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 the safety margins and layers of defense 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) are not reflected in either the PRA or traditional engineering analyses.

In addition, there is some flexibility that can be gained in the operations and maintenance of the nuclear plant that leverages the implementation of the defense-in-depth philosophy in the design of the

[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)

plant. For example, testing and maintenance of SSCs or corrective action to restore an engineered safety system may be allowed for short periods while remaining at power, consistent with established Technical Specifications. The NRC recognizes and allows these temporary configurations within these established programs. If a licensee requests a risk-informed change to the plant's licensing basis to permit new or extended entry into temporary conditions, the licensee should demonstrate that the plant condition is justified and consistent with the defense-in-depth philosophy as described in this section.

For the purposes of this RG, nuclear power plant defense-in-depth is taken to consist of layers of defense and successive measures to protect the public:

- 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 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 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 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 and operation before the proposed change. The NRC recognizes that there may be aspects of a plant's design or operation that may cause one or more of the layers to be adversely affected. For these situations, the balance between the other layers becomes especially important when evaluating the impact of a proposed change to the LB and its impact on defense-in-depth.

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

   Some proposed changes to the LB may involve or require compensatory measures; that is, measures taken to compensate for some reduced functionality, availability, reliability, redundancy, or other feature of the plant's design. Such compensatory measures are often associated with temporary plant configurations. Compensatory measures may include hardware

(e.g., skid-mounted temporary power supplies), human actions (e.g., manual system actuation), or some combination of these measures. The preferred approach for accomplishing *safety functions* is through engineered systems. Therefore, when a proposed change necessitates reliance on *programmatic activities* as compensatory measures, the licensee should justify that this reliance is not excessive.

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. The intent of this factor is not to preclude the use of such programs as compensatory measures, but to ensure that the use of such measures does not significantly compromise the capability of the design features (e.g., hardware).

3. Preserve system redundancy, independence, and diversity commensurate with the expected frequency, consequences of challenges to the system, and uncertainties.

A substantial reduction in the ability to accomplish system safety functions is not consistent with the defense-in-depth philosophy. The importance of system redundancy, independence and diversity is to ensure that the system safety function can be achieved. As stated in Section 2.1.1 above, the defense-in-depth philosophy has traditionally been applied in reactor design and operation to provide multiple means to accomplish safety functions. System redundancy, independence, and diversity not only result in high availability and reliability of SSCs, but also help ensure that system safety functions are not reliant on any single feature of the design.

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.

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

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.

5. Maintain multiple fission product barriers.

Physical fission product barriers (e.g., the fuel cladding, reactor coolant system pressure boundary, and containment) 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.

6. Preserve sufficient defense against human errors.

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 other plant staff 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 considerations, e.g., communication protocols, may also be important.

7. Continue to meet the intent of the plant's design criteria[2].

For plants licensed under 10 CFR Part 50 or Part 52, the plant's design criteria are set forth in the current licensing basis of the plant, which is documented in the plant's FSAR, as updated. 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.

For plant's licensed under 10 CFR Part 52, this factor should also address those design features for the prevention and mitigation of severe accidents that are described and analyzed in accordance with 10 CFR 52.47(a)(23) for DC applications and 10 CFR 52.79(a)(38) for COL applications. For this factor, the potential impacts on these severe accident design features should also be evaluated to ensure the intent of the design features continue to be met.[3]

---

[2] The General Design Criteria of Appendix A to 10 CFR 50 form the basis for the design criteria for newer plants licensed under 10 CFR Part 50 or Part 52. 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 FSAR, as updated. This factor of defense-in-depth should consider the current licensing basis of the plant and how the proposed change would continue to meet the intent of the plant's design criteria.

[3] Section C.I.19.8 of Regulatory Guide 1.206, "Combined License Applications for Nuclear Power plants (LWR Edition)," issued June 2007, provides guidance on implementing these requirements and ties the requirements to the issues and performance goals identified in SECY-90-016, "Evolutionary Light-Water Reactor (LWR) Certification Issues and Their Relationship to Current Regulatory Requirements," dated January 12, 1990 and SECY-93-087, "Policy, Technical, and Licensing issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993, which the Commission approved in staff requirements memoranda (SRMs) dated June 26, 1990, and July 21, 1993, respectively. In addition, Regulatory Guide 1.216, Containment Structural Integrity Evaluation for Internal Pressure Loadings above Design-Basis Pressure," dated August 2010, provides acceptable methods for an analysis that specifically addresses the issues and performance goals identified in SECY-90-016 and SECY-93-087 and related SRMs for containment structures in nuclear power plants under severe accident conditions.

