NRC Handout for Discussion, September 1, 2011 NRC Public Meeting

# PROPOSED CHANGES TO CLARIFY THE DEFENSE-IN-DEPTH PHILOSOPHY OF REGULATORY GUIDE RG 1.174, "AN APPROACH FOR USING PROBABILISTIC RISK ASSESSMENT IN RISK-INFORMED DECISIONS ON PLANT-SPECIFIC CHANGES TO THE LICENSING BASIS"

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

One aspect of the engineering evaluations is to show that the fundamental safety principles on which the plant design was based are not compromised by the proposed change. Design-basis accidents (DBAs) play a central role in nuclear power plant design. 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 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 associated with these considerations; therefore, the licensee should reevaluate them to support a requested LB change. As part of this evaluation, the impact of the proposed LB change on affected equipment functionality, reliability, and availability should be determined. The plant's licensing basis and any risk insights identified in the FSAR are the starting points for judging whether a proposed change adversely impacts defense-in-depth or safety margins.

### 2.1.1 *Defense-in-Depth*

The engineering evaluation should evaluate whether the impact of the proposed LB change (individually and cumulatively) is consistent with the defense-in-depth philosophy. In this regard, the intent of this principle is to ensure that the philosophy of defense-in-depth is maintained, not to prevent changes in the way defense-in-depth is achieved. 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. The defense-in-depth philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility. The net effect of incorporating defense-in-depth into design, construction, maintenance, and operation is that the facility or system in question tends to be more tolerant of failures and external challenges.

If a comprehensive risk analysis is done, it can provide insights into whether the extent of defense-in-depth (e.g., balance among core damage prevention, containment failure, and consequence mitigation) is appropriate to ensure protection of public health and safety. However, to address the unknown and unforeseen failure mechanisms or phenomena, traditional defense-in-depth considerations should be used or maintained. The evaluation should consider the intent of the general design criteria in Appendix A, "General Design Criteria

for Nuclear Power Plants," to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," national standards, and engineering principles, such as the single-failure criterion. Further, the evaluation should consider the impact of the proposed LB change on barriers (both preventive and mitigative) to core damage, containment failure or bypass, and the balance among defense-in-depth attributes. As stated earlier, the licensee should select the engineering analysis techniques, whether quantitative or qualitative, traditional or probabilistic, appropriate to the proposed LB change.

The licensee should assess whether the proposed LB change maintains the defense-in-depth philosophy. Defense-in-depth consists of a number of elements, and consistency with the defense-in-depth philosophy is maintained if the following occurs:

- Means (i.e., factors) for preventing core damage, preventing containment failure, and mitigating radiological consequences are provided and a reasonable balance among these factors is preserved.

  A reasonable balance of these factors helps to ensure an apportionment in the plant's capabilities between limiting disturbances to the plant and mitigating them. However, it is not meant to imply an equal apportionment of capabilities. To determine whether there is a reasonable balance, it is important to understand these factors. Core damage prevention can be considered as those measures used to prevent the uncontrolled migration of radionuclides within the plant in excess of normal operation limits. Containment failure prevention can be considered as those measures used to prevent the uncontrolled migration of radionuclides from the plant to the environment in excess of normal operating limits. Consequence mitigation can be considered as those measures used to alleviate the effects of the uncontrolled release of radionuclides to the environment that are in excess of normal operating limits.

  A reasonable balance is preserved if the proposed plant change does not result in significant reduction in the effectiveness of a factor that exists in the plant design before the proposed change. It is recognized that there may be aspects of a plant's design where one of the three factors may not be fully effective. For these situations, the balance between the other two factors becomes especially important when evaluating the impact of a proposed change to the licensing basis and its impact on defense-in-depth. For example, some accidents (e.g., PWR steam generator tube rupture events) bypass primary containment, and therefore, the only effective factors are core damage prevention and consequence mitigation. In such a case, any proposed changes to the licensing basis should not adversely affect, for example core damage prevention, such that the plant is primarily reliant on consequence mitigation.

  Examples:

  — The proposed change is to remove certain radiation monitoring equipment or meteorological instruments based on no impact on core damage frequency. This change may challenge this element of defense-in-depth because the instruments may provide information needed to make recommendations for sheltering or

evacuating the close-in population in the event of a reactor accident. These types of systems support the consequence mitigation aspect of defense-in-depth and need to be retained. However, if there are other monitors or instruments that provide the same function, a licensee may be able justify such a change.

