

May 25, 2000

The Honorable Richard A. Meserve  
Chairman  
U.S. Nuclear Regulatory Commission  
Washington, D.C. 20555-0001

Dear Chairman Meserve:

SUBJECT: USE OF DEFENSE IN DEPTH IN RISK-INFORMING NMSS ACTIVITIES

During the 118<sup>th</sup> meeting of the Advisory Committee on Nuclear Waste (ACNW), March 27-29, 2000 and the 472<sup>nd</sup> meeting of the Advisory Committee on Reactor Safeguards (ACRS), May 11-13, 2000, the Committees completed their review of the use of defense in depth in risk-informing the activities of the Office of Nuclear Material Safety and Safeguards (NMSS). On January 13-14, 2000, the Joint Subcommittee of the ACRS/ACNW held a meeting to discuss the NRC's defense-in-depth philosophy in the regulatory process emphasizing its role in NMSS activities, particularly in the licensing of a high-level radioactive waste repository. Members of the Joint Subcommittee, invited experts Robert Bernero, Robert Budnitz, and Thomas Murley, and representatives of the NRC staff, the Nuclear Energy Institute (NEI), and Westinghouse Electric Company provided presentations and held discussions on defense in depth. We also had the benefit of the documents referenced.

#### OBSERVATIONS AND RECOMMENDATIONS

1. The various compensatory measures taken for the purposes of defense in depth can be graded according to the risk posed by the activity, the contribution of each compensatory measure to risk reduction, the uncertainties in the risk assessment, and the need to build stakeholders trust.
2. The treatment of defense in depth for transportation, storage, processing and fabrication should be similar to its treatment for reactors. Defense in depth for industrial and medical applications can be minimal and addressed on the basis of actuarial information.
3. Defense in depth for protecting the public and the environment from high-level waste (HLW) repositories is both a technical and a policy issue. It is important that a reasonable balance be achieved in the contribution of the various compensatory measures to the reduction of risk. The staff should develop options on how to achieve the desired balance. The opinions of experts and other stakeholders should be sought regarding the appropriateness of each option.

4. Since the balancing of compensatory measures to achieve defense in depth depends on the acceptability of the risk posed by the facility or activity, risk-acceptance criteria should be developed for all NMSS-regulated activities.

## BACKGROUND

We agree that there is a need for a common understanding of defense in depth as it relates to a risk-informed regulatory system and that a good working definition is provided in the Commission's White Paper on Risk-Informed and Performance-Based Regulation (Reference 1):

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.

As noted in Reference 2, this safety philosophy was formulated in the early days of nuclear power development when it was recognized that the probabilities of accidents with severe consequences must be kept low. At that time, the methods of probabilistic risk assessment (PRA) did not exist, therefore, representative values for these probabilities were unavailable. Although the philosophy of defense in depth has served the nuclear power industry well, two criticisms have been raised.

- Potentially significant accident sequences were overlooked due to the inability to analyze nuclear plants as integrated systems. An example is the interfacing systems loss-of-coolant accident that was identified by the Reactor Safety Study (Reference 3).
- At times, unnecessary burden was imposed on the licensees due to the inability to quantify the impact of the compensatory measures on risk.

There are ways to improve the implementation of the defense-in-depth philosophy because we now have the ability to analyze nuclear facilities as integrated systems and have improved significantly the ability to quantify risk.

The defense-in-depth philosophy remains pertinent because our ability to quantify risks is imperfect. There are uncertainties, primarily due to inadequate models, that current risk assessments do not quantify. The question "what if we are wrong?" is still valid for PRAs and performance assessments (PAs) and speaks to the need for defense in depth. Also, defense in depth is valuable to the NRC's effort to communicate with stakeholders.

The primary need for improving the implementation of defense in depth in a risk-informed regulatory system is guidance to determine how many compensatory measures are appropriate and how good these should be. To address this need, we believe that the following guiding principles are important:

- Defense in depth is invoked primarily as a strategy to ensure public safety given the unquantified uncertainty in risk assessments. The nature and extent of compensatory measures should be related, in part, to the degree of uncertainty.

- The nature and extent of compensatory measures should depend on the degree of risk posed by the licensed activity.
- How good each compensatory measure should be is, to a large extent, a value judgment and, thus, a matter of policy.

### Nuclear Reactors

To demonstrate the significance of these guiding principles, we use an example from reactors. A PRA that includes determination of parameter uncertainties can result in probability distributions for the failures of various safety functions in place to control core damage frequency (CDF).