2.1.1.3 Evaluating the Impact of the LB Change on Defense-in-Depth

The seven factors described above are an acceptable way for a licensee to evaluate the impact of a proposed change to the LB on defense-in-depth. While such an evaluation of a change against the seven factors is qualitative, the licensee should be able to conclude that the change maintains consistency of the plant design with the defense-in-depth philosophy by showing that the intent of each factor still is met following the proposed change.

The seven factors could be arranged in a hierarchical manner. For example, the first factor is an over-arching, high level description of how defense-in-depth is achieved. Factors two through six may apply at any of the layers of defense to aid the analyst in justifying that the proposed change maintains suitable balance among the layers. Finally, factor seven helps ensure completeness of the assessment of how the proposed change could affect defense-in-depth. Nevertheless, in the interest of simplicity, the seven factors should each be addressed for any proposed risk-informed change to the licensing basis. If a proposed change has no impact on a given factor, that should be stated with a brief justification as appropriate. Licensees are encouraged to structure their discussion of how a proposed change maintains the defense-in-depth philosophy by addressing the seven factors; such an approach should facilitate the licensee's analysis as well as make for a more efficient review by the NRC staff. The licensee should demonstrate/justify that there has not been a significant impact to LB for each of the factors.

Note that the focus here is on the effect of the change on defense-in-depth. When a nuclear power plant is licensed, NRC regulations result in some amount of protection or defense at each of the layers of defense. The seven factors presented above are not intended to define how defense-in-depth is implemented in a plant's design, but to help licensees assess the impact of the proposed change.

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.

Evaluating Factor 1: Preserve a reasonable balance among the layers of defense.

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 should not be the only justification for meeting this factor.

To demonstrate that this factor is met, the licensee should address each of the layers in turn.

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 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. In addition, qualitative and quantitative insights from the PRA may help justify the balance across all the layers.

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 and insights 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:

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

- Prevention of a severe accident (core damage) should an event occur - the change should not significantly impact the availability and reliability of SSCs that provide the safety functions that prevent plant challenges from progressing to core damage;

- Containment of the source term should a severe accident occur - the change should not significantly impact the containment function or SSCs that support that function, such as containment fan coolers and sprays; and,

- Protection of the public from any releases of radioactive material - the change should not significantly 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

Evaluating Factor 2: Preserve adequate capability of design features without an overreliance on programmatic activities as compensatory measures.

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 an intended reduction in the capability of engineered safety features is not excessive

To demonstrate that this factor is met, the licensee should first determine whether the proposed change necessitates compensatory measures. If not, this should be stated as the reason this factor is met. If compensatory measures are needed to support the proposed change, the licensee should determine the extent to which programmatic activities, as compared to design features, are being relied upon. The intent of this factor is not to preclude the use of programs as compensatory measures, but to ensure that this use is not excessive.

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.

Evaluating Factor 3: Preserve system redundancy, independence, and diversity commensurate with the expected frequency, consequences of challenges to the system, and uncertainties.

A proposed change should not significantly impact the ability for the system function to be performed.

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 and does not introduce a new single failure.

To demonstrate that this factor is met, the licensee should ensure that there is not a substantial reduction in the ability to accomplish a safety function. 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. Plant changes that introduce new dependencies among systems or functions, or that introduce new common cause failures (addressed under factor 4), should not result in a disproportionate increase in risk. That is, system redundancy, independence and diversity can be assumed to be preserved if, given the proposed licensing change, the affected system safety function can be accomplished assuming a new single failure has not been introduced.

Some proposed changes are temporary[4] in nature and result in the plant being in an operational condition where certain design features are not available to perform their intended functions. For example, a single train of a multi-train system may be out of service. It is not the intent of this factor of defense-in-depth to preclude such temporary plant configurations. In general, a proposed change would meet the intent of this factor provided no permanent change to the plant's design or change in operation that affects the redundancy, independence or diversity of the design was being contemplated. There are other controls on temporary plant configurations, such as the Technical Specifications, that limit the exposure to risk during such periods.

