justify that reliance on these measures is not excessive. Use of compensatory measures may be considered overreliance when a program 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.

The NRC also recognizes that 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 measures that rely on plant programs to compensate for reduced capability of engineered systems, or for one-time to allow completion of corrective action to restore engineered systems to match the design and licensing basis. For such situations, the licensee should demonstrate that the plant condition requiring such compensatory measures would occur at a sufficiently low frequency or that the time frame to effect corrective action is commensurate with the significance of the non-conforming condition.

c. Examples

[Under development]

3. Maintain sufficient availability and reliability of SSC commensurate with their importance to safety.

a. Guidance

*A proposed change should not* defeat the redundancy, independence, or diversity of design features.

*The evaluation of the proposed change should demonstrate that the change does not* result in a substantial reduction in the availability or reliability of the associated SSCs, e.g., introduction of a new single failure.

b. Discussion

The importance of system redundancy, independence and diversity is to ensure that the system function can be achieved. A proposed risk-informed change should consider both safety-related and nonsafety-related SSCs that are important to core damage or large early release. 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 would likely undermine the effectiveness of a layer of defense-in-depth and, therefore, would not be 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.

c. Examples

[Under development]

4. Preserve adequate defense against potential common-cause failures (CCF).

a. Guidance

*A proposed change should not* reduce defenses against CCFs that could defeat the redundancy, independence, and/or diversity of DID layers, fission product barriers, and engineered safety features.

*The evaluation of the proposed change should demonstrate that the change does not* result in a reduction of existing CCF defenses or introduce new CCF dependencies.

b. Discussion

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.

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.

c. Examples

[Under development]

5. Maintain multiple fission product barriers.

a. Guidance

*A proposed change should not* significantly reduce the effectiveness of the multiple fission product barriers.

*The evaluation of the proposed change should demonstrate that the change does not:*

- Create a significant increase in the likelihood or consequence of an event that simultaneously challenges multiple barriers and is within the plant's existing licensing basis.

- Introduce the possibility of a new event that would simultaneously impact multiple barriers.

b. Discussion

This factor refers to the physical fission product barriers e.g., the fuel cladding, reactor coolant system pressure boundary, and containment. This includes the physical barriers themselves and any equipment relied upon to protect the barriers (e.g., containment spray). In general, these barriers are designed to perform independently so that a complete failure of one barrier does not disable the next subsequent barrier. For example, one barrier, the containment, is designed to withstand a double-ended guillotine break of the largest pipe in the reactor coolant system, another barrier.

A plant's licensing basis may contain events that, by their very nature, challenge multiple barriers simultaneously. Examples include interfacing-system LOCA and SGTR. Therefore, complete independence of barriers, while a goal, may not be achievable for all possible scenarios.

To demonstrate that this factor is met, the licensee should demonstrate that the change does not create a significant increase in the likelihood or consequence of an event that simultaneously challenges multiple barriers and is within the plant's existing licensing basis.

Furthermore, the licensee should demonstrate that the change does not introduce the possibility of a new event that would simultaneously impact multiple barriers. If this cannot be shown, the licensee should:

- Perform a deterministic analysis to show that the simultaneous challenge to multiple barriers caused by the new event can be mitigated. This may be done by assuming that the new event has occurred and performing an analysis (using conservative assumptions) demonstrating that affected barriers would perform their safety function or;

- Use the results of the plant's PRA to demonstrate that the likelihood of the new event is sufficiently low such that independence of barriers would not be significantly affected by the proposed change.

c. Examples

[Under development]

6. Preserve sufficient defense against human errors.

a. Guidance

*A proposed change should not* significantly increase the potential for or create new human errors that may adversely affect one or more layers of defense.

*The evaluation of the proposed change should demonstrate that the change does not*

– create new human failure events that have a significant adverse impact on risk;
– significantly increase the burden on the operators responding to events; or,
– significantly increase the human error probability of existing operator actions.

b. Discussion

Human errors include the failure of operators to perform the actions necessary to operate the plant or respond to off-normal conditions and accidents, errors committed during test and maintenance, and operators performing an incorrect action. 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 plant design and operation includes defenses to prevent the occurrence of such errors and events. These defenses generally involve the use of procedures, training, and human engineering; however, other factors, e.g., communication protocols, may also be important.

In determining whether these defenses are preserved, the licensee should assess whether the proposed change would create new operator actions that significantly impact the change in risk, place a greater mental/physical demand 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.

c. Examples

[Under development]

7. Continue to meet the intent of the plant's design criteria. **[ NRC staff is considering deleting this evaluation factor and expanding the narrative of the first paragraph of Section 2.1.1 of this document to more fully explain the concept of this factor. ]**

a. Guidance

*A proposed change should not* affect meeting the intent of the plant's design criteria referenced in the licensing basis.

*The evaluation of the proposed change should demonstrate that the change does not* affect meeting the intent of the plant's design criteria referenced in the licensing basis.

b. Discussion

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. The plant's design criteria define minimum requirements that achieve aspects of 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 or more of the defense-in-depth layers. When evaluating the effect of the proposed change, the licensee should demonstrate that the intent of the plant's design criteria continue to be met.

The General Design Criteria of Appendix A to 10 CFR 50 form the basis for the design criteria for newer plants. In some cases, exemptions to specific GDC may have been granted. Older plants may have been licensed to other criteria, such as the AEC draft design criteria. A given plant's design criteria are summarized in its UFSAR. This factor of defense-in-depth should consider the current licensing basis of the plant.

c. Examples

[Under development]