The probability distributions for each of these compensatory measures provide very useful insights into what is currently achievable regarding the performance of each measure. The distribution of the CDF is the result of the propagation of these distributions through the accident sequences. It is the CDF distribution that should determine if additional compensatory measures are needed due to inadequate models. In general, the more such measures are added, the more this distribution shifts to lower frequency values. What CDF distribution is acceptable is a matter of policy. As noted above, the current regulatory system for reactors has evolved without the benefit of these probability distributions. Consequently, the structuralist approach to defense in depth was employed that involves placing compensatory measures on important safety cornerstones to satisfy acceptance criteria for defined design-basis accidents that represent the range of important accident sequences.

The adequacy of the models that have produced probability distributions is an important consideration. Having the results of the risk assessment, we may be able to evaluate the significance of the inadequacies of the models in the context of the probability distributions that have been calculated. Although we can always express our confidence in the risk results in terms of probability curves, we know that to do so in some cases would require excessive reliance on expert judgments. Thus, it remains a matter of policy to decide what compensatory measures should be taken to account for model inadequacies.

### Nuclear Materials

The issue of defense in depth and the suggested guiding principles have to be considered somewhat differently when it comes to nuclear materials. For example, there is much less experience in the application of PRA methods to nuclear materials than for nuclear reactors. Although materials systems are not as complex as those for reactors in terms of the assessment of risk, there is greater diversity in materials licensed activities. Perhaps the biggest difference relates to the basic differences in the safety issues between reactors and nuclear waste disposal, especially with regard to HLW repositories. The principal concern in the safety of such repositories is not a catastrophic release of radiation resulting from an accident, but rather the loss through contamination of a valuable life-supporting resource such as ground water or land use. Both can be pathways for radiation exposure to humans. On the other hand, both lend themselves to simple interdiction and intervention measures for the protection of public health and safety. Therefore, the concept of defense in depth for

repositories should be targeted more towards protecting resources where there are high uncertainties due to the very long time involved. Although the accident perspective is somewhat important during pre-closure operations, it is not the dominant safety issue in the area of nuclear waste. Pre-closure operations do, however, lend themselves to using risk-assessment methods similar to those applied to reactor facilities.

With respect to the issue of the diversity of nuclear materials, SECY-99-100 categorizes nuclear materials into four groups. The four groups are abbreviated here as nuclear material activities involving: (1) disposal, (2) transportation and storage, (3) processing and fabrication, and (4) industrial and medical applications.

For disposal (Group 1), the reactor example suggests an approach for considering the effectiveness of protective barriers. For waste disposal facilities, defense in depth is implemented through the use of multiple barriers. For transportation and processing facilities (Groups 2 and 3), PRA methods similar to those applied to reactors can be used and defense in depth can be treated as it is for reactors. For industrial and medical applications (Group 4), we believe that sufficient data exist for many of these nuclear materials activities so that the uncertainties in estimating risks are relatively small. For Group 4 materials, defense in depth can be minimal and can be addressed on the basis of actuarial information, an advantage not available to the same extent for Groups 1-3.

## DISCUSSION

Implementation of regulations within a risk-informed framework, including the use of defense in depth, requires the establishment of risk-acceptance criteria for each regulated activity. In most cases, a facility (or a proposed design) already exists with compensatory measures in place. The questions then become (1) Are these measures sufficient for the facility or design to meet the risk-acceptance criteria? (2) Do the measures compensate sufficiently for uncertainties in their assessment? (3) Will the measures gain stakeholder acceptance? Answering these questions is the most difficult aspect of the appropriate utilization of defense in depth in a risk-informed regulatory framework and is the key to establishing limits of necessity and sufficiency.

Establishing the sufficiency and balance of compensatory measures (how many and how good) is, in our view, equivalent to an allocation of the risk reduction (to meet the acceptance criteria) among the various compensatory measures; that is, establishing a regulatory objective based on the balance between prevention and mitigation and perhaps including the balanced allocation among events.

In the power reactor area, there exists a precedent for such allocation. A CDF mean value of  $10^{-4}$ /reactor-year and a conditional containment failure probability of 0.1 have been utilized as the appropriate allocation between prevention and mitigation. These values meet the  $10^{-5}$ /reactor-year risk-acceptance criterion for large, early release frequency as expressed in Regulatory Guide 1.174. This allocation, as described in this Guide, is only for the purpose of evaluating proposed changes to individual plant licensing basis. The staff now has also proposed to use these allocations to guide the defense in depth and risk-informed aspects of 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," by evaluating the risk contribution of each event sequence class against these measures to ensure a balance in the contribution of the sequences.