— The proposed change is to increase the period between containment integrated leak rate tests. This change could impact this element of defense-in-depth by reducing the level of assurance that the containment is intact in the event of a reactor accident. However, if there is industry operating experience that demonstrates favorable containment performance and the absence of degradation mechanisms so that the longer time interval between tests still provides the reasonable assurance of containment ability to fulfill its function, the licensee may be able to justify such a change.

- Over-reliance on programmatic activities as compensatory measures associated with the change in the LB is avoided.

  Programmatic activities are administrative controls as opposed to engineered safety features. Although programmatic activities are used to ensure key safety functions, the regulations demonstrate a definite preference for engineered safety features. This preference should be adhered to, and therefore, the licensee should assess (1) whether the proposed change would increase the need for compensatory measures in the form of a programmatic activity, and (2) that any increase is not excessive (e.g., “over-reliant”). This increase can be considered to be over-reliant when a programmatic activity is substituted for an engineered means of performing a safety function or failure of the programmatic activity could prevent a engineered safety feature from performing its intended function. It is also recognized that programmatic activities used as compensatory measures are generally associated with temporary conditions. For these situations, the licensee should demonstrate that the plant condition requiring such compensatory measures would occur at a sufficiently low frequency.

  Examples:

  — The proposed plant change involves removal of fire doors with an associated compensatory measure of placing a fire watch. The compensatory measure as a permanent change to the plant may be considered to be over-reliant on a programmatic activity. However, if the compensatory measure was implemented, for example, on a temporary basis (e.g., until the next fuel reload or other appropriate interval), the licensee may be able to justify such a change.

  — The proposed change involves a power uprate that results in containment pressure increase which could affect the performance of the containment heat removal pumps. Consequently, the proposed change also included writing a procedure to direct operators to secure non-safety containment fan coolers in the event of a reactor accident. This action helps ensure the availability of the containment heat removal pumps by keeping the containment pressure above the

pumps net positive suction head (NPSH) limit. This procedure could be considered over-reliant on a programmatic activity. However, if it can be demonstrated, for example, that this additional operator action is reliable and feasible, does not overburden the operators or adversely affect their ability to respond to an accident, or otherwise impact plant safety, the licensee may be able to justify such a change.

- System redundancy, independence, and diversity are preserved.

  An important aspect of ensuring key safety functions is to guard against impacting those plant features that provide system redundancy, independence, and diversity. Redundancy enables failure or unavailability of at least one set of equipment to be tolerated without loss of the function. Independence among systems is achieved by the use of functional isolation, physical separation, and physical protection. Diversity is applied to redundant systems or components that perform the same function by incorporating 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 key safety function is not consistent with the defense-in-depth philosophy. A key safety function may be compromised (and therefore system redundancy, independence and diversity not preserved) when a proposed change would introduce new dependencies among plant equipment or would defeat one of the features. The introduction of new dependencies could reduce the level of redundancy, independence or diversity for fulfilling a key safety function. The licensee should demonstrate that new dependencies have not been introduced that could adversely impact system redundancy, independence or diversity, or that the change itself is not defeating one of the features. A licensee could use risk assessment techniques to identify any increase in system dependency or risk importance resulting from the proposed change.

  Examples:

  — The proposed plant change involves extending the Technical Specification completion time for a risk-significant system. During the time the system is out of service, there may be no redundancy for the function that the system provides. Removing the redundant train from the plant entirely would not be consistent with this element of defense-in-depth. However, if it can be demonstrated, for example, that the proposed completion time is short enough to meet the risk acceptance guidelines in RG 1.174 and RG 1.177, that adequate margins are maintained, and the other principles of risk-informed regulation set forth earlier in this section, the licensee may be able to justify such a change.

- Defense against potential common-cause failures is preserved, and the potential for the introduction of new common-cause failure mechanisms is assessed.

An important aspect of ensuring key safety functions is to guard against common cause failures (CCF). Failure of several devices or components to function may occur as a result of a single specific event or cause. Such failures may affect several different items important to safety simultaneously. 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 ensure it does not increase 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.

Examples:

- The proposed change is a new corrosion-resistant material for one component of the plant's seawater pumps. There may be uncertainty regarding how this new material will perform with respect to the other materials in the pump, creating the potential for new failure mechanisms (e.g., galvanic corrosion). Changing this part in all service water pumps within a short time period could create a CCF mechanism, and therefore, defenses against CCF would not be preserved. However, if it could be demonstrated, for example, that implementation of a performance monitoring program or enhanced inspection program reduces the potential for CCF from the new material, the licensee may be able to justify such a change.