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

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

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

To understand a defense strategy against a CCF event, it is necessary to understand that defending against a CCF event is no different than defending against an independent failure that has a single root cause, except that more than one failure has occurred and the failures are related through a coupling mechanism.

[4] Temporary is not meant to imply excessive periods of time.

The defense mechanisms for the CCF system include functional barrier, physical barrier, monitoring and awareness, maintenance staffing and scheduling, component identification, and diversity. These defenses are constructed primarily based on defending against the CCF coupling factors. A coupling factor is the condition or mechanism through which multiple components could be affected (or coupled) by the same cause. Coupling factors can be based on attributes, such as hardware quality (manufacturing, installation), design (component part, system configuration), maintenance (schedule, procedure, staff), operation (procedure, staff), and environment (external, internal).

There are three methods of defense against a CCF: (1) defend against the failure cause, (2) defend against the CCF coupling factor, or (3) defend against both items 1 and 2. A defense strategy against causes typically includes design control, use of qualified equipment, testing and preventive maintenance programs, procedure review, personnel training, quality control, redundancy, diversity, and barriers. For coupling factors, a defense strategy typically includes diversity (functional, equipment, and staff), barriers, and staggered testing and maintenance. A defense strategy addressing both the cause and coupling factor is the most comprehensive.[5]

To demonstrate that this factor is met, 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.

Evaluating Factor 5: Maintain multiple fission product barriers.

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.

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

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. To do this, the licensee should consider the following objectives to ensure that the proposed change maintains appropriate safety within the defense-in-depth philosophy:

- The change does not result in a significant increase in the existing challenges to the integrity of the barriers.

- The proposal does not significantly increase the failure probability of any individual barrier.

- The proposal does not introduce new or additional failure dependencies among barriers that significantly increase the likelihood of failure compared to the existing conditions.

[5] Refer to NUREG/CR-6268, Revision 1, Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding, for further discussions on major failure cause categories, coupling factor categories, and defense mechanisms.

- The overall redundancy and diversity among the barriers is sufficient to ensure compatibility with the risk acceptance guidelines.

Evaluating Factor 6: Preserve sufficient defense against human errors.

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 plant staff responding to events; or,
- Significantly increase the human error probability of existing human actions.

In determining whether these defenses are preserved, the licensee should assess whether the proposed change would create new human actions that significantly impact the change in risk, place a greater mental/physical demand in responding to events, or increase the probability of existing human 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.

Evaluating Factor 7: Continue to meet the intent of the plant's design criteria.

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 significantly compromise meeting the plant's design criteria thereby significantly reducing the effectiveness of one or more defense-in-depth layers.

This factor of defense-in-depth should consider the current licensing basis of the plant and how the proposed change would continue to meet the intent of the plant's design criteria and, for Part 52 plants, continue to meet the intent of the severe accident design features. It is recognized that, in general, the consideration of *applicable regulations* under the first principle of risk-informed regulation would be expected to address this factor of defense-in-depth. Also, it is not the intent of this factor that changes to the plant's design criteria or severe accident design features cannot be requested. However, the licensee should fully understand any impacts that the proposed change may have on the design criteria or severe accident design features of the plant.

For example, for some hazards and for some licensees, defense-in-depth may be defined in the plants LB. For example, the fire protection program for licensed nuclear power plants requires that fire protection defense-in-depth, which is scenario-based, be maintained. Any proposed plant change must be evaluated against any plant-specific LB defense-in-depth requirements in addition to the guidance presented herein.

2.1.2 ***Safety Margin***

The engineering evaluation should assess whether the impact of the proposed LB change is consistent with the principle that sufficient safety margins are maintained. Here also, the licensee is expected to choose the method of engineering analysis appropriate for evaluating whether sufficient safety margins would be maintained if the proposed LB change were to be implemented. An acceptable set of guidelines for making that assessment is summarized below. Other equivalent acceptance guidelines may also be used. With sufficient safety margins, the following are true:

- Codes and standards or their alternatives approved for use by the NRC are met.

- Safety analysis acceptance criteria in the LB (e.g., FSAR, supporting analyses) are met or proposed revisions provide sufficient margin to account for analysis and data uncertainty.

The NRC has developed application-specific guidelines reflecting this general guidance which may be found in the application-specific regulatory guides (Refs. 5–9).