



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS  
ADVISORY COMMITTEE ON NUCLEAR WASTE  
WASHINGTON, D.C. 20555

March 7, 2000

OFFICE OF  
ACRS/ACNW

MEMORANDUM TO: ACRS/ACNW Members

FROM:

*Michele S. Kelton for*  
John N. Sorensen, Senior Fellow  
ACRS/ACNW

SUBJECT:

CERTIFIED MINUTES OF THE ACRS/ACNW JOINT SUBCOMMITTEE  
MEETING ON THE SUBJECT OF DEFENSE IN DEPTH

The proposed minutes of the ACRS/ACNW Joint Subcommittee meeting on the subject of defense in depth, have been certified as the official record of the proceedings for that meeting.

Attachment:

Certified Minutes of the Joint Subcommittee Meeting on  
the Subject of Defense in Depth, January 13-14, 2000

cc: J. Larkins, ACRS/ACNW  
H. Larson, ACRS/ACNW  
ACRS/ACNW Staff



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS  
ADVISORY COMMITTEE ON NUCLEAR WASTE  
WASHINGTON, D.C. 20555

OFFICE OF  
ACRS/ACNW

MEMORANDUM TO: John N. Sorensen, Senior Fellow  
ACRS/ACNW

FROM: Thomas S. Kress, ACRS  
B. John Garrick, ACNW

SUBJECT: CERTIFIED MINUTES OF THE ACRS/ACNW JOINT SUBCOMMITTEE  
MEETING ON THE SUBJECT OF DEFENSE IN DEPTH

I certify that, based on my review of these minutes<sup>1</sup>, and to the best of my knowledge and belief, I have observed no substantive errors or omissions in the record of this proceeding subject to the comments noted below.

Comments:

J. S. Kress  
Thomas S. Kress, Co-Chairman

B. John Garrick  
B. John Garrick, Co-Chairman

3/3/2000  
Date

3/3/2000  
Date

<sup>(1)</sup> Minutes of Joint Subcommittee Meeting held on January 13-14, 2000, dated March 2, 2000.

## **1. Opening Remarks**

(Michael T. Markley was the Designated Federal Official for this meeting)

Dr. Thomas S. Kress convened the meeting at 8:30 a.m. on January 13, 2000. He explained that the purpose of the meeting was to discuss the role of the Nuclear Regulatory Commission's defense in depth philosophy in the regulatory process, including its role in the licensing of a high-level waste repository, its role in revising the regulatory structure for nuclear reactors, and how the two applications should be related to each other. He noted that the discussion would also include the role of defense in depth in the regulation of nuclear materials applications, and other related matters. He then introduced three invited experts: Dr. Thomas Murley, former director of the NRC Office of Nuclear Reactor Regulation, Dr. Robert Budnitz, former director of the Office of Nuclear Regulatory Research, and Mr. Robert Bernero, former director of the Office of Nuclear Material Safety and Safeguards.

## **2. Presentations by Joint Subcommittee Members**

Dr. Kress began the discussions with a presentation of his views on defense in depth and its role in a risk-based regulatory system. He described defense in depth as a design and operational philosophy for dealing with uncertainty in risk assessment. He then noted that this description lacks both precision, which he described as establishing "design-to" requirements, and limits, which he stated are necessary to determine when sufficient defense in depth has been provided. To deal with these shortcomings, he suggested that a design defense in depth philosophy consist of four principles: (1) prevent accidents from starting (initiation), (2) stop accidents at early stages (intervention), (3) provide for mitigating release of the hazard vector (mitigation), and (4) provide sufficient instrumentation to diagnose the type and progress of any accident (diagnosis). He then offered the following definition: "Design defense in depth is a strategy of providing design features to achieve acceptable risk (in view of the uncertainties) by the appropriate allocation of the risk reduction to both prevention and mitigation." He concluded that this definition could be implemented to put limits on defense in depth by emphasizing "appropriate allocation" to prevention and mitigation. Risk acceptance criteria must be specified, and criteria must be chosen to reflect the relative preference for prevention versus mitigation.

Dr. Budnitz commented that Dr. Kress's principles and definition appeared to exclude facility siting as a component of defense in depth. Dr. Kress acknowledged that siting could be an element of defense in depth.

Following Dr. Kress's presentation, Dr. Garrick presented his thoughts on a conceptual framework for the quantification of defense in depth. He used the structure of a probabilistic risk assessment for a boiling water reactor, starting with the frequency distributions of initiating events. By combining the initiating event frequency distributions with the frequency distributions of safety system unavailabilities, a distribution of core damage frequency can be obtained. By calculating the core damage frequency distribution both with and without the availability of a particular safety system, he argued that the contribution of that safety system to reducing core damage frequency could be quantified. Such a process can thus be used to quantify the role of various protection systems in reducing core damage frequency, and hence quantify their contribution to defense in depth.

Dr. Garrick acknowledged that application of a similar process to a nuclear waste repository needed to account for the fact that passive systems and the natural geologic setting would dominate the analysis. Nonetheless, he argued that the contribution to overall performance of individual components, such as the fuel cladding or back-fill, could be quantified in a similar manner. In all cases, the performance measure could be calculated with and without the contribution of a particular barrier or design feature, and hence a quantitative measure of that barrier's contribution to defense in depth could be established.

Following Dr. Garrick's presentation, Dr. Apostolakis presented a perspective on defense in depth prepared by Dr. Dana Powers, Chairman of the Advisory Committee on Reactor Safeguards, who was unable to attend this meeting of the Joint Subcommittee. In Dr. Power's view, defense in depth is a strategy that developed in the reactor safety community because there was little experience in the operation of nuclear power plants, and there were great uncertainties in both the likelihood of occurrence of accidents and their possible consequences. He notes that two schools of thought have developed on defense in depth, with the structuralist school holding that specific requirements for defense in depth are embedded in the regulations, and the rationalist school advocating defense in depth can be limited to accommodating uncertainties that cannot be quantified. Dr. Powers sees the possibility of a paradox arising in the rationalist approach when analyses are used to specify where defense in depth is applied to protect against the possibility that the analyses are wrong. Dr. Powers concludes that the conditions that encouraged the development of defense in depth for nuclear reactors are generally not present in the activities of nuclear material licensees. In particular, in many cases consequences are easily bounded, there is a wealth of operating experience, severe accidents with large consequences develop slowly, and phenomenological uncertainties are modest. He would therefore argue against the general imposition of a defense in depth philosophy on materials licensees.

Following his presentation of Dr. Powers' views, Dr. Apostolakis presented his own thoughts. He posed the question, "What is it that has changed over the years that has made us have meetings like this, publish papers, and think about defense in depth and its role in reactor regulation?" He then suggested that the answer is ". . . uncertainties that forced the pioneers to come up with defense in depth now . . . can be quantified, whereas in those days they could not quantify them." He then suggested that the potential conflict is between those who take defense in depth as a principle, and those who use defense in depth as a standard engineering tool to determine the level of risk and quantify uncertainty. He offered the following definition: "Defense in depth is a safety philosophy that requires that a set of provisions be taken to manage unquantified uncertainty associated with the performance of engineered systems." He argued that calling defense in depth a "principle" makes it impervious to analysis, and that focusing on unquantified uncertainty forces an examination of the quality of the analysis and suggests improvement. He also held that "multiple barriers" and "defense in depth" were not identical concepts. He concluded that Dr. Powers' recommendation against imposing defense in depth on nuclear materials licensees could be justified when there are no unquantified uncertainties in such applications.

### **3. Presentations by Invited Experts**

Dr. Budnitz began by describing what he perceived to be an ambiguity in the NRC's proposed 10 CFR Part 63 for a high-level waste repository at Yucca Mountain. Specifically, Part 63 would require that the repository comprise multiple barriers, as dictated by the Nuclear Waste Policy Act, but the Supplementary Information to Part 63 states that, "The Commission does not intend to specify numerical goals for the performance of individual barriers." The Supplementary Information goes on to state, "The proposed requirements will provide for a system of multiple barriers . . . to ensure defense in depth and increase confidence that the postclosure performance objective will be achieved." Dr. Budnitz argued that the net result of these statements was to establish a requirement for defense in depth, and yet provide no guidance on how compliance with that requirement would be judged. He contended that eventually the NRC would need to provide guidance on the relative contribution of each barrier to meeting the performance standard, or on the process for determining that sufficient defense in depth had been provided in the design. He concluded by saying, "Without specificity, you don't know how to regulate."

Dr. Murley began his discussion by saying that, based on his experience, ". . . defense in depth is not a regulatory requirement. It's not a principle. It never was. I would characterize defense in depth as an after-the fact explanation to Congress and to the public of how NRC achieves safety for reactors." Dr. Murley stated that he reviewed a 1989 document which presented findings on the Shoreham nuclear plant emergency plan. The document identified emergency preparedness as one element of the defense in depth philosophy, and identified the other levels of defense in depth as related to preventing accident initiators, terminating accident sequences, and mitigating the effects of accidents. He noted, however, that in judging the licensability of Shoreham, the specific features of the facility were compared to specific requirements in the regulations, not to attributes of defense in depth. He indicated that the defense in depth philosophy shaped the regulatory staff's thinking about reactor safety issues, and directed attention to events that might defeat several levels of defense. He noted, for example, that following the Chernobyl accident, he realized that safety culture was an extremely important safety concept because a poor safety culture had the potential to defeat several defense-in-depth barriers. He said that defense in depth should continue to be a guiding philosophy because it is a good way to think about safety, but that it should not be made a regulatory requirement. Dr. Murley concluded his remarks by saying that he supported the development of risk-informed regulation, but cautioned that it should not be allowed to become a code word for deregulation. He was uneasy with the notion of elevating defense in depth to the level of a principle or a requirement, and also with any attempt to allocate numerical goals to the levels of defense in depth.

Following Dr. Murley, Mr. Bernero began his presentation with the definition of defense in depth from SECY-98-144, "White Paper on Risk-Informed and Performance-Based Regulation." The definition reads, in part, "Defense in depth is an element of the NRC's Safety Philosophy that employs successive, compensatory measures to prevent accidents or mitigate damage . . . ." Mr. Bernero suggested that there is an overarching philosophy of defense in depth as a strategy of safety analysis. He further suggested that the defense in depth strategy should prevent undue reliance on any single contributor to safety, such as the rarity of an initiating event, a design feature, a barrier or a performance model. He noted that the current safety goals and

objectives lacked clarity with respect to intended span of protection (e.g. public safety vs. worker safety) and the range of authorized practices (e.g. reactors, fuel cycle facilities, and industrial uses). He also noted that the role of defense in depth in reactor safety was different than its role in materials regulation. In the regulation of waste disposal, he concluded that defense in depth definitely applies to the barriers to release. He also said the proposed Part 63 used a sound approach to defense in depth, and encouraged the development of the body of information required to exercise judgement. He felt that graded goals were needed for graded uncertainties, ranging from clearly acceptable to tolerable to unacceptable.

Following Mr. Bernero's presentation, Dr. Apostolakis suggested defining several points that could be used to focus the discussion for the remainder of the morning. Subcommittee members agreed, and the points that were selected were (1) whether or not defense in depth should be placed in the context of uncertainty, (2) should defense in depth involve the allocation of risk to prevention and mitigation, (3) how defense in depth should be used in the high level waste repository, (4) whether or not licensing decisions should be made solely on probabilistic risk assessments or total system performance assessments, and (5) should the NRC establish and regulate to risk acceptance criteria?

Dr. Apostolakis said that the reason we are revisiting the issue of defense in depth is that we can now quantify much of the uncertainty associated with system performance. He held that defense in depth was an inappropriate term for uncertainties that have been quantified. He would reserve the term defense in depth for dealing with unquantified uncertainties.

Dr. Garrick challenged Dr. Kress's idea of specifying the allocation of risk reduction between prevention and mitigation. Dr. Kress responded that he considered a high level allocation to be appropriate. Specifically, he had in mind an allocation between core damage frequency and conditional containment failure probability. Dr. Budnitz and Mr. Bernero argued that the distinction between prevention and mitigation was difficult to determine in the context of a high level waste repository. Dr. Apostolakis argued that perhaps allocation was not the correct concept for reactors, because core damage events are considered undesirable in and of themselves.

Dr. Budnitz noted that when Part 60 was written, there was not a great deal of confidence in what is now called performance assessment. Because of that, he believes, the staff felt it necessary to include subsystem requirements such as ground water travel time. Since performance assessment has now been developed to the point where it merits substantial confidence, specific performance criteria for individual barriers are no longer necessary or appropriate. Dr. Apostolakis asked what were the major unquantified uncertainties in performance assessment. Dr. Budnitz replied that they were model uncertainties.

Dr. Wymer gave a brief discussion of chemical uncertainties for the high level waste repository. He identified the corrosion behavior of the canister material, the formation of secondary precipitates in the fuel material that would tend to delay the release of radionuclides, and the effects of backfill material such as depleted uranium dioxide. Mr. Levenson pointed out that not all the uncertainties were negative, and that in fact a substantial number were positive.

#### **4. Presentations by the Office of Nuclear Material Safety and Safeguards**

John Greeves, Director of the Division of Waste Management, introduced the speakers for the Office of Nuclear Material Safety and Safeguards, Dr. Norman Eisenberg and Ms. Christiana Lui. Dr. Eisenberg began with a discussion of motivations for examining defense in depth in materials applications. First, the activity to develop a framework for risk-informing materials regulation as proposed in SECY-99-100, "Framework for Risk-Informed Regulations in the Office of Nuclear Material Safety and Safeguards," requires consideration of the role of defense in depth in that framework. Also, proposed 10 CFR 63 addresses defense in depth through multiple barriers. Other relevant activities include risk informing the regulation of interim spent fuel storage facilities, consideration of integrated safety assessments for fuel cycle facilities, and risk informing transportation regulations.

Dr. Eisenberg stated that the regulatory environment NMSS deals with includes considerable diversity, with facility complexity ranging from smoke detectors to gaseous diffusion plants, and hazard levels ranging from small to substantial. The types of risk are also diverse, and include both risks to workers and to members of the public from normal operations and accidents. He noted that the principal factors affecting the current requirements for defense in depth in materials applications include the nature of licensees and activities regulated and the current mix of risk-informed, performance-based and prescriptive, deterministic regulations. He noted that for some licensed activities, the hazard does not warrant very strong preventive measures of any type. He characterized the overall NMSS safety philosophy as providing reasonable assurance of protecting public health and safety, the common defense and security, and the environment. He stated that concepts that assisted in achieving defense in depth in this context included safety margin, diversity, redundancy, no single point of failure, and quality assurance. Referring to the May 19, 1999 ACRS letter to the Commission on the role of defense in depth in a risk-informed regulatory system, Dr. Eisenberg noted that the "rationalist" approach to defense in depth articulates a philosophy that relates defense in depth to the residual uncertainties in the system. He then stated that NMSS considers the rationalist approach appropriate for risk-informed, performance-based regulation.

Dr. Apostolakis asked whether residual uncertainties were the same as unquantified uncertainties. After some discussion, it was agreed that residual uncertainties would not include quantified uncertainties. Dr. Eisenberg went on to list the types of uncertainty in safety assessments as parameter, model, scenario, and programmatic. Dr. Apostolakis commented that he would consider model uncertainty to include scenario and programmatic uncertainty, and Dr. Garrick agreed. Dr. Eisenberg went on to characterize the two types of residual uncertainty as incompleteness in the state of knowledge (Type 1) and incompleteness in the safety analysis (Type 2). He then drew a distinction between defense in depth and margin by describing margin as the difference between the expected performance of a system and a safety limit. He characterized defense in depth as the ability of a system to compensate for unanticipated performance results owing to limitations on knowledge.

As a means of illustrating the important relationships, Dr. Eisenberg displayed a graphic relating uncertainty in performance, relative hazard, and defense in depth. Little defense in depth would be indicated for low hazard systems, such as a smoke detector, even if their safety performance was highly uncertain. More defense in depth would be indicated in well understood situations

involving relatively higher hazard, such as gamma radiography. Defense in depth requirements would be greatest where performance characteristics involved substantial uncertainties and/or where potential hazards were the highest. Dr. Garrick cautioned that there might be system properties not adequately represented in the graphic, such as the stored energy in a reactor, that would influence the degree of risk involved.

Dr. Eisenberg summarized his presentation by saying that defense in depth is related to, but different from, other safety concepts such as margin, redundancy and diversity. He further suggested it can be implemented as an overall system requirement rather than a set of subsystem requirements, and that the degree of defense in depth required is proportional to the residual uncertainties. Dr. Apostolakis suggested, as an alternative, that the residual uncertainty might be examined for each element of the system (each subsystem), and then the degree of defense in depth could be determined by combining those uncertainties so as to represent the uncertainty of the whole system. Dr. Eisenberg agreed.

Dr. Eisenberg concluded his presentation with a partial list of issues to be resolved. The list included how to measure the degree of defense in depth, how to measure the degree of uncertainty in the performance of a system, and how to measure the degree of potential hazard posed by a system. The list also included how to make reasonable tests for sufficient defense in depth in light of incomplete knowledge, and how to communicate to stakeholders the flexibility inherent in a risk-informed, performance-based approach to defense in depth. Dr. Kress agreed that it was a good list of issues, but thought that further explanation was needed on the term "degree of hazard."

Following Dr. Eisenberg, Ms. Christiana Lui discussed implementing the multiple barrier requirement in a geologic repository for high-level waste. She noted that the public comment period on the proposed rule governing the disposal of high level wastes at Yucca Mountain, 10 CFR Part 63, ended on June 30, 1999, and that the final rule was due to the Commission by March 31, 2000. She stated that multiple barriers would be implemented as an assurance requirement in Part 63 to provide confidence that known uncertainties are appropriately captured in the compliance demonstration calculations and that the repository system is sufficiently robust to account for imperfect knowledge. She indicated that the process required of the Department of Energy (DOE) would be to assess all negative impacts on safety, identify all barriers, quantify the capabilities of the barriers, and show that safety does not wholly depend on any single barrier. This point was discussed at some length by the subcommittee members and the invited experts. Dr. Apostolakis and Dr. Garrick were concerned that "showing safety does not wholly depend on a single barrier" appeared to discourage providing a single barrier that could, by itself, meet the performance goal. Mr. Bernero suggested that "wholly depend" be replaced with "unduly depend." Dr. Budnitz argued that "wholly depend" was acceptable because it permitted two or more barriers, each of which could meet the performance standard alone.

Ms. Lui continued, saying that the demonstration of multiple barriers consisted of showing that the balance of the repository system has the ability to compensate for an under-performing barrier so public health and safety are protected. Dr. Apostolakis suggested that the under-performance scenarios chosen for analysis should include consideration of their probability of occurrence. Dr. Eisenberg responded that the under-performance would be related to the



degree of uncertainty in that particular barrier. Dr. Budnitz expressed concern that no criteria were being established to determine when the results of a particular under-performance analysis would result in denying a license.

Ms. Lui concluded by saying that multiple barriers were a legislative requirement. DOE must show that both geologic and engineered barriers contribute to safety, and that the repository system has the ability to compensate for the under-performance of any one barrier. There followed substantial discussion among the subcommittee members and invited experts as to whether this process could be sufficiently well defined and whether clear acceptance criteria could be established. In closing the NMSS presentation, Mr. Greeves noted that the proposed rule (Part 63) was still under development, and that the comments offered by the subcommittee and invited experts were helpful and would be taken into consideration.

#### **5. Presentation by Offices of Nuclear Reactor Regulation and Nuclear Regulatory Research**

Following a ten minute recess, Gary Holahan of the Office of Nuclear Reactor Regulation (NRR) and Tom King of the Office of Nuclear Regulatory Research (RES) presented a perspective on defense in depth for risk informing 10 CFR Part 50, the regulations governing the design, construction and operation of nuclear reactors. Mr. Holahan began by noting that there is no formal regulation or policy statement on defense in depth, and that the reactor program was starting from the same philosophical base as the materials program. The defense in depth philosophy is included in reactor regulation (through, for example, the General Design Criteria), the licensing and license amendment processes, and the reactor oversight program. Current Part 50 requirements include defense in depth considerations, such as provisions for accident prevention and mitigation, the single failure criterion, redundancy and diversity requirements, multiple barriers to fission product release, and quality of design and operation. He said the physical barriers, functional barriers, or risk allocation as suggested by Dr. Kress, could all be manifestations of defense in depth. As an example of functional barriers, he cited preventing accident initiators, providing safety systems to terminate accident sequences, providing safety systems for mitigation such as containment, and planning for accident management. Physical barriers are represented by the fuel pellet, cladding, reactor coolant system, containment, and the exclusion area. He pointed out that the structure and content of the General Design Criteria in 10 CFR 50 Appendix A reflected the defense in depth philosophy.

Mr. Holahan discussed the new reactor oversight program, and pointed out that it was structured using cornerstones which were chosen to reflect defense in depth. For example, the cornerstones for reactor safety are initiating events, mitigation systems, barrier integrity and emergency preparedness. Furthermore, in evaluating licensee performance relative to these cornerstones, the regulatory response is graded according to the perceived threat to, or weakening of, defense in depth.

Mr. Holahan next discussed the current issues related to application of defense in depth in risk-informed reactor activities. In the reactor licensing and license amendment process as reflected in Regulatory Guide 1.174 (An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, July 1998), maintaining

the defense in depth philosophy is one of the five safety principles considered in evaluating proposed changes. Defense in depth is considered to have seven elements:

- balance between prevention and mitigation
- avoiding over-reliance on programmatic activities
- system redundancy, diversity, independence
- defense against common cause failures
- independence of barriers
- defense against human errors
- meeting the intent of the General Design Criteria
- 

The process for evaluating license amendment requests based on risk arguments includes testing the proposed amendment against the above elements to ensure that an appropriate level of defense in depth is maintained.

Dr. Apostolakis stated his belief that the staff's views on maintaining the defense in depth philosophy implicitly assumed its application to the current generation of nuclear power plants. Mr. Holahan responded that the application also extended to the currently proposed evolutionary and advanced reactors. He noted that reactor applications of defense in depth were different from typical materials applications because reactor regulation primarily provided protection from low probability, high consequence events. As a result, defense in depth judgements were usually based on very limited experience. A brief discussion followed among Dr. Budnitz, Dr. Apostolakis, Mr. King and Mr. Holahan on the degree to which operating reactor events analyzed in the accident sequence precursor (ASP) program provided confidence in our understanding of reactor accidents. Dr. Apostolakis held that system unavailabilities obtained from the ASP program were consistent with those from current probabilistic risk assessments, and therefore indicated that "what we are doing is not off the mark."

The NRC is currently pursuing two projects to develop risk-informed revisions to 10 CFR Part 50, referred to internally as Option 2 and Option 3, both of which involve developing a working definition of defense in depth. Mr. Holahan concluded by describing the objective of Option 2, the project being carried out by NRR. Option 2 will look at issues related to operational performance and those parts of the plant that get special treatment such as quality assurance, technical specifications and maintenance. "Risk-informing" will involve changing the scope of the rules from those systems, structures and components (SSCs) now designated as "safety related," to those which would be designated as "risk-significant." The process of designating SSCs as risk-significant will involve not only probabilistic risk assessments, but also insights from experienced plant personnel. Dr. Apostolakis observed that the degree to which the seven identified elements of defense in depth are maintained in this process could depend on the quality and quantity of risk information supported by applicable experience.

At this point, Mr King picked up the discussion and described the Option 3 technical study being conducted in the Office of Research. He said that while Option 2 was looking at the scope of what ought to be regulated based on risk insights, Option 3 was looking at the functions and design requirements that should be changed based on risk insights. He noted that the related policy issues, whether or not a definition of defense in depth was needed in the Safety Goal

Policy and whether or not a separate policy statement was needed on defense in depth, would be the subject of a separate ACRS briefing within the next month or two.

Mr. King said that both Option 2 and Option 3 depended on developing a working definition of defense in depth that provides multiple lines of defense, balance between prevention and mitigation, and a framework to address uncertainties in accident scenarios. He suggested that the definition should consist of two parts: fundamental elements that should be present in all cases, and implementation elements that may vary depending on uncertainty and risk goals. He characterized the fundamental elements as "structuralist" and the implementation elements as "rationalist," implicitly referring to the May 19, 1999 ACRS letter to the Commission on defense in depth. The fundamental elements would build on the cornerstone concept and address initiating events, prevention of core melt, fission product containment and emergency planning. Prevention and mitigation would be assured by providing reliable core melt prevention for all credible initiating events, by providing the ability to contain fission products given a core melt, and by providing emergency planning and response. Overall, the fundamental elements would assure a balance between prevention and mitigation to achieve a level of safety consistent with a core damage frequency less than or equal to  $10^{-4}$  per reactor year, and a large early release frequency less than or equal to  $10^{-5}$ . He then described a conceptual framework based on the cornerstones to achieve this balance between prevention and mitigation, and in addition limit the frequency of significant dose to an offsite individual to  $10^{-6}$ .

A lengthy discussion of the framework and its implementation followed. Drs. Garrick and Kress questioned whether the effects of emergency response were included in the goal for large early release. Mr. King responded that it was. Dr. Kress asked if there were different responses for frequent vs. infrequent initiators. Mr. Holahan responded that it will probably turn out that systems important for more frequent initiators, such as small break loss of coolant, will be unimportant for less frequent initiators, such as very large breaks. Dr. Apostolakis questioned why the goals and indicators should not be site specific. Mr. Holahan responded that he didn't think that level of refinement could be justified. Dr. Kress agreed. Dr. Apostolakis suggested that limits be established in addition to goals; for example, in addition to a goal of  $10^{-4}$  for core damage frequency, an acceptability limit of  $10^{-3}$  could be established. Dr. Kress suggested that the goal for conditional containment failure probability should be lowered in order to minimize the uncertainty in large early release frequency. Mr. King agreed to give their suggestions some thought.

Mr. King concluded by stating that neither the probabilistic goals nor a definition of defense in depth would be included in the regulations. Instead they would be used to derive deterministic requirements that would be in the regulations. Dr. Kress and Dr. Apostolakis indicated that they liked the overall approach.

## **6. Presentations by the Nuclear Energy Institute, Electric Power Research Institute, and Westinghouse.**

Alex Marion of the Nuclear Energy Institute (NEI), introduced Rodney McCollum, the NEI project manager involved in high level waste management. Mr. McCollum acknowledged the need for decision-making tools to address uncertainty, but he questioned the applicability of reactor

# **CERTIFIED**

Issued: 3/2/2000

3/3/2000

By Thomas S. Kress and  
B. John Garrick

## **CERTIFIED MINUTES OF THE MEETING OF THE ACRS/ACNW JOINT SUBCOMMITTEE JANUARY 13-14, 2000 ROCKVILLE, MARYLAND**

The U. S. Nuclear Regulatory Commission (NRC) Joint Subcommittee of the Advisory Committee on Reactor Safeguards (ACRS) and the Advisory Committee on Nuclear Waste (ACNW) held a meeting on January 13-14, at Two White Flint North, Room T-2 B 3, 11545 Rockville Pike, Rockville, Maryland. The purpose of this meeting was to provide a forum for attendees to discuss and take appropriate action on the items listed in the agenda (Appendix B). The entire meeting was open to the public.

A transcript of the meeting is available in the NRC's Public Document Room at the Gelman Building, 2120 L Street, NW, Washington, DC 20555-0001. Copies of the transcript are available for purchase from Ann Riley & Associates, Ltd., 1025 Connecticut Ave, NW, Suite 1014, Washington, DC 20036. Transcripts are also available for downloading from, or reviewing on, the Internet at <http://www.nrc.gov/ACRSACNW>.

### **ATTENDEES**

Joint Subcommittee members who attended this meeting were Dr. Thomas S. Kress, ACRS, Joint Subcommittee Co-Chairman, Dr. B. John Garrick, ACNW, Joint Subcommittee Co-Chairman, Dr. George Apostolakis, ACRS, and Dr. Raymond Wymer, ACNW. Also present were Mr. Milton Levenson, consultant to the ACNW, and invited experts Dr. Thomas E. Murley, Dr. Robert J. Budnitz, and Mr. Robert M. Bernero. NRC staff presentations were made by John Greeves, Norman Eisenberg and Christiana Lui of the Office of Nuclear Material Safety and Safeguards, Gary Holahan of the Office of Nuclear Reactor Regulation, and Thomas King of the Office of Nuclear Regulatory Research. Presentations or prepared statements were also made by industry representatives Alex Marion and Rodney McCollum of the Nuclear Energy Institute, Gary Vine of the Electric Power Research Institute, and Brian McIntyre of Westinghouse Electric Company. For a list of other attendees, see Appendix C.

notions of defense in depth to the repository development process. He cited his prior experience as a Department of Energy manager, and the difficulties he encountered trying to make NRC regulatory requirements apply to DOE facilities. Mr. McCollum held that the differences between Yucca Mountain and reactors are so fundamental that it is impossible to relate reactor defense in depth to multiple barriers in the repository. He questioned whether defense in depth was an appropriate term for Yucca Mountain, and suggested using the term multiple barriers instead. He concluded that DOE then needs to address what each of the barriers means to the safety case, and what the uncertainties are.

Mr. Marion next offered comments from the perspective of operating reactors. Referring to Dr. Murley's earlier admonition regarding elimination of barriers, Mr. Marion supported that admonition, but counseled staying alert for opportunities to use risk insights and operating experience to better define implementation of specific barriers. Mr. Marion said that the defense in depth philosophy balanced with risk-informed approaches is fundamental to the industry's thinking on regulatory reform, specifically in risk informing 10 CFR Part 50.

Dr. Apostolakis, also referring to Dr. Murley's caution and a possible perception that risk-informed regulatory approaches were being used to remove regulatory requirements, held that the opposite has been true in the past. He said that, for the past 20 years, where PRA indicated additional requirements were needed, the NRC had acted to establish those requirements and had thereby created a somewhat hostile industry view of PRA. He noted that if the agency is finally looking at removing some requirements, it should not be forgotten that many were already added. Dr. Kress expressed his agreement.

Mr. Marion then introduced Gary Vine of the Electric Power Research Institute. Mr. Vine described how defense in depth had been implemented in the Advanced Light Water Reactor Utility Requirements Document, and its implications on the balance between prevention and mitigation. He described how PRA was used in the development of the ALWR designs to achieve calculated core damage frequencies of much less than  $10^{-5}$ . The strategy to ensure licensability was to provide demonstrable margin between regulatory requirements and actual design performance. Mr. Vine concluded that risk-informed regulation was essential for future advanced reactor deployment, and that the "rationalist model" (as described in the May 19, 1999 ACRS letter mentioned earlier) should be the future approach to defense in depth. He noted that the International Nuclear Safety Advisory Group (INSAG) recommended a structural model for defense in depth, and that he thought U.S. leadership to promote the rationalist model was important.

Following Mr. Vine's presentation, Brian McIntyre of Westinghouse discussed the implementation of defense in depth in the design of the Westinghouse AP-600 advanced light water reactor. He explained the role of PRA in establishing design features, and the multiple levels of defense in depth that included non-safety active systems and passive safety features. He indicated that the basic difficulty encountered with the NRC licensing staff was understanding the staff's desired balance between prevention and mitigation, and how it could be determined when sufficient mitigation had been provided. In one example of trying to determine this balance, the staff required the addition of a containment spray to the AP-600, a requirement that the ACRS endorsed in a June 17, 1997 letter to the Commission. Mr. McIntyre suggested that

the decision making processes for defense in depth discussed earlier in the day by Mr. King and Mr. Holahan of the NRC staff might now lead to a different conclusion.

Following the Westinghouse presentation, the meeting was recessed until the following morning.

## **7. Roundtable Discussions**

Dr. Kress reconvened the meeting at 8:30 a.m. on Friday, January 14, 2000. He asked Dr. Garrick if he had any opening remarks. Dr. Garrick said the previous day's discussions had highlighted the large differences between reactor applications and materials applications, and also the large differences among materials applications. He suggested that part of the meeting be devoted to non-high-level waste issues, and how defense in depth might apply to those. He then noted that one of the objectives coming into the meeting was to try to identify an overarching philosophy of defense in depth, and suggested that some time be spent on that issue. Dr. Apostolakis agreed with Dr. Garrick's comments, and further suggested that if the Joint Subcommittee was going to prepare a letter the discussion be structured around specific points to be included in the letter. Dr. Budnitz questioned whether it was either necessary or desirable to seek an overarching philosophy. Mr. Bernero suggested first trying to characterize defense in depth, then considering the application of risk information to defense in depth, and finally discussing applications in specific fields such as reactors, materials, or high level waste. There was general agreement to that approach.

There was a lengthy discussion of whether or not the characterization of defense in depth in SECY-98-144, "White Paper on Risk-Informed and Performance-Based Regulation," was an appropriate starting point, or whether changes were required. Dr. Budnitz argued against trying to do too much with a single definition. Mr. Holahan observed that if the ACRS and ACNW says nothing about the definition, then the words in the white paper are left in place. Dr. Apostolakis felt strongly that the concept of defense in depth as a means to address uncertainty should be made explicit. Dr. Kress thought it was important to retain the idea of successive protective measures. Dr. Garrick thought the definition in the white paper communicated the idea of defense in depth well. Mr. Levenson suggested the Subcommittee accept the white paper definition of defense in depth, and concentrate instead on describing how its application should be different for reactor, waste repositories, and other material applications. Dr. Wymer expressed support for that approach. Dr. Apostolakis noted that the ACRS's May 19, 1999, letter to the Commission said that defense in depth has been invoked primarily to compensate for our uncertainty in the knowledge of accident progression at nuclear power plants, and that applications of defense in depth should be justified with respect to both necessity and sufficiency. He then reiterated his position that "uncertainty" should be part of any definition. Dr. Larkins suggested proceeding with a discussion of the implementation of defense in depth, and then revisiting the definition if that appeared necessary.

Mr. Markley suggested that rather than revisiting the definition, the application of defense in depth could be clarified in a policy statement or similar document, and then elements or sub-elements for various applications could be identified. Dr. Garrick thought this approach could accomplish the goal of identifying the "overarching" aspects of defense in depth. Mr. Bernero suggested that the application of defense in depth should be risk-informed. Dr. Kress agreed that risk-informed defense in depth provided the correct perspective for reactor applications, and

noted that this idea was consistent with the presentation made earlier in the meeting by Mr. King and Mr. Holahan. Dr. Garrick noted that one difference between the high level waste repository and reactors is the lack of performance data for the repository, which he cited as a reason for not establishing subsystem requirements. He argued that the regulatory requirements for the repository should focus on the performance measure rather than on surrogates of that measure. Dr. Apostolakis pointed out that Dr. Garrick's viewpoint was consistent with the idea that there were large uncertainties associated with the performance of each barrier, and that the decision on allocating performance among the barriers was simply being postponed. Mr. Levenson added that uncertainty is important only if the consequences of that uncertainty are serious.

Dr. Apostolakis summarized his position with three points: (1) defense in depth was developed to manage uncertainty, (2) if the uncertainties are quantified, there is a way to limit defense in depth, (3) it would be acceptable to use the term "risk-informed defense in depth" for quantified uncertainties. Dr. Eisenberg reinforced Mr. Levenson's comment by noting that many material activities involved very small risks, and that protective measures appropriate to prevent high radiation doses were inappropriate if the threat was very low doses. Dr. Kress commented that his proposed definition of defense in depth included the term "acceptable risk" for the same reason, that different levels of risk should result in different strategies.

Dr. Wymer began to outline his thoughts on how a Joint Subcommittee letter emerging from this meeting might be structured. He suggested that the letter begin with a general statement of what is meant by defense in depth, and then develop two separate themes, one relating to reactors and the other relating to high level waste and materials applications. Each committee, ACRS or ACNW, would be responsible for developing its point of view in its area of responsibility. He suggested the ACNW portion of the letter comprise five points. First, there are uncertainties in performance assessments. Because there is much less experience with waste repositories than with reactors, uncertainties in repository performance are greater than uncertainties in reactor performance. Second, performance and risk assessment requirements are not as well understood for waste repositories as they are for reactors. These differences should be recognized in any defense in depth philosophy statements. Third, there should be several lines of defense against release of radioisotopes and resultant radiation exposures. Types and numbers of lines of defense should be directly related to the uncertainties and relative hazards of system performance. Fourth, defense in depth requirements for waste repositories and for nuclear reactors are different in very important ways. This is related to the physical nature of the systems and the very large time dependent and potential energy differences. Fifth, NRC should specify clearly how the performance assessment should be done in DOE's license application for Yucca Mountain. Sixth, because of the nature of the interactions between the NRC and license applications for complex systems, there will always be a strong possibility of an iterative licensing process.

Dr. Apostolakis noted that there was a strong underlying theme about uncertainties in Dr. Wymer's points. Dr. Kress observed that the definition of defense in depth the subcommittee had been referring to was actually a footnote in the white paper on risk-informed, performance-based regulation. The paper itself discusses a relationship among risk insights, defense in depth, and uncertainty. Risk insights can make the elements of defense in depth clearer by quantifying them. Quantifying these elements and uncertainties can aid in determining how much defense in depth makes regulatory sense. Dr. Kress went on to say that decisions on the

adequacy or necessity of elements of defense in depth should reflect risk insights from the individual performance of each defense system in relation to the overall performance.