- The proposed change is to use new "improved" grease in the MOVs at the plant. Maintenance procedures would be changed to specify using the new grease. There may be uncertainty regarding the potential for new failure modes as a result of the new grease, which could occur to all MOVs where the new grease is applied. This change could impact this element of defense-in-depth. However, if it could be demonstrated, for example, that implementation of a performance monitoring program or enhanced inspection program reduces the uncertainty introduced with the new material the licensee may be able to justify such a change.

- Independent, redundant and diverse barriers to the release or fission products are preserved.

  The plant's licensing basis includes fission product barriers and engineered structures, systems and components that support or maintain those barriers. These barriers, as exemplified in current reactors, are generally considered to be the fuel elements' cladding, reactor coolant system pressure boundary, and containment systems and structure. Since the barriers also play a mitigative role, barrier integrity can also be achieved by complementary measures and procedures to arrest accident progression and by alleviating the consequences of selected reactor accidents.

Complete independence of barriers is not always possible in practice; for example, a completely independent primary containment structure might have to be concentric and have no penetrations. However, these barriers are considered to be redundant and independent as they provide separate means to contain and mitigate. These attributes of defense-in-depth are compromised if the proposed plant change causes one of the barriers to be ineffective; that is, there is a cause and effect relationship between the barrier and the aspect of the plant being proposed to be changed. The licensee should evaluate the impact of the proposed change on the fission product barriers and supporting systems.

Examples:

- The proposed change involves a power uprate that results in containment pressure increase which could affect the performance of the emergency core cooling system (ECCS) pumps. The proposed change also includes allowing the increased pressure in the containment (as a result of an accident) to be included in the calculation of ECCS pump NPSH. A potential dependency is created between two fission product barriers: if the containment were to fail, the ECCS pumps could cavitate and possibly fail. This failure of the pumps could in turn lead to core damage. In this situation, independence of the barriers is not preserved. However, if it can be demonstrated, for example, that the pumps may operate with some cavitation, and therefore, the independence of the two fission product barriers have not been significantly degraded, the licensee may be able to justify such a change.

- Defense against human error is preserved.

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 maintenance, and (3) operators performing an incorrect action. The plant 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. 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 error-likely situations, not only for operators, but for maintenance personnel and other plant staff.

Examples:

- The proposed change results in an operator action, although necessary in the long term, is counter intuitive and could potentially increase the likelihood of the operator failing to properly perform the action. In this situation, defenses against

human error may not be preserved. However, if it can be demonstrated, for example, that increased training involving educating the operator's understanding of the action and practicing the action can offset this potential error, the licensee may be able to justify such a change.

— The proposed plant change involves a change to the loading of spent fuel whereby a single human error in loading would then lead to criticality. In this situation, defenses against human errors would not be preserved. However, if it can be demonstrated, for example, that implementation of other reliable methods would prevent this human error, the licensee may be able to justify such a change.

- The intent of the plant's design criteria is maintained.

  The plant's design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety; that is, structures, systems, and components that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public. The General Design Criteria (GDC) in Appendix A of 10 CFR Part 50 provide a set of criteria for evaluating whether a proposed change could adversely affect the defense-in-depth provided in the plant design. In evaluating the effect of the proposed change, the licensee should determine whether any of the GDC is impacted. If the objective of a GDC is compromised, that is, it cannot be met with reasonable assurance, then the intent of that GDC has not been maintained, and therefore, the plant's design criteria is not maintained.

  Examples:

  — The change is to eliminate inservice inspection of reactor vessel welds based on very low probability of vessel rupture. GDC 1 states that structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Inservice inspection of the reactor vessel is an important part of ensuring the continued reliability of the vessel. Moreover, the plant design does not include systems to mitigate reactor vessel rupture. Consequently, vessel rupture is expected to lead to core damage, and ultimately the potential for damaged fuel outside the vessel challenging containment integrity. Therefore, elimination of inservice inspection does not maintain this defense-in-depth element. However, if it can be demonstrated, for example, that reduction in inspection frequency maintains the intent of the GDC, the licensee may be able to justify such a change in this manner (i.e., reduction versus elimination).

The elements presented above can help focus the licensee's justification that the proposed change maintains the philosophy of defense-in-depth. The elements are not intended to define how defense-in-depth is implemented in a plant's original design, but as aids to assessing the impact of the proposed change with respect to the elements of defense-in-depth. It is also not

the intent that the defense-in-depth philosophy be used as a “go/no-go” factor in risk-informed decision-making, but rather in an integrated fashion with risk and safety margins. The licensee can use these elements as guidelines for making their assessment. Other, similar guidelines may also be used if justified by the licensee for the specific proposed change.