Dr. Garrick suggested that the notion of risk be the prevailing notion in the proposed subcommittee letter. Dr. Apostolakis suggested starting by saying the main idea is to manage risk, and then distinguishing among the applications. Reactors would be recognized as having a high risk potential because of timing and energetics, waste repositories as having less stored energy and much longer time scales, and other NMSS activities as having lower risks and unique circumstances. A brief discussion among subcommittee members followed, and several suggestions were made to add to or modify Dr. Apostolakis' points.

Dr. Kress suggested concluding the meeting by asking each of the invited experts to summarize their impressions from the past day and a half of discussion and their thoughts on what the proposed letter should contain. He also asked that they provide a written summary following the meeting.

Mr. Bernero said he saw the white paper as the appropriate starting point. Defense in depth should be acknowledged as a policy, strategy, approach or philosophy, but not as a requirement. He thought Dr. Apostolakis had excellent arguments for associating defense in depth with uncertainty, but that the key idea was to avoid undue reliance on any single element of defense. He said it was important to admit the possibility of removing a traditional barrier, or omitting a traditional barrier in a new application. As an example of the latter, he cited providing emergency planning for a waste repository as entirely inappropriate. He concluded that imposition of defense in depth to the broad range of materials applications should not result in inappropriate requirements for situations that involve little risk.

Dr. Budnitz stated that it would be an error to elevate defense in depth to a higher level. He thought it would be a better strategy to downplay its role, and that defense in depth should emerge from sound engineering practices rather than be imposed from the top. He recommended that the subcommittee downplay the idea that defense in depth is some sort of principle. Instead, the subcommittee should adopt the view that defense in depth emerges in different ways in different arenas as dictated by sound engineering practice in those arenas. Thus it would have different manifestations in low level waste, high level waste, transportation, and reactors to accomplish managing risk to an acceptable level with due consideration for uncertainty.

Mr. Levenson suggested that the letter might be a useful device to prevent the proliferation of defense in depth to fields other than reactors. It should take the position that defense in depth, as presently understood and utilized, applies to high energy, high risk facilities, and that the generic concept of not being vulnerable to a single failure for other facilities, such as a repository, is accomplished by multiple passive barriers. If the subcommittee says defense in depth is tied to risk significance, then that allows different rules for lesser facilities.

Prior to concluding the meeting, Dr. Kress invited summary comments from the NRC staff. Mr. Holahan said he thought it would be useful to the staff and the Commission if the subcommittee recorded some of the perspectives on defense in depth articulated during the meeting. He noted Dr. Budnitz's view that defense in depth is not an absolute, and said that the staff has not



applied defense in depth in cases where the consequences or frequencies of events were very low. He concluded that if defense in depth is a principle, it is a derived principle rather than a fundamental principle. He said that uncertainties are the more important issue, and that if the subcommittee could shed light on where defense in depth has its largest role, that would be of value.

Mr. King said that after listening to the discussion at the meeting he no longer thought a Commission policy statement on defense in depth was appropriate. He believed that many of the perspectives on the application of defense in depth discussed in the meeting were worth documenting, and the subcommittee might suggest a vehicle for doing so.

Dr. Eisenberg said that the big concern of the NMSS staff is that an overarching principle geared to reactor regulation be imposed on materials regulation. He thought the discussion throughout the meeting reflected an understanding of that concern. He stated that NMSS was going to move further into risk-informing its regulatory practices, and that some of the traditional concepts of safety and defense in depth would have to change in that environment.

Mr. Steve Hanauer of the Department of Energy said that he believed the discussions during the meeting over-estimated the state of knowledge and therefore underestimated the contribution that defense in depth and multiple barriers make to achieving acceptable levels of safety. The uncertainties are greater than the risk analysts generally believe. Public skepticism for some pronouncements from the technical community is justified, and that defense in depth and multiple barriers are a legitimate response to this skepticism.

Janet Kotra of the NMSS staff pointed out that in 1983, in promulgating 10 CFR Part 60, the Commission invoked defense in depth and stated that the imposition of quantitative subsystem requirements was essential to its assurance. The present Commission has approved a different direction, and Dr. Kotra believes that change of direction will have to be addressed when the Part 63 final rule is submitted.

Dr. Garrick reiterated that the emphasis of the letter should be on trying to encourage the quantification of defense in depth. He expressed a lack of enthusiasm for allocation of risk or subsystem performance requirements.

Following a brief discussion of the mechanics of drafting a letter, Dr. Kress adjourned the meeting at 11:06 a.m.

For the Nuclear Regulatory Commission.  
**David B. Matthews,**  
*Director, Division of Regulatory Improvement  
 Programs, Office of Nuclear Reactor  
 Regulation.*  
 [FR Doc. 99-33022 Filed 12-20-99; 8:45 am]  
 BILLING CODE 7590-01-P

## NUCLEAR REGULATORY COMMISSION

### Advisory Committee on Reactor Safeguards and Advisory Committee on Nuclear Waste; Joint Subcommittee Meeting; Notice of Meeting

The ACRS and ACNW Joint Subcommittee will hold a meeting on January 13-14, 2000, Room T-2B3, 11545 Rockville Pike, Rockville, Maryland.

The meeting will be open to public attendance.

The agenda for the subject meeting shall be as follows:

*Thursday, January 13, 2000—8:30 a.m.  
 until 5 p.m.*

*Friday, January 14, 2000—8:30 a.m.  
 until 12 Noon*

The Advisory Committee on Reactor Safeguards and Advisory Committee on Nuclear Waste Joint Subcommittee will discuss the defense-in-depth philosophy in the regulatory process, including its role in the licensing of a high-level waste repository, its role in revising the regulatory structure for nuclear reactors, and how the two applications should be related to each other. The discussion will also include the role of defense in depth in the regulation of nuclear materials applications, and other related matters. The purpose of this meeting is to gather information, analyze relevant issues and facts, and formulate proposed positions and actions, as appropriate, for deliberation by the full Committees.

Oral statements may be presented by members of the public with the concurrence of the Subcommittee; written statements will be accepted and made available to the Subcommittee. Electronic recordings will be permitted only during those portions of the meeting that are open to the public, and questions may be asked only by members of the Subcommittee, its consultants, and staff. Persons desiring to make oral statements should notify the cognizant ACRS/ACNW staff members named below five days prior to the meeting, if possible, so that appropriate arrangements can be made.

During the initial portion of the meeting, the Subcommittee, along with any consultants who may be present, may exchange preliminary views

regarding matters to be considered during the balance of the meeting.

The Subcommittee will then hear presentations by and hold discussions with representatives of the NRC staff, its consultants, and other interested persons regarding these matters.

Further information regarding topics to be discussed, whether the meeting has been canceled or rescheduled, the Subcommittee's ruling on requests for the opportunity to present oral statements and the time allotted therefor can be obtained by contacting the cognizant senior fellow, John N. Sorensen (telephone 301/415-7372) between 8 a.m. and 5:45 p.m. (EST) or by e-mail JNS@NRC.gov or staff engineer, Michael T. Markley (telephone: 301-415-6885). Persons planning to attend this meeting are urged to contact the above-named individuals one to two working days prior to the meeting to be advised of any potential changes in the proposed agenda, etc., that may have occurred.

Dated: December 15, 1999.

**Howard J. Larson,**

*Acting Associate Director for Technical  
 Support, ACRS/ACNW.*

[FR Doc. 99-33019 Filed 12-20-99; 8:45 am]

BILLING CODE 7590-01-P

## NUCLEAR REGULATORY COMMISSION

[Docket No. 70-754-MLA and ASLBP No.  
 00-774-02-MLA]

### General Electric Company; Designation of Presiding Officer

Pursuant to delegation by the Commission dated December 29, 1972, published in the *Federal Register*, 37 FR 28,710 (1972), and Sections 2.1201 and 2.1207 of Part 2 of the Commission's Regulations, a single member of the Atomic Safety and Licensing Board Panel is hereby designated to rule on petitions for leave to intervene and/or requests for hearing and, if necessary, to serve as the Presiding Officer to conduct an informal adjudicatory hearing in the following proceeding:

**General Electric Company, Vallecitos  
 Nuclear Center**

The hearing, if granted, will be conducted pursuant to 10 CFR Part 2, Subpart L, of the Commission's Regulations, "Informal Hearing Procedures for Adjudications in Materials and Operator Licensing Proceedings." This proceeding concerns a request for hearing submitted by Tri-Valley CAREs, the Western States Legal Foundation, Save Our Sunol, and Citizens Along the Roads and Tracks.

The request was filed in response to a notice of consideration by the Nuclear Regulatory Commission of a request for renewal of the 10 CFR Part 70 license for the General Electric Vallecitos Nuclear Center. The renewal application requests authorization to receive and possess special nuclear material and to use special nuclear material in research and development activities involving chemical and physical analysis. The notice of consideration of the renewal application and opportunity for hearing was published in the *Federal Register* at 64 FR 45,289 (Aug. 19, 1999).

The Presiding Officer in this proceeding is Administrative Judge Alan S. Rosenthal. Pursuant to the provisions of 10 CFR 2.722, 2.1209, Administrative Judge Thomas D. Murphy has been appointed to assist the Presiding Officer in taking evidence and in preparing a suitable record for review.

All correspondence, documents, and other materials shall be filed with Judge Rosenthal and Judge Murphy in accordance with 10 CFR 2.1203. Their addresses are:

Administrative Judge Alan S. Rosenthal,  
 Presiding Officer, Atomic Safety and  
 Licensing Board Panel, U.S. Nuclear  
 Regulatory Commission, Washington,  
 DC 20555-0001

Administrative Judge Thomas D.  
 Murphy, Special Assistant, Atomic  
 Safety and Licensing Board Panel,  
 U.S. Nuclear Regulatory Commission,  
 Washington, DC 20555-0001

Issued at Rockville, Maryland, this 15th  
 day of December 1999.

**G. Paul Bollwerk III,**

*Chief Administrative Judge, Atomic Safety  
 and Licensing Board Panel.*

[FR Doc. 99-33018 Filed 12-20-99; 8:45 am]

BILLING CODE 7590-01-P

## NUCLEAR REGULATORY COMMISSION

### Draft Regulatory Guide; Issuance, Availability

The Nuclear Regulatory Commission has issued for public comment a draft of a new guide in its Regulatory Guide Series. This series has been developed to describe and make available to the public such information as methods acceptable to the NRC staff for implementing specific parts of the NRC's regulations, techniques used by the staff in evaluating specific problems or postulated accidents, and data needed by the staff in its review of applications for permits and licenses.

The draft guide, temporarily identified by its task number, DG-1086

1/12/2000

**ADVISORY COMMITTEE ON REACTOR SAFEGUARDS  
ADVISORY COMMITTEE ON NUCLEAR WASTE  
MEETING OF THE JOINT ACRS/ACNW SUBCOMMITTEE  
ROOM T-2B3, 11545 ROCKVILLE PIKE, ROCKVILLE, MD  
JANUARY 13-14, 2000**

ACRS/ACNW Contacts:     Jack Sorensen (301) 415-7372  
                                  Michael T. Markley (301) 415-6885

**- PROPOSED SCHEDULE -**

<u>TOPIC</u>	<u>PRESENTER</u>	<u>TIME</u>
<b><u>January 13, 2000</u></b>		
<b>1) Introduction</b>		8:30-9:00 am
<ul style="list-style-type: none"><li>● Review goals and objectives for this meeting:</li><li>- ACRS/ACNW interest/issues in defense-in-depth</li><li>- Comments/recommendations</li></ul>	T. Kress, ACRS J. Garrick, ACNW	
<b>2) ACRS/ACNW Invited Expert Presentations (30 min. each)</b>		9:00-10:00 am
<ul style="list-style-type: none"><li>● R. Budnitz</li><li>● T. Murley</li></ul>		
<b>** BREAK **</b>		10:00-10:15 am
<b>3) ACRS/ACNW Invited Expert Presentations - continued</b>		10:15-10:45 am
<ul style="list-style-type: none"><li>● R. Bernero</li></ul>		
<b>4) General discussion</b>		10:45-12:00 noon
<ul style="list-style-type: none"><li>● Continued discussion of topics</li><li>● Issues for further consideration</li></ul>		
<b>** LUNCH **</b>		12:00-1:00 pm

- 5) **NRC Staff Presentations** 1:00-2:30 pm
- Defense-in-depth in reactor regulation G. Holahan, NRR  
T. King, RES
- \*\* BREAK \*\*** 2:30-2:45 pm
- 6) **NRC Staff Presentations** 2:45-4:45 pm
- Defense-in-depth in high-level waste and materials regulation C. Lui, N. Eisenberg, NMSS
- \*\* BREAK \*\*** 4:45-5:00 pm
- 7) **Stakeholder Presentations** 5:00-5:30 pm
- NEI A. Marion  
Westinghouse B. McIntyre

**January 14, 2000**

- 8) **Introduction** 8:30-8:45 am
- Review goals and objectives for this meeting: T. Kress, ACRS  
J. Garrick, ACNW
  - Summary of January 13, 2000 discussions
  - Suggestions and possible options
- 9) **Roundtable Discussions** 8:45-10:00 am
- ACRS/ACNW members, invited experts, and NRC staff, et. al.
- \*\* BREAK \*\*** 10:00-10:15 am
- 10) **Roundtable Discussions - continued** 10:15-11:30 am
- ACRS/ACNW members, invited experts, and NRC staff, et. al.
- 11) **General Discussion and Adjournment** 11:30-12:00 noon
- General discussion and comments by Members of the Subcommittee; possible ACRS/ACNW report, items for future meetings T. Kress, ACRS  
J. Garrick, ACNW

**Note: Presentation time should not exceed 50% of the total time allocated for a specific item. Number of copies of presentation materials to be provided to the ACRS - 35.**

**ADVISORY COMMITTEE ON REACTOR SAFEGUARDS**

**JOINT ACRS/ACNW SUBCOMMITTEE MEETING**

**JANUARY 13-14, 2000**

Date(s)

**JANUARY 13, 2000**

Today's Date

**NRC STAFF SIGN IN FOR ACRS MEETING**

PLEASE PRINT

NAME	BADGE #	AFFILIATION
TIM REED	B 6986	NRR / DRIP / RGE B
Charles Haughney	A 6157	NMSS / IMNS
Tim McCarth	A 6760	NMSS / DWM
DAVE Esh	B 8289	NMSS / DWM
Stacey Rosenberg	B 7440	NMSS / IMNS
William Beckner	B 6059	NRR / DRIP / TSB
Bakr Ibrahim	B 6292	NMSS / DHLW
BOB PALCA	B 6891	NRR / DSSA
SANDRA WASTLER	B 7239	NRC / NMSS / DWM
Mary Monim	B 7583	NRC / RES
GARETH PARRY	B-8060	NRR / DSSA
Goutam Bagchi	B 8626	NRR / DE
Nanette Gilles	B 8558	NRR / DRIP
Latif Hamdan	B 5210	NMSS / DWM
Bonad Jagannath	B. 6305	NMSS
Mike Cheek	B-7917	NRR / DSSA
PHILIP JUSTUS	B-8150	NMSS / WM / HLWB
Mysore Nataraja	<del>B 875</del> B 6841	NMSS / WM / HLWB

JOHN RANDALL	B6972	ACNW
PHIL REED	B6985	RES
Alan Levin	B6675	OCM/RAM
Janet Kotra	B7761	NMSS/DWM
Christiana Lee	B6709	NMSS/DWM
Mohammed Shuaibi	B-8538	NRC/ISSA/SKXS
SHUNICHIRO MITA		NMSS/DWM
John Lubinski		OCM/NJD
Tao M. Ahn		NMSS/DWM
J. S. Hyslop		NRC/SFSB
King Stablen	A6723	NRC/NMSS
Tom Hertz	B-8250	NRC/OCM
TAMARA BLOOME	B-8680	NRC/NMSS
John D. McCann		Maine Yankee
J. A. MURPHY	A6556	
S. D. Rubin	B-8420	NRC/RES
Brian O'Connell	<del>A66</del>	NARC
James Firth	B7707	NRC/NMSS
Charlotte Abrams	B6004	NRC/NMSS
Jeffrey Winkler		Jason Tech Corp.



ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

JOINT ACRS/ACNW SUBCOMMITTEE MEETING

JANUARY 13-14, 2000

Date(s)

JANUARY 13, 2000

Today's Date

ATTENDEES - PLEASE SIGN BELOW

PLEASE PRINT

NAME

AFFILIATION

TOM MURLEY

SELF

BOB BERNERO

SELF

Stan ECHOLS

WINSTON + STRAWN

Steve Hanauer

DOE

TOM COTTON

JKRA

Mike Scott

CRWMS M+O

John Russell

ENWRA

Jim York

Booz Allen & Hamilton

DAN FEHRINGER

NWTRB

Bob Christie

Performance Technology

Alex Marion

Nuclear Energy Institute

Rod McCollum

NEI

Dan Metlay

NWTRB

Carl Hunter

DOE

JACK BARKEY

TRW

Dr. McINTYRE

Worthington

Kate Mulligan

Booz Allen & Hamilton

DIANE D'ARRIGO

NIRS



ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

JOINT ACRS/ACNW SUBCOMMITTEE MEETING

JANUARY 13-14, 2000

Date(s)

JANUARY 14, 2000

Today's Date

ATTENDEES - PLEASE SIGN BELOW

PLEASE PRINT

NAME

AFFILIATION

Steve Hanauer

DOE

Mike Scott

CRWMS M+O

JIM YORK

Broz. Allen & Hamilton

BOB BERNERO

SELF

TOM COTTON

JKRA

Dan McHugh

NWTRB

Carol Hawley

DOE

List of handouts provided at the ACRS/ACNW Joint Subcommittee Meeting,  
January 13&14, 2000

1. Design Defense-In-Depth in a Risk-Based Regulatory System with Imperfect PRA or Beating a Dead Horse With a Red Herring, T. S. Kress
2. Draft Technical Note on the Quantification of Defense In Depth, January 13, 2000, B. John Garrick
3. Some Comments on Defense In Depth As a Safety Strategy, D. A. Powers
4. Thoughts on Defense In Depth, D. A. Powers
5. A Definition of Defense in Depth, G. Apostolakis, January 13, 2000
6. Defense-In-Depth for Yucca Mountain: Some Comments, Robert J. Budnitz, Future Resources Associates, Inc.
7. Memorandum to Dr. B. John Garrick and Dr. Thomas S. Kress, from J. N. Sorensen, dated January 5, 2000, regarding: Background Material for the Joint Subcommittee Meeting on the Defense in Depth Philosophy, January 13-14, 2000, Rockville Maryland
8. Defense In Depth Joint Subcommittee of ACRS/ACNW January 13-14, 2000, Robert M. Bernero
9. A presentation for the Joint ACRS/ACNW Subcommittee, January 13, 2000, Defense-In-Depth for Risk-Informed, Performance-Based Regulation: A Provisional NMSS Perspective, Norman A. Eisenberg
10. Presentation to the Joint ACRS/ACNW Subcommittee, January 13, 2000, regarding: Implementing the Multiple Barriers Requirement in a Geologic Repository for High-Level Waste: Current Thinking, Christiana H. Lui
11. Presentation to the Joint ACRS/ACNW Subcommittee, January 13, 2000, Defense-In-Depth: Perspective for Risk-Informing 10 CFR 50, T. L. King, RES, G. M. Holahan, NRR
12. ACRS/ACNW Meeting, January 13, 2000, Gary Vine, Sr. Washington Representative: Defense-in-Depth Application to ALWR
13. Defense in Depth and the AP600, January 13, 2000, Brian A. McIntyre, Manager, Advanced Plant Safety and Licensing, Westinghouse Electric Company
14. EPRI, Executive Summary, Advanced Light Water Reactor, Utility Requirements Document, issued 12/95
15. DID Issues Emphasizing The Yucca Mountain Repository, Ray Wymer, 1/14/2000
16. Notes on Defense In Depth, B. John Garrick, January 14, 2000.

ACRS/ACNW Joint Subcommittee meeting  
January 13-14, 2000

List of background documents

Tab 1. ACRS report dated June 17, 1997 from R. L. Seale, Chairman, ACRS to Shirley Ann Jackson, Chairman, NRC, Subject: Proposed Staff Position Regarding Inclusion of a Containment Spray System in the AP600 Design

Tab 2. Memorandum from J. N. Sorensen to ACRS Members, Subject: Historical Notes on Defense in Depth, October 15, 1997

Tab 3. PRA Policy Statement (8/16/95)

Tab 4. Advanced Nuclear Power Plant Policy Statement (7/12/94)

Tab 5. Safety Goal Policy Statement (8/4/86)

Tab 6. ACNW report dated October 31, 1997 from B. John Garrick, Chairman, ACNW to Shirley Ann Jackson, Chairman, NRC, Subject: Recommendations Regarding the Implementation of the Defens-in-Depth Concept in the Revised 10 CFR Part 60

Tab 7. Regulatory Guide 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, July 1998

Tab 8. SECY-98-225, Subject: Proposed Rule: 10 CFR Part 63 --- "Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada," September 28, 1998 (Only the SECY paper, the SRM governing its development (Attachment 1), and the portion of Attachment 2 which discusses defense in depth and performance assessment are included here. Attachment 2 in its entirety is about 160 pages.)

Tab 9. Memorandum from J. N. Sorensen to Andrew C. Campbell, Subject: Defense in Depth in the Geologic Repository, February 11, 1999

Tab 10. SECY-98-144, Subject: White Paper on Risk-Informed and Performance-Based Regulation, and its associated SRM, February 24, 1999

Tab 11. ACRS report dated May 19, 1999 from Dana A. Powers, Chairman, ACRS to Shirley Ann Jackson, Chairman, NRC, Subject: The Role of Defense in Depth in a Risk-Informed Regulatory System, and attached paper by J. N. Sorensen et al., "On the Role of Defense in Depth in Risk-Informed Regulation."

Tab 12. SECY-98-300, Subject: Options for Risk-Informed Revisions to 10 CFR Part 50 - "Domestic Licensing of Production and Utilization Facilities," December 23, 1998, and its associated SRM dated June 8, 1999

Tab 13. Letter from Robert J. Budnitz, Future Resources Associates, Inc., to B. John Garrick, Chairman, ACNW dated June 25, 1999 regarding the treatment of defense in depth in the proposed Part 63

Tab 14. SECY-99-186, Subject: Staff Plan for Clarifying How Defense-in-Depth Applies to the Regulation of a Possible Geologic Repository at Yucca Mountain, Nevada, July 16, 1999

Tab 15. SECY-99-191, Subject: Modifications to the Safety Goal Policy Statement, July 22, 1999, and associated SRM dated October 28, 1999

Tab 16. SECY-99-256. Subject: Rulemaking Plan for Risk-Informing Special Treatment Requirements, October 29, 1999 (without attachments)

Tab 17. ACRS report dated October 12, 1999 from Dana A. Powers, Chairman, ACRS, to Greta Joy Dicus, Chairman, NRC, Subject: Proposed Plans for Developing Risk-Informed Revisions to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities"

Tab 18. ACRS/ACNW report dated November 17, 1999 from Dana A. Powers, Chairman, ACRS, and B. John Garrick, Chairman, ACNW to Richard A. Meserve, Chairman, NRC, Subject: Implementing a Framework for Risk-Informed Regulation in the Office of Nuclear Material Safety and Safeguards

List of handouts provided at the ACRS/ACNW Joint Subcommittee Meeting,  
January 13&14, 2000

1. Design Defense-In-Depth in a Risk-Based Regulatory System with Imperfect PRA or Beating a Dead Horse With a Red Herring, T. S. Kress
2. Draft Technical Note on the Quantification of Defense In Depth, January 13, 2000, B. John Garrick
3. Some Comments on Defense In Depth As a Safety Strategy, D. A. Powers
4. Thoughts on Defense In Depth, D. A. Powers
5. A Definition of Defense in Depth, G. Apostolakis, January 13, 2000
6. Defense-In-Depth for Yucca Mountain: Some Comments, Robert J. Budnitz, Future Resources Associates, Inc.
7. Memorandum to Dr. B. John Garrick and Dr. Thomas S. Kress, from J. N. Sorensen, dated January 5, 2000, regarding: Background Material for the Joint Subcommittee Meeting on the Defense in Depth Philosophy, January 13-14, 2000, Rockville Maryland
8. Defense In Depth Joint Subcommittee of ACRS/ACNW January 13-14, 2000, Robert M. Bernero
9. A presentation for the Joint ACRS/ACNW Subcommittee, January 13, 2000, Defense-In-Depth for Risk-Informed, Performance-Based Regulation: A Provisional NMSS Perspective, Norman A. Eisenberg
10. Presentation to the Joint ACRS/ACNW Subcommittee, January 13, 2000, regarding: Implementing the Multiple Barriers Requirement in a Geologic Repository for High-Level Waste: Current Thinking, Christiana H. Lui
11. Presentation to the Joint ACRS/ACNW Subcommittee, January 13, 2000, Defense-In-Depth: Perspective for Risk-Informing 10 CFR 50, T. L. King, RES, G. M. Holahan, NRR
12. ACRS/ACNW Meeting, January 13, 2000, Gary Vine, Sr. Washington Representative: Defense-in-Depth Application to ALWR
13. Defense in Depth and the AP600, January 13, 2000, Brian A. McIntyre, Manager, Advanced Plant Safety and Licensing, Westinghouse Electric Company
14. EPRI, Executive Summary, Advanced Light Water Reactor, Utility Requirements Document, issued 12/95
15. DID Issues Emphasizing The Yucca Mountain Repository, Ray Wymer, 1/14/2000
16. Notes on Defense In Depth, B. John Garrick, January 14, 2000.

DESIGN DEFENSE-IN-DEPTH  
in a  
RISK-BASED REGULATORY SYSTEM  
with  
IMPERFECT PRA

or

*BEATING A DEAD HORSE WITH A RED HERRING*

T. S. Kress  
ACRS

Presented at  
ACRS/ACNW Joint Subcommittee Meeting  
on  
Defense-in-Depth  
January 13-14, 2000  
Washington DC

## CONCERNS

WE ALL CAN AGREE THAT DEFENSE-IN-DEPTH IS A DESIGN (AND OPERATIONAL) STRATEGY (PHILOSOPHY?) FOR DEALING WITH UNCERTAINTY IN RISK ASSESSMENT

BUT.....

1. THIS DOES NOT CONSTITUTE A PRECISE (DESIGN-TO) DEFINITION IN TERMS OF RISK ASSESSMENT

2. THERE DOESN'T CURRENTLY EXIST A DEFINITION OR CRITERIA THAT ALLOWS FOR PLACING LIMITS ON DID (how do we recognize it and how much is enough?).

***I SEE A MAJOR OBJECTIVE OF THIS MEETING TO BE TO ADDRESS THESE TWO CONCERNS.***

TODAY, I WOULD LIKE TO FOCUS ON *DESIGN* DEFENSE-IN-DEPTH (AS OPPOSED TO OPERATIONAL) AND GENERALIZE THE CONCEPT TO ANY HAZARDOUS ACTIVITY (NOT SPECIFIC TO NUCLEAR POWER GENERATION).

FOR ANY HAZARDOUS ACTIVITY, A DESIGN DEFENSE-IN-DEPTH PHILOSOPHY COULD CONSIST OF FOUR PRINCIPLES:

- |              |   |
|--------------|---|
| Prevention   | 1. PREVENT ACCIDENTS FROM STARTING<br>(INITIATION)  |
| Mitigation   | 2. STOP ACCIDENTS AT EARLY STAGES BEFORE THEY<br>PROGRESS TO UNACCEPTABLE CONSEQUENCES<br>(INTERVENTION)  |
|              | 3. PROVIDE FOR MITIGATING THE RELEASE OF THE<br>HAZARD VECTOR<br>(MITIGATION)                             |
| Prev. & Mit. | 4. PROVIDE SUFFICIENT INSTRUMENTATION TO DIAGNOSE<br>THE TYPE AND PROGRESS OF ANY ACCIDENT<br>(DIAGNOSIS) |



BASED ON THE FOUR PRINCIPLES, MY PREFERRED GENERALIZED AND RISK RELATED DEFINITION OF DEFENSE-IN-DEPTH IS:

***DESIGN DEFENSE-IN-DEPTH IS A STRATEGY OF PROVIDING DESIGN FEATURES TO ACHIEVE ACCEPTABLE RISK (IN VIEW OF THE UNCERTAINTIES) BY THE APPROPRIATE ALLOCATION OF THE RISK REDUCTION TO BOTH PREVENTION AND MITIGATION.***

HOW CAN THIS DEFINITION BE IMPLEMENTED TO PUT LIMITS ON DEFENSE-IN-DEPTH?

THE KEYWORDS ARE ..... "APPROPRIATE ALLOCATION"

- YOU MUST HAVE RISK ACCEPTANCE CRITERIA THAT YOU DESIRE TO ALLOCATE (PREFERABLE EXPRESSED IN TERMS OF CONFIDENCE LEVELS)
  - Quantifiable uncertainty should come out of the PRA
  - "Unquantifiable" uncertainty should be estimated by expert opinion
  - The acceptance criteria should include both uncertainties
  
- ALLOCATION IS A VALUE JUDGMENT .... WE NEED CRITERIA FOR HOW MUCH WE VALUE PREVENTION VERSUS MITIGATION
  - Could depend on the level of inherent hazard (the more hazardous the activity the more we should value prevention)
  - Could depend on the extent of uncertainty in the risk assessment
  - Could depend on how much of the uncertainty is unquantifiable
  - May want to minimize uncertainty (after all this is a classic optimization problem)
  - May be based on the "loss function" of decision theory

## **Draft Technical Note**

### **ON THE QUANTIFICATION OF DEFENSE IN DEPTH**

B. John Garrick  
January 13, 2000

#### **PURPOSE**

To propose a conceptual framework for quantifying the "defense-in-depth" aspects of the various levels of protection, provided in nuclear plants and nuclear waste repositories, against the release of radiation to the public and the environment.

#### **GENERAL FEATURES OF THE APPROACH**

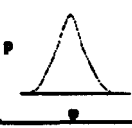



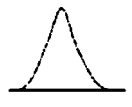
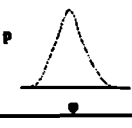

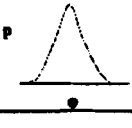
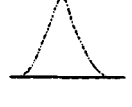
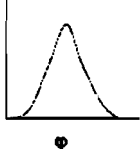
The question is how can we best use probabilistic risk (performance) assessment (PRA and PPA) results to quantify and make visible the performance of the various "defense-in-depth" systems designed to provide multiple "levels of protection" against the release of radiation. Part of the answer lies in the way that the results are presented.

The key to the proposed approach, therefore, is a presentation format that clearly displays 1) the role that the individual safety systems play in providing protection against the release of radiation to the environment and 2) the effect of the individual systems acting in concert. This format allows for important risk and performance comparisons to be made at both the functional and system levels of a nuclear plant or a nuclear repository. It helps us make the important judgments of whether we are getting our money's worth from these multiple levels of defense, and whether we need more or less.

The approach utilizes the results of PRA and PPA. The scope of the PRAs and PPAs must include quantifications of information and modeling uncertainties, in the parameters used to measure risk or safety performance, and explicit identification of the supporting evidence on which these quantifications are based. The PRAs and PPAs must be structured in such a way as to reveal the process of assembling the results into the final measures of risk or performance, and to reveal the contributions, to these final measures, of the various levels of protection.

#### **SPECIFIC FEATURES OF THE APPROACH**

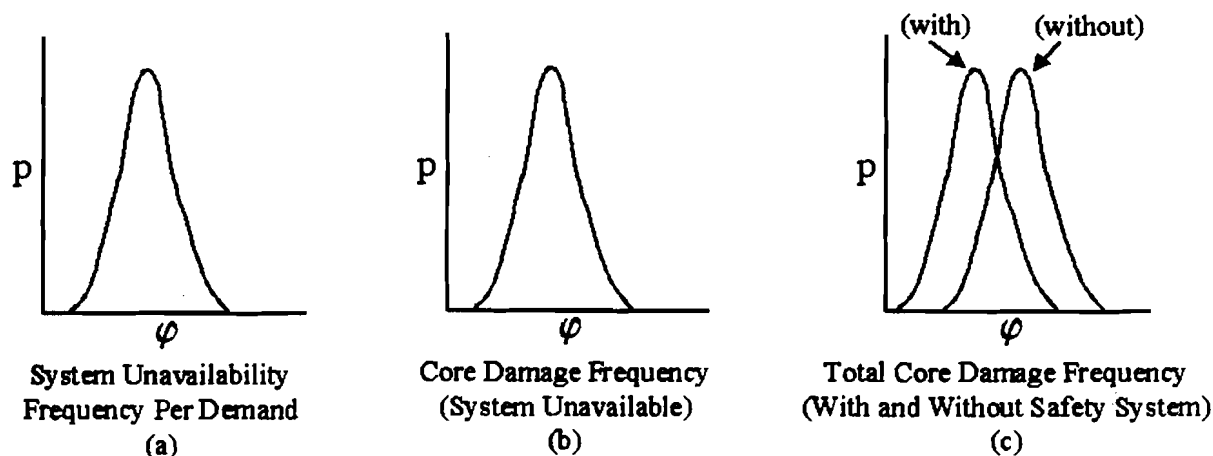
The answer to "how can we best use PRA and PPA results to quantify --- defense-in-depth ---" is believed effectively addressed using a two-dimensional structuring of risk and performance results. The structuring can be done in stages or phases in the spirit of a top-down approach. To illustrate the process at the functional level for reactors, consider Figure 1 with respect to the PRA of a boiling water reactor.

(1) Classes of Initiating Events	Safety Functions				(6) Core Damage Frequency
	(2) Reactivity Control	(3) Inventory Control	(4) Heat Removal	(5) Radionuclide Containment	
Low of Coolant 	1.  2.  3. 	Etc.			
Transients 					
External Events 					
Total Core Damage Frequency	 $\sum(\text{CDFs of Column 6})$				

**FIGURE 1. BWR SAFETY FUNCTIONS**

The rows of Figure 1 represent classes of initiating events at the functional level that can lead to core damage. In the first column (column 1) we plot probability curves showing our state of knowledge about the frequencies of the initiating events in the "probability of frequency" format. Columns 2—5 now represent the various safety functions that may respond to a particular class of initiating events. Column 6 contains the core damage frequencies for each class of initiating events. The sum of the Column 6 results represents the total core damage frequency, as illustrated in the last row.

The question is what entries should go in the boxes under the safety functions? The answer is to show the entries that best expose the defense-in-depth contributions of the safety functions. There are many possibilities. One possibility is to include three entries in each grid box, as shown in Figure 2.



**FIGURE 2. SYSTEM PERFORMANCE INDICATORS**

As discussed further below, Entry 1 (Figure 2a) could be a probability curve indicating the unavailability frequency per demand of the safety function, given the particular class of initiating events. Entry 2 (Figure 2b) could be the core damage frequency, given the unavailability of the safety function, and Entry 3 (Figure 2c) could compare this result with the total core damage frequency of the last row. Doing this for each of the grid boxes would provide a clear perspective of the amount of protection provided by each of the functions. Different combinations of safety function availability and unavailability could be presented through the use of additional columns for making performance comparisons. Such analyses and comparisons provide a process for quantifying the role of various levels of protection, and hence, a quantification of contribution to defense-in-depth provided by different levels of protection.

### **TURNING UP THE MICROSCOPE**

Now, the functional level shown in Figure 1 is too high a level to reveal performance characteristics of specific systems and barriers. To do that we need to turn up the microscope. Consider the grid box formed by the intersection of "Loss of Coolant" and "Inventory Control" of Figure 1. Suppose we detail that grid box into Figure 3.

Loss of Coolant Initiators	Safety Systems								Core Damage Frequency
	Vessel Level Makeup							Reactor Coolant System	
	Feedwater and Condensate	High-Pressure Core Spray	Reactor Core Isolation Cooling	Automatic Depressurization	Residual Heat Removal (Low-Pressure Coolant Injection)	Low-Pressure Core Spray	Flow Water		
Extreme LOCA	1. 2. 3.	Etc.							
Large LOCA									
Small LOCA									
Breaks Outside Containment									
Interacting System LOCA									
Other LOCAs									
Core Damage Frequency Due to Loss of Coolant IEs	$\phi = \sum (\text{CDFs of IE Categories})$								

**FIGURE 3. BWR SAFETY SYSTEMS**

Figure 3 divides the “Loss of Coolant” class of initiating events into six initiating event categories. It divides the “Inventory Control Systems” into eight more clearly defined protection systems. This level of detail is usually sufficient to provide quantitative engineering information on the levels of protection against exposing the public and the environment to radiation. The entries in the grid boxes can be the same as Figure 1 or modified as appropriate. In particular, Figure 2a indicates the unavailability of the safety system on demand, given the applicable initiating event. It reveals the reliability of the system under the conditions that the system is called on to operate and is the input used in the calculation of the core damage frequency for each specific category of initiating events. Figure 2b is the core damage frequency as a result of a particular category of initiating events, given the unavailability of the safety system (e.g., if that safety system were not present).

Figure 2c is a key result in the quantification of the defense-in-depth of safety system protection. It is the total core damage frequency with and without the specific safety system being analyzed. It is important to note that Figure 2c is a different CDF than the one on which Figure 2b is based. The Figure 2b CDFs are those of Column 6. The Figure 2c CDF is the probabilistic sum of the Column 6 CDFs.

## APPLICATION TO NUCLEAR WASTE REPOSITORIES

Defense-in-depth of a nuclear waste repository takes the form of passive barriers whose performance must be analyzed over tens and hundreds of thousands of years. A two-dimensional display similar to the above can be constructed to exhibit the contributions of the levels of defense associated with a repository design. The functional barriers protecting the biosphere from radioactive contamination are, as shown in Figure 4, the spatial and flow control of water, the waste package containment, and the control of the mobilization and transport of radionuclides. The effectiveness of these barriers must be analyzed under a set of "geological scenarios" representing the possible climatological and geological events that might occur over tens and hundreds of thousands of years of the repository history. In Figure 4 these scenarios are represented in rows 2, 3, and 4. Row 1 represents the "base case" or "expected" scenario.

The point of Figure 4 is to display the contribution of the individual functional barriers to preventing the release of radioactivity to the biosphere. For this purpose we take, as the repository performance measure, the peak annual release to the biosphere, measured in curies.

In Figure 4, the rightmost column shows our state of knowledge about the peak annual release to the biosphere under the four geological scenarios. In the individual boxes of Figure 4 we display a pair of curves of the type shown in Figure 5. The curves show the contributions of the individual protective barriers by showing how the peak annual release would increase if that barrier were not present.

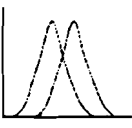
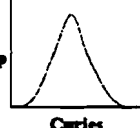
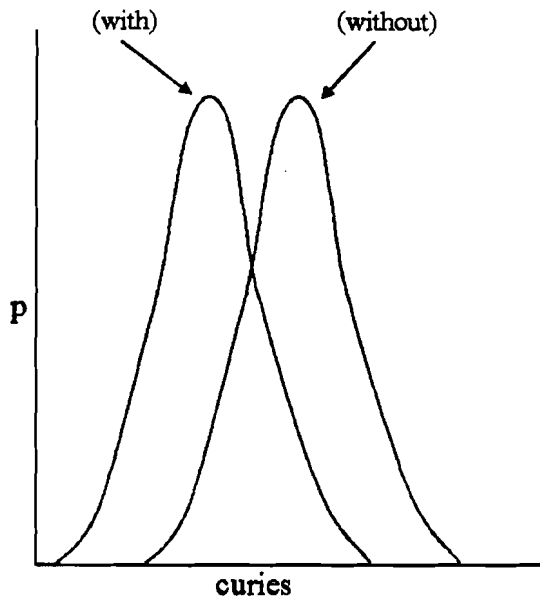
Initiating Conditions	Protective Barrier Functions			Peak Annual Release to the Biosphere (Curies)
	Water Flow and Spatial Control	Waste Package Containment	Radionuclide Mobility Control	
Current Climate		Etc.		
Geotechnical Events				
Wet Climate				
Increased Geotechnical Activity				

FIGURE 4. REPOSITORY PROTECTIVE BARRIER FUNCTIONS

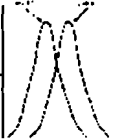
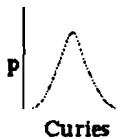


Peak Annual Release  
(With and Without Barrier)

**FIGURE 5. PERFORMANCE COMPARISON**

In Figure 6 we "turn up the microscope" on Figure 4 and recognize that the "barriers" shown in Figure 4 are actually composed of specific protective barriers. For example, the barrier "Water Flow and Spatial Control" of Figure 4 is now recognized as being composed of "Surface Runoff," which refers to a drainage system on the surface above the repository. Such a drainage system would divert the surface rainfall so as to prevent it from infiltrating into the ground above the repository. The column labeled "Water Diversion (Geotechnical)" refers to engineering the subsurface geology such as by the design of a Richards barrier. The column labeled "Water Diversion (Engineered Systems)" represents those engineered systems in the near field explicitly introduced to keep water from reaching the waste package. The rest of the columns are pretty much self-explanatory.



Initiating Conditions	Protective Barriers							Peak Annual Release to the Biosphere (Curies)
	Water Flow & Spatial Control Systems			Waste Package Containment		Radionuclide Mobility Control Systems		
	Surface Runoff	Water Diversion (Geotechnical)	Water Diversion (Engineered Systems)	Corrosion Resistance	Fuel Cladding	Chemical Additives	Solubility, Retardation, Dilution	
Current Climate		Etc.						
Geotechnical Events								
Wet Climate								
Increased Geotechnical Activity								

**FIGURE 6. PROTECTIVE BARRIERS**

The individual boxes of Figure 6 show the impact of the protective barriers on repository performance by displaying what the peak annual release would be if that protective barrier were not present.

# **SOME COMMENTS ON DEFENSE IN DEPTH AS A SAFETY STRATEGY**

D.A. Powers

Chairman  
Advisory Committee on Reactor Safeguards

I regret that I cannot be with you in the meeting of the Joint ACRS/ACNW Subcommittee. I do, however, want to share with you some of my thoughts on the subject of defense in depth as a safety strategy and, especially, as a safety strategy for materials licensees. Some of these thoughts are included in a paper coauthored with Jack Sorensen and other members of the ACRS.

Defense in depth is a safety strategy that has served the nuclear power industry well. Defense in depth is, however, a very expensive safety strategy. Because of the expense associated with defense in depth, even the nuclear reactor safety community that has been so well served by this strategy is wrestling with ways to limit the imposition of defense in depth. We ought, then, to think carefully before imposing such a safety strategy in other areas. At the very least, we need to think of how to limit the requirements for a defense-in-depth safety strategy. Two schools of thought have emerged within the nuclear reactor safety community on the limitation of defense in depth. One of these, the 'Structuralists' school of thought does not extrapolate to any other field of endeavor. The other school of thought, the 'Rationalist' school, can be extrapolated to other areas. The Rationalist school of thought would restrict application of the defense-in-depth safety philosophy to those areas where safety analysis capabilities (PRA in the reactor safety world) cannot be applied or areas where these safety analysis methods yield very uncertain results.

Though this Rationalist approach to the limitation of defense in depth has much merit within the reactor safety community where the PRA methods of safety analysis are being aggressively developed and applied, I question whether this approach "travels well" so it can be applied in areas that have different or less developed methods of safety analysis. But, mostly, I question the Rationalist's approach because I see defense in depth as a method for addressing the question of what happens if the analyses are wrong and potentially consequential accidents do occur. If this is, indeed, the purpose of defense in depth, then one ought not use the error-prone analysis methodologies to determine where defense in depth is needed. I am confident that paradoxes will arise if this method of self-identification is used.

I think one has to go back and understand why defense in depth was adopted as a safety strategy for nuclear power plants if one is to understand its applicability to other areas. Defense in depth sounds so good as a safety strategy. It just sounds strong and reassuring. I do not

discount, then, the importance of the good ring to the widespread acceptance of defense in depth as a strategy for nuclear power plants. One has still to ask why the reactor safety community felt that such a robust safety strategy was needed.

My reading of the history of the nation's nuclear power enterprise leads me to believe that defense in depth was created as a safety strategy because:

- there was limited experience dealing with large nuclear power reactors,
- there were no applicable industrial standards for the safe operation of nuclear power plants,
- there was a confidence that accidents at nuclear power plants were unlikely, but there were very serious uncertainties about the consequences of accidents should they occur,
- a severe accident at a nuclear power plant that could pose substantial consequences would be most difficult to interdict once it was underway, and
- there was a confidence that a nuclear accident that affected the public near any facility would lead to shutdown of all nuclear facilities.

Lack of experience was quite an important issue at the time. Even after years of operational experience with research reactors and nuclear materials production reactors, the technical community was still encountering new physical phenomena (Xenon instabilities were fresh in safety analysts' minds.). Uncertainties in the behavior of radionuclides under accident conditions are much mentioned in the literature of the time, and, indeed, even today we have only the most primitive of an understanding of how radionuclides will behave in reactor accidents. We have no codes, for instance, that will predict all of the behaviors of fission products observed during the Chernobyl accident. The Windscale accident certainly emphasized the difficulty of interdicting a severe accident once it was underway. The widespread belief in the inevitable progression of a severe accident in a nuclear power plant has not been completely overturned even by the experience of the Three Miles Island accident. But, I suspect that the most driving concern that led to development of the defense in depth was concern over the political fallout from an accident that affected the public.

Though one can debate which of the safety issues was most important for the development of defense in depth, I believe that the existence of all five of the conditions listed above was necessary to the widespread acceptance of defense in depth within the reactor safety community. It is apparent, however, that maintenance of this safety strategy does not require that all five conditions still exist. Still, as any one of the conditions is mitigated (for instance as one gains experience in the operation of nuclear power plants) one becomes more willing to chip away at the defense-in-depth structure.

I do not believe that the five conditions that led to the imposition of defense in depth on the nuclear power industry exist in any of the four categories of licensees regulated by NMSS. As has been noted in the discussions of the Joint Subcommittee, many of the licensees have a great deal of operational experience. Many of the applications have the potential to produce only modest consequences even if bounding accident events occur. Even in the case of nuclear waste repositories where very severe accidents can be envisaged, these accidents will develop quite slowly and there will be opportunities to interdict. In none of the licensee activities will an accident result in the general shutdown of an entire industry even if the accident affects the public.

Were I with you at the meeting, I would argue vigorously against the imposition of defense in depth concepts on the material licensees. I don't think such a costly safety strategy is at all needed to achieve very high levels of safety. For most material licensees a standards-based safety strategy akin to the ASME boiler and pressure vessel safety code, but based, perhaps, on results of risk analysis ought to be adequate. Even in the case of a large, geologic repository for spent fuel, a safety strategy based on conservative engineering analyses guided by risk analyses ought to be satisfactory. In this regard, I hasten to add that I am not a 'fan' of design basis accidents for safety analyses, but this is a subject for some future meeting.

If defense in depth is imposed on material licensees, one immediately encounters the problem of rationally limiting the defense in depth. That is, if defense in depth is a strategy to address the possibility that analyses are wrong, there is in principle no end to the number of independent layers of increasing conservatism that can be applied to an activity. A rational basis not based on an arbitrary judgement is difficult to define. Within the reactor safety community the limitations on defense in depth were done arbitrarily. Now there is an ongoing effort to further limit defense in depth. The analysis capability to follow the Rationalists' approach to the limitation of defense in depth does not exist for many of the licensees. I do not see within the affected safety community an enthusiasm to marshal the wherewithal that would be necessary to develop a suitable analysis capability.

# **THOUGHTS ON DEFENSE IN DEPTH**

**D.A. Powers**

**January, 2000**

# **A Definition of Defense in Depth**

**G. Apostolakis, January 13, 2000**

**Defense in depth is a safety philosophy that requires that a set of provisions be taken to manage unquantified uncertainty associated with the performance of engineered systems.**

## **Observations:**

- **"Defense in depth" and "multiple barriers" are not identical concepts. For quantified uncertainties, "multiple barriers" are standard engineering tools.**
- **"Multiple barriers" will always be used regardless of whether defense in depth is a principle or not.**
- **"Unquantified uncertainty" is primarily due to model inadequacy.**
- **The focus on unquantified uncertainty will force an examination of the quality of the analyses and will suggest improvements.**

- **Crucial question: Under what conditions, if any, is defense in depth a *principle*?**
- **Calling defense in depth a *principle* makes it impervious to analysis.**
- **"I am much more comfortable with defense in depth as a means to address the question of what if we are wrong in our analyses. You can argue that this is just a kind of uncertainty, but I think that argument trivializes the problem or implies that we know more than we do." (D. Powers)**
- **This is what is wrong with declaring defense in depth a *principle*. Regardless of the quality of the analysis, a Damoklean sword<sup>1</sup> will always hang over my head. Why should I even try to improve my analysis? (GA)**

---

<sup>1</sup>Damokles: A courtier of ancient Syracuse held to have been seated at a banquet beneath a sword hung by a single hair.

**DEFENSE-IN-DEPTH for YUCCA MOUNTAIN:**

**SOME COMMENTS**

**ROBERT J. BUDNITZ**

**Future Resources Associates, Inc.**

**2039 Shattuck Avenue, Suite 402**

**Berkeley, California 94704 USA**

**Tel: (510) 644-2700**

**e-mail: BUDNITZ @ PACBELL.NET**

**ACRS-ACNW JOINT SUBCOMMITTEE MEETING**

**ON DEFENSE-IN-DEPTH**

**JANUARY 13 - 14, 2000**



## **A DILEMMA**

**"The Commission does not intend to specify numerical goals for the performance of individual barriers." [page 8649, third column]**

**"In implementing this [defense-in-depth] approach, the Commission proposes to incorporate flexibility into its regulations by requiring DOE to demonstrate that the geologic repository comprises multiple barriers, but ....."**

**BUT**

**"... but not prescribe which barriers are important to waste isolation or the methods to describe their capability to isolate waste." [page 8650, first column]**

**[from "Supplementary Information" to Draft Part 63, Section VIII]**

**SECTION VIII near the end, page 8650**

**"The proposed requirements will provide for a system of multiple barriers ..... to ensure defense in depth and increase confidence that the postclosure performance objective will be achieved."**

## **QUESTION ONE:**

**Will NRC use defense-in-depth as a decision criterion?**

**or, more directly,**

**Can DOE's license application "flunk" based on insufficient defense-in-depth, even if it would otherwise "pass"?**

**[The answer to this Question is apparently "yes".]**

## **QUESTION TWO:**

**If so, how? How will the decision be framed and made?**

**Observation: The decision criteria need to be clear, fair, and technically logical.**

### QUESTION THREE

**Perhaps, in practice – and despite NRC's words to the contrary --  
- DOE will never actually be found to "flunk", but defense-in-  
depth will be used by NRC instead more like ALARA: "Do what  
you can, beyond meeting the bare regulations, whenever it's  
cost-effective".**

**How does NRC conceive that this would work in practice? Might  
NRC ask for more protection from one or another barrier in the  
name of defense-in-depth, even if the overall performance  
"passes"?**

**What if one barrier provides "90% of the total protection?"  
Maybe DOE would "weaken" that barrier so that it would only  
provide 40%; if the entire repository still "passes", is this  
desirable?**

**[I am sorry to be sarcastic here – it is obviously undesirable. But  
this is related to a complaint that I've heard along the lines of  
"DOE's protection almost all comes from the canister; DOE is  
engineering their way around a poor site."]**

## **ISSUES**

- (1) If NRC lets DOE decide what "under-performance" means, what is to prevent the terrible problem known as "Bring me a rock --- sorry, wrong rock" ?**
  
- (2) DOE will presumably not assume so much "under-performance" that the repository's overall ability to contain the waste is seriously compromised. But in fact, isn't that just what NRC's concern is, to look for combinations of "under-performance" that might lead to serious compromises?**
  
- (3) So perhaps NRC needs to tell DOE how much "under-performance" to assume. Yet this leads to its own problems --- namely, NRC is trying not to be overly prescriptive!**

**ONE BASIC ISSUE: These are "sensitivity studies" that are always a good idea anyway. Why invoke them in the name of a philosophical notion like "defense-in-depth" that brings with it so much other baggage?**

MEMORANDUM

TO: Dr. B. John Garrick, Co-Chairman  
Dr. Thomas S. Kress, Co-Chairman  
ACRS/ACNW Joint Subcommittee

From: J. N. Sorensen *JNS*

Subject: Background Material for the Joint Subcommittee Meeting  
on the Defense in Depth Philosophy, January 13-14,  
2000, Rockville, Maryland

Date: January 5, 2000

Attached is a letter from Tom Murley to John Larkins discussing the defense in depth safety philosophy. Attached to the letter is a copy of "Director's Findings Regarding Shoreham Emergency Preparedness." Dr. Murley suggests that the formulation of defense in depth in that document may be useful in preparing for the January 13-14 meeting.

Attachment: As stated.

c: G. Apostolakis  
R. Bernero  
R. Budnitz  
L. Deering  
J. Larkins  
H. Larson  
M. Levenson  
R. Major  
M. Markley  
T. Murley  
R. Wymer

In summary, the following conclusions have been reached:

1. The Shoreham site compares favorably with other nuclear plant sites in the U.S. There are no unique features of the site that render emergency planning at Shoreham fundamentally more difficult than for other nuclear sites.
2. The Shoreham offsite emergency plan as implemented by LERO results in a response capability that is equivalent to or better than the response capability for many other sites in the U.S.
3. Because of the thoroughness of the LERO plan and the demonstrated ability of LERO to rapidly mobilize well trained personnel, effective emergency response actions can and will be taken in conjunction with the best efforts of State and County emergency response organizations.
4. The LERO plan has been found by FEMA to be adequate based on a thorough review of the plan as well as an evaluation of a full-participation exercise at Shoreham on June 7-9, 1988.
5. Each of the outstanding emergency planning contentions has been satisfactorily resolved.

It is concluded, therefore, that there is reasonable assurance that adequate protective actions can and will be taken in the event of a radiological emergency at Shoreham.

**DEFENSE IN DEPTH**

-----

**JOINT SUBCOMMITTEE OF  
ACRS AND ACNW**

-----

**JANUARY 13-14, 2000**

-----

**ROBERT M. BERNERO**



## **QUESTIONS TO BE ADDRESSED**

---

- 1. What is defense in depth?**
- 2. Is there an overarching philosophy of defense in depth?**
- 3. Are current safety goals and objectives clear for general use?**
- 4. What is the role of defense in depth in risk-informed regulation of nuclear reactors?**
- 5. What is the role for defense in depth in risk-informed regulation of radioactive material processes and uses?**
- 6. What is the role for defense in depth in risk-informed regulation of radioactive waste disposal?**

## WHAT IS DEFENSE IN DEPTH?

---

- **“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.”**
- **Defense in depth is not a formula for adequate protection; it is a part of the safety philosophy, a strategy for safety analysis.**

## **IS THERE AN OVERARCHING PHILOSOPHY OF DID?**

---

- **Yes, as a strategy of safety analysis.**
- **Defense in depth: Prevent undue reliance on any single:**
  - **rarity of occurrence**
  - **design feature**
  - **barrier**
  - **performance model**
- **Not a formula for acceptability, defense in depth may not be enough defense.**
- **Risk-informed: Achieve a sufficient margin of safety, neither too close nor too far from the unacceptable.**

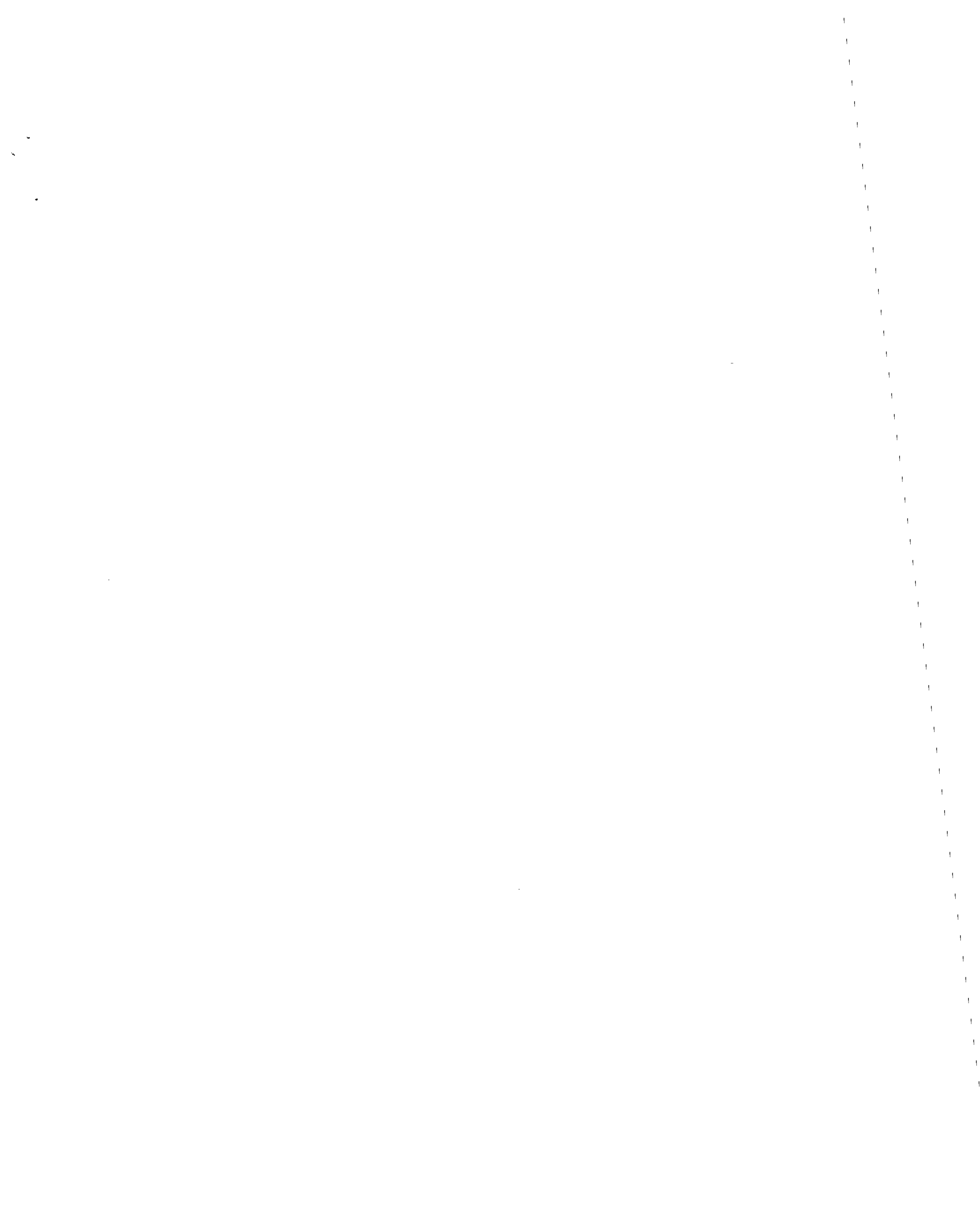
## **ARE CURRENT SAFETY GOALS AND OBJECTIVES CLEAR?**

---

- **No, not for general use.**
- **The span of protection**
  - **Public safety**
  - **Worker safety**
  - **Patient safety**
  - **Environmental protection**
- **Range of authorized practices**
  - **Reactors**
  - **Fuel cycle facilities**
  - **Industrial and medical uses**
  - **Exempt distribution**
  - **Transportation**

## **WHAT IS THE ROLE OF DID IN REGULATION OF REACTORS?**

- **Does not apply to routine releases.**
- **Basis for evaluating areas of heavy reliance in accident analysis, e.g.:**
  - **Seismic safety**
  - **RPV rupture**
  - **SG tube rupture**
  - **Human action**
- **Graded defense with graded goals.**



## **WHAT IS THE ROLE OF DID IN REGULATION OF MATERIALS?**

- **May sometimes apply to routine releases, e.g., exempt products.**
- **Need graded goals for graded defenses.**
- **Think it through:**
  - **Potential consequences**
  - **Potential barriers**
  - **Potential actions**
  - **Balanced choice of defense**
- **Knotty problems, e.g., patient safety and medical QA**

## **WHAT IS THE ROLE OF DID IN REGULATION OF WASTE?**

---

- **Definitely applies to release barriers.**
- **One fundamental basis of acceptability is the TSPA, with proper uncertainty analysis.**
- **Apparent confusion since DID analysis is a form of uncertainty analysis.**
- **Part 63 proposal is a sound approach to DID, develop the body of information for the exercise of judgement.**
- **Need graded goals for graded uncertainties: clearly acceptable, acceptable, clearly tolerable, tolerable, life-threatening, unacceptable.**



<b>10 Sv (1000 Rem)</b>	<b>Certain death</b>
<b>1 Sv (100 Rem)</b>	Floor for exposure threatening prompt death, Clearly predictable proportion to threat of induced cancer, Clinically detectable effects of radiation exposure, Exposure limit for rescue workers in nuclear war or emergency.
<b>0.1 Sv (10 Rem)</b>	Floor for clearly predictable proportion to threat of induced cancer (based on bomb survivor data), Typical standard for limit of public individual accident exposure.
<b>0.01 Sv (1 Rem)</b>	Clearly acceptable annual exposure limit for radiation workers, Tolerable level of public exposure in recognized situations which are difficult to change, e.g., radon in the home, high natural background radiation, Average total background radiation is below this level, dominated by radon exposure which varies considerably.
<b>1 mSv ( 100 mrem)</b>	Clearly acceptable annual exposure to a member of the public from all permitted sources, Typical background radiation from terrestrial and cosmic ray sources, Additional cosmic ray exposure suffered by frequent flyers.
<b>0.1 mSv (10 mrem)</b>	Typical proposed limit for exposure of the public from waste releases or a single permitted source, Too small to be discerned as a change in background radiation.
<b>0.01 mSv (1 mrem)</b>	Negligible individual exposure.

A Presentation for the Joint ACRS/ACNW Subcommittee  
January 13, 2000

**DEFENSE-IN-DEPTH FOR RISK-INFORMED,  
PERFORMANCE-BASED REGULATION:  
A PROVISIONAL NMSS PERSPECTIVE**

Norman A. Eisenberg

(301) 415-7285  
nae@nrc.gov

Senior Advisor for Performance Assessment  
Division of Waste Management  
Office of Nuclear Material Safety and Safeguards

# OUTLINE

1. NMSS Motivations for Defense-in-Depth (DID)
2. What is DID?
3. How does DID differ from margin and other safety concepts?
4. Provisional conclusions
5. Residual issues
6. Summary

# **NMSS MOTIVATIONS FOR DEFENSE-IN-DEPTH**

- Risk-informing NMSS activities will include reexamination of regulatory approaches, including defense-in-depth (DID)
- Proposed Part 63 addresses DID with multiple barriers provision; many public comments on this subject
- Risk-informing regulation of interim spent fuel storage facilities
- ISA's for Fuel Cycle Facilities
- Risk-informing transportation regulations

# REGULATORY ENVIRONMENT IN NMSS

- Wide range of licensees and systems regulated
  - Diverse systems
    - Complexity
    - Human interaction versus engineered aspects
    - Levels of hazard
  - Diverse capabilities for analysis among licensees
  - Diverse need/benefit/cost for risk-informing regulations
  
- Risk Considerations
  - individual risk to workers and public
  - normal and accident risk
  - perceived risk and actual risk
  - variety of initiators
    - mechanical failures
    - external events
    - human error

# **PRINCIPAL FACTORS OF DID IN NMSS: CURRENT STATUS**

- Nature of licensees and activities regulated
- NMSS regulates systems with less hazard than nuclear power reactors
- NMSS regulations are a mix of performance-based and/or risk-informed and prescriptive, deterministic approach
- For some NMSS licensed activities, the hazard does not warrant very strong preventive measures of any type, performance-based or prescriptive

# NMSS SAFETY PHILOSOPHY

- Goal is reasonable assurance of protecting:
  - Public health and safety
  - Common defense and security
  - The environment
  
- Safety Concepts assist in achieving DID include:
  - Safety Margin
  - Diversity
  - Redundancy
  - No single point of failure
  - QA
  
- DID is a component of risk management

# **DEFINITION OF DEFENSE-IN-DEPTH**

**(FROM THE COMMISSION WHITE PAPER ON  
RISK-INFORMED PERFORMANCE-BASED REGULATION)**

- **Safety is not wholly dependent on any single element of the system**
- **Incorporation of DID produces a facility with greater tolerance of failures and external challenges**



# STRUCTURALIST AND RATIONALIST APPROACHES TO DID

- STRUCTURALIST APPROACH:
  - The need for and extent of DID is related to the system structure
  - Many manifestations are based on knowledge and perspectives current when the systems were first developed or licensed
  - Some manifestations have an ad hoc basis
- RATIONALIST APPROACH:
  - The need for and extent of DID is related to the residual uncertainties in the system
  - The rationalist approach is just beginning to be applied in a risk-informed, performance-based regulatory environment

# TYPES OF UNCERTAINTY IN SAFETY ASSESSMENTS

- **Parameter**
- **Model**
- **Scenario (including exposure scenario)**
- **Programmatic Factors (e.g., QA)**

# **TYPES OF RESIDUAL UNCERTAINTY**

## **TYPE 1. (BEST AVAILABLE RISK ASSESSMENT)**

A system for which a fairly complete risk analysis or safety analysis has been performed, so residual uncertainty relates to the confidence or lack of confidence in the analysis; i.e., the analysis does not represent all uncertainty, because the state of knowledge is incomplete.

## **TYPE 2. (LIMITED RISK ASSESSMENT)**

A system for which the risk or safety analysis is somehow limited, e.g. by not being complete, or not quantifying certain types of uncertainty.

# **TYPE 1 LIMITATIONS OF RISK ANALYSES**

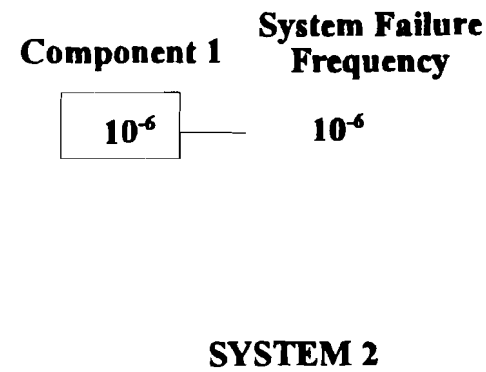
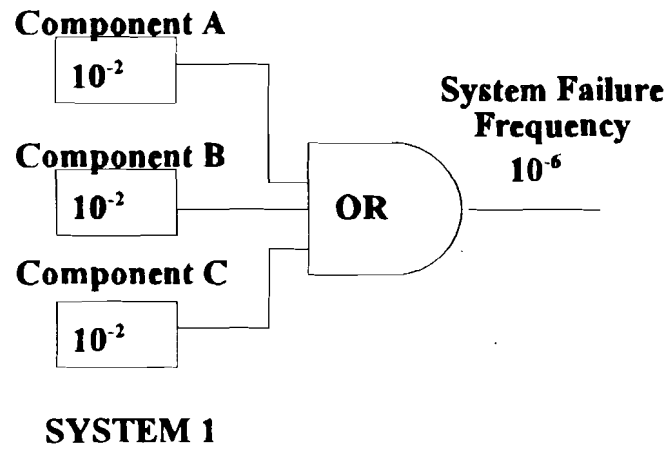
- Risk Assessments are incomplete
  - Not all failure modes are included, because failure modes, not known now, are a threat to system performance
  - Currently unknown or unrecognized phenomena are not included in consequence models
- The range of variability in system parameters has been underestimated or biased
- Probabilities and consequences for rare events are based on sparse or non-existent data
- Models used to estimate consequences and probabilities in some cases cannot be validated
- Although systematic analyses can give great insights into the performance of new systems, some problems only come to light with experience
- The state of knowledge is evolving

# **TYPE 2 LIMITATIONS OF RISK ANALYSES**

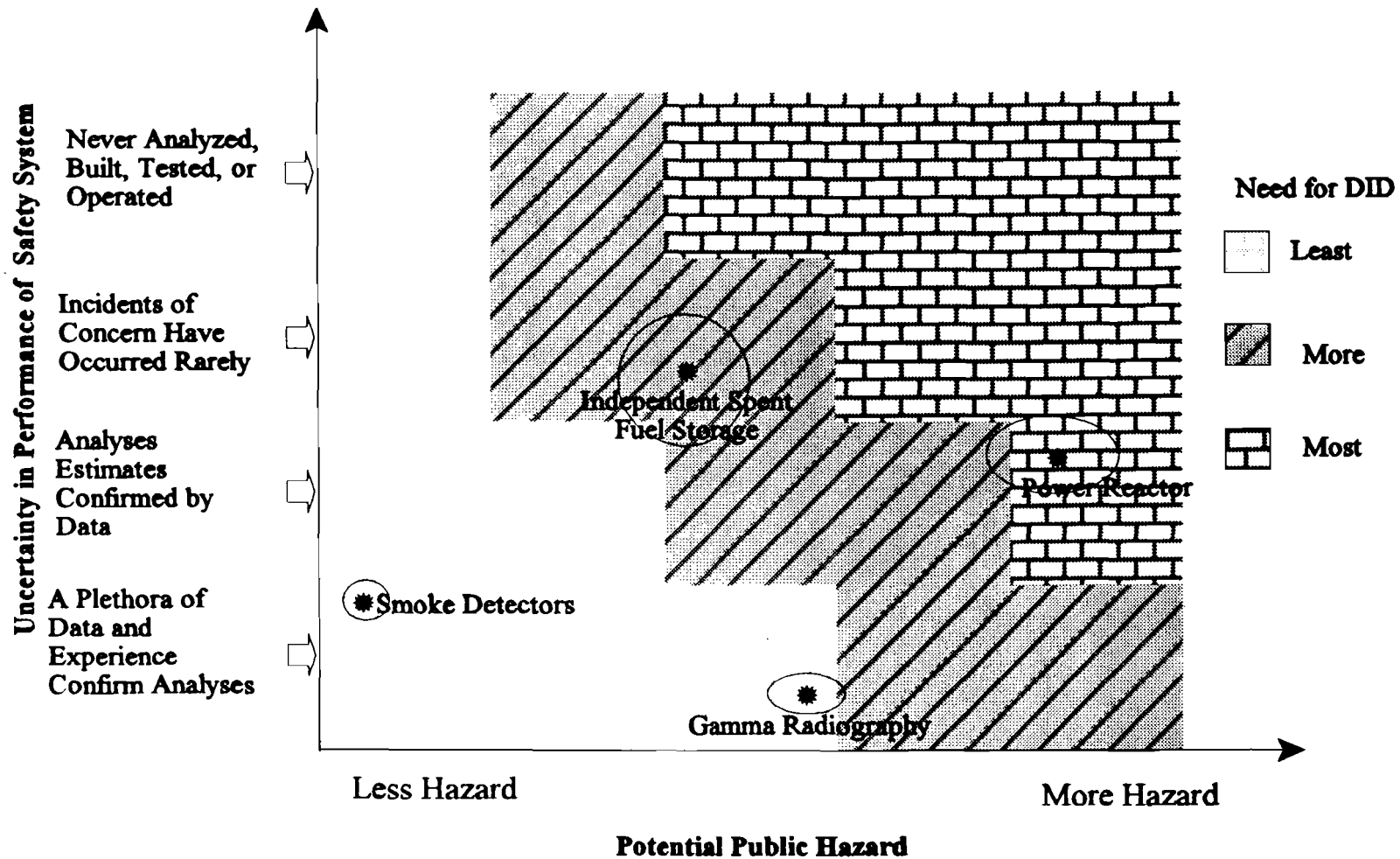
- **Risk Assessments are incomplete**
  - **Not all failure modes are included**
    - **Because of limitations on time and resources**
    - **Because procedures to enumerate all failure modes were misapplied and some failure modes were left out**
  - **Phenomena are not included in consequence models, because they are incorrectly considered unimportant or for reasons of economy**
- **Only certain kinds of uncertainty are explicitly represented in the risk assessment**
  - **Parameter uncertainty may or may not be propagated in consequence models**
  - **Model uncertainty may or may not be represented**
  - **Probabilities of various scenarios and uncertainty in the probabilities may or may not be represented**
  - **Not all quantifiable uncertainty may be quantified**
- **Models used to estimate consequences and probabilities have not been validated.**

# DIFFERENCES BETWEEN DID AND MARGIN

- Margin relates to the “cushion” between required performance and anticipated or predicted performance.
- DID relates to the characteristic of the system to: (1) not rely on any single element of the system and (2) be more robust to challenges
- Margin describes expected performance of a system versus the safety limit; DID describes the ability of the system to compensate for unanticipated performance, which results from limitations on knowledge.
- Increasing margin in a system that relies on a single component, does not necessarily increase DID.
- DID provides that if any component under-performs, the rest of the system compensates, so consequences are not unacceptable.



**Two different systems, both meeting the system risk goal of  $10^{-4}$ , but exhibiting different DID characteristics.**



Example of how need for defense-in-depth can be related to: (1) the uncertainty in the performance of the safety system and (2) the potential hazard posed by the system. Note: the positions of the various systems involves uncertainty on both axes.



# PROVISIONAL CONCLUSIONS ABOUT DID

1. DID is related to, but different from, other safety concepts such as safety margin, redundancy, and diversity.
2. DID is not necessarily equivalent to meeting a safety goal or the margin associated with meeting the goal.
3. DID can be implemented in a risk-informed, performance-based regulatory context as a system requirement, rather than as a set of subsystem requirements.
4. DID can be used to address residual uncertainties concerning the performance of a safety system.
5. The need for DID depends on:
  - a. Degree of residual uncertainty
  - b. Degree of hazard

# **PARTIAL LIST OF ISSUES TO BE RESOLVED**

- How to measure the degree of DID?
- How to measure the degree of uncertainty in performance of the safety system, encompassing quantified and unquantified uncertainty?
- How to measure the degree of potential hazard posed by a system?
- How to implement DID when the degree of uncertainty about different system components is not uniform?
- How to use current state of knowledge to make reasonable tests for a system to have sufficient DID, which allows for incomplete knowledge?
- How to explain to stakeholders the flexibility inherent in a risk-informed, performance-based approach to DID, which also provides reasonable assurance of safety?

# SUMMARY

- NMSS intends to consider implementation of DID in the context of risk-informed, performance-based regulation.
  - In ongoing regulatory activities
  - As part of the evolving risk-informed framework for NMSS
- As a general safety principle, the degree of DID needed to assure safety depends on several factors including:
  - Degree of residual uncertainty
  - Degree of hazard
- NMSS plans to implement DID as a system requirement, where feasible, rather than by prescriptive, subsystem requirements.
- NMSS needs flexibility in any overall approach in implementing DID to permit appropriate regulation for the range of systems regulated

# BACKUP SLIDES

# **COMMISSION WHITE PAPER ON RISK-INFORMED PERFORMANCE-BASED REGULATION**

“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.”

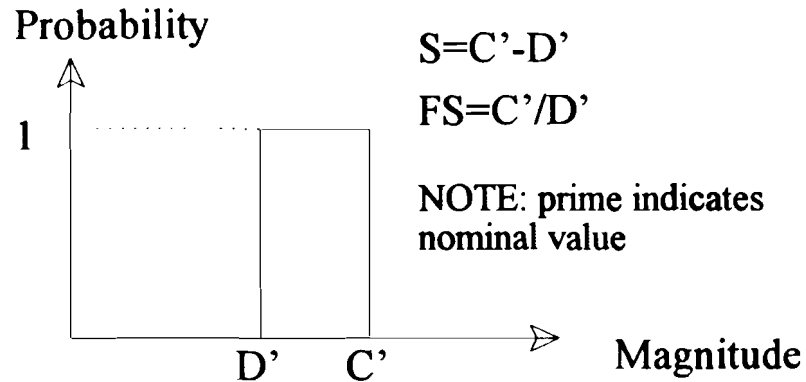


Figure (a) Deterministic System

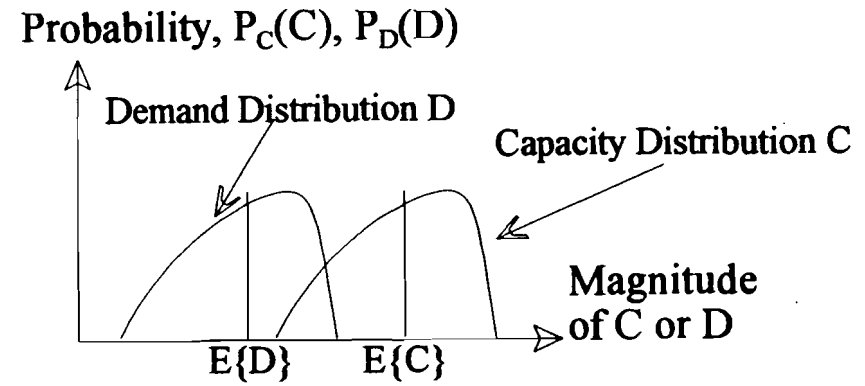


Figure (b) Capacity-Demand Model

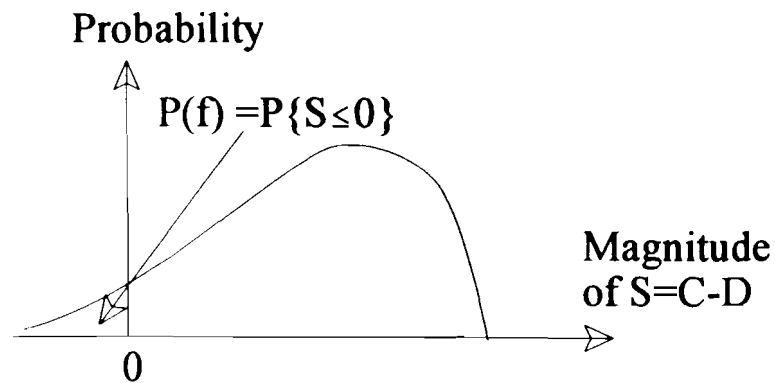


Figure (c) Safety Margin as a random variable.

D = Demand

C = Capacity

$S = C - D =$  Safety Margin

$FS = C/D =$  Factor of Safety

$CFS = E\{C\}/E\{D\} =$  Central Factor of Safety

## THE CONCEPT OF MARGIN IN A PROBABILISTIC CONTEXT

# Implementing the Multiple Barriers Requirement in a Geologic Repository for High-Level Waste: Current Thinking



Presentation to the Joint ACRS/ACNW Subcommittee  
January 13, 2000

Christiana H. Lui  
Division of Waste Management/NMSS  
(301)415-6200/CXL@NRC.GOV



# Introduction

- ◆ Extended public comment period on the proposed 10 CFR Part 63 ended on June 30, 1999; final rule to the Commission by March 31, 2000
- ◆ Work in progress
  - Objective is to share staff's best current thinking in clarifying the multiple barriers provision for postclosure safety evaluation
  - Defense in depth in preclosure safety evaluation is implemented through accident prevention, mitigation and intervention (e.g., emergency planning)





# Intent Of Multiple Barriers

- ◆ Consistent with NRC's safety philosophy as stated in *Commission's White Paper on Risk-Informed and Performance-Based Regulation*
- ◆ Implemented as an assurance requirement in Part 63 to provide confidence that
  - ✓ Known uncertainties are appropriately captured in the compliance demonstration calculations
  - ✓ The repository system is sufficiently robust to account for imperfect knowledge



# Consideration of Multiple Barriers Requirements in Part 63

- ◆ Assess all significant negative impacts on safety in the compliance demonstration calculations
- ◆ Identify all barriers in the above analysis
- ◆ Describe and quantify capabilities of the barriers
- ◆ Perform additional analyses to show **safety does not wholly dependent on any single barrier**
- ◆ Provide technical basis



# Demonstration of Multiple Barriers

- ◆ Show balance of the repository system has the ability to compensate for an under-performing barrier so public health and safety are protected



# Technical Issues For Multiple Barriers Analysis

- ◆ What should be the degree of barrier under-performance?
  - Performance-based
  - Prescriptive
- ◆ How should NRC evaluate the outcome of barrier under-performance analysis?



# Demonstration of Multiple Barriers - Staff's Best Current Thinking

- ◆ Uses individual dose to evaluate the outcome of barrier under-performance analysis
- ◆ DOE quantifies the amount of under-performance for each barrier that can be compensated by the balance of the repository system to illustrate the extent of system resilience



# Summary

- ◆ Multiple barrier is a system requirement for licensing a potential high-level waste repository at Yucca Mountain
- ◆ NRC will determine whether DOE has shown that the repository meets applicable regulations
  - ✓ Both geologic and engineered barriers contribute to safety
  - ✓ The repository system has the ability to compensate for under-performance of any one barrier
  - ✓ Not seeking complete redundancy



## Summary (Continued)

- ◆ Extended public comment period on the proposed 10 CFR Part 63 ended on June 30, 1999; final rule to the Commission by March 31, 2000
  - Staff consideration of the public comments is well underway
  - Information received during this meeting will be available to the staff in preparing responses to the public comments, drafting the final rule and developing guidance in the Yucca Mountain Review Plan
  - Transcript of this meeting will be made available to the public on the rulemaking website



DEFENSE-IN-DEPTH: PERSPECTIVE FOR

RISK-INFORMING 10 CFR 50

presentation to

JOINT ACNW/ACRS SUBCOMMITTEE

T. L. King, RES

G. M. Holahan, NRR

January 13, 2000



## BACKGROUND

- No formal regulation or agency policy statement on DID
- Commission White Paper on Risk-Informed Regulation (March 11, 1999):  
“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.”
- This philosophy is implemented in a number of ways depending on the specific program.

REACTOR PROGRAM  
DEFENSE-IN-DEPTH

- Included in Reactor Regulation (e.g., GDC, SRP ... )
- Included in Licensing and License Amendment Process
- Included in Reactor Oversight Process

## APPLICATION OF DID IN REACTOR REGULATION

- Current Part 50 requirements include DID considerations:
  - prevention and mitigation
  - single failure criterion
  - redundancy/diversity
  - barriers to FP release (cladding, RCS, containment)
  - EP
  - quality of design and operation
  
- Application of DID varies:
  - AOOs - DID in response to initiating events
    - DID preserves barrier integrity
  - DBAs - DID in response to and mitigation of initiating events
    - DID preserves mitigation
  - Severe Accidents - DID in mitigation

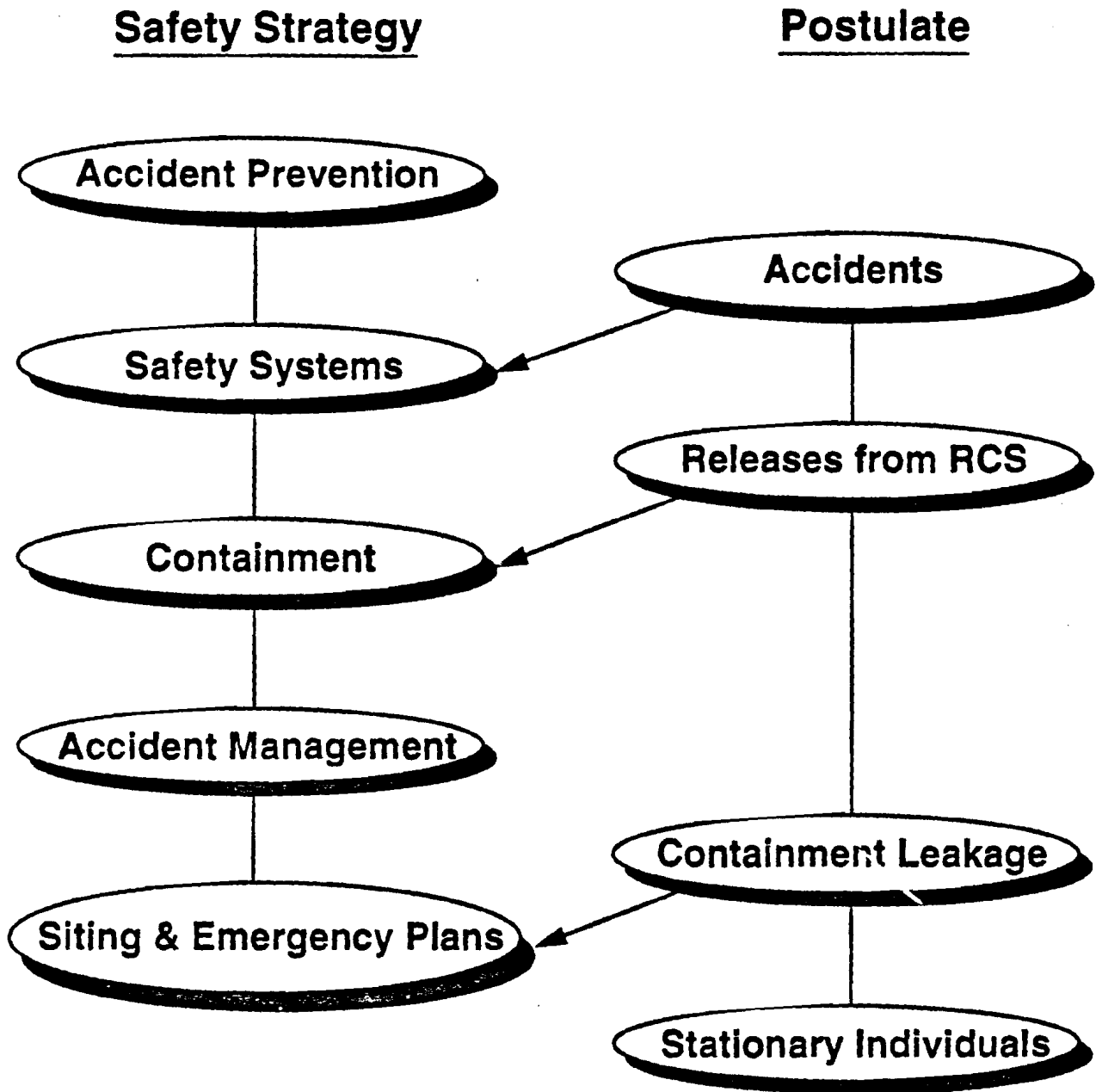


Figure 1.1-1 Defense in depth, safety strategies

**TABLE 1.1-1  
DEFENSE IN DEPTH  
MULTILAYER PROTECTION FROM FISSION PRODUCTS**

<b>Barrier or Layer</b>	<b>Function</b>
1. Ceramic fuel pellets	Only a fraction of the gaseous and volatile fission products is released from the pellets.
2. Metal cladding	The cladding tubes contain the fission products released from the pellets. During the life of the fuel, less than 0.5 percent of the tubes may develop pinhole sized leaks through which some fission products escape.
3. Reactor vessel and piping	The 8- to 10-inch (20- to 25-cm) thick steel vessel and 3- to 4-inch (7.6- to 10.2-cm) thick steel piping contain the reactor cooling water. A portion of the circulating water is continuously passed through filters to keep the radioactivity low.
4. Containment	The nuclear steam supply system is enclosed in a containment building strong enough to withstand the rupture of any pipe in the reactor coolant system.
5. Exclusion area	A designated area around each plant separates the plant from the public. Entrance is restricted.
6. Low population zone, evacuation plan	Residents in the low population zone are protected by emergency evacuation plans.
7. Population center distance	Plants are located at a distance from population centers.

REACTOR PROGRAM  
DEFENSE-IN-DEPTH

General Design Criteria

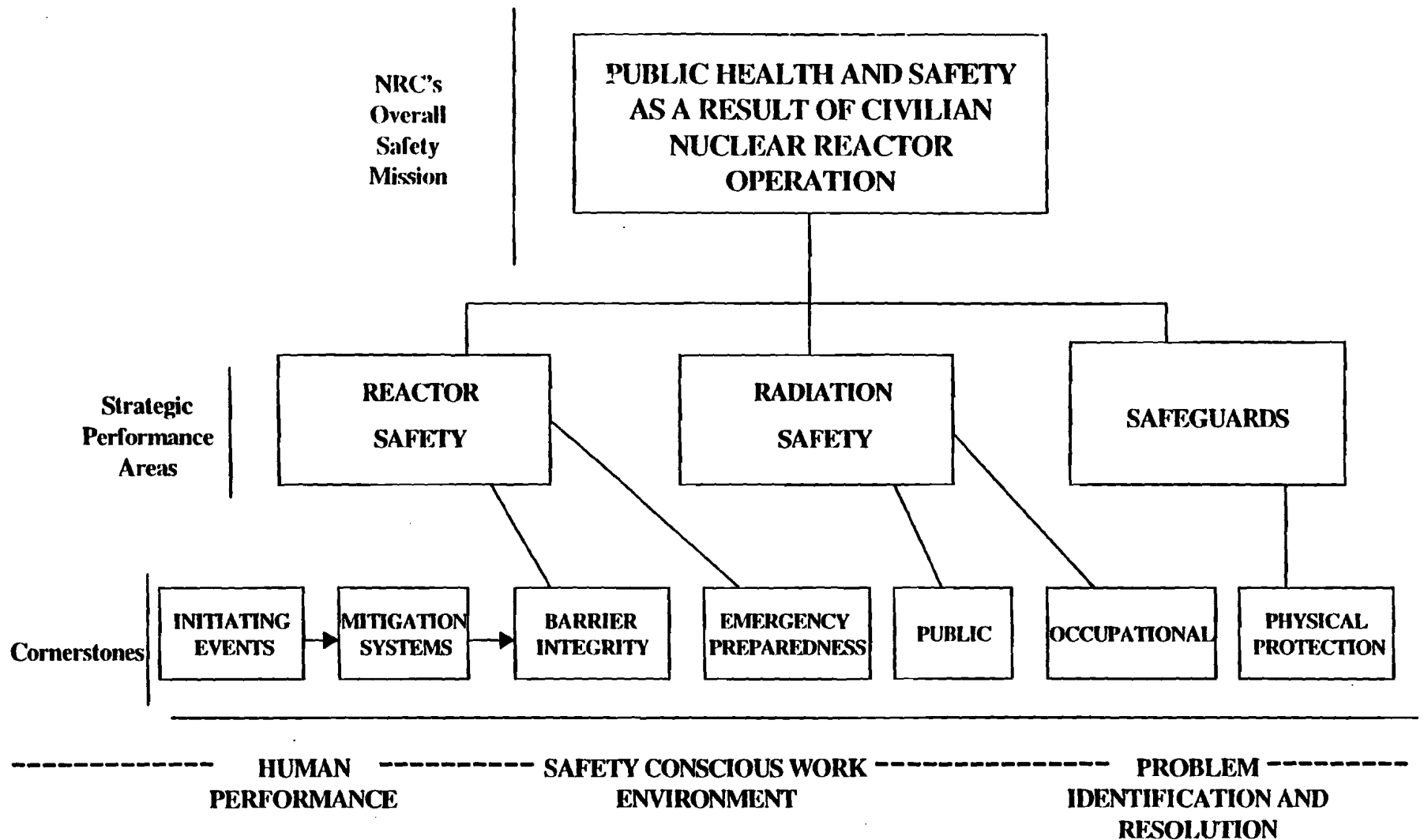
- I. (GDC1-5) Overall Requirements
- II. (GDC 10-18) Protection by Multiple Fission Product Barriers
- III. (GDC 20-29) Protection and Reactivity Control Systems
- IV. (GDC 30-46) Fluid Systems
- V. (GDC 50-57) Reactor Containment
- VI. (GDC 60-64) Fuel and Radioactivity Control

## REACTOR OVERSIGHT PROGRAM

### DEFENSE-IN-DEPTH

- Reactor Oversight Process uses “cornerstones” as a central element in its formulation
- Cornerstones are a Defense-in-depth concept

DEFENSE IN DEPTH IN THE REACTOR OVERSIGHT PROGRAM



- PERFORMANCE INDICATOR
- INSPECTION
- OTHER INFORMATION SOURCES
- DECISION THRESHOLDS

Figure 1- Cornerstones of Safety



**Table 1 - PERFORMANCE INDICATORS**

Cornerstone	Indicator		Thresholds		
			Increased Regulatory Response Band	Required Regulatory Response Band	Unacceptable Performance Band
Initiating Events	Unplanned scrams per 7000 critical hours (automatic and manual scrams)		>3	>6	>25
	Risk-significant scrams per 3 years		>4	>10	>20
	Transients per 7000 critical hours		>8	N/A	N/A
Mitigating Systems	Safety System Performance Indicator Unavailability	HPCI and RCIC	>0.04	>0.12	>0.5
		HPCS	>0.015	>0.04	>0.2
		Emergency Power	>0.025	>0.05 (>2EDG >0.1)	>0.1 (>2EDG >0.2)
		RHR	>0.015	>0.05	TBD
		AFW	>0.02	>0.06	>0.12
		HPSI	>0.015	>0.05	TBD
	Safety System Failures		>5 - prior 4 qtrs	N/A	N/A
Barriers - Fuel Cladding  - Reactor Coolant System  - Containment	Reactor coolant system (RCS) specific activity		>50% of TS limit	>100% of TS limit	N/A
	RCS leak rate		>50% of TS limit	>100% of TS limit	N/A
	Containment leakage		>100% L <sub>A</sub>	N/A	N/A
Emergency Preparedness	Emergency Response Organization (ERO) drill/exercise performance		<75% - prior 6 months; <90% - prior 2 years	<55% - prior 6 months; <70% - prior 2 years	N/A

**Table 1 - PERFORMANCE INDICATORS**

Cornerstone	Indicator	Thresholds		
		Increased Regulatory Response Band	Required Regulatory Response Band	Unacceptable Performance Band
	ERO readiness (percentage of ERO shift crews that have participated in a drill or exercise in the past 24 months)	<80% - prior 2 years; <90% - prior 3 years	<60% - prior 2 years; <70% - prior 3 years	N/A
	Alert and Notification System performance (percentage of availability time)	<94% per year	<90% per year	N/A
<b>Occupational Radiation Safety</b>	Occupational exposure control effectiveness (the number of non-compliances with 10 CFR 20 requirements for (1) high (greater than 1000 mRem/hour) and (2) very high radiation areas, and uncontrolled personnel exposures exceeding 10% of the stochastic or 2% of the non-stochastic limits)	6 or more occurrences in 3 years (rolling average); 3 or more in 1 year	12 or more occurrences in 3 years (rolling average); 6 or more in 1 year	N/A
<b>Public Radiation Safety</b>	Offsite release performance (number of effluent events that are reportable per 10 CFR 20, 10 CFR 50 Appendix I, Offsite Dose Calculation Manual, or Technical Specifications)	7 or more events in 3 years (rolling average); 4 or more events in 1 year	14 or more events in 3 years (rolling average); 8 or more events in 1 year	N/A
<b>Physical Protection</b>	Protected Area security equipment performance (availability of systems to perform their intended functions)	<95% per year	<85% per year	N/A
	Vital Area security equipment performance (availability of systems to perform their intended functions)	<95% per year	<85% per year	N/A
	Personnel screening process performance (acceptable implementation of the access authorization program)	3-5 reportable events	6 or more reportable events	N/A

LICENSEE PERFORMANCE INCREASING SAFETY SIGNIFICANCE ----->						
RESULTS		I. All Assessment Inputs (PIs and Cornerstone Inspection Areas) Green; Cornerstone Objectives Fully Met	II. One or Two Inputs White (in different cornerstones); Cornerstone Objectives Fully Met	III. One Degraded Cornerstone (2 Inputs White or 1 Input Yellow) or any 3 White Inputs; Cornerstone Objectives Met with Minimal Reduction in Safety Margin	IV. Repetitive Degraded Cornerstone, Multiple Degraded Cornerstones, or Multiple Yellow Inputs; Cornerstone Objectives Met with Significant Reduction in Safety Margin	V. Overall Red (Unacceptable) Performance; Plants Not Normally Permitted to Operate Within this Band, Unacceptable Margin to Safety
	Management Meeting	Routine Resident Inspector Interaction	SRI/BC Meet with Licensee	DD/RA Meet with Licensee Management	EDO Meet with Senior Licensee Management	Commission meeting with Senior Licensee Management
RESPONSE	Licensee Action	Licensee Corrective Action	Licensee Corrective Action with NRC Oversight	Licensee Self Assessment with NRC Oversight	Licensee Performance Improvement Plan with NRC Oversight	
	NRC Inspection	Risk-Informed Baseline Inspection Program	Inspection Follow-up	Inspection Focused on Cause of Degradation	Team Inspection Focused on Cause of Overall Degradation	
	Regulatory Actions	None	-Document Response to Degrading Area in Inspection Report	-Docket Response to Degrading Condition (Consider N+1 Inspection for 2 Consecutive Cycles in This Range)	-10 CFR 50.54(f) Letter - CAL/Order (Consider N+1 Inspection for 2 Consecutive Cycles in This Range)	Order to Modify, Suspend, or Revoke Licensed Activities
COMMUNICATION	Assessment Report	DD review/sign assessment report (w/ inspection plan)	DD review/sign assessment report (w/ inspection plan)	RA review/sign assessment report (w/ inspection plan)	RA review/sign assessment report (w/ inspection plan)	RA review/sign assessment report (w/ inspection plan)
	Public Assessment Meeting	SRI or Branch Chief Meet with Licensee	SRI or Branch Chief Meet with Licensee	RA Discuss Performance with Licensee	EDO Discuss Performance with Senior Licensee Management	Commission Meeting with Senior Licensee Management to Discuss Licensee Performance
<----- Regional Review   Agency Review ----->						

Table 5 - Action Matrix

## ISSUES RELATED TO APPLICATION OF DID IN REACTOR RISK-INFORMED ACTIVITIES

- RI - License Amendments:
  - RG 1.174 guidance on DID.
  
- RG 1.174 - lists elements of DID
  - balance between prevention and mitigation
  - avoid over-reliance on programmatic activities
  - system redundancy, diversity, independence
  - defense against common cause failures
  - independence of barriers
  - defense against human errors
  - intent of GDCs
  
- RI - Part 50:
  - working definition of DID for:
    - OPTION 2 (scope)
    - OPTION 3 (technical requirements)
  
- Policy Issues:
  - is a definition of DID needed in the Safety Goal Policy?
  - is a separate policy statement needed on DID?

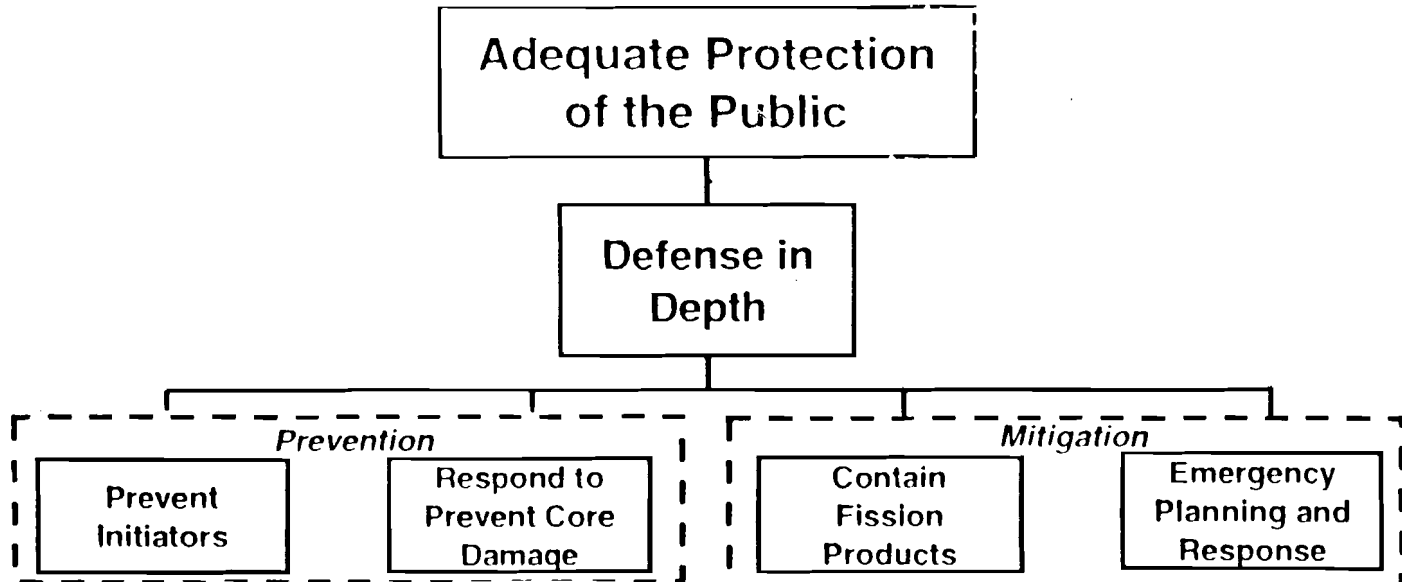
## DEVELOPMENT OF A WORKING DEFINITION OF DID

- Purpose of Working Definition of DID:
  - establish an approach to be used in risk-informing 10 CFR Part 50 that provides:
    - multiple lines of defense
    - balance between prevention and mitigation
    - a framework to address uncertainties in accident scenarios:
      - likelihood
      - reliability
      - consequence (phenomena modeling)
      - success criteria
      - completeness
  
- Elements of Working Definition:
  - DID should consist of two parts:
    - fundamental elements that should be provided in all cases
    - implementation elements that may vary depending on uncertainty and reliability and risk goals.

## WORKING DEFINITION OF DID FOR REACTORS

- Fundamental Elements:
  - build upon cornerstone concept:
    - initiating events
    - prevent core melt
    - contain fission products
    - EP & R
  - assure prevention and mitigation by providing:
    - reliable core melt prevention for all credible initiating events:
      - single failure criterion?
      - active vs. passive failure?
      - human performance?
      - redundancy/diversity?
    - ability to contain FP given a core melt
    - EP & R
  - assure balance between prevention and mitigation to achieve overall level of safety consistent with:
    - $\leq 10^{-4}/\text{RY CDF}$
    - $\leq 10^{-5}/\text{RY LERF}$

# CONCEPTUAL FRAMEWORK FOR BALANCE BETWEEN PREVENTION AND MITIGATION



Guidelines:(1) Consider the four cornerstones in pairs:

Initiators and Responses  $<1E-4$  and Containment and Emergency Planning  $<.01$ , OR

(2) Consider the cornerstones individually, based on initiator frequency

Anticipated

Initiators $<1/yr$	$1E-4$	$.1$	$\leq .1$
--------------------	--------	------	-----------

Infrequent

Initiators $<.01$	$1E-2$	$.1$	$\leq .1$
-------------------	--------	------	-----------

Rare

Events $<1E-6$	$1$	$1$	$1$
----------------	-----	-----	-----

Basis: The overall metric is frequency of significant dose to an offsite individual  
Each row results in  $1E-6$  (summed over the events)

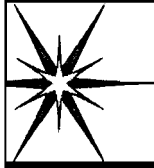
## WORKING DEFINITION (CONT.)

- Implementation Elements:
  - use of redundancy, diversity, and safety margins would be variable, as necessary, to achieve reliability and risk goals and balance of prevention and mitigation
  - use of QA, EQ, IST, etc., would be variable, as necessary, to achieve reliability goals
  - use mean values in assessing risk
  - must consider full power and shutdown condition.



## APPLICATION OF WORKING DEFINITION

- Use for top down look at 10 CFR 50
- Apply to each credible initiating event.
- Do regulations, R.Gs., SRPs requirements result in achieving:
  - risk goals
  - balance between prevention and mitigation
  - lines of defense
- Do regulations, R.G. SRPs, adequately specify analysis methods and acceptance criteria?



# **Defense-in-Depth Application to ALWR**

**ACRS/ACNW Meeting  
13 Jan. 2000**

**Gary Vine  
Sr. Washington Representative**

**EPRI**

DOE-EPRI-98-1



## **Overview**

- **U.S. ALWR Program guided ALWR policies, design, development, & regulatory approval process from mid-'80s to late '90s**
- **Broad participation: ind./govt.; international**
- **ALWR Program embraced traditional D-in-D philosophy; drove designs to improved D-in-D**
  - **Primary approach followed "Structuralist Model"\***
  - **Areas of effort toward "Rationalist Model"\* (later)**  
(\*as defined in ACRS paper by Sorensen et. al)

**EPRI**

DOE-EPRI-98-2



## ALWR Policies

- Simplification
- Design Margin
- Human Factors
- Safety
- Design Basis vs. Safety Margin
- Regulatory Stabilization
- Standardization
- Proven Technology
- Maintainability
- Constructibility
- Quality Assurance
- Economics
- Sabotage Protection
- Good Neighbor

EPRI

DOE-EPRI-04-1



## Areas of Emphasis Toward More Risk-Informed Approach

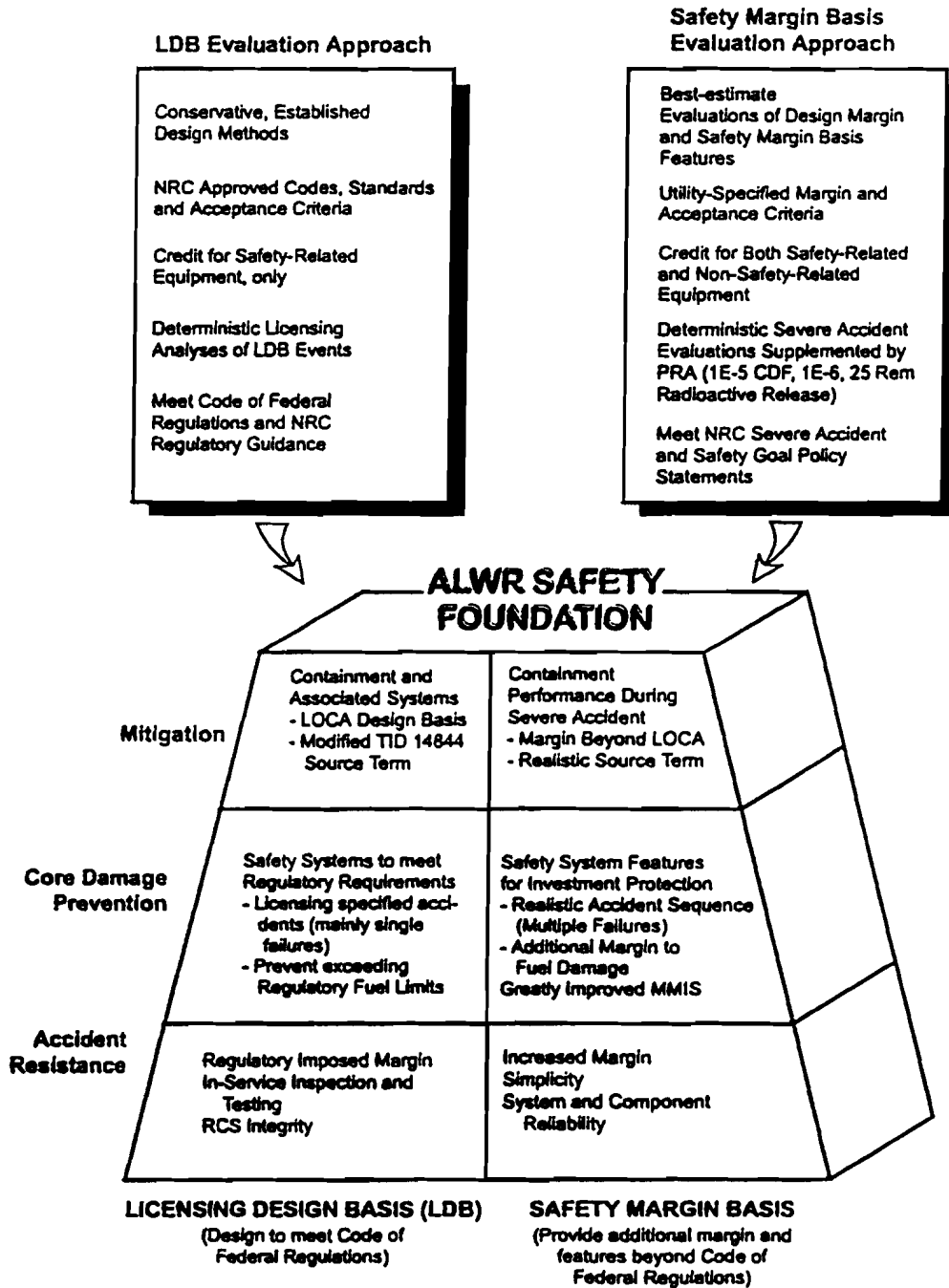
- **Primary emphasis on accident resistance and prevention; balanced emphasis on mitigation**
  - **Safety is critical to BOTH owner & NRC**
  - **Investment protection also critical to owner**
  - **Cost-effective design typically favored prevention**
  - **Created some issues wrt “balance” in D-in-D**
- **Explicit consideration of severe accidents via Safety Margin Basis (best est., outside LDB)**

EPRI

DOE-EPRI-04-4

# VOLUME I: POLICY AND TOP-TIER DESIGN REQUIREMENTS

FIGURE 2 - ALWR SAFETY FOUNDATION





## Areas of Emphasis Toward More Risk-Informed Approach

- Major reliance on PRA in design process
  - Drove many URD and vendor design decisions
  - critically important use for passive plants: RTNSS
  - Regulatory use primarily confirmatory. Selective use to support new requirements (ex: approval of some “optimization issues” proposed by industry)
- Industry’s quantitative safety requirements improved both prevention and mitigation
  - CDF < 10 E-5; <25 Rem @ site boundary for sequences with cumulative frequency >10 E-6)
  - opposed numerical coupling of D-in-D reqts.

EPRI



## Areas of Emphasis Toward More Risk-Informed Approach

- Regulatory Stabilization; assured licensability
  - generic resolution of issues in advance of DC
  - exceed regulations where feasible (provide margin to regulatory limits)
- “Optimization Issues” -- proposed changes to regulations where needed, typically driven by risk-insights
- Economic policy necessitated smart choices

EPRI



## Concluding Remarks

- Risk-informed Regulation essential for future of advanced reactor deployment
- Die is cast. “Rationalist Model” for D-in-D will become the future approach
- No downsides to Rationalist Model, if implemented properly. Major advantages
- Risk-Informed Regs by definition require consideration of D-in-D; use of eng. judgment
- US leadership on D-in-D issues important

EPRI



---

# **DEFENSE IN DEPTH AND THE AP600**

**January 13, 2000**

**Brian A. McIntyre**

**Manager, Advanced Plant Safety and Licensing**

**WESTINGHOUSE ELECTRIC COMPANY**

# **DEFENSE IN DEPTH DEFINITION / HISTORY**

---



**Traditionally a Part of the Prescriptive-Deterministic Regulatory Process**

- **3 Barriers to Release**
- **Worst Single failure Assumption**
- **2 means of Providing Shutdown Capability**
- **Large Break LOCA**
- **10 CFR Appendix K**
- **Accident Mitigation by Only Safety Related Equipment**
- **Etc**

**Invoked to Offset Perceived Uncertainties in Knowledge**

**Never Sure Exactly What it was**

**Never Sure When Enough was Enough**

**Now Appropriate to Strike a Balance with Risk Informed**



# DEFENSE IN DEPTH IN THE AP600

---



## Unquantifiable Aspects (Applicable Beyond Nuclear Power Plants)

- **Part of the Design Philosophy**
- **PRA Used as a Design Tool to Identify Potential Areas of Improvement**
- **Examined a Broad Range of Conditions**
  - Shutdown and Low Power Operations
  - Single and Multiple Steam Generator Tube Rupture
  - With and Without Nonsafety-Related Systems
  - Common Mode Failures
  - Operator Errors
  - Hazards (Fire, Flood)
- **Examined Broad Range of Initiating Events**

## Quantifiable Aspects

- **Low Core Damage Frequency**
  - Focused PRA Results
- **Low Large Release Frequency**
  - SAMDA

# AP600 PRA RESULTS



	Core Damage Frequency			Large Release Frequency		
	At-Power	Shutdown	Total	At-Power	Shutdown	Total
Baseline PRA	1.7E-07	9.0E-08	2.6E-07	1.8E-08	1.5E-08	3.3E-08
Focused PRA	7.7E-06	4.1E-07	8.1E-06	5.5E-07	2.6E-07	8.1E-07
NRC Safety Goal			1E-04			1E-06

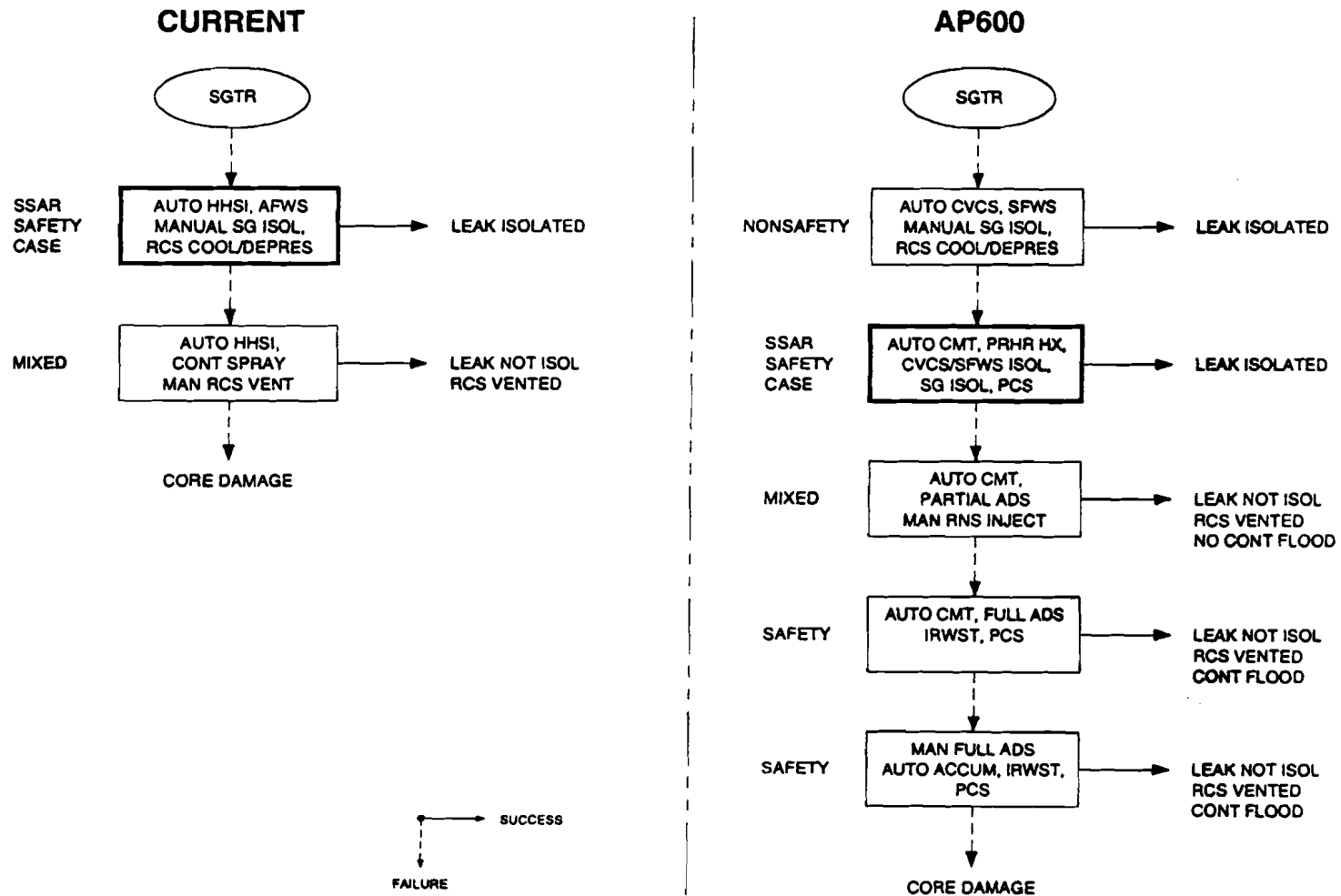
REF: AP600 Design Control Document

# System Defense In Depth



- **AP600 Provides Multiple Levels of Defense**
  - First feature is usually nonsafety active feature
    - High quality industrial grade equipment
  - One feature is safety passive feature
    - Provides safety case for SSAR
    - Highest quality nuclear grade equipment
  - Other passive features provide additional defense-in-depth
    - Example; passive feed/bleed backs up PRHR HX
  - Available for all shutdown conditions as well as at power
  - More likely events have more levels of defense

# SG Tube Rupture



# AP600 PRA

---



- **PRA Used as Design and Licensing Tool**
  - 7 PRA iterations performed on AP600; first in 1987, final in 1997
    - Extensive NRC review / comment
  - Plant designers interacted with risk analysis
- **Each PRA / Design Iteration Included**
  - Plant design input and PRA model development
  - Quantification and sensitivity studies
    - Importance of nonsafety features, operators, etc.
  - Review / understanding of results
  - Improvement of PRA and plant
    - PRA analysis (event/fault trees, success criteria T/H analysis)
    - Plant operating procedures
    - Plant design
  - Subsequent PRA studies became more detailed
    - Internal/fire/flood events from at-power & shutdown conditions

# AP600 PRHR HX FAILURE

---



- **Possible PRHR HX Failure Mechanisms**
  - Failure of AOV to open
    - Mechanical failure
    - Actuation failure
  - Isolation valves miss-positioned closed
  - Plugging of flow path
  - Inadequate IRWST water level
  - Non-condensable gas binding
  - Water hammer
  - Inadequate heat transfer

# IRWST WATER LEVEL

---



- **IRWST Water Required For PRHR HX Operation**
- **Means of Losing IRWST Water Quantified in PRA**
  - IRWST rupture following PRHR HX actuation
- **Means of Losing IRWST Water Not Quantified in PRA**
  - Leakage prior to PRHR HX actuation
    - Redundant (4) IRWST level instruments with alarms
  - Boil off due to PRHR HX operation
    - PRHR HX can operate >72 hr without water return
    - With water return can operate indefinitely

# AP600 PRHR HX GAS BINDING

---



- **PRHR HX Gas Binding Is Prevented By AP600 Design**
- **Air from Shutdown Operations**
  - Procedures require venting
  - Level detectors alarm condition allowing operators to manually vent
- **H2 from RCS or Pressurizer**
  - H2 in RCS is saturated at 30 psig so it can not come out of solution
  - Level instruments would alarm condition
- **N2 from Accumulator Discharge**
  - Accumulators empty at very low pressures, about 100 psig
  - During transients RCS does not drop to such pressures
  - During LOCAs PRHR HX is assumed to fail when N2 enters RCS
- **Severe Core Damage**
  - PRHR HX is assumed to fail when H2 is generated by core damage



# PRHR HX WATER HAMMER

---



- **Water Hammer Prevented By Design**
  - Inlet line to PRHR HX normally open
    - Pressure difference across isolation valve only 30 psi
    - No chance for low pressure void to exist downstream of isolation valve
  - Inlet line routed to maintain hot
    - Hot water prevents water hammer if HL becomes voided during accident
  
- **Water Hammer Not Included In PRA**

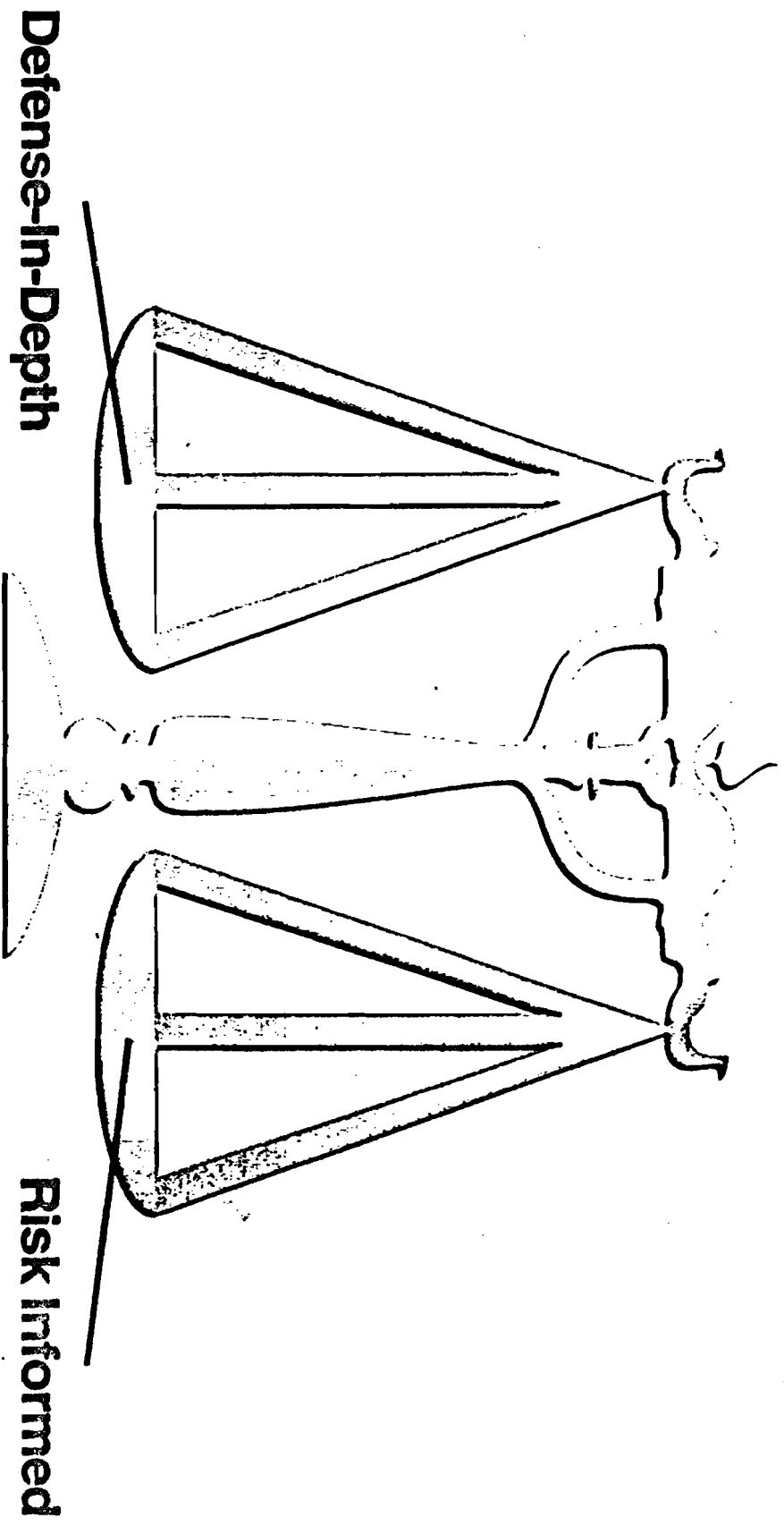
# INADEQUATE HEAT TRANSFER

---



- **PRHR HX Sized On Data From AP600 Test**
  - Three full sized tubes tested at full pres/temp
  
- **PRHR HX Included In AP600 Integrated Tests**
  - SPES-2 and OSU
  
- **PRHR HX Will Be Tested In Each Plant**
  - Startup tests at full pres/temp
  - IST each refueling at reduced pres/temp

# AP-600 CONTAINMENT SPRAY SYSTEM-?



# RISK INFORMED PERSPECTIVE

<u>AP-600 Release Mode</u>	<u>Risk Contribution*</u>
Containment Isolation Failure	9.6-%
Early Containment Failure	83.9-%
Containment Bypass	5.8-%
Other	0.7-%

\*population boundary dose risk -72 hr; PRA-Rev. 9

# AP600 RISK SUMMARY



Release	Frequency (per year)	72 Hour Population TEDE Dose (man-rem)	Risk (man-rem/yr)
Early Failure	6.6E-9	1.0E6	6.8E-3
Intermediate Failure	1.3E-11	3.5E5	4.6E-6
Late Failure	1.5E-11	1.5E4	2.2E-7
Isolation Failure	3.6E-10	2.1E6	7.7E-4
Bypass	1.1E-8	4.2E4	4.7E-4
Totals			8.06E-3

# AP600 RISK REDUCTION ESTIMATE LOW FLOW, NONSAFETY SPRAY



Release	Frequency (per year)	72 Hour Population TEDE Dose (man-rem)	Risk (man-rem/yr)	Reduced Risk Crediting Sprays (man-rem/yr)	Comment
Early Failure	6.6E-9	1.0E6	6.8E-3	3.8E-3	Approximately 2 hours between start of release and CF
Intermediate Failure	1.3E-11	3.5E5	4.6E-6	0.	Assumes tens of hours of spraying before CF
Late Failure	1.5E-11	1.5E4	2.2E-7	0.	Assumes tens of hours of spraying before CF
Isolation Failure	3.6E-10	2.1E6	7.7E-4	5.8E-5	Assumes 1 hour worth of spray decontamination
Bypass	1.1E-8	4.2E4	4.7E-4	4.7E-4	No spray reduction
Totals			8.06E-3	4.3E-3	

**EXECUTIVE**

**SUMMARY**

---

**EPRI**

---

**A L W R**



**A D V A N C E D  
L I G H T W A T E R R E A C T O R**

---

**ADVANCED LIGHT WATER REACTOR**  
**Utility Requirements Document**

**Issued 12/95**

### *Introduction*

The U.S. utilities are leading an industry wide effort to establish the technical foundation for the design of the Advanced Light Water Reactor (ALWR). This effort, the ALWR Program, is being managed for the U.S. electric utility industry by the Electric Power Research Institute (EPRI) and includes participation and sponsorship of several international utility companies and close cooperation with the U.S. Department of Energy (DOE). The cornerstone of the ALWR Program is a set of utility design requirements which are contained in the ALWR Utility Requirements Document.

### *Purpose of the Utility Requirements Document*

The purpose of the Utility Requirements Document is to present a clear, complete statement of utility desires for their next generation of nuclear plants. The Utility Requirements Document consists of a comprehensive set of design requirements for future LWRs. The requirements are grounded in proven technology of 35 years of commercial U.S. and international LWR experience. Furthermore, the utility design requirements build on this LWR experience base, correcting problems which existed in operating plants and incorporating features which assure a simple, robust, more forgiving design.

The anticipated uses of the Utility Requirements Document are threefold:

- Establish a stabilized regulatory basis for future LWRs which includes the NRC's agreement on resolution of outstanding licensing issues and severe accident issues, and which provides high assurance of licensability;
- Provide a set of utility design requirements for a standardized plant which are reflected in individual reactor and plant supplier certification designs;
- Provide a set of utility technical requirements which are suitable for use in an ALWR investor bid package for eventual detailed design, licensing and construction, and which provide a basis for strong investor confidence that the risks associated with the initial investment to complete and operate the first ALWR are minimal.



### *Scope of Requirements Document*

The Utility Requirements Document covers the entire plant up to the grid interface. It therefore is the basis for an integrated plant design, i.e., nuclear steam supply system and balance of plant, and it emphasizes those areas which are most important to the objective of achieving an ALWR which is excellent with respect to safety, performance, constructibility, and economics. The document applies to both Pressurized Water Reactors (PWRs) and Boiling Water Reactors (BWRs).

The Utility Requirements Document is organized in three volumes. Volume I summarizes ALWR Program policy statements and top-tier utility requirements.

Volumes II and III present the complete set of top-tier and detailed utility requirements for specific ALWR design concepts. Volume II covers Evolutionary ALWRs. These are simpler, much improved versions of existing LWRs, up to 1350 MWe, employing conventional but significantly improved, active safety systems. Volume III covers Passive ALWRs, greatly simplified, smaller (i.e., reference size 600 MWe) plants which employ primarily passive means (i.e., natural circulation, gravity drain, stored energy) for essential safety functions. Two passive design concepts are addressed in Volume III, the Passive BWR with pressure suppression containment and the loop-type Passive PWR with dry containment. While these Volume III concepts are not yet as completely developed as the Evolutionary ALWR, they extensively utilize existing LWR experience and Evolutionary ALWR utility requirements, and are expected to offer substantial advantages in constructibility and operability as well as the potential to surpass the very high ALWR safety standards.

In addition to the above Volume II and III ALWR concepts, there may be other design concepts which could be developed to meet ALWR Program objectives. Such design concepts are, however, not explicitly addressed in the Utility Requirements Document at this time.

### *ALWR Policies*

The ALWR Program has formulated policies in a number of key areas in order to provide guidance for overall Utility Requirements Document development, and to provide guidance to the Plant Designer in applying the requirements. While not design requirements themselves, the policies cover fundamental ALWR principles which have a broad influence on the design requirements. A summary of key policy statements is as follows:

- Simplification -** Simplification is fundamental to ALWR success. Simplification opportunities are to be pursued with very high priority and assigned greater importance in design decisions than has been done in recent, operating plants; simplification is to be assessed primarily from the standpoint of the plant operator.
- Design Margin -** Like simplicity, design margin is considered to be of fundamental importance and is to be pursued with very high priority. It will be assigned greater importance in design decisions than has been done in recent, operating plants. Design margins which go beyond regulatory requirements are not to be traded off or eroded for regulatory purposes.
- Human Factors -** Human factors considerations will be incorporated into every step of the ALWR design process. Significant improvements will be made in the main control room design.
- Safety -** The ALWR design will achieve excellence in safety for protection of the public, on-site personnel safety, and investment protection. It places primary emphasis on accident prevention as well as significant additional emphasis on mitigation. Containment performance during severe accidents will be evaluated to assure that adequate containment margin exists.
- Design Basis Versus Safety Margin -** The ALWR design will include both safety design and safety margin requirements. Safety design requirements (referred to as the Licensing Design Basis [LDB]) are necessary to meet the NRC's regulations with conservative, licensing-based methods. Safety margin requirements (referred to as the Safety Margin Basis [SMB]) are Plant Owner-initiated features which address investment protection and severe accident prevention and mitigation on a best estimate basis.
- Regulatory Stabilization -** ALWR licensability is to be assured by resolving open licensing issues, appropriately updating regulatory requirements, establishing acceptable severe accident provisions, and achieving a design consistent with regulatory requirements.

- Standardization -**      The ALWR utility requirements will form the technical foundation which leads the way to standardized, certified ALWR plant designs.
- Proven Technology -**    Proven technology will be employed throughout the ALWR design in order to minimize investment risk to the plant owner, control costs, take advantage of existing LWR operating experience, and assure that a plant prototype is not required; proven technology is that which has been successfully and clearly demonstrated in LWRs or other applicable industries such as fossil power and process industries.
- Maintainability -**      The ALWR will be designed for ease of maintenance to reduce operations and maintenance costs, reduce occupational exposure, and to facilitate repair and replacement of equipment.
- Constructibility -**      The ALWR construction schedule will be substantially improved over existing plants and must provide a basis for investor confidence through use of a design-for-construction approach, and completed engineering prior to initiation of construction.
- Quality Assurance -**    The responsibility for high quality design and construction work rests with the line management and personnel of the Plant Designer and Plant Constructor organizations.
- Economics -**            The ALWR plant will be designed to have projected busbar costs that provide a sufficient cost advantage over the competing baseload electricity generation technologies to offset higher capital investment risk associated with nuclear plant utilization.
- Sabotage Protection -**    The design will provide inherent resistance to sabotage and additional sabotage protection through plant security and through integration of plant arrangements and system configuration with plant security design.
- Good Neighbor -**        The ALWR plant will be designed to be a good neighbor to its surrounding environment and population by minimizing radioactive and chemical releases.

### *ALWR Top-Tier Design Requirements*

A brief summary of top-tier utility design requirements is provided in Table 1 for the ALWR. The top-tier utility design requirements are categorized by major functions, including safety and investment protection, performance, and design process and constructibility. There is also a set of general utility design requirements, such as simplification and proven technology, which apply broadly to the ALWR design, and a set of economic goals for the ALWR program. The top-tier utility design requirements are described further in Volume I and are formally invoked as utility requirements in Volumes II and III. These requirements reflect the ALWR Program policies described above and form the basis for developing the detailed system design requirements for specific ALWR concepts in Volumes II and III. Figure 1 shows the relationship of Volumes I, II, and III.

### *ALWR Implementation*

Assuring that the role of the Utility Requirements Document is understood and is successfully carried out depends on an understanding of the relationship between the various activities which comprise ALWR implementation. Accordingly, implementation scenarios for the Evolutionary and Passive ALWRs have been developed. Though uncertainties still exist at this point, these scenarios are plausible enough to provide reasonable understanding of the relationships noted above. A key assumption in the implementation scenarios is that increasing demand for electricity in combination with concerns over the environment and greenhouse gas effects associated with fossil fuel burning will result in significant improvements in political and public acceptance of nuclear power in the U.S. The implementation scenarios are also based on the ALWR policy that a prototype plant is not required. Figure 2 shows the major milestones in the Evolutionary and Passive ALWR implementation scenarios.

***Table 1. Summary of Top-Tier ALWR Plant Design Requirements***

<i>Subject Area of Requirement</i>	<i>Statement of Requirement</i>
<b>GENERAL UTILITY DESIGN REQUIREMENTS</b>	
Plant type and size	PWR or BWR, applicable to a range of sizes up to 1350 MWe <ul style="list-style-type: none"> <li>• Reference size for Evolutionary ALWR: 1200-1300 MWe per unit;</li> <li>• Reference size for Passive ALWR: 600 MWe per unit.</li> </ul>

# EXECUTIVE SUMMARY

---

Safety system concept	Simplified safety system concepts: <ul style="list-style-type: none"><li>• Evolutionary ALWR - simplified, improved active systems;</li><li>• Passive ALWR - primarily passive systems; safety-related ac electric power shall not be required.</li></ul>
Plant design life	60 years
Design philosophy	Simple, rugged, high design margin, based on proven technology; no power plant prototype required.
Plant siting envelope	Must be acceptable for most available sites in U.S.; 0.3g Safe Shutdown Earthquake (SSE).

## SAFETY AND INVESTMENT PROTECTION

Accident resistance	Design features that minimize the occurrence and severity of initiating events, such as: <ul style="list-style-type: none"><li>• Fuel thermal margin <math>\geq 15\%</math>;</li><li>• Slower plant response to upset conditions through features such as increased coolant inventory;</li><li>• Use of best available materials.</li></ul>
Core damage prevention	Design features that prevent initiating events from progressing to the point of core damage.
• Core damage frequency than $10^{-5}$ per reactor year.	Demonstrate by PRA that core damage frequency is less
• LOCA protection	No fuel damage for up to a 6-inch break
• Station blackout coping time for core cooling	8 hours minimum (indefinite for Passive ALWR)
• Operator action	For passive ALWR, no core protection regulatory limits exceeded for at least 72 hours assuming no operator action for LDB events including loss of all power.
Mitigation	
• Severe accident frequency and consequence	Demonstrate by PRA that the whole body dose is less than 25 rem at the site boundary for severe accidents with cumulative frequency greater than $10^{-6}$ per year.

## EXECUTIVE SUMMARY

---

- Containment Design Large, rugged containment building with design pressure based on Licensing Design Basis pipe break.
- Containment Margin Margin in containment design is sufficient to maintain containment integrity and low leakage during severe accident.
- Licensing source term Similar in concept to existing Regulatory Guide, TID 14841 approach, but with more technically correct release fractions, release timing, and chemical form.
- Hydrogen control to ensure containment integrity under hydrogen burn Control concentration to less than 10% in PWR containment for 100% active clad oxidation.
- Emergency planning For Passive ALWR, provide technical basis for simplification of off-site emergency plan.

### PERFORMANCE

- |  |  |
|--|--|
| Design availability                    | 87%  |
| Refueling interval                     | 24-month capability  |
| Unplanned automatic scrams             | Less than 1/year   |
| Maneuvering                            | Daily load follow  |
| Load rejection                         | Loss of load without reactor trip or turbine trip for PWR (from 100% power) and for BWR (from 40% power).  |
| Low level radio active waste produced  | Based on best current plants   |
| Site spent fuel wet storage capability | 10 years of operation plus one core off load   |
| Occupational radiation exposure        | Less than 100 person rem per year  |
| Operability and maintainability        |  |
| • Design for operation                 | Operability features designed into plant, such as: forgiving plant response for operators, design margin, and operator environment.  |
| • Design for maintainance              | Maintainability features designed into plant, such as: standardization of components, equipment design for minimal maintenance needs, provision of adequate access, improved working conditions. |

- Equipment access                      Ready access to equipment.
- Equipment replacement              Facilitate replacement of components, including steam generators.

Man-Machine Interface

- Instrumentation and control systems      Advanced technology, including software based systems, alarm prioritization, fault tolerance, automatic testing, multiplexing, and computer driven displays.
- Operations simplicity                  A single operator able to control plants during normal power operation.
- Control stations                         Human engineered to enhance operator effectiveness, utilizing mockups, dynamic simulation, and operator input to design.

**DESIGN PROCESS AND CONSTRUCTABILITY**

Total time from owner commitment to construct to commercial operation      1300 MWe evolutionary plant designed for less than or equal to 72 months  
 600 MWe passive plant designed for less than or equal to 60 months

Construction time from first structural concrete to commercial operation      1300 MWe evolutionary plant designed for less than or equal to 54 months  
 600 MWe passive plant designed for less than or equal to 42 months

Design status at time of initiation of construction      90% complete

Design and plan for construction                      Design for simplicity and modularization to facilitate construction; develop an integrated construction plan through Plant Owner acceptance.

Design process

- Design integration                      Manage and execute design as a single, integrated process.
- Configuration management          Comprehensive system to control plant design basis and installed equipment and structures.
- Information management              Computerized system to generate and utilize an integrated plant information management system during design, construction, and operation.

## ECONOMICS

- |                                 |  |
|---------------------------------|--|
| Cost goal                       | ALWR plants will have a sufficient cost advantage over competing baseload electricity generation technologies to offset a higher capital investment risk associated with nuclear plant utilization.  |
| Resulting quantified cost goals | Levelized January 1994 constant dollars for a 30-year capital amortization period, plant startup in 2005, and a mid-range-cost U.S. location (Kenosha, Wisconsin).   |
| • Median busbar cost            | Sufficiently less than 43 mills/Kwh to offset the higher capital investment risk associated with nuclear plant utilization.  |
| • Uncertainty                   | Projected 95th percentile non-exceedance cost substantially less than 53 mills/Kwh both to offset a higher capital investment risk associated with nuclear plant construction and to recognize that cost uncertainties with alternative generating technologies will decrease with time. |



Figure 1.    RELATIONSHIP OF THE THREE VOLUMES OF  
THE ALWR REQUIREMENTS DOCUMENT

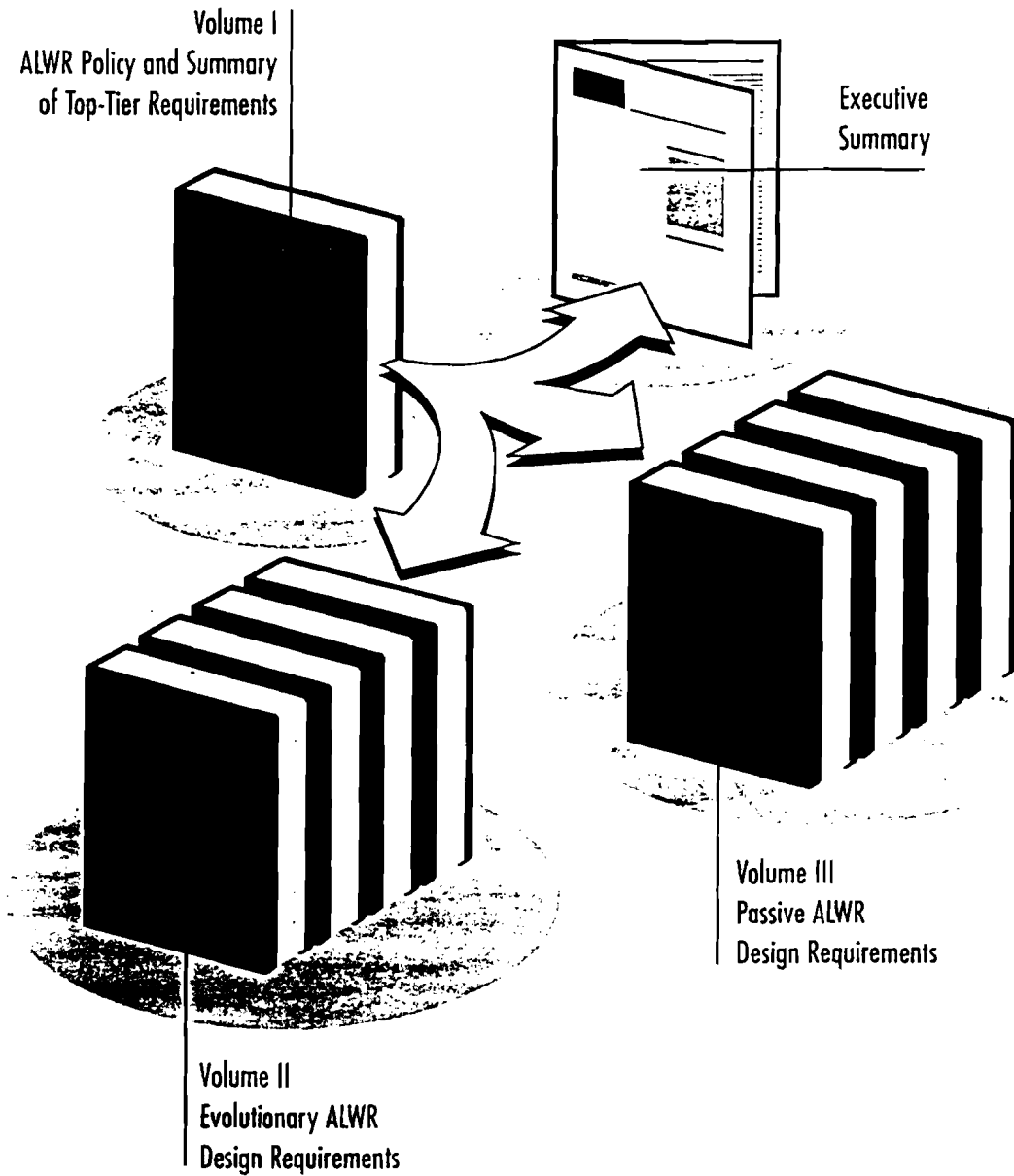
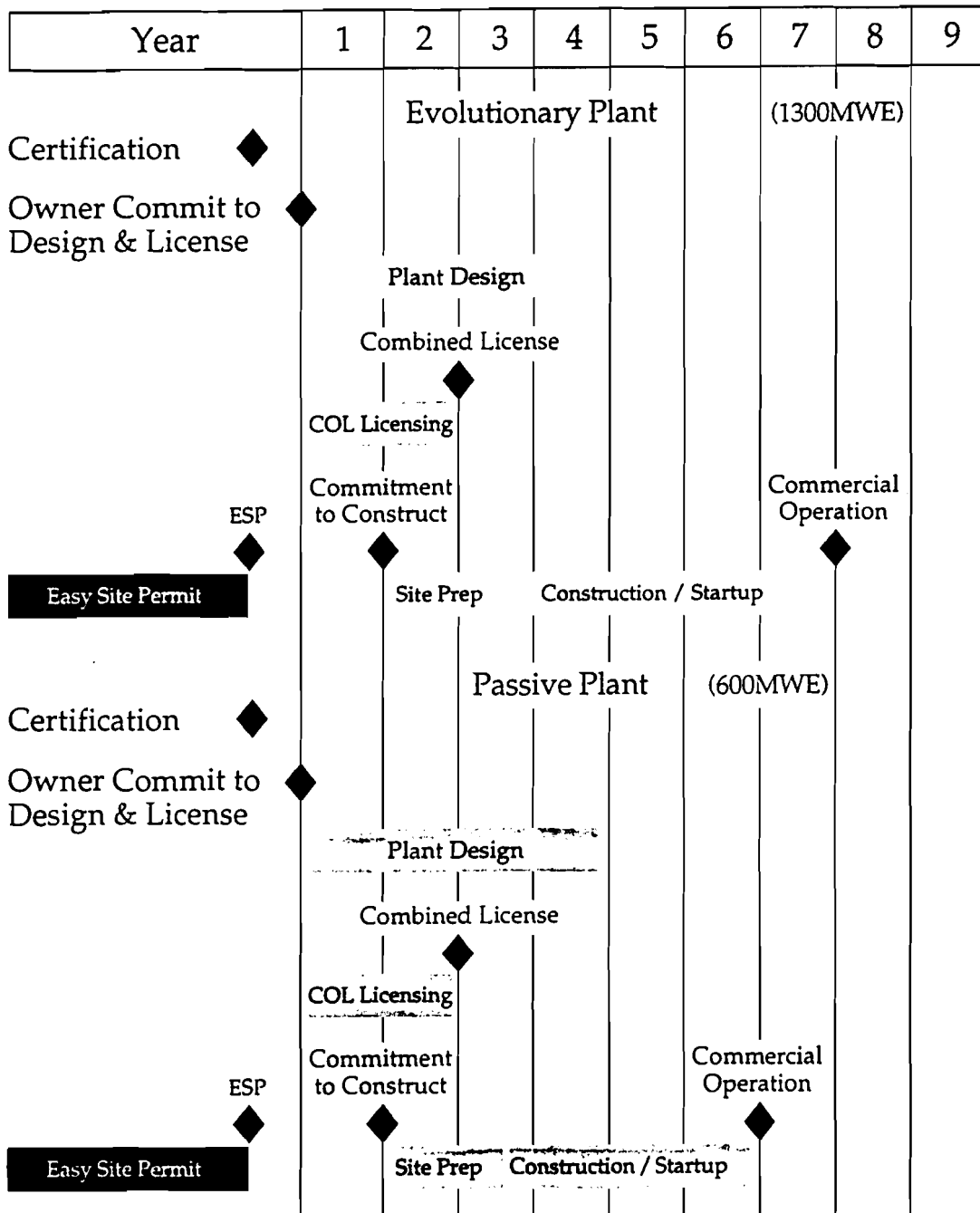


Figure 2. PLAUSIBLE ALWR IMPLEMENTATION SCENARIO



*Roy W. Yoder*  
1/14/2000

## DID ISSUES EMPHASIZING THE YUCCA MOUNTAIN REPOSITORY

1. There are uncertainties in PAs. There is much less experience (data) with waste repositories than with reactors, so uncertainties in repository system performance are larger for waste repositories.
2. Performance and risk assessments requirements are not as well understood for waste repositories as for reactors. We need to elucidate and explain these many differences and recognize them in the DID philosophy statements.
3. There should be several lines of defense (DID) against release of radioisotopes and the resultant radiation exposures. The types and number of lines of defense should be directly related to the uncertainties *in system performance and related hazards of*
4. DID requirements for waste (and nuclear materials) are different in very important ways from DID for nuclear reactors. For example, in the case of the YM repository after closure there is little probability of an accident of the type that reactors may have. This is related to the physical nature of the systems and to the fact that there are very large time-dependent and potential energy differences.
5. NRC should specify *in* clearly how the PA/PRA should be done by DOE in its LA for the YM repository, and what it should include. If the NRC guidance is good then the assessment should be able to be done well without further specific NRC guidance.
6. Because of the nature of the interactions between NRC and license applications for complex systems there will always be a strong possibility of an iterative licensing process (i.e., overtones of "bring me another rock").

## **NOTES ON DEFENSE IN DEPTH**

**B. John Garrick  
January 14, 2000**

- **Support the notion that defense in depth is a philosophy and approach to assuring safety to the public of nuclear facilities. It should not be converted to an algorithm or analytical process. Do not support making DID a formal requirement.**
- **As a philosophy, prefer that DID not be explicitly defined for fear of the surrogate syndrome—i.e., putting licensing emphasis on surrogates rather than on the required overall performance or risk measure. We should support the concept of transitioning to a risk-informed, performance-based regulatory approach.**
- **Favor allocation if by allocation is meant guidance on the quantification of protection systems (lines of defense) and the form of PRA and PPA results. Do not favor prescribing the performance of individual protection systems or protective barriers. We should continue to put the emphasis on quantifying the role and contribution of individual protection systems to the overall measures of risk and safety performance.**
- **In the spirit of quantifying the performance of protection systems, which includes quantifying uncertainty, we should seek assurance that the protection systems contribute to the bottom line measures of performance and risk, including allowance for “unquantified uncertainties”.**
- **We should continue to embrace the concept of total system performance, where total captures not only the physical systems involved, but the support infrastructure as well, including human performance, procedures, software, and the quality assurance and administrative process.**

ACRS/ACNW Joint Subcommittee meeting  
January 13-14, 2000

List of background documents

Tab 1. ACRS report dated June 17, 1997 from R. L. Seale, Chairman, ACRS to Shirley Ann Jackson, Chairman, NRC, Subject: Proposed Staff Position Regarding Inclusion of a Containment Spray System in the AP600 Design

Tab 2. Memorandum from J. N. Sorensen to ACRS Members, Subject: Historical Notes on Defense in Depth, October 15, 1997

Tab 3. PRA Policy Statement (8/16/95)

Tab 4. Advanced Nuclear Power Plant Policy Statement (7/12/94)

Tab 5. Safety Goal Policy Statement (8/4/86)

Tab 6. ACNW report dated October 31, 1997 from B. John Garrick, Chairman, ACNW to Shirley Ann Jackson, Chairman, NRC, Subject: Recommendations Regarding the Implementation of the Defense-in-Depth Concept in the Revised 10 CFR Part 60

Tab 7. Regulatory Guide 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, July 1998

Tab 8. SECY-98-225, Subject: Proposed Rule: 10 CFR Part 63 --- "Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada," September 28, 1998 (Only the SECY paper, the SRM governing its development (Attachment 1), and the portion of Attachment 2 which discusses defense in depth and performance assessment are included here. Attachment 2 in its entirety is about 160 pages.)

Tab 9. Memorandum from J. N. Sorensen to Andrew C. Campbell, Subject: Defense in Depth in the Geologic Repository, February 11, 1999

Tab 10. SECY-98-144, Subject: White Paper on Risk-Informed and Performance-Based Regulation, and its associated SRM, February 24, 1999

Tab 11. ACRS report dated May 19, 1999 from Dana A. Powers, Chairman, ACRS to Shirley Ann Jackson, Chairman, NRC, Subject: The Role of Defense in Depth in a Risk-Informed Regulatory System, and attached paper by J. N. Sorensen et al., "On the Role of Defense in Depth in Risk-Informed Regulation."

Tab 12. SECY-98-300, Subject: Options for Risk-Informed Revisions to 10 CFR Part 50 - "Domestic Licensing of Production and Utilization Facilities," December 23, 1998, and its associated SRM dated June 8, 1999

Tab 13. Letter from Robert J. Budnitz, Future Resources Associates, Inc., to B. John Garrick, Chairman, ACNW dated June 25, 1999 regarding the treatment of defense in depth in the proposed Part 63

Tab 14. SECY-99-186, Subject: Staff Plan for Clarifying How Defense-in-Depth Applies to the Regulation of a Possible Geologic Repository at Yucca Mountain, Nevada, July 16, 1999

Tab 15. SECY-99-191, Subject: Modifications to the Safety Goal Policy Statement, July 22, 1999, and associated SRM dated October 28, 1999

Tab 16. SECY-99-256. Subject: Rulemaking Plan for Risk-Informing Special Treatment Requirements, October 29, 1999 (without attachments)

Tab 17. ACRS report dated October 12, 1999 from Dana A. Powers, Chairman, ACRS, to Greta Joy Dicus, Chairman, NRC, Subject: Proposed Plans for Developing Risk-Informed Revisions to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities"

Tab 18. ACRS/ACNW report dated November 17, 1999 from Dana A. Powers, Chairman, ACRS, and B. John Garrick, Chairman, ACNW to Richard A. Meserve, Chairman, NRC, Subject: Implementing a Framework for Risk-Informed Regulation in the Office of Nuclear Material Safety and Safeguards



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS  
WASHINGTON, D. C. 20555

June 17, 1997

The Honorable Shirley Ann Jackson  
Chairman  
U. S. Nuclear Regulatory Commission  
Washington, D.C. 20555-0001

Dear Chairman Jackson:

SUBJECT: PROPOSED STAFF POSITION REGARDING INCLUSION OF A  
CONTAINMENT SPRAY SYSTEM IN THE AP600 DESIGN

During the 442nd meeting of the Advisory Committee on Reactor Safeguards, June 11-14, 1997, we met with representatives of the NRC staff and the Westinghouse Electric Corporation to discuss the proposed staff position that the AP600 design should include a containment spray system or equivalent for accident management following a severe accident. We also had the benefit of the documents referenced.

The staff position is that the addition of a nonsafety-related containment spray system in the AP600 design would achieve an appropriate balance between prevention and mitigation of severe accidents. The staff stated that such a system would compensate for the uncertainties associated with natural removal mechanisms for aerosols during severe accidents and provide for accident mitigation and operator intervention capability as part of a long-term accident management strategy. The staff believes that a containment spray system or equivalent is consistent with the AP600 passive design philosophy and the Commission's defense-in-depth philosophy.

The Westinghouse position is that the AP600 design meets existing regulatory prevention and mitigation criteria, including the Safety Goals. This may well be the case; however, we have not yet completed our review. Westinghouse also contends that a requirement for additional systems is neither justified nor warranted. The information presented to us by Westinghouse did not address the relevant uncertainties associated with the AP600 probabilistic risk assessment.

Ideally, the determination of the need for a containment spray system should be based on a judgment as to the levels of

uncertainties associated with aerosol depletion and overall risk, as well as on the value of additional accident management capability. The first question of interest is, what are the nature and extent of the uncertainties of concern. If all uncertainties were quantifiable, it would be fairly straightforward to determine whether sufficient defense-in-depth is built into the system by assessing the risk status with respect to the subsidiary Safety Goals (core damage frequency and large, early release frequency). At present, however, a large component of uncertainties remain unquantified. The identification of these uncertainties and the qualitative judgments regarding their impact on regulatory decisions would make the debate more specific and would enhance communication among the stakeholders.

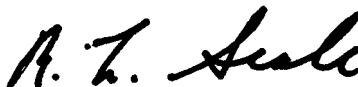
In judging the usefulness of a containment spray system in compensating for these uncertainties, both positive and negative impacts of this system should be evaluated in a quantitative and qualitative way. A judgment based on such an evaluation would help make the decision more acceptable to stakeholders because the basis for the decision would be explicit and transparent. Furthermore, such an evaluation process would be a good first step towards the integration of risk and traditional concepts such as defense-in-depth.

Although we prefer to have the information from the evaluation outlined above, based on our current state of knowledge, we support the staff's contention that the addition of a severe accident mitigation system is appropriate. The addition of a spray system to the AP600 containment would significantly increase its effectiveness in fission product control and provide the ability to intervene and control the course of an accident. We believe, however, that the spray design concept suggested by the staff is marginally adequate.

The debate associated with this issue and the difficulty of making a decision highlight our belief that the NRC needs to develop a new policy statement that would provide more guidance on the extent and nature of defense-in-depth expected by the Commission.

Dr. Dana A. Powers did not participate in the Committee's deliberations regarding this matter.

Sincerely,



R. L. Seale  
Chairman



References:

1. ACRS letter dated June 15, 1995, from T. S. Kress, Chairman, ACRS, to James M. Taylor, Executive Director for Operations, NRC, Subject: Proposed Commission Paper on Staff Positions on Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design.
2. ACRS report dated August 15, 1996, from T. S. Kress, Chairman, ACRS, to Shirley Ann Jackson, Chairman, NRC, Subject: SECY-96-128, "Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design."
3. Memorandum dated November 12, 1996, from James M. Taylor, Executive Director for Operations, NRC, to the NRC Commissioners, Subject: Clarification of Staff Position in SECY-96-128, "Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standard Pressurized Reactor Design."
4. Memorandum dated January 15, 1997, from John C. Hoyle, Secretary, NRC, to Hugh L. Thompson, Jr., Acting Executive Director for Operations, NRC, and Karen D. Cyr, General Counsel, NRC, Subject: Staff Requirements - SECY-96-128 - Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design.
5. Memorandum dated February 19, 1997, for the Commissioners, from Hugh L. Thompson, Jr., Acting Executive Director for Operations, NRC, Subject: SECY-97-044, "Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design."
6. Memorandum dated March 18, 1997, from L. Joseph Callan, Executive Director for Operations, NRC, to Chairman Jackson, Subject: Use of Non-Safety-Related Equipment to Address Safety Concerns on Nuclear Power Plants.
7. Letter dated March 13, 1997, from Brian A. McIntyre, Westinghouse Electric Corporation, to John Hoyle, Secretary, NRC, Subject: Westinghouse Comments on SECY-97-044, "Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standard Pressurized Reactor Design."
8. Memorandum dated May 16, 1997, from L. Joseph Callan, Executive Director for Operations, NRC, to the NRC Commissioners, Subject: Westinghouse Comments on SECY-97-044, "Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standard Pressurized Reactor Design."



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS  
ADVISORY COMMITTEE ON NUCLEAR WASTE  
WASHINGTON, D.C. 20555

MEMORANDUM

OFFICE OF  
ACRS/ACNW

TO: ACRS Members

FROM:   
J. N. Sorensen

DATE: October 15, 1997

SUBJECT: Historical Notes on Defense in Depth

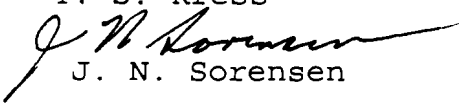
Attached for your information is a memorandum I prepared for Dr. Kress on the history of the term "defense in depth." This memo documents the preparation done for the August 27, 1997 meeting of the Subcommittee on Regulatory Policies and Practices, and adds some new material to the discussion of the use of the term "defense in depth" in Commission policy statements.

Attachment: As stated

cc w/attachment: ACRS/ACNW Staff  
J. T. Larkins  
R. P. Savio

MEMORANDUM

TO: T. S. Kress

FROM:  J. N. Sorensen

SUBJECT: Historical Notes on Defense in Depth

DATE: October 9, 1997

The ACRS has been discussing the concept of defense in depth and its impact on the design, operation and regulation of nuclear power plants in a number of contexts during the past year. The basic questions that have been formulated appear to revolve around two concerns: (1) how is defense in depth defined and (2) how can it be determined that specific design or regulatory requirements are necessary or sufficient to achieve defense in depth? The purpose of this memo is to document the historical research done to support discussion of those two issues.

The term "defense in depth" occurs frequently in the documented history of nuclear reactor safety. In fact, it is used so frequently that its evolution, meaning(s) and function in the design and regulatory processes are not always clear. For example, the term "defense in depth" does not appear in Title 10 of the Code of Federal Regulations except in Appendix R of Part 50, where it appears once. The specific statement occurs in Section II.A, General Requirements, Fire Protection Program, which states in part, "The fire protection program shall extend the concept of defense-in- depth to fire protection in fire areas important to safety, with the following objectives:

- o To prevent fires from starting;
- o To detect rapidly, control, and extinguish promptly those fires that do occur;
- o To provide protection for systems, structures and components important to safety so that a fire that is not promptly extinguished . . . will not prevent the safe shutdown of the plant."

Note the choice of words, ". . . extend the concept of defense-in-depth . . ." This phrase implies that the concept of defense in depth is well understood at this point in the document, and

that it has been used in other sections of the regulations. In fact, the term itself is not defined in Title 10, and has no prior or subsequent appearances. The concept of defense in depth permeates the General Design Criteria in 10 CFR 50 Appendix A, and underlies other Title 10 requirements as well. One might reasonably conclude from this that the only requirements to implement defense in depth are those that are implicit in other, explicitly stated, requirements. (Perhaps defense in depth should properly be thought of as a response to specific design and regulatory requirements, since it does not appear to be a regulatory requirement per se. A configuration management perspective suggests that this may be an important thought. I will return to it in a later memo.)

Joint Committee on Atomic Energy Hearings, 1967

The earliest definition of defense in depth that I found (with the assistance of NRC historian Sam Walker) was in an April 1967 statement submitted by Clifford Beck, then Deputy Director of Regulation, to the Joint Committee on Atomic Energy. The following two pages quote extensively from the paper because there may be some significance in how narrowly Beck defines defense in depth relative to the extremely broad view he takes of contributors to reactor safety. In discussing the system of safety protection for power reactors, the statement reads:

"For safety, three basic lines of defense are built into the physical systems of nuclear power reactor facilities.

1. The first and most important line of safety protection is the achievement of superior quality in design, construction and operation of basic reactor systems important to safety, which insures a very low probability of accidents. . . . Emphasis on this objective is reflected in:

The stress placed on selection of proper materials, quality controls in fabrication of components, rigorous systems of inspection and testing, appropriate techniques and controls in workmanship.

The requirement of high standards of engineering practice in design for critical components and systems. For example, the principles of fail-safe design,

redundancy and backup, defense-in-depth, and extra margins of safety at key points are employed. The principle of defense-in-depth is illustrated by the successive barriers provided against the escape of fission products: (1) the ceramic uranium oxide fuel matrix has a very high retention capacity . . .; (2) the fuel pins are sheathed in impervious claddings of stainless steel or zirconium; (3) the fuel core is enclosed in a high-integrity, pressure-tested primary coolant system . . .; (4) a high-integrity pressure-and-leak-tested containment building entirely surrounds each reactor structure.

Regularly scheduled equipment checks and maintenance programs; prompt and thorough investigation and correction of abnormal events, failures or malfunctions.

The requirements of sound and well defined principles of good management in operation; a competent and well-trained staff, clearly assigned duties, written procedures, checks and balances in the procedures for revisions, periodic internal audits of operations, etc. . . .

2. The second line of defense consists of the accident prevention safety systems which are designed into the facility.

These systems are intended to prevent mishaps and perturbations from escalating into major accidents. Included are such devices as redundancy in controls and shutdown devices; emergency power from independent sources - sometimes in triplicate - and emergency cooling systems.

3. The third line of defense consists of consequences-limiting safety systems. These systems are designed to confine or minimize the escape of fission products to the environment in case accidents should occur with the release of fission products from the fuel and the primary system. These include the containment building itself, building spray and washdown system, building cooling system . . ., and an internal filter-collection system.

Three related elements in the system of protection consist of the means for ensuring the effectiveness of

these three basic lines of defense in the physical facility.

1. A major element is systematic analysis and evaluation of the proposed reactor design . . . up to and including the so-called "maximum credible accident."
2. The system of numerous independent reviews by experts in the safety analysis and evaluation of a proposed facility by licensee experts and consultants, by the regulatory staff, the ACRS, the Atomic Safety and Licensing Boards, and the Commission . . .
3. A system of surveillance and inspection is the final element mentioned here. During construction and after the reactor becomes operative, surveillance . . . is maintained by means of periodic inspections, periodic reports from the company, examination of operating records, and investigation of facility irregularities."

The broad picture Beck draws is of "three basic lines of defense." Within the "first line," he illustrates "the principle of defense-in-depth" by example, choosing the multiple physical barriers of fuel matrix, clad, primary system and containment. He then goes on to describe what he calls the second and third lines of defense, namely, accident prevention and limiting the consequences of accidents. Does he mean the term "defense-in-depth" to apply to his three broad "lines of defense"? It does not seem so. For example, within his discussion of the first line of defense, he lists and apparently intends to differentiate among the attributes "fail safe design, redundancy and backup, defense in depth, and extra margins of safety." If we accept this reading at face value, then he has defined defense in depth very narrowly and not very clearly by his example. (The example is clear, but its extension is not.) On the other hand, how could one avoid interpreting "three levels of defense" as "defense in depth"?

Internal Study Group, 1969

Another reference to defense in depth occurs in the "Report to the Atomic Energy Commission on the Reactor Licensing Program," by the Internal Study Group, June 1969. This study was initiated by the AEC in June 1968 to help assure that procedures keep pace with the rapid expansion of the nuclear industry. The study group members were appointed from the AEC staff, the ACRS, and the Atomic Safety and Licensing Board Panel. The Group considered the general questions of (1) the adequacy of the protection of the health and safety of the public and (2) whether regulatory procedures and requirements have adversely affected the development of the industry. The report states

"The achievement of an adequate level of safety for nuclear power plants is generally recognized to require defense-in-depth in the design of the plant and its additional engineered safety features. The degree of emphasis on defense-in-depth in the nuclear field is new to the power industry.

In seeking reliability of safety systems, there has been much attention in the nuclear field to redundancy, diversity, and quality control. As a result of the evolution of designs, and the large number of new orders for nuclear plants, questions have been raised regarding the proper balance among back-up systems with respect to the requirements of basic plant design.

The Study Group endorses the defense-in-depth concept, but believes that the greatest emphasis should be placed on the first line of defense, i.e., on designing, constructing, testing and operating a plant so that it will perform during normal and abnormal conditions in a reliable and predictable manner."

Two things seem evident from the preceding discussion. The first is that the issue of "balance," and a relationship between balance and defense in depth, had already been identified. The second is that the writers considered the "first line of defense" as described by Clifford Beck to be one element of defense in depth.

ECCS Hearings, 1971

The third historical document of interest is the testimony of the AEC Regulatory Staff at the Public Rulemaking Hearings on Interim Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Power Reactors, issued December 28, 1971. The introduction to this document includes a subsection titled "Defense in Depth." The testimony states,

"The safety goal, therefore, is the prevention of exposure of people to this radioactivity. This goal can be achieved with a high degree of assurance, though not perfectly, by use of the concept of defense in depth. The principal defense is through the prevention of accidents. All structures, systems, and components important to safety must be designed, built, and operated so that the probability of an accident occurring is very small. The keys to achievement of this objective are quality and quality assurance, independently and concurrently. The work must be done well and then checked well, in order for the chance for errors and flaws to be reduced to an acceptable level.

However, excellent the design and execution, and however comprehensive the quality assurance, they must be acknowledged to be imperfect. As a second line of defense, protective systems are provided to take corrective actions as required should deviations from expected behavior occur, despite all that is done to prevent them. The protective systems include redundant elements, provision for periodic in-service testing, and other features to enhance performance and reliability.

Yet another defense - the third line - is provided by installing engineered safety features to mitigate the consequences of postulated serious accidents, in spite of the fact that these accidents are highly unlikely because of the first two lines of defense. Analogously to protective systems, engineered safety features are furnished with redundant elements, separate sources of energy and fluids, protection against natural phenomena and manmade accidents, and other similar elements to



ensure their correct functioning in the unlikely event they are called upon.

The three separate lines of the defense in depth provided for power reactors are considered appropriate to reduce to an acceptable value the probability and potential consequences of radioactive releases. Extensive and comprehensive quality assurance programs are required and used to assure the integrity of each line of defense and to maintain the different lines as nearly independent as practicable."

The same introductory section includes a subsection titled "Probability and Margins." That subsection states,

". . . the ECCS is part of the third line of defense, in the defense-in-depth concept used to ensure reactor safety. The design basis for ECCS is the postulated spectrum of LOCAs, for which the ECCS is required to provide protection for the public. This is consistent with defense-in-depth, and we believe the provision of such protection, with this design basis, to be proper."

The subsection goes on to list conservatisms that the authors apparently consider to be an addition to, but not part of, defense-in-depth.

"Further, the design of the ECCS is required to be adequate to provide this protection in spite of additional conservative assumptions such as non-availability of offsite power, single failures of redundant components, and partial loss of cooling water. Still further, in evaluating the suitability of a site proposed for a light-water power reactor, the AEC requires an analysis to be made of the potential offsite effects of a postulated LOCA. Additional elements of conservatism are included in this analysis, including assumptions of high release fractions of fission products from the fuel, containment leakage continuously for 30 days, and unfavorable meteorology."

And in a subsection titled "Conclusions":

". . . Quality in the design, manufacture, installation and operation of the primary system is a necessary part of the defense-in-depth. . . ."

In this document, the writers clearly equate the "three levels of defense" discussed earlier by Beck, with "defense-in depth." Beck made no such equation. They also appear to distinguish between "defense-in-depth" and "margin" as reflected by conservatisms introduced in analyzing the consequences of accidents.

#### WASH-1250, 1973

Another document that was in development at the same time the above testimony was prepared is WASH-1250, "The Safety of Nuclear Power Reactors (Light Water Cooled) and Related Facilities." This document was completed in 1973.

The first chapter, "Description of Light Water Reactor Power Plants and Related Facilities," states that "While differences in detail exist among PWR plants and among BWR plants, the basic features of each type are much the same. All are massive and complex structures, designed and built to provide multiple barriers to the escape of radioactive material, from whatever cause, and to withstand the occurrences of natural forces . . . without compromising these barriers . . ." The term "defense-in-depth" is not introduced at that point.

Chapter 2, titled "Basic Philosophy and Practices for Assuring Safety," states that "the basic philosophy underlying the AEC Rules of Procedure and Regulatory Standards, and underlying industrial practices . . . is frequently called a 'defense in depth' philosophy." The discussion goes on to note that "Previous mention has been made of the use of multiple barriers against the escape of radioactivity . . . Of equal importance, however, is the need to assure that these barriers will not be jeopardized by off-normal occurrences . . . In this regard, the industry strives to protect the plant, the plant operators, and the health and safety of the public by application of a "defense in depth" design philosophy, as required within the variation allowed by the regulatory envelope of rules, procedures, criteria

and standards. A convenient method of describing this "defense in depth" is to discuss it in the broader concept of three levels of safety."

Thus, the authors draw a distinction between multiple barriers against the release of fission products and defense in depth, by associating the latter term with protection of the barriers against off-normal occurrences. The discussion then goes on to say that defense in depth can be conveniently described by discussing it in the broader concept of "three levels of safety." Those three levels are then described as: (1) design for unquestionable safety in normal operation, (2) assume incidents will occur and provide safety systems accordingly, and (3) provide additional safety systems to protect against hypothetical accidents where level two safety systems are assumed to fail. These three levels of safety clearly equate to the three lines of defense described by Clifford Beck in his 1967 paper. Also like Beck, the term "defense in depth" is not associated directly with those levels of safety. There are differences, however. While Beck treats defense in depth as a subsidiary element of the first line of defense, and cites the four fission product barriers as an example, WASH-1250 treats defense in depth as the things that are done to protect the barriers, rather than the barriers themselves. The Internal Study Group, on the other hand, equates defense in depth with the lines of defense (Beck's term) or levels of safety (WASH-1250 term). Similarly, the AEC staff testimony in the ECCS hearings firmly equates defense in depth with the same "three lines of defense" described by Beck.

#### Other Documents Examined

One of the interesting aspects of the history of "defense in depth" is that it often does not appear where it logically might be expected. Title 10, as described earlier, is one example. I could find no occurrences of the term in the Statements of Consideration of 10 CFR 50 Appendix A, although it does occur in the SOC for the final rule on Disposal of High Level Radioactive Wastes in Geologic Repositories, 10 CFR 60 (48 FR 28194-28299). It is interesting to note that both Appendix R and Part 60 were added to Title 10 at about the same time, early 1980s, and are thus relatively recent additions.

The occurrence, or more precisely the lack of occurrence, of "defense-in-depth" in other historical documents is equally interesting. David Okrent's history of light water reactor safety covers the time period from the early 1960's to 1977. As far as I could determine, the only appearance of the term is in a quotation from a 1977 document prepared by the United Kingdom's Nuclear Installation Inspectorate. That document, in describing generic pressurized water reactor safety issues, refers to the containment as "the last of a series of defenses in depth . . .". In Okrent's discussion of AEC and ACRS activities there are references to "several levels of safety," but the term defense in depth is not used. Similarly, the "Report of the Advisory Task Force on Power Reactor Emergency Cooling," the so-called Ergen Committee report, completed in 1967, does not use the term defense in depth. There is a discussion of the same three levels of safety discussed in Clifford Beck's paper, and later in WASH-1250, but "defense in depth" is not used.

The term "defense in depth" appears ten times in the section of the Standard Review Plans on fire protection (Section 9.5.1) and only twice in the section on containments (Section 6.2). In the latter case it is simply used to describe the containment as the "final barrier in the defense in depth concept," in two different places.

The term occurs in three Commission Policy Statements: the Final PRA Policy Statement, the Safety Goal Policy Statement and the Advanced Nuclear Power Plant Policy Statement. None of these documents offer a definition of defense in depth, except by example or implication. The implied definitions in all three policy statements are somewhat different, but not inconsistent with other historical examples. For example, the Commission Policy on Regulation of Advanced Reactors contains the following statement: "Among the attributes that could assist in establishing the acceptability or licensability of a proposed advanced reactor design . . . are . . . [d]esigns that incorporate defense-in-depth philosophy by maintaining multiple barriers against radiation release, and by reducing the potential for and consequences of severe accidents."

The Safety Goal Policy Statement associates defense-in-depth with compensating for uncertainty in probabilistic analyses. The policy states, in part, ". . . it is necessary that proper

attention be given not only to the range of uncertainty surrounding probabilistic estimates, but also to the phenomenology that most influences uncertainties. . . . The results of sensitivity studies should be displayed showing, for example, the range of variation together with the underlying science or engineering assumptions that dominate this variation. [J]udgements can be made by the decisionmaker about the degree of confidence to be given to these estimates and assumptions. . . . This defense in depth approach is expected to continue to ensure the protection of public health and safety."

The PRA policy statement stipulates that the use of PRA technology should support the "NRC's traditional defense-in-depth philosophy." The policy statement recognizes that "complete reliance for safety cannot be placed on any single element of the design, maintenance, or operation of a nuclear power plant." The statement goes on to note that ". . . PRA technology will continue to support the NRC's defense-in-depth philosophy by allowing quantification of the levels of protection and by helping to identify and address weaknesses or overly conservative regulatory requirements . . ." The policy statement specifically recognizes "the philosophy of a multiple-barrier approach against fission product release," and notes that such barrier principles are mandated by the Nuclear Waste Policy Act of 1982.

#### 10 CFR Part 60, Statements of Consideration

As noted earlier, "defense in depth" does appear in the statements of Consideration for 10 CFR 60. In this case defense in depth appears to be defined in terms of multiple barriers (as much systematic as physical), and the concept of balance is introduced. Specifically, the SOC for the final rule (48 FR 28194-28299), contain the statement: "The Commission suggested that a course that would be "reasonable and practical" would be to adopt a "defense-in-depth" approach that would prescribe minimum performance standards for each of the major elements of the geologic repository, in addition to prescribing the EPA standard as a single overall performance standard. . . . There was general acceptance of the Commission's multiple barrier approach, with its identification of two major engineered barriers (waste package and underground facility) in addition to the natural barrier provided by the geologic setting." Later the SOC state "There is nothing inconsistent between the multiple

barrier, defense-in-depth approach and a unitary EPA standard . . ." The description here clearly includes the concept of defense in depth as multiple barriers.

### Post-TMI Definitions and Examples

In approximately the same time frame that Part 60 was published, R.J. Breen, Deputy Director of EPRI's Nuclear Safety Analysis Center, published a paper titled "Defense in Depth Approach to Safety in Light of the Three Mile Island Accident (Nuclear Safety, Vol. 22, No. 5, Sept.-Oct. 1981). Breen refers to defense in depth as a "concept," and states that ". . . the principle of guarding against unwanted events by providing successive protective barriers is frequently called "defense in depth." Breen acknowledges that there are various ways of describing the application of defense in depth, and then chooses a "fairly common three level description emphasizing functions," which he lists as:

- (1) Preventing initiation of incidents (conservative design margins, etc.)
- (2) Capability to detect and terminate incidents
- (3) Protecting the public.

Breen then goes on to pose the question, to what extent can defense in depth be quantified? He appears to accept without question that one of the functions of PRA, when the technology is more fully developed, is to help quantify defense in depth. Until that time arrives, when confronted with a long list of possible safety enhancements, the problem is to determine which activities make the greatest contribution to safety. He mentions that NRC used a point system in NUREG-660, and then goes on to describe a ranking system developed by NSAC and the Atomic Industrial Forum. The system was based on (1) the number of important accident sequences affected, (2) the likelihood that the specified action can be implemented and will reduce risk, (3) a downside assessment (hazards or risks that may result from implementing a proposed action), and (4) the time required to implement the proposed action.

Two aspects of this paper are worthy of note relative to the questions currently being considered regarding defense in depth. The first is that Breen believed that defense in depth should be quantifiable. He saw PRA as one way of doing the quantification,

but he also identified alternatives that were available at the time. The second point is that Breen's definition of defense in depth was essentially the same as that used in WASH-1250, the 1969 Internal Study Group report, and the AEC staff's testimony in the Interim Acceptance Criteria for Emergency Core Cooling Systems.

### Addressing Limitations

Another paper that appeared about the same time as the Breen article mentioned above was one by Stan Kaplan, "Safety Goals and Related Questions," Reliability Engineering, 1982. Although the paper deals with "safety goals" as opposed to "defense in depth," I believe it states a principle that cannot be ignored when we are trying to determine what limits should be placed on requirements in the name of defense in depth. Kaplan argues that the question of "how safe is safe enough" can never be answered without consideration of all available alternatives, including the costs, benefits, and damages for each alternative. The essential point is that evaluation of a proposed safety requirement, in the name of defense in depth or some other high principle, ultimately must consider the question of cost.

### NUREG/CR-6042, Perspectives on Reactor Safety, 1994

A recent summary of the history and application of defense in depth is contained in NUREG/CR-6042, "Perspectives on Reactor Safety," by F. E. Haskin (University of New Mexico) and A. L. Campbell (Sandia National Laboratory), 1994. The document describes a one week course in reactor safety concepts offered by the NRC Technical Training Center. It is significant in the context of examining the issue of defense in depth for two reasons. The first is that the authors, in developing their discussion of defense in depth and in coming to their conclusions, examined that same history that has been partially recounted here. The second is that it represents what is being taught to NRC employees regarding the definition and application of defense in depth.

NUREG/CR-6042 introduces defense in depth by listing ". . . the key elements of an overall safety strategy that began to emerge in the early 1950s and has become known as defense in depth." The key elements listed are accident prevention, safety systems,

containment, accident management, and siting and emergency plans. This picture of defense in depth is consistent with that described in WASH-1250 and other documents which considered defense in depth as "multiple levels of safety." NUREG/CR-6042 also associates defense in depth with multiple barriers or layers, as opposed to the systematic view just mentioned. The barriers identified, each with an associated function, are: ceramic fuel pellets, metal cladding, reactor vessel and piping, containment, exclusion area, low population zone and evacuation plan, and population center distance.

#### INSAG -3, 1988

Finally, in considering the history and definition of defense in depth, it is worth noting the description by the International Nuclear Safety Advisory Group in INSAG-3, "Basic Safety Principles for Nuclear Power Plants," IAEA, 1988. INSAG-3 states, "All safety activities, whether organizational, behavioural or equipment related, are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large. This idea of multiple levels of protection is the central feature of defence in depth, and it is repeatedly used in the specific safety principles that follow."

The document then goes on to state the principle of defense in depth: "To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred on several levels of protection including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barrier by averting damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective." The preceding definition appears to be entirely consistent with what one might derive from the history recounted in this memorandum.

Chairman Jackson has also recently provided her thoughts on defense in depth. In a July 22, 1997 talk at the MIT Nuclear Power Reactor Safety Course, she states, "The defense-in-depth concept should be viewed as complementary to risk-informed,



performance-based approaches, as opposed to a competitive process. . . . Defense-in-depth is a design and operational concept that ensures that successive compensatory measures are incorporated to mitigate potential failures. . . . The notion of Probabilistic Risk Assessment results being used to compromise the defense-in-depth concept is related to the issue of uncertainty (emphasis in original). The magnitude of a single number cannot be used to eliminate safety barriers without due consideration of uncertainty. Multiple barriers provide assurance against catastrophic events."

### Conclusions

There are a number of conclusions and some inferences one can draw from the preceding historical perspective. While acknowledging that many of them already have been stated by other writers, I include them here for the sake of completeness.

First, there is no "best" or "most acknowledged" definition for defense in depth. The closest one comes to a common definition is the "three levels of safety" described by a number of authors relative (primarily) to nuclear power plant design: (1) design, build and operate so the probability of an accident is small, (2) provide protection systems for unexpected behavior, (3) provide engineered safety features to mitigate consequences of postulated accidents. However, few writers firmly equate defense in depth with these three levels; rather these levels are used to set the context for discussing defense in depth. All the "definitions," discussions, and examples are similar, yet each is a little different.

The concept of "multiple barriers" is frequently cited as an example or illustration of defense in depth. Most often, the reference is to the fission product barriers in a nuclear power plant: fuel matrix, clad, primary coolant system, and containment. Other examples are mentioned where the barriers are at least in part systematic as well as physical.

Defense in depth is most often characterized as a concept, an approach, a philosophy, or a principle, and is most frequently defined by example.

None of the discussions, definitions or examples of defense in depth which were reviewed contained any element of limitation. Limits on what can be or should be demanded in the name of defense in depth were not mentioned.

Distribution:

ACRS

ACNW

Staff

Fellows

## POLICY STATEMENTS

meeting the objectives of 10 CFR 26.10; or

10. Threats of discrimination or restrictive agreements which are violations under NRC regulations such as 10 CFR 50.7(f).

**D. Severity Level IV—Violations involving for example:**

1. Incomplete or inaccurate information of more than minor significance that is provided to the NRC but not amounting to a Severity Level I, II, or III violation;
2. Information that the NRC requires be kept by a licensee and that is incomplete or inaccurate and of more than minor significance but not amounting to a Severity Level I, II, or III violation;
3. An inadequate review or failure to review under 10 CFR Part 27 or other procedural violations associated with 10 CFR Part 21 with more than minor safety significance;
4. Violations of the requirements of Part 26 of more than minor significance;
5. A failure to report acts of licensed operators or supervisors pursuant to 10 CFR 26.73; or
6. Discrimination cases which, in themselves, do not warrant a Severity Level III categorization.

### Supplement VIII—Emergency Preparedness

This supplement provides examples of violations in each of the four severity levels as guidance in determining the appropriate severity level for violations in the area of emergency preparedness. It should be noted that citations are not normally made for violations involving emergency preparedness occurring during emergency exercises. However, where exercises reveal (i) training, procedural, or repetitive failures for which corrective actions have not been taken, (ii) an overall concern regarding the licensee's ability to implement its plan in a manner that adequately protects public health and safety, or (iii) poor self-critiques of the licensee's exercises, enforcement action may be appropriate.

**A. Severity Level I—Violations involving for example:**

In a general emergency, licensee failure to promptly (1) correctly classify the event, (2) make required notifications to responsible Federal, State, and local agencies, or (3) respond to the event (e.g., assess actual or potential offsite consequences, activate emergency response facilities, and augment shift staff).

**B. Severity Level II—Violations involving for example:**

1. In a site emergency, licensee failure to promptly (1) correctly classify the event, (2) make required notifications to responsible Federal, State, and local agencies, or (3) respond to the event (e.g., assess actual or potential offsite consequences, activate emergency response facilities, and augment shift staff); or

2. A licensee failure to meet or implement one emergency planning standard involving assessment or notification.

**C. Severity Level III—Violations involving for example:**

1. In an alert, licensee failure to promptly (1) correctly classify the event, (2) make required notifications to responsible Federal, State, and local agencies, or (3) respond to the event (e.g., assess actual or potential offsite consequences, activate emergency response facilities, and augment shift staff);

2. A licensee failure to meet or implement more than one emergency planning standard involving assessment or notification; or

3. A breakdown in the control of licensed activities involving a number of violations that are related (or, if isolated, that are recurring violations) that collectively represent a potentially significant lack of attention or carelessness toward licensed responsibilities.

**D. Severity Level IV—Violations involving for example:**

A licensee failure to meet or implement any emergency planning standard or requirement not directly related to assessment and notification.

Dated at Rockville, Maryland, this 23rd day of June 1995.

For the Nuclear Regulatory Commission.

John C. Hoyle,

Secretary of the Commission.

60 FR 42622  
Published 8/16/95  
Effective 8/16/95

### Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement

AGENCY: Nuclear Regulatory Commission.

ACTION: Final policy statement.

**SUMMARY:** This statement presents the policy that the Nuclear Regulatory Commission (NRC) will follow in the use of probabilistic risk assessment (PRA) methods in nuclear regulatory matters. The Commission believes that an overall policy on the use of PRA methods in nuclear regulatory activities should be established so that the many potential applications of PRA can be implemented in a consistent and predictable manner that would promote regulatory stability and efficiency. In addition, the Commission believes that the use of PRA technology in NRC regulatory activities should be increased to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's

## POLICY STATEMENTS

deterministic approach. The pertinent comments received from the published draft policy statement are reflected in this final policy statement. This policy statement will be implemented through the execution of the NRC's PRA Implementation Plan.

**EFFECTIVE DATE:** August 16, 1995.

**ADDRESSES:** The proposed policy statement and the comments received may be examined at: NRC Public Document Room, 2120 L Street, NW. (Lower Level), Washington, DC.

**FOR FURTHER INFORMATION CONTACT:** Anthony Hsia, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, Washington, DC 20555. Telephone (301) 415-1075.

### SUPPLEMENTARY INFORMATION:

- I. Background.
- II. Summary of Public Comments and NRC Responses.
- III. Deterministic and Probabilistic Approaches to Regulation.
- IV. The Commission Policy.
- V. Availability of Documents.

#### I. Background

The NRC has generally regulated the use of nuclear material based on deterministic approaches. Deterministic approaches to regulation consider a set of challenges to safety and determine how those challenges should be mitigated. A probabilistic approach to regulation enhances and extends this traditional, deterministic approach, by: (1) Allowing consideration of a broader set of potential challenges to safety, (2) providing a logical means for prioritizing these challenges based on risk significance, and (3) allowing consideration of a broader set of resources to defend against these challenges.

Until the accident at Three Mile Island (TMI) in 1979, the Atomic Energy Commission (now the NRC), only used probabilistic criteria in certain specialized areas of licensing reviews. For example, human-made hazards (e.g., nearby hazardous materials and aircraft) and natural hazards (e.g., tornadoes, floods, and earthquakes) were typically addressed in terms of probabilistic arguments and initiating frequencies to assess site suitability. The Standard Review Plan (NUREG-0800) for licensing reactors and some of the Regulatory Guides supporting NUREG-0800 provided review and evaluation guidance with respect to these probabilistic considerations.

The TMI accident substantially changed the character of the analysis of severe accidents worldwide. It led to a substantial research program on severe accident phenomenology. In addition,

both major investigations of the accident (the Kemeny and Rogovin studies) recommended that PRA techniques be used more widely to augment the traditional nonprobabilistic methods of analyzing nuclear plant safety. In 1984, the NRC completed a study (NUREG-1050) that addressed the state-of-the-art in risk analysis techniques.

In early 1991, the NRC published NUREG-1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants." In NUREG-1150, the NRC used improved PRA techniques to assess the risk associated with five nuclear power plants. This study was a significant turning point in the use of risk-based concepts in the regulatory process and enabled the Commission to greatly improve its methods for assessing containment performance after core damage and accident progression. The methods developed for and results from these studies provided a valuable foundation in quantitative risk techniques.

PRA methods have been applied successfully in several regulatory activities and have proved to be a valuable complement to deterministic engineering approaches. This application of PRA represents an extension and enhancement of traditional regulation rather than a separate and different technology. Several recent Commission policies or regulations have been based, in part, on PRA methods and insights. These include the Backfit Rule (§ 50.109, "Backfitting"), the Policy Statement on "Safety Goals for the Operation of Nuclear Power Plants" (51 FR 30028; August 21, 1986), the Commission's "Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants" (50 FR 32138; August 8, 1985), and the Commission's "Final Policy Statement on Technical Specifications Improvement for Nuclear Power Reactors" (58 FR 39132; July 22, 1993). PRA methods also were used effectively during the anticipated transient without scram (ATWS) and station blackout (SBO) rulemaking, and supported the generic issue prioritization and resolution process. Additional benefits have been found in the use of risk-based inspection guides to focus NRC inspector efforts and make more efficient use of NRC inspection resources. Probabilistic analyses were extensively used in the development of the recently proposed rule change to reactor siting criteria in 10 CFR Part 100 (59 FR 52255; October 17, 1994). The proposed rule change invoked the use of a probabilistic approach to estimate the Safe Shutdown Earthquake Ground Motion for a nuclear reactor site, instead

of the purely deterministic method currently specified in Appendix A to 10 CFR Part 100.

Currently, the NRC is using PRA techniques to assess the safety importance of operating reactor events and is using these techniques as an integral part of the design certification review process for advanced reactor designs. In addition, the Individual Plant Examination (IPE) program and the Individual Plant Examination—External Events (IPEEE) program (an effort resulting from the implementation of the Commission's "Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants") have resulted in commercial reactor licensees using risk-assessment methods to identify any vulnerabilities needing attention.

The Commission has been developing performance assessment methods for low-level and high-level waste since the mid-1970s and these activities intensified using performance assessments techniques in the late 1980s and early 1990s. This has involved the development of conceptual models and computer codes to model the disposal of waste. Because waste-disposal systems are passive, certain analysis methods used for active systems in PRA studies for power reactors had to be adapted to provide scenario analysis for the performance assessment of the potential geologic repository at Yucca Mountain, Nevada. In regard to high-level waste, the NRC staff participates in a variety of international activities (e.g., the Performance Assessment Advisory Group of the Organization for Economic Cooperation and Development, Nuclear Energy Agency) to ensure that consistent performance assessment methods are used to the degree appropriate.

The Commission believes that an overall policy on the use of PRA in nuclear regulatory activities should be established so that the many potential applications of PRA methodology can be implemented in a consistent and predictable manner that promotes regulatory stability and efficiency and enhances safety. In May 1994, the NRC staff forwarded a draft PRA policy statement to the Advisory Committee on Reactor Safeguards (ACRS) for review and briefed ACRS on the same subject. On August 18, 1994, the NRC staff proposed a PRA policy statement to the Commission in SECY-94-218, "Proposed Policy Statement on the Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities." In that Commission paper, the staff proposed that an overall policy on the use of probabilistic risk

## POLICY STATEMENTS

assessment (PRA) methods in nuclear regulatory activities should be established and that the use of PRA technology in NRC regulatory activities should be increased. Comments from the ACRS regarding the policy statement as documented in a letter dated May 11, 1994, were incorporated. On August 19, 1994, the staff forwarded SECY-94-219, "Proposed Agency-Wide Implementation Plan for Probabilistic Risk Assessment (PRA)," to the Commission. On August 30, 1994, the staff discussed the PRA policy statement and the PRA implementation plan in a public meeting with the Commission. On September 13 and October 4, 1994, the Secretary issued two staff requirements memoranda (SRMs) providing Commission guidance regarding the draft policy statement. In these SRMs, the Commission directed the staff to revise the proposed PRA policy statement, publish the policy statement for public comment in the Federal Register, and conduct a public workshop on the PRA implementation plan.

As directed by the Commission, the staff conducted a public workshop on December 2, 1994, to discuss the PRA implementation plan. The purpose of the workshop was to inform the public of NRC activities related to increasing the use of PRA methods and techniques in regulatory applications and to receive public comments on these activities. After the staff incorporated the comments from the SRMs, the proposed policy statement "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities" was published in the Federal Register on December 8, 1994 (59 FR 63389). The public comment period expired on February 7, 1995.

### II. Summary of Public Comments and NRC Responses

In January and February 1995, the NRC received 17 letters commenting on the proposed policy statement on "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities". These comments were from the following organizations: Six utilities—PECO Energy Company, Detroit Edison, Washington Public Power Supply System, Carolina Power and Light Company, Virginia Power Company, and Centor Energy; three State regulatory agencies—State of Illinois Department of Nuclear Safety, State of New Jersey Department of Environmental Protection, State of Nevada Agency for Nuclear Projects; two industry groups—Nuclear Energy Institute and Westinghouse Owners Group; two engineering firms—PLG,

Inc. and ICF Kaiser Engineers, Inc.; University of California at Los Angeles; Ohio Citizens For Responsible Energy; Winston and Strawn, Counsel to the Nuclear Utility Backfitting and Reform Group; and the Department of Energy. Copies of the letters may be examined at the NRC Public Document Room at 2120 L Street., NW. (Lower Level), Washington, DC.

### General Comments

Twelve commenters explicitly supported the basic tenet of the policy to increase the use of PRA technology in NRC's regulatory activities. The other commenters did not object to the policy statement but provided recommendations for the NRC to modify and improve the policy statement and/or the PRA implementation plan. Five commenters indicated that they agreed with the NEI comments on the proposed PRA policy statement. The NRC staff has reviewed the comments and summarized them in the following areas. The staff response to the comments are also included in this final policy statement.

### Use of PRA in Regulatory Decisions

Several comments dealt with the scope of the PRA applications (where can PRA be used) and the implementation of the policy statement (how can PRA be used).

One commenter felt that neither the policy statement nor the PRA implementation plan provided consistent decision criteria for accepting PRA results as part of the justification for licensing decisions. The commenter was concerned that the short term effect of the policy statement would likely be an increased burden on the licensees. For the long term, the commenter recommended a systematic review of the rules and regulations to identify opportunities for elimination of unnecessary regulations. The proposed policy statement directed the staff to use PRA and associated analyses, where appropriate, as part of the justification for licensing decisions. The PRA implementation plan describes how the stated policy is to be implemented. Appropriate decision criteria will be developed and documented as part of the PRA implementation plan. The Commission has already performed a systematic review of the many current rules and regulations to identify opportunities for the elimination of unnecessary regulations. In 1993, the NRC established the Regulatory Review Group (RRG) to conduct a structured review of power reactor regulations with special attention on the opportunity to reduce unnecessary regulatory burdens.

The RRG recommendations to reduce the regulatory burden included the suggestion to use more risk-based approaches in quality assurance, inservice inspection and testing, and the concept of a PRA plan. The RRG recommendations were documented in SECY-94-003. To better focus the NRC's effort on the PRA related activities recommended by the RRG, the PRA Working Group, and the Regulatory Analysis Steering Group, the PRA implementation plan was developed in 1994. The implementation plan included a task to develop guidelines for determining when it is practical to use PRA technology and results in regulatory activities. The NRC has had discussions with volunteer licensees regarding the pilot applications of risk-based regulatory initiatives. Results from the pilot applications will be incorporated in the NRC's guidance for PRA applications in regulatory activities. A number of current regulatory requirements are being considered as part of the PRA implementation plan to determine if alternative risk-based approaches are practical. Over time, the Commission would expect some streamlining and refocusing of its rules and regulations as part of this process. The Commission has implemented a continuing regulatory improvement program which is responsive to the commenter's recommendation of a systematic examination of marginal regulatory requirements.

Another commenter recommended that the policy statement be amended to state that when backfitting analyses are performed, mean risk levels be the exclusive basis of regulatory decision-making when comparisons are made against the \$1000/person-rem criterion. The Commission does not feel this policy statement needs to address the issue regarding the use of mean risk level as the exclusive basis for applying the \$1000/person-rem criterion because the Commission's safety goal policy statement has already spoken to the use of mean values of risk in connection with the cost-benefit analyses. Furthermore, this issue is addressed in the proposed Revision 2 of NUREG/BR-0058, "Regulatory Analysis Guidelines of the U. S. Nuclear Regulatory Commission, Draft Report for Comment." This commenter also recommended that the policy statement should direct the staff to use the relevant plant specific PRA in assessing the need for any backfitting action at that plant. For generic backfits, this commenter recommended that the policy should allow licensees to take

## POLICY STATEMENTS

credit for plant specific information to justify relief from NRC imposed action. The Commission believes that the use of the plant specific PRA in the backfit analysis to evaluate whether there is a substantial increase in the overall protection or to justify relief from NRC imposed action is acceptable when combined with other relevant deterministic considerations, as appropriate.

Regarding the use of safety goals, one commenter recommended retention of the language in SECY-94-218 to effect that safety goals could be used in granting relief from unnecessary requirements. Another commenter recommended that the safety goals should be used as a minimum goal, rather than the maximum level of safety. As stated in the proposed PRA policy statement published on December 8, 1994, the Commission's safety goals are " \* \* \* intended to be generically applied by the NRC as opposed to plant specific applications," and " \* \* \* to be used with appropriate consideration of uncertainties in making regulatory judgements in the context of backfitting new generic requirements on nuclear power plant licensees." In the Staff Requirement Memorandum (SRM) dated June 15, 1990, regarding the implementation of safety goals, the Commission directed that "Safety goals are to be used in a more generic sense and not to make specific licensing decisions." Therefore, at this time, the NRC would use the safety goals in making regulatory decisions regarding backfitting new generic requirements but not to make specific licensing decisions including granting relief from unnecessary requirements. Any changes to the safety goal policy are outside the scope of the PRA policy statement and would, therefore, need to be pursued independently.

Referring to paragraphs 1 and 2 of the proposed policy statement, a commenter suggested that it should include the application to NRC enforcement decisions, including the severity levels. As noted in NUREG-1525, "Assessment of the NRC Enforcement Program," the Commission does not support defining severity levels using PRA results. The NRC's basis for severity level categorization clearly is safety significance. In judging safety significance, the NRC considers (1) Actual consequences, (2) potential consequences, and (3) regulatory significance. It is recognized that PRA results may be helpful to provide risk insights on the likelihood and significance of potential consequences. The NRC plans to continue to consider the use of PRA results where relevant as

part of the integrated process considering all facets surrounding the violation in support of enforcement decisions.

Several commenters discussed the role of PRA in reducing the unnecessary conservatism in regulations and to support additional regulatory requirements. One commenter's concern was that the proposed policy statement appeared to be biased in the direction of using PRA to support deregulation. Another commenter was concerned with the implication that PRA could result in an additional layer of regulation. The policy statement addressed the need to remove unnecessary conservatism associated with regulatory requirements. It is not the Commission's intent to replace traditional defense-in-depth concepts with PRA, but rather to exploit the use of PRA insights to further understand the risk and improve risk-effective safety decision-making in regulatory matters. In doing so, the Commission is focusing its attention and resource allocation to areas of true safety significance. Where appropriate, PRA should be used to support additional regulatory requirements, according to 10 CFR 50.109 (Backfit Rule).

One commenter recommended that the policy statement should explicitly state that the use of PRA by licensees in regulatory matters is at the discretion of each licensee. The commenter also believed that the NRC should not prescribe how and when PRA methods should be used by licensees in regulatory matters, but should address the potential impact the expanded use of PRA may have on regulatory interactions with licensees. The Commission's PRA policy statement is intended only to encourage the NRC staff and industry to use probabilistic risk assessment methods in regulatory matters. It is not intended to prescribe or require any of the many potential PRA applications. Any requirements for licensees to perform PRA analyses would be expected to occur through formal rulemaking.

One commenter's concern was that there was a wide range of applications for which PRA was being applied without consistency and standards. This commenter urged the NRC to insist on quality PRAs commensurate with the intended applications and to develop standards which require rigorous and living PRAs by regulation for nuclear power plant applications. The commenter also questioned whether the PRA analyses for the IPE may be used for other applications because of a lack of PRA standards. Another commenter expressed the concern that strict

conformance to detailed PRA standards would not be desirable, and recommended that flexibility in PRA models should be allowed. The Commission issued Generic Letter (GL) 88-20 with the primary purpose of generating IPEs to identify severe accident vulnerabilities. The PRAs which supported the IPE efforts may be useful for other applications, however, this would have to be evaluated on a case-by-case basis under well-defined objectives. After the Commission briefing on the IPE program, the Commission recognized, as stated in the SRM dated April 28, 1995, that current industry IPE results do not provide a complete basis for supporting risk-based regulatory decision-making. The SRM suggested that " \* \* \* the industry should, in coordination with the staff, initiate the actions necessary to develop PRAs that are acceptable for risk-based regulatory use (i.e., standardized methods, assumptions, level of detail)." The industry is encouraged to formulate a general approach for performing PRAs acceptable for regulatory use. This approach should include guidance on standardizing approaches for use of PRA techniques for specific applications, narrowing some of the variability in the IPE results, and strengthening its usefulness in the regulatory and safety decision-making process. The Commission is currently considering the quality level and scope of assessment necessary to justify use of specific PRAs for specific regulatory applications. The Commission will require PRA quality commensurate with the proposed application.

### *PRA Methodology*

One commenter agreed with the NRC that the probabilistic approach should be used to complement the deterministic approach and that PRA numbers alone should not be used to make regulatory decisions. The commenter also believed that uncertainties should not prevent or delay the implementation of PRA in regulatory activities. The Commission understands that uncertainties exist in any regulatory approach. These uncertainties are derived from knowledge limitations that are not created by PRA, but are often exposed by it. The PRA implementation plan has provided a framework to assess the significance of potential uncertainties and to develop a strategy to accommodate them in the regulatory process.

One commenter stated that probabilistic analysis is simply an extension of deterministic analysis. They are not separate and distinctive

## POLICY STATEMENTS

concepts. The Commission agrees with this concept as the proposed policy statement stated that "The probabilistic approach to regulation is, therefore, considered an extension and enhancement of traditional regulation by considering risk in a more coherent and complete manner." The Commission believes that the PRA method plays a complementary role in relationship to the deterministic method. This was reflected in the policy statement that "Deterministic-based regulations have been successful in protecting the public health and safety and PRA techniques are most valuable when they serve to focus the traditional, deterministic-based, regulations and support the defense-in-depth philosophy."

One commenter recommended that the most efficient use of NRC resources should be to enhance or improve the existing methods, but not to develop new ones. The Commission's principal focus will be on improving the existing methods, but some new methods development may also be useful.

Another commenter recommended that the PRA policy statement should seek a uniform and standard application of PRA within the NRC, and begin with a commitment to ensure that PRA is used consistently and is not ignored when required by those unfamiliar or reluctant to apply it. The Commission's PRA policy statement specifically emphasizes the need for consistent and predictable application of PRA within the Commission to promote regulatory stability and efficiency. The Commission believes that this goal can be achieved through the implementation plan which will ensure that the appropriate use of PRA is implemented by the staff.

### *Schedule of PRA Activities*

Two letters commented that the activities discussed in the PRA implementation plan appeared to be on a protracted schedule and recommended that priority and urgency be stressed and reflected in the plan, including the use of PRA and PRA insights in the near term. The Commission's PRA implementation plan showed the target completion dates for all the tasks. The Commission fully realizes the need for near term PRA applications and has included them in the implementation plan wherever possible. These milestones include examples such as pilot applications for risk-based initiatives and transfer of IPE insights to NRC staff members for use in regulatory matters in the near term. The Commission plans to periodically review the progress of the "living" PRA

implementation plan and, as appropriate, to adjust the priorities.

One letter commented that the NRC review and approval of licensing actions that are based on PRA insights should not be contingent upon the schedule for implementation of the plan. The plan should not be an impediment to moving forward toward the goals outlined in the policy statement. The Commission's implementation plan had been developed to effectively and expeditiously establish a framework for increasing the use of PRA technology inside the Commission. Since it is a "living" plan, new tasks could be added and existing tasks could be modified, as the plan progresses. The Commission agrees that the plan should not be an impediment to moving forward to achieve the goals stated in the policy. The Commission welcomes risk-based regulatory initiatives from the industry as the plan is being carried out and will adjust resources, as appropriate.

One commenter asked how the NRC will propose to control the utilities' application of PRA and the timeframe to implement the consistent use of PRA within the NRC. The Commission's PRA implementation plan describes the activities and schedule to effect a coherent and consistent PRA application within the agency. As the plan is implemented, the NRC expects to interact with licensees and publish guidelines for the application of PRA in their submittal to the NRC.

### *PRA Training*

Two commenters advocated PRA training for appropriate NRC and licensee staff as soon as possible to ensure proper application of PRA in regulatory matters. A PRA training program has been in place for the NRC staff for a number of years. As part of the PRA implementation plan, the existing training program is being enhanced. The existing PRA training curriculum serves as the basis on which to build a more comprehensive staff PRA training program. Six new courses have been incorporated in the training program to address the short term needs from the increasing use of PRA in regulatory activities. As a result of the PRA implementation plan, the number of NRC staff participating in the training program has increased significantly during the first half of fiscal year 1995.

One commenter recommended that NRC's PRA training should be extended to State agencies that can justify attendance. Historically, attendance at NRC courses has been routinely available on a space-available, no-cost basis to State personnel as well as for other non-NRC personnel (such as

foreign regulators, EPA, DOE, and other Federal personnel). This has included training in the PRA area for a limited number of State regulators. In courses that were under-subscribed by NRC personnel, many had sufficient available space to allow acceptance of outside personnel. Logistics for these arrangements are handled by the NRC office responsible for interactions with the outside group (i.e., Office of State Programs for States or Office of International Programs for foreign personnel). NRC training currently is not available to NRC licensees. Because of recent budgetary constraints, as described in SECY-95-017 "Reinventing NRC Fee Policies," full cost reimbursements from States for NRC training is expected in future years. However, NRC will continue its space-available policy for all courses, including PRA courses.

### *Data Collection*

Several commenters expressed concerns about the potential data collection implications of the proposed PRA policy. They are summarized as follows:

One commenter stated that the desire to collect detailed data related to equipment and human reliability should not prohibit the use of PRA for applications or support for decision-making. The collection of plant-specific data must be commensurate with the benefit that specific information might have on the quality or insight from the PRA. Plant-specific information may not be statistically significant. Furthermore, requiring all plants to collect the same information without a focus based on plant performance, is counter to the concept behind the Maintenance Rule.

Another commenter stated that the discussion of uncertainties in Part II.(B) of the proposed policy statement is appropriate. However, in the implementation of this part of the policy, care must be exercised to restrain from requiring or implying the need for massive plant-specific component level failure rate data collection programs. Several commenters expressed concerns that a new or expanded nuclear power plant experience data collection rulemaking could further burden the licensees and the resulting benefit may well be marginal.

The Commission agrees that it should make every effort to avoid any unnecessary regulatory burdens in connection with collecting reliability and availability data. Specific comments on the types of data that should or should not be collected will be addressed in connection with proposed

## POLICY STATEMENTS

data collection requirements when they are published for comment.

### *Radiation Medicine*

One commenter recommended that NRC should abandon the use of the linear hypothesis in estimating radiation-induced cancer and mutation risk. The commenter further stated that the NRC's PRA implementation plan refers to risk analysis to analyze nuclear medical devices and that, " \* \* \* there are no nuclear medicine devices that have risk to be analyzed."

The International Commission on Radiation Protection, the United Nations Scientific Committee on the Effects of Atomic Radiation, and the National Academy of Sciences' Committee on the Biological Effects of Ionizing Radiation believe that, in the absence of convincing evidence that there is a dose threshold or that low levels of radiation are beneficial, the assumptions regarding a linear nonthreshold dose-effect model for cancers and genetic effects and the existence of thresholds only for certain nonstochastic effects remain appropriate for formulating radiation protection standards. NRC follows their guidelines. Although some data suggest the possible use of other models, there are still many scientists who believe there are insufficient data to deviate from the "linear" hypothesis. The issue of realism involved in continuing the use of the "linear" hypothesis is expected to be a matter of debate over the coming years.

The NRC regulates radiation medicine, which includes both nuclear medicine and radiation oncology. The intent of the policy statement concerning medical applications is to refer to medical devices containing byproduct material, in particular, those used in radiation oncology. The term "nuclear medical device" was revised in the recent status update on the PRA implementation plan (SECY-95-079) and clarified in the policy statement.

### *Nuclear Waste*

One commenter recommended that the NRC expand its use of PRA to other areas such as radiological dose assessment during the site decommissioning process. The NRC intends to consider expansion of PRA techniques into additional areas with the proviso that the application of these techniques to these facilities should be tempered according to the complexity of the disposal system, its uncertainties and the estimated risk.

One commenter provided comments on several aspects of the proposed policy statement in the nuclear waste

area. Regarding the scope of the policy statement, the commenter recommended that the policy statement be amended to include risk assessment applications other than power reactors. The Commission agrees with that comment. The use of PRA should be considered for those applications that involve projecting system performance for very long time periods, such as hundreds or thousands of years. The policy statement stated that the use of PRA technology should be increased in all regulatory matters. Another recommendation was to temper the commitment to PRA to reflect inherent risk differences associated with different waste management facilities. Because of inherent differences in the regulations and practices associated with the licensing of waste management facilities, the application of performance assessment (PRA is called performance assessment for waste management systems) techniques to these facilities should be tempered according to the complexity of the disposal system, uncertainties surrounding the system performance, and the estimated risk. The Commission also agrees with the comments regarding uncertainties in projecting repository performance and the use of technical expert judgment in assessing these uncertainties, but feels the PRA policy statement is not the appropriate forum to discuss these items applicable only to waste management.

Regarding the suggestion of describing the reasons for using the PRA and the application of PRA in regulatory activities, the Commission included the reasons for using PRA in Section III of the policy statement and added a description of the impact of PRA on the rule changes to 10 CFR Part 100 in the background discussion.

Another commenter expressed concern that the proposed policy statement inappropriately encouraged the use of PRA in the licensing and regulation of nuclear waste disposal facilities. The Commission disagrees with this comment since PRA techniques are acceptable in a performance assessment for the geologic repository, but are only part of the requirements for a license. The commenter was also concerned that any new regulations proposed by the Environmental Protection Agency (EPA) and the NRC's 10 CFR Part 80 for a high-level waste (HLW) disposal facility proposed for Yucca Mountain will probably prohibit use of PRA for these facilities because of Type I faults at this site. The Commission anticipates that both probabilistic and deterministic hazard assessment methodologies will be applied to assess the significance of

faulting at Yucca Mountain.

Furthermore, the Commission does not interpret 10 CFR Part 80 so as to preclude the use of PRA as a basis for licensing a proposed repository at Yucca Mountain. The commenter did not agree with NRC's characterization of the waste disposal system as passive and believed that, at this time, there is no alternative to the use of deterministic techniques for waste disposal application because PRA techniques are in the embryonic stage. The "Fault Tree Handbook" (NUREG-0492, January 1981) refers to "passive" as a " \* \* \* mechanism (e.g., wire) whereby the output of one 'active' component becomes the input to a second 'active' component." "Passive" is generally used for "engineered" components that have no moving parts. Since there are no "engineered" components that are "active" (or causing motion in another engineered component) in the post-closure phase of the potential geologic repository at Yucca Mountain, the NRC has applied the traditional PRA concept to the waste disposal system and referred to it as a "passive system." The remanded 1985 EPA Standard, 40 CFR 190, required a probabilistic analysis for a geologic repository. The NRC has developed this type of analysis since 1970 and has attained a state of maturity for these analyses that is accepted by internationally-known organizations (e.g., Organization for Economic Cooperation and Development (OECD)/ Nuclear Energy Agency (NEA)).

A number of editorial comments were received on the role of PRAs in the licensing of waste disposal facilities. The NRC has incorporated the appropriate comments in this final PRA policy statement.

### III. Deterministic and Probabilistic Approaches to Regulation

#### *(A) Extension and Enhancement of Traditional Regulation*

The NRC established its regulatory requirements to ensure that a licensed facility is designed, constructed, and operated without undue risk to the health and safety of the public. These requirements are largely based on deterministic engineering criteria. Simply stated this deterministic approach establishes requirements for engineering margin and for quality assurance in design, manufacture, and construction. In addition, it assumes that adverse conditions can exist (e.g., equipment failures and human errors) and establishes a specific set of design-basis events. It then requires that the licensed facility design include safety systems capable of preventing and/or



## POLICY STATEMENTS

mitigating the consequences of those design-basis events to protect the public health and safety.

The deterministic approach contains implied elements of probability (qualitative risk considerations), from the selection of accidents to be analyzed as design-basis accidents (e.g., reactor vessel rupture is considered too improbable to be included) to the requirements for emergency core cooling (e.g., safety train redundancy and protection against single failure). The approach by the Commission for the use of performance assessment to implement its regulations for disposal of radioactive nuclear waste (10 CFR Part 60 for high-level waste disposal and 10 CFR Part 61 for low-level waste disposal) also contains implied elements of probability. The results of the numerous calculations obtained from a performance assessment for a given performance measure and for a particular type of facility (e.g., a spectrum of values for ground-water travel time or individual dose) are expressed in terms of statistical distributions that express the probability that a given measure of performance will be attained. When this distribution is compared to the appropriate deterministic standard in the Commission's regulations, the probability of not exceeding the standard can be obtained from the part of the distribution that falls below this standard.

PRA addresses a broad spectrum of initiating events by assessing the event frequency. Mitigating system reliability is then assessed, including the potential for multiple and common cause failures. The treatment therefore goes beyond the single failure requirements in the deterministic approach. The probabilistic approach to regulation is, therefore, considered an extension and enhancement of traditional regulation by considering risk in a more coherent and complete manner. A natural result of the increased use of PRA methods and techniques would be the focusing of regulations on those items most important to safety. Where appropriate, PRA can be used to eliminate unnecessary conservatism and to support additional regulatory requirements. Deterministic-based regulations have been successful in protecting the public health and safety and PRA techniques are most valuable when they serve to focus the traditional, deterministic-based, regulations and support the defense-in-depth philosophy. In addition, PRA techniques are appropriately used when considering regulations defined in probabilistic terms, and for estimating

safety of systems with very large uncertainties such as waste disposal systems (Note that PRA is called performance assessment for these waste disposal systems).

Beyond its deterministic criteria, the NRC has formulated guidance, as in the safety goal policy statement, that utilizes quantitative, probabilistic risk measures. The safety goal policy statement establishes top-level objectives to help assure safe operation of nuclear power plants. The safety goals are intended to be applied generically and are not for plant-specific applications. For the purpose of implementation of the safety goals, subsidiary numerical objectives on core damage, frequency and containment performance have been established. The safety goals provide guidance on where plant risk is sufficiently low that further regulatory action is not necessary. Also, as noted above, the Commission has been using PRA in performing regulatory analysis for the proposed backfit of cost-beneficial safety improvements at operating reactors (as required by 10 CFR 50.109) for a number of years.

### *(B) Uncertainties and Limitations of Deterministic and Probabilistic Approaches*

The treatment of uncertainties is an important issue for regulatory decisions. Uncertainties exist in any regulatory approach and these uncertainties are derived from knowledge limitations. These uncertainties and limitations existed during the development of deterministic regulations and attempts were made to accommodate these limitations by imposing prescriptive, and what was hoped to be, conservative regulatory requirements. A probabilistic approach has exposed some of these limitations and provided a framework to assess their significance and assist in developing a strategy to accommodate them in the regulatory process.

Human performance is an important consideration in both deterministic and probabilistic approaches. Assessing the influence of errors of commission and organizational and management issues on human reliability is an example that illustrates where current PRA methods are not fully developed. While this lack of knowledge contributes to the uncertainty in estimated risks, the PRA framework offers a powerful tool for logically and systematically evaluating the sensitivity and importance to risk of these uncertainties. Improved PRA techniques and models to address errors of commission and the influence of organizational factors on human

reliability are currently being developed.

It is important to note that not all of the Commission's regulatory activities lend themselves to a risk analysis approach that utilizes fault tree methods. In general, a fault tree method is best suited for power reactor events that typically involve complex systems. Events associated with industrial and medical uses of nuclear materials generally involve a simple system, involve radiation overexposures, and result from human error, not equipment failure. Because of the characteristics of medical and industrial events, as discussed above, analysis of these events using relatively simple techniques can yield meaningful results. Power reactor events, however, generally involve complex systems and human interactions, can potentially involve more than one adverse consequence, and often result from equipment failures. Therefore, power reactor events can require greater use of more complex risk analysis techniques, such as fault tree analysis, to yield meaningful insights. PRA methods need to be adapted for waste disposal systems because they are passive systems subjected to interlocking natural and man-made processes and events that are dominated by complex phenomenology.

Given the dissimilarities in the nature and consequences of the use of nuclear materials in reactors, industrial situations, waste disposal facilities, and medical applications, the Commission recognizes that a single approach for incorporating risk analyses into the regulatory process is not appropriate. However, PRA methods and insights will be broadly applied to ensure that the best use is made of available techniques to foster consistency in NRC risk-based decision-making.

### *(C) Defense-in-Depth Philosophy*

In the defense-in-depth philosophy, the Commission recognizes that complete reliance for safety cannot be placed on any single element of the design, maintenance, or operation of a nuclear power plant. Thus, the expanded use of PRA technology will continue to support the NRC's defense-in-depth philosophy by allowing quantification of the levels of protection and by helping to identify and address weaknesses or overly conservative regulatory requirements applicable to the nuclear industry. Defense-in-depth is a philosophy used by NRC to provide redundancy for facilities with "active" safety systems, e.g., a commercial nuclear power, as well as the philosophy of a multiple-barrier approach against fission product

## POLICY STATEMENTS

releases. Such barrier principles are mandated by the Nuclear Waste Policy Act of 1982, which provides redundancy for a geologic repository to contain and isolate nuclear waste from the human environment.

### IV. The Commission Policy

Although PRA methods and information have thus far been used successfully in nuclear regulatory activities, there have been concerns that PRA methods are not consistently applied throughout the agency, that sufficient agency PRA/statistics expertise is not available, and that the Commission is not deriving full benefit from the large agency and industry investment in the developed risk assessment methods. Therefore, the Commission believes that an overall policy on the use of PRA in nuclear regulatory activities should be established so that the many potential applications of PRA can be implemented in a consistent and predictable manner that promotes regulatory stability and efficiency. This policy statement sets forth the Commission's intention to encourage the use of PRA and to expand the scope of PRA applications in all nuclear regulatory matters to the extent supported by the state-of-the-art in terms of methods and data. Implementation of the policy statement will improve the regulatory process in three areas: Foremost, through safety decision making enhanced by the use of PRA insights; through more efficient use of agency resources; and through a reduction in unnecessary burdens on licensees.

Therefore, the Commission adopts the following policy statement regarding the expanded NRC use of PRA:

(1) The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.

(2) PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices. Where appropriate, PRA should be used to support the proposal for additional regulatory requirements in accordance with 10 CFR 50.109 (Backfit Rule). Appropriate procedures for including PRA in the process for

changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations shall be complied with unless these rules and regulations are revised.

(3) PRA evaluations in support of regulatory decisions should be as realistic as practicable and appropriate supporting data should be publicly available for review.

(4) The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments on the need for proposing and backfitting new generic requirements on nuclear power plant licensees.

### Policy Implications

There are several important regulatory or resource implications that follow from the goal of increased use of PRA techniques in regulatory activities. First, the NRC staff, licensees, license applicants, and Commission must be prepared to consider changes to regulations, to guidance documents, to the licensing process, and to the inspection program. Second, the NRC staff and Commission must be committed to a shift in the application of resources over a period of time based on risk findings. Third, the NRC staff must undertake a training and development program, which may include recruiting personnel with PRA experience, to significantly enhance the PRA expertise necessary to implement these goals. Additionally, the NRC staff must continue to develop new and improved PRA methods and regulatory decision-making tools and must significantly enhance the collection of equipment and human reliability data for all of the agency's risk assessment applications, including those associated with the use, transportation, and storage of nuclear materials. However, it is recognized that there may be situations with material users where it may not be cost-effective to use PRA in their specific regulatory applications.

This policy statement affirms the Commission's belief that PRA methods can be used to derive valuable insights, perspective, and general conclusions as a result of an integrated and comprehensive examination of the design of nuclear facilities, facility response to initiating events, the expected interactions among facility structures, systems, and components, and between the facility and its operating staff.

The Commission also recognizes, and encourages, continuation of industry initiatives to improve PRA methods, applications and data collection to support increased use of PRA techniques in regulatory activities.

### V. Availability of Documents

Copies of documents cited in this section are available for inspection and/or for reproduction for a fee in the NRC Public Document Room, 2120 L Street, NW, (Lower Level), Washington, DC 20037. Copies of NUREGs cited in this document may be purchased from the Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082. Copies are also available for purchase from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

In addition, copies of (1) SECY-94-218, "Proposed Policy Statement on the Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities," (2) SECY-94-219, "Proposed Agency-Wide Implementation Plan for Probabilistic Risk Assessment (PRA)," (3) the Commission's Staff Requirements Memorandum of September 13, 1994, concerning the August 30, 1994, Commission meeting on SECY-94-218 and SECY-94-219, and (4) the Commission's Staff Requirements Memorandum of October 4, 1994, on SECY-94-218 can be obtained electronically by accessing the NRC electronic bulletin board system (BBS) Tech Specs Plus. These four WordPerfect® 5.1 documents are located in the BBS MISC library directory under the single filename "PRAPLAN.ZIP". The WordPerfect® 5.1 file for the final policy statement on the "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities," is located in the BBS MISC library directory under the filename "PRPOLICY.ZIP". The BBS operates 24 hours a day and can be accessed through a toll-free number, 1-800-679-5784, at modem speeds up to 9600 baud with communication parameters set at 8 data bits, no parity, 1 stop bit, full duplex, and using ANSI terminal emulation.

Dated at Rockville, Maryland, this 10th day of August, 1995.

For the Nuclear Regulatory Commission,  
Andrew L. Bates,  
Acting Secretary of the Commission.

## POLICY STATEMENTS

the facility would not impair the licensee's ability to fully fund the plan submitted to the NRC (or, if no plan has been filed, the actions necessary to permit release of the site for unrestricted use). A licensee would, for example, have to show that the decommissioning actions potentially taken out of sequence of any decommissioning plan submitted (or reasonable decommissioning alternatives if no plan has been submitted) would not significantly increase decommissioning costs or impair its ability to obtain the funds necessary to complete decommissioning.

4. Before the NRC approves a decommissioning plan, licensees can be allowed to undertake any decommissioning activity (as the term "decommission" is defined in 10 CFR 50.2) that does not: (a) Foreclose the release of the site for possible unrestricted use, (b) significantly increase decommissioning costs, (c) cause any significant environmental impact not previously reviewed, or (d) violate the terms of the licensee's existing license (e.g., OL, POL, or OL with confirmatory shutdown order) or 10 CFR 50.59 as applied to the existing license.

This criterion seeks to ensure that funds are only used for those decommissioning activities that would be allowed to proceed before the NRC approves a decommissioning plan. Items (a) and (b) have already been addressed by this policy statement. For items (c) and (d), a licensee and the NRC would evaluate the proposed activity to ensure that the activity may proceed under the current license and that the proposed activity will not result in any significant environmental impact not previously reviewed.

As stated above, the NRC may permit licensees to use their decommissioning funds for the decommissioning activities permitted above (as the term "decommission" is defined in 10 CFR 50.2), notwithstanding the fact that their decommissioning plans have not yet been approved by the NRC. After review of the licensee's proposed activities and fund withdrawal using the above criteria, the NRC would permit the licensee to use decommissioning funds and to undertake the proposed activities by tacitly consenting to the proposed withdrawals by not interposing, within a specified time, an objection to the licensee's proposal. The NRC would need 60 days to complete an effective review of a licensee's proposal and justification of how the above criteria will be met.

### Ancillary Issue

In the past, licensees have asked the NRC informally whether they would be able to withdraw funds from their trusts to pay for developing the \$ 50.82 decommissioning plan and for other post-shutdown administrative expenses. The NRC believes that these withdrawals should be allowed before the NRC approves the final decommissioning plan, provided the licensee meets the following guidelines:

1. The sum of withdrawals for such purposes should be *de minimis*, that is, less than \$5 million.<sup>3</sup>
2. The decommissioning trust balance would not fall below an amount needed for safe storage.
3. The licensee provided for these costs in its site-specific decommissioning cost estimate and increased its overall trust fund balances accordingly.

Dated at Rockville, Maryland, this 12th day of January, 1994.

For the Nuclear Regulatory Commission,  
James L. Blaha,  
Acting Executive Director for Operations.

<sup>3</sup> In talking informally with several licensees, the NRC understands that most licensees expect to spend from \$1 million to \$3 million for completing decommissioning plans and for immediate post-shutdown administrative expenses. The amount of \$5 million, therefore, is based on a "best-guess" estimated, but is small enough not to significantly deplete the decommissioning trust.

59 FR 35461  
Published 7/12/94  
Effective 7/12/94

### 10 CFR Part 50

#### Regulation of Advanced Nuclear Power Plants; Statement of Policy

AGENCY: Nuclear Regulatory Commission.

ACTION: Final Policy Statement.

**SUMMARY:** The Nuclear Regulatory Commission (NRC) intends to improve the licensing environment for advanced nuclear power reactors to minimize complexity and uncertainty in the regulatory process. This statement gives the Commission's policy regarding the review of, and desired characteristics associated with, advanced reactors. This policy statement is a revision of the final policy statement titled "Regulation of Advanced Nuclear Power Plants, Statement of Policy" that was published on July 8, 1986. The purpose of this revision is to update the Commission's policy statement on advanced reactors to reference the Commission's metrication policy.

**EFFECTIVE DATE:** July 12, 1994.

**FOR FURTHER INFORMATION CONTACT:** Stephen P. Sands, U.S. Nuclear Regulatory Commission, Washington, DC 20555, Telephone: 301-504-3154.

#### SUPPLEMENTARY INFORMATION:

##### Background

On July 8, 1986 (51 FR 24643), the Commission published its final policy statement on advanced reactors in the Federal Register. The Commission's primary objectives in issuing the advanced reactor policy statement were threefold:

- First, to maintain the earliest possible interaction of applicants, vendors, and government agencies, with the NRC;
- Second, to provide all interested parties, including the public, with the

## POLICY STATEMENTS

Commission's views concerning the desired characteristics of advanced reactor designs; and

- Third, to express the Commission's intent to issue timely comment on the implications of such designs for safety and the regulatory process.

On August 10, 1988, Congress passed the Omnibus Trade and Competitiveness Act [the Act], [19 U.S.C. 2901 *et seq.*], which amended the Metric Conversion Act of 1975, [15 U.S.C. 205a *et seq.*]. Section 5164 of the Act (15 U.S.C. 205a) designates the metric system as the preferred system of weights and measures for U.S. trade and commerce.

In an effort to effect an orderly change to the metric system, the Act requires that all Federal agencies convert to the metric system of measurement in their procurement, grants, and other business-related activities by the end of fiscal year 1992, "except to the extent that such use is impractical or is likely to cause significant inefficiencies or loss of markets to U.S. firms, such as when foreign competitors are producing competing products in non-metric units." Section 5614(b)(2).

In response to the Act, the NRC published its metrication policy statement for comment in the Federal Register on February 10, 1992 (57 FR 4891). The purpose of the metrication policy statement was to inform NRC licensees and the public how the Commission intended to meet its obligations under the Act. Comments on the draft statement were submitted by 12 responders, including 5 power reactor licensees, 3 standards organizations, a reactor vendor, a materials licensee, the Nuclear Management and Resources Council, and a joint letter submitted by three individuals. All commenters supported the Commission's position and the final policy statement was published on October 7, 1992 (57 FR 46202).

The Commission supports and encourages the use of the metric system of measurement by NRC licensees and applicants. However, Commission experience to date in design certification reviews is that it is impracticable and uneconomical to convert a design to the metric system late in the design process and that applicants should consider metrication early in the design process. Therefore, the Commission is revising the advanced reactor policy statement to incorporate its policy on metrication to

encourage licensees and license applicants to employ the metric system of measurement wherever and whenever its use is not potentially detrimental to the public health and safety or is not economically impracticable.

### Commission Policy

Consistent with its legislative mandate, the Commission's policy with respect to regulating nuclear power reactors is to ensure adequate protection of the public health and safety and the environment. Regarding advanced reactors, the Commission expects, as a minimum, at least the same degree of protection of the public and the environment that is required for current-generation light water reactors. Furthermore, the Commission expects that advanced reactors will provide enhanced margins of safety and/or utilize simplified, inherent, passive, or other innovative means to accomplish their safety functions. The Commission also expects that advanced reactor designs will comply with the Commission's safety goal policy statement and the policy statement on conversion to the metric system.

Among the attributes that could assist in establishing the acceptability or licensability of a proposed advanced reactor design, and that therefore should be considered in advanced designs, are:

- Highly reliable and less complex shutdown and decay heat removal systems. The use of inherent or passive means to accomplish this objective is encouraged (negative temperature coefficient, natural circulation, etc.).

- Longer time constants and sufficient instrumentation to allow for more diagnosis and management before reaching safety systems challenge and/or exposure of vital equipment to adverse conditions.

- Simplified safety systems that, where possible, reduce required operator actions, equipment subjected to severe environmental conditions, and components needed for maintaining safe shutdown conditions. Such simplified systems should facilitate operator comprehension, reliable system function, and more straightforward engineering analysis.

- Designs that minimize the potential for severe accidents and their consequences by providing sufficient inherent safety, reliability, redundancy, diversity, and independence in safety systems.

- Designs that provide reliable equipment in the balance of plant (BOP)

(or safety-system independence from BOP) to reduce the number of challenges to safety systems.

- Designs that provide easily maintainable equipment and components.

- Designs that reduce potential radiation exposures to plant personnel.

- Designs that incorporate defense-in-depth philosophy by maintaining multiple barriers against radiation release, and by reducing the potential for and consequences of severe accidents.

- Design features that can be proven by citation of existing technology or that can be satisfactorily established by commitment to a suitable technology development program.

If specific advanced reactor designs with some or all of the above foregoing attributes are brought to the NRC for comment and/or evaluation, the Commission can develop preliminary design safety evaluation and licensing criteria for their safety-related aspects. Combination of some or all of the above attributes may help obtain early licensing approval with minimum regulatory burden. Designs with some or all of these attributes are also likely to be more readily understood by the general public. Indeed, the number and nature of the regulatory requirements may depend on the extent to which an individual advanced reactor design incorporates general attributes such as those listed above. However, until such time as conceptual designs are submitted, the Commission believes that regulatory guidance must be sufficiently general to avoid placing unnecessary constraints on the development of new design concepts.

To provide for more timely and effective regulation of advanced reactors, the Commission encourages the earliest possible interaction of applicants, vendors, other government agencies, and the NRC to provide for early identification of regulatory requirements for advanced reactors, and to provide all interested parties, including the public, with a timely, independent assessment of the safety characteristics of advanced reactor designs. Such licensing interaction and guidance early in the design process will contribute toward minimizing complexity and adding stability and predictability in the licensing and regulation of advanced reactors.

While the NRC itself does not develop new designs, the Commission intends to develop the capability for timely

## POLICY STATEMENTS

assessment and response to innovative and advanced designs that might be presented for NRC review. Prior experience has shown that new reactor designs—even variations of established designs—may involve technical problems that must be solved in order to ensure adequate protection of the public health and safety. The earlier such design problems are identified, the earlier satisfactory resolution can be achieved. Prospective applicants are reminded that, while the NRC will undertake to review and comment on new design concepts, the applicants are responsible for documentation and research necessary to support a specific license application. (NRC research is conducted to provide the technical bases for rulemaking and regulatory decisions, to support licensing and inspection activities, and to increase NRC's understanding of phenomena for which analytical methods are needed in regulatory activities.)

During the initial phase of advanced reactor development, the Commission particularly encourages design innovations that enhance safety and reliability (such as those described above) and that generally depend on technology that is either proven or can be demonstrated by a straightforward technology development program. In the absence of a significant history of operating experience on an advanced concept reactor, plans for innovative use of proven technology and/or new technology development programs should be presented to the NRC for review as early as possible, so that the NRC can assess how the proposed program might influence regulatory requirements. To achieve these broad objectives, the Advanced Reactor Projects Directorate (PDAR) was established in the Office of Nuclear Reactor Regulation. This group is the focal point for NRC interaction with the Department of Energy, reactor designers, and potential applicants, and coordinates the development of regulatory criteria and guidance for proposed advanced reactors. In addition, the group maintains knowledge of advanced reactor designs, developments, and operating experience in other countries, and provides guidance on an NRC-funded advanced reactor safety research program to ensure that it supports, and is consistent with, the Commission's advanced reactor policy. The PDAR also provides guidance regarding the timing and format of submittals for review. The Advisory Committee on Reactor Safeguards plays a significant role in

reviewing proposed advanced design concepts and supporting activities.

The NRC believes that conversion to the metric system is important to the national interest. The Commission strongly encourages its licensees and license applicants to employ the metric system of measurement wherever and whenever its use is not potentially detrimental to the public health and safety or is not economically infeasible. In order to facilitate use of the metric system by licensees and applicants, the NRC began publishing, as of January 7, 1993, the following documents in dual units: new regulations, major amendments to existing regulations, regulatory guides, NUREG-series documents, policy statements, information notices, generic letters, bulletins, and all written communications directed to the public. Licensees and applicants should follow the guidance outlined in the Commission's position and final policy statement on metrication published on October 7, 1992 (57 FR 46202).

Dated at Rockville, Maryland, this 5th day of July, 1994.

For the Nuclear Regulatory Commission.  
John C. Hoyle,  
*Acting Secretary of the Commission.*

## POLICY STATEMENTS

51 FR 28044  
Published 8/4/86

51 FR 30028  
Published 8/21/86  
Effective 8/4/86

10 CFR Part 50

### **Safety Goals for the Operations of Nuclear Power Plants; Policy Statement; Republication**

[Editorial Note.—The following document was originally published at page 28044 in the issue of Monday, August 4, 1986. It is being republished in its entirety, with corrections, at the request of the agency.]

**AGENCY:** Nuclear Regulatory Commission.

**ACTION:** Policy statement.

---

**SUMMARY:** This policy statement focuses on the risks to the public from nuclear power plant operation. Its objective is to establish goals that broadly define an acceptable level of radiological risk. In developing the policy statement, the NRC sponsored two public workshops during 1981, obtained public comments and held four public meetings during 1982, conducted a 2-year evaluation during 1983 to 1985, and received the views of its Advisory Committee on Reactor Safeguards.

The Commission has established two qualitative safety goals which are supported by two quantitative objectives. These two supporting objectives are based on the principle that nuclear risks should not be a significant addition to other societal risks. The Commission wants to make clear that no death attributable to nuclear power plant operation will ever be "acceptable" in the sense that the Commission would regard it as a routine or permissible event. The Commission is discussing acceptable risks, not acceptable deaths.

• The *qualitative safety goals* are as follows:

—Individual members of the public should be provided a level of

## POLICY STATEMENTS

protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.

—Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.

• The following *quantitative objectives* are to be used in determining achievement of the above safety goals:

—The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.

—The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes.

**EFFECTIVE DATE:** August 4, 1986.

**FOR FURTHER INFORMATION CONTACT:** Merrill Taylor, Regional Operations and Generic Requirements Staff, Office of the Executive Director for Operations, U.S. Nuclear Regulatory Commission, Washington, DC 20555. Telephone (301/492-4356).

**SUPPLEMENTARY INFORMATION:** The following presents the Commission's Final Policy Statement on Safety Goals for the Operation of Nuclear Power Plants:

### I. Introduction

#### A. Purpose and Scope

In its response to the recommendations of the President's Commission on the Accident at Three Mile Island, the Nuclear Regulatory Commission (NRC) stated that it was "prepared to move forward with an explicit policy statement on safety philosophy and the role of safety-cost tradeoffs in the NRC safety decisions." This policy statement is the result.

Current regulatory practices are believed to ensure that the basic statutory requirement, adequate protection of the public, is met. Nevertheless, current practices could be improved to provide a better means for testing the adequacy of and need for current and proposed regulatory requirements. The Commission believes that such improvement could lead to a more coherent and consistent regulation of nuclear power plants, a more predictable regulatory process, a public

understanding of the regulatory criteria that the NRC applies, and public confidence in the safety of operating plants. This statement of NRC safety policy expresses the Commission's views on the level of risks to public health and safety that the industry should strive for in its nuclear power plants.

This policy statement focuses on the risks to the public from nuclear power plant operation. These are the risks from release of radioactive materials from the reactor to the environment from normal operations as well as from accidents. The Commission will refer to these risks as the risks of nuclear power plant operation. The risks from the nuclear fuel cycle are not included in the safety goals.

These fuel cycle risks have been considered in their own right and determined to be quite small. They will continue to receive careful consideration. The possible effects of sabotage or diversion of nuclear material are also not presently included in the safety goals. At present there is no basis on which to provide a measure of risk on these matters. It is the Commission's intention that everything that is needed will be done to keep these types of risks at their present very low level; and it is the Commission's expectation that efforts on this point will continue to be successful. With these exceptions, it is the Commission's intent that the risks from all the various initiating mechanisms be taken into account to the best of the capability of current evaluation techniques.

In the evaluation of nuclear power plant operation, the staff considers several types of releases. Current NRC practice addresses the risks to the public resulting from operating nuclear power plants. Before a nuclear power plant is licensed to operate, NRC prepares an environmental impact assessment which includes an evaluation of the radiological impacts of routine operation of the plant and accidents on the population in the region around the plant site. The assessment undergoes public comment and may be extensively probed in adjudicatory hearings. For all plants licensed to operate, NRC has found that there will be no measurable radiological impact on any member of the public from routine operation of the plant. (Reference: NRC staff calculations of radiological impact on humans contained in Final Environmental Statements for specific nuclear power plants: e.g., NUREG-0779, NUREG-0812, and NUREG-0854.)

The objective of the Commission's policy statement is to establish goals that broadly define an acceptable level of radiological risk that might be imposed on the public as a result of

nuclear power plant operation. While this policy statement includes the risks of normal operation, as well as accidents, the Commission believes that because of compliance with Federal Radiation Council (FRC) guidance, (40 CFR Part 190), and NRC's regulations (10 CFR Part 20 and Appendix I to Part 50), the risks from routine emissions are small compared to the safety goals. Therefore, the Commission believes that these risks need not be routinely analyzed on a case-by-case basis in order to demonstrate conformance with the safety goals.

#### B. Development of this Statement of Safety Policy

In developing the policy statement, the Commission solicited and benefited from the information and suggestions provided by workshop discussions. NRC-sponsored workshops were held in Palo Alto, California, on April 1-3, 1981 and in Harpers Ferry, West Virginia, on July 23-24, 1981. The first workshop addressed general issues involved in developing safety goals. The second workshop focused on a discussion paper which presented proposed safety goals. Both workshops featured discussions among knowledgeable persons drawn from industry, public interest groups, universities, and elsewhere, who represented a broad range of perspectives and disciplines.

The NRC Office of Policy Evaluation submitted to the Commission for its consideration a Discussion Paper on Safety Goals for Nuclear Power Plants in November 1981 and a revised safety goal report in July 1982.

The Commission also took into consideration the comments and suggestions received from the public in response to the proposed Policy Statement on "Safety Goals for Nuclear Power Plants," published on February 17, 1982 (47 FR 7023). Following public comment, a revised Policy Statement was issued on March 14, 1983 (48 FR 10772) and a 2-year evaluation period began.

The Commission used the staff report and its recommendations that resulted from the 2-year evaluation of safety goals in developing this final Policy Statement. Additionally, the Commission had benefit of further comments from its Advisory Committee on Reactor Safeguards (ACRS) and by senior NRC management.

Based on the results of this information, the Commission has determined that the qualitative safety goals will remain unchanged from its March 1983 revised policy statement, and the Commission adopts these as its safety goals for the operation of nuclear power plants.

## POLICY STATEMENTS

### II. Qualitative Safety Goals

The Commission has decided to adopt qualitative safety goals that are supported by quantitative health effects objectives for use in the regulatory decisionmaking process. The Commission's first qualitative safety goal is that the risk from nuclear power plant operation should not be a significant contributor to a person's risk of accidental death or injury. The intent is to require such a level of safety that individuals living or working near nuclear power plants should be able to go about their daily lives without special concern by virtue of their proximity to these plants. Thus, the Commission's first safety goal is—

*Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.*

Even though protection of individual members of the public inherently provides substantial societal protection, the Commission also decided that a limit should be placed on the societal risks posed by nuclear power plant operation. The Commission also believes that the risks of nuclear power plant operation should be comparable to or less than the risks from other viable means of generating the same quantity of electrical energy. Thus, the Commission's second safety goal is—

*Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.*

The broad spectrum of expert opinion on the risks posed by electrical generation by coal and the absence of authoritative data make it impractical to calibrate nuclear safety goals by comparing them with coal risks based on what we know today. However, the Commission has established the quantitative health effects objectives in such a way that nuclear risks are not a significant addition to other societal risks.

Severe core damage accidents can lead to more serious accidents with the potential for life-threatening offsite release of radiation, for evacuation of members of the public, and for contamination of public property. Apart from their health and safety consequences, severe core damage accidents can erode public confidence in the safety of nuclear power and can lead to further instability and unpredictability for the industry. In order to avoid these adverse consequences, the Commission intends

to continue to pursue a regulatory program that has as its objective providing reasonable assurance, while giving appropriate consideration to the uncertainties involved, that a severe core damage accident will not occur at a U.S. nuclear power plant.

### III. Quantitative Objectives Used To Gauge Achievement of The Safety Goals

#### A. General Considerations

The quantitative health effects objectives establish NRC guidance for public protection which nuclear plant designers and operators should strive to achieve. A key element in formulating a qualitative safety goal whose achievement is measured by quantitative health effects objectives is to understand both the strengths and limitations of the techniques by which one judges whether the qualitative safety goal has been met.

A major step forward in the development and refinement of accident risk quantification was taken in the Reactor Safety Study (WASH-1400) completed in 1975. The objective of the Study was "to try to reach some meaningful conclusions about the risk of nuclear accidents." The Study did not directly address the question of what level of risk from nuclear accidents was acceptable.

Since the completion of the Reactor Safety Study, further progress in developing probabilistic risk assessment and in accumulating relevant data has led to a recognition that it is feasible to begin to use quantitative safety objectives for limited purposes. However, because of the sizable uncertainties still present in the methods and the gaps in the data base—essential elements needed to gauge whether the objectives have been achieved—the quantitative objectives should be viewed as aiming points or numerical benchmarks of performance. In particular, because of the present limitations in the state of the art of quantitatively estimating risks, the quantitative health effects objectives are not a substitute for existing regulations.

The Commission recognizes the importance of mitigating the consequences of a core-melt accident and continues to emphasize features such as containment, siting in less populated areas, and emergency planning as integral parts of the defense-in-depth concept associated with its accident prevention and mitigation philosophy.

#### B. Quantitative Risk Objectives

The Commission wants to make clear at the beginning of this section that no death attributable to nuclear power plant operation will ever be "acceptable" in the sense that the

Commission would regard it as a routine or permissible event. We are discussing acceptable risks, not acceptable deaths. In any fatal accident, a course of conduct posing an acceptable risk at one moment results in an unacceptable death moments later. This is true whether one speaks of driving, swimming, flying or generating electricity from coal. Each of these activities poses a calculable risk to society and to individuals. Some of those who accept the risk (or are part of a society that accepts risk) do not survive it. We intend that no such accidents will occur, but the possibility cannot be entirely eliminated. Furthermore, individual and societal risks from nuclear power plants are generally estimated to be considerably less than the risk that society is now exposed to from each of the other activities mentioned above.

#### C. Health Effects—Prompt and Latent Cancer Mortality Risks

The Commission has decided to adopt the following two health effects as the quantitative objectives concerning mortality risks to be used in determining achievement of the qualitative safety goals—

• *The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.*

• *The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes.*

The Commission believes that this ratio of 0.1 percent appropriately reflects both of the qualitative goals—to provide that individuals and society bear no significant additional risk. However, this does not necessarily mean that an additional risk that exceeds 0.1 percent would by itself constitute a significant additional risk. The 0.1 percent ratio to other risks is low enough to support an expectation that people living or working near nuclear power plants would have no special concern due to the plant's proximity.

The average individual in the vicinity of the plant is defined as the average individual biologically (in terms of age and other risk factors) and locationally who resides within a mile from the plant site boundary. This means that the average individual is found by accumulating the estimated individual



## POLICY STATEMENTS

risks and dividing by the number of individuals residing in the vicinity of the plant.

In applying the objective for individual risk of prompt fatality, the Commission has defined the vicinity as the area within 1 mile of the nuclear power plant site boundary, since calculations of the consequences of major reactor accidents suggest that individuals within a mile of the plant site boundary would generally be subject to the greatest risk of prompt death attributable to radiological causes. If there are no individuals residing within a mile of the plant boundary, an individual should, for evaluation purposes, be assumed to reside 1 mile from the site boundary.

In applying the objective for cancer fatalities as a population guideline for individuals in the area near the plant, the Commission has defined the population generally considered subject to significant risk as the population within 10 miles of the plant site. The bulk of significant exposures of the population to radiation would be concentrated within this distance, and thus this is the appropriate population for comparison with cancer fatality risks from all other causes. This objective would ensure that the estimated increase in the risk of delayed cancer fatalities from all potential radiation releases at a typical plant would be no more than a small fraction of the year-to-year normal variation in the expected cancer deaths from nonnuclear causes. Moreover, the prompt fatality objective for protecting individuals generally provides even greater protection to the population as a whole. That is, if the quantitative objective for prompt fatality is met for individuals in the immediate vicinity of the plant, the estimated risk of delayed cancer fatality to persons within 10 miles of the plant and beyond would generally be much lower than the quantitative objective for cancer fatality. Thus, compliance with the prompt fatality objective applied to individuals close to the plant would generally mean that the aggregate estimated societal risk would be a number of times lower than it would be if compliance with just the objective applied to the population as a whole were involved. The distance for averaging the cancer fatality risk was taken as 50 miles in the 1983 policy statement. The change to 10 miles could be viewed to provide additional protection to individuals in the vicinity of the plant, although analyses indicate that this objective for cancer fatality will not be the controlling one. It also provides more representative societal

protection, since the risk to the people beyond 10 miles will be less than the risk to the people within 10 miles.

### IV. Treatment of Uncertainties

The Commission is aware that uncertainties are not caused by use of quantitative methodology in decisionmaking but are merely highlighted through use of the quantification process. Confidence in the use of probabilistic and risk assessment techniques has steadily improved since the time these were used in the Reactor Safety Study. In fact, through use of quantitative techniques, important uncertainties have been and continue to be brought into better focus and may even be reduced compared to those that would remain with sole reliance on deterministic decisionmaking. To the extent practicable, the Commission intends to ensure that the quantitative techniques used for regulatory decisionmaking take into account the potential uncertainties that exist so that an estimate can be made on the confidence level to be ascribed to the quantitative results.

The Commission has adopted the use of mean estimates for purposes of implementing the quantitative objectives of this safety goal policy (i.e., the mortality risk objectives). Use of the mean estimates comports with the customary practices for cost-benefit analyses and it is the correct usage for purposes of the mortality risk comparisons. Use of mean estimates does not however resolve the need to quantify (to the extent reasonable) and understand those important uncertainties involved in the reactor accident risk predictions. A number of uncertainties (e.g., thermal-hydraulic assumptions and the phenomenology of core-melt progression, fission product release and transport, and containment loads and performance) arise because of a direct lack of severe accident experience or knowledge of accident phenomenology along with data related to probability distributions.

In such a situation, it is necessary that proper attention be given not only to the range of uncertainty surrounding probabilistic estimates, but also to the phenomenology that most influences the uncertainties. For this reason, sensitivity studies should be performed to determine those uncertainties most important to the probabilistic estimates. The results of sensitivity of studies should be displayed showing, for example, the range of variation together with the underlying science or engineering assumptions that dominate this variation. Depending on the decision needs, the probabilistic results

should also be reasonably balanced and supported through use of deterministic arguments. In this way, judgements can be made by the decisionmaker about the degree of confidence to be given to these estimates and assumptions. This is a key part of the process of determining the degree of regulatory conservatism that may be warranted for particular decisions. This defense-in-depth approach is expected to continue to ensure the protection of public health and safety.

### V. Guidelines For Regulatory Implementation

The Commission approves use of the qualitative safety goals, including use of the quantitative health effects objectives in the regulatory decisionmaking process. The Commission recognizes that the safety goal can provide a useful tool by which the adequacy of regulations or regulatory decisions regarding changes to the regulations can be judged. Likewise, the safety goals could be of benefit in the much more difficult task of assessing whether existing plants, designed, constructed and operated to comply with past and current regulations, conform adequately with the intent of the safety goal policy.

However, in order to do this, the staff will require specific guidelines to use as a basis for determining whether a level of safety ascribed to a plant is consistent with the safety goal policy. As a separate matter, the Commission intends to review and approve guidance to the staff regarding such determinations. It is currently envisioned that this guidance would address matters such as plant performance guidelines, indicators for operational performance, and guidelines for conduct of cost-benefit analyses. This guidance would be derived from additional studies conducted by the staff and resulting in recommendations to the Commission. The guidance would be based on the following general performance guideline which is proposed by the Commission for further staff examination—

*Consistent with the traditional defense-in-depth approach and the accident mitigation philosophy requiring reliable performance of containment systems, the overall mean frequency of a large release of radioactive materials to the environment from a reactor accident should be less than 1 in 1,000,000 per year of reactor operation.*

To provide adequate protection of the public health and safety, current NRC regulations require conservatism in design, construction, testing, operation

## POLICY STATEMENTS

and maintenance of nuclear power plants. A defense-in-depth approach has been mandated in order to prevent accidents from happening and to mitigate their consequences. Siting in less populated areas is emphasized. Furthermore, emergency response capabilities are mandated to provide additional defense-in-depth protection to the surrounding population.

These safety goals and these implementation guidelines are not meant as a substitute for NRC's regulations and do not relieve nuclear power plant permittees and licensees from complying with regulations. Nor are the safety goals and these implementation guidelines in and of themselves meant to serve as a sole basis for licensing decisions. However, if pursuant to these guidelines, information is developed that is applicable to a particular licensing decision, it may be considered as one factor in the licensing decision.

The additional views of Commissioner Asselstine and the separate views of Commissioner Bernthal are attached.

Dated at Washington, DC, this 30th day of July 1986.

For the Nuclear Regulatory Commission,  
Lendo W. Zech, Jr.,  
*Chairman.*

### Additional Views by Commissioner Asselstine on the Safety Goal Policy Statement

The commercial nuclear power industry started rather slowly and cautiously in the early 1960's. By the late 1960's and early 1970's the growth of the industry reached a feverish pace. New orders were coming in for regulatory review on almost a weekly basis. The result was the designs of the plants outpaced operational experience and the development of safety standards. As experience was gained in operational characteristics and in safety reviews, safety standards were developed or modified with a general trend toward stricter requirements. Thus, in the early 1970's, the industry demanded to know "how safe is safe enough." In this Safety Goal Policy Statement, the Commission is reaching a first attempt at answering the question. Much credit should go to Chairman Palladino's efforts over the past 5 years to develop this policy statement. I approve this policy statement but believe it needs to go further. There are four additional aspects which should have been addressed by the policy statement.

#### Containment Performance

First, I believe the Commission should have developed a policy on the relative

emphasis to be given to accident prevention and accident mitigation. Such guidance is necessary to ensure that the principle of defense-in-depth is maintained. The Commission's Advisory Committee on Reactor Safeguards has repeatedly urged the Commission to do so. As a step in that direction, I offered for Commission consideration the following containment performance criterion:

In order to assure a proper balance between accident prevention and accident mitigation, the mean frequency of containment failure in the event of a severe core damage accident should be less than 1 in 100 severe core damage accidents.

Since the Chernobyl accident, the nuclear industry has been trying to distance itself from the Chernobyl accident on the basis of the expected performance of the containments around the U.S. power reactors. Unfortunately, the industry and the Commission are unwilling to commit to a level of performance for the containments.

The argument has been made that we do not know how to develop containment performance criteria (accident mitigation) because core meltdown phenomena and containment response thereto are very complex and involve substantial uncertainties. On the other hand, to measure how close a plant comes to the quantitative guidelines contained in this policy statement and to perform analyses required by the Commission's backfit rule, one must perform just those kinds of analyses. I find these positions inconsistent.

The other argument against a containment performance criterion is that such a standard would overspecify the safety goal. However, a containment performance objective is an element of ensuring that the principle of defense-in-depth is maintained. Since we cannot rule out core meltdown accidents in the foreseeable future, given the current level of safety, I believe it unwise not to establish an expectation on the performance of the final barrier to a substantial release of radioactive materials to the environment, given a core meltdown.

#### General Performance Guideline

While I have previously supported an objective of reducing the risks to an as low as reasonably achievable level, the general performance guideline articulated in this policy (i.e., ". . . the overall mean frequency of a large release of radioactive materials to the environment from a reactor accident should be less than 1 in 1,000,000 per year of reactor operation.") is a suitable

compromise. I believe it is an objective that is consistent with the recommendations of the Commission's chief safety officer and our Director of Research, and past urgings of the Advisory Committee on Reactor Safeguards. Unfortunately, the Commission stopped short of adopting this guideline as a performance objective in the policy statement, but I am encouraged that the Commission is willing at least to examine the possibility of adopting it. Achieving such a standard coupled with the containment performance objective given above would go a long way toward ensuring that the operating reactors successfully complete their useful lives and that the nuclear option remains a viable component of the nation's energy mix.

In addition to preferring adoption of this standard now, I also believe the Commission needs to define a "large release" of radioactive materials. I would have defined it as "a release that would result in a whole body dose of 5 rem to an individual located at the site boundary." This would be consistent with the EPA's emergency planning Protective Action Guidelines and with the level proposed by the NRC staff for defining an Extraordinary Nuclear Occurrence under the Price-Anderson Act. In adopting such a definition, the Commission would be saying that its objective is to ensure that there is no more than a 1 in 1,000,000 chance per year that the public would have to be evacuated from the vicinity of a nuclear reactor and that the waiver of defenses provisions of the Price-Anderson Act would be invoked. I believe this to be an appropriate objective in ensuring that there is no undue risk to the public health and safety associated with nuclear power.

#### Cost-Benefit Analyses

I believe it is long overdue for the Commission to decide the appropriate way to conduct cost-benefit analyses. The Commission's own regulations require these analyses, which play a substantial role in the decisionmaking on whether to improve safety. Yet, the Commission continues to postpone addressing this fundamental issue.

#### Future Reactors

In my view, this safety goal policy statement has been developed with a steady eye on the apparent level of safety already achieved by most of operating reactors. That level has been arrived at by a piecemeal approach to designing, constructing and upgrading of the plants over the years as experience

## POLICY STATEMENTS

was gained with the plants and as the results of required research became available. Given the performance of the current generation of plants, I believe a safety goal for these plants is not good enough for the future. This policy statement should have had a separate goal that would require substantially better plants for the next generation. To argue that the level of safety achieved by plant designs that are over 10 years old is good enough for the next generation is to have little faith in the ingenuity of engineers and in the potential for nuclear technology. I would have required the next generation of plants to be substantially safer than the currently operating plants.

### Separate Views of Commissioner Bernthal on Safety Goals Policy

I do not disapprove of what has been said in this policy statement, but too much remains unsaid. The public is understandably desirous of reassurance since Chernobyl; the NRC staff needs clear guidance to carry out its responsibilities to assure public health and safety; the nuclear industry needs to plan for the future. All want and deserve to see clear, unambiguous, practical safety objectives that provide the Commission's answer to the question, "How safe is safe enough?" at U.S. nuclear power plants. The question remains unanswered.

It is unrealistic for the Commission to expect that society, for the foreseeable future, will judge nuclear power by the same standard as it does all other risks. The issue today is not so much calculated risk; the issue is public acceptance and, consistent with the intent of Congress, preservation of the nuclear option.

In these early decades of nuclear power, TMI-style incidents must be rendered so rare that we would expect to recount such an event only to our grandchildren. For today's population of reactors, that implies a probability for severe core damage of  $10^{-6}$  per reactor year; for the longer term, it implies something better. I see this as a straightforward policy conclusion that every newspaper editor in the country understands only too well. If the Commission fails to set (and realize) this objective, then the nuclear option will cease to be credible before the end of the century. In other words, if TMI-style events were to occur with 10-15 year regularity, public acceptance of nuclear power would almost certainly fail.

And while the Commission's primary charge is to protect public health and safety, it is also the clear intent of Congress that the Commission, if possible, regulate in a way that preserves rather than jeopardizes the nuclear option. So, for example, if the

Commission were to find 100 percent confidence in some impervious containment design, but ignored what was inside the containment, the primary mandate would be satisfied, but in all likelihood, the second would not. Consistent with the Commission's long-standing defense-in-depth philosophy, both core-melt and containment performance criteria should therefore be clearly stated parts of the Commission's safety goals.

In short, this pudding lacks a theme. Meaningful assurance to the public; substantive guidance to the NRC staff; the regulatory path to the future for the industry—all these should be provided by plainly stating that, consistent with the Commission's "defense-in-depth" philosophy:

(1) Severe core-damage accidents should not be expected, on average, to occur in the U.S. more than once in 100 years;

(2) Containment performance at nuclear power plants should be such that severe accidents with substantial offsite damages are not expected, on average, to occur in the U.S. more than once in 1,000 years;

(3) The goal for offsite consequences should be expected to be met after conservative consideration of the uncertainties associated with the estimated frequency of severe core-damage and the estimated mitigation thereof by containment.<sup>1</sup>

The term "substantial offsite damages" would correspond to the Commission's legal definition of "extraordinary nuclear occurrence." "Conservative consideration of associated uncertainties" should offer at least 90 percent confidence (typical good engineering judgment, I would hope) that the offsite release goal is met.

The broad core-melt and offsite-release goals should be met "for the average power plant"; i.e., for the aggregate of U.S. power plants. The decision to fix or not to fix a specific plant would then depend on achieving "the goal for offsite consequences." As a practical matter, this offsite societal risk objective would (and should) be significantly dependent on site-specific population density.

The absence of such explicit population density considerations in the Commission's 0.1 percent goals for

<sup>1</sup> Interestingly enough, the Commission has adopted proposed goals similar to the above core-melt and containment performance objectives—without clearly saying so. Taken together, the Commission's: (1) 0.1 percent offsite prompt fatality goals; (2) proposed  $10^{-6}$  per-reactor-year "large offsite release" criterion; (3) commitment "to provide reasonable assurance . . . that a severe core-damage accident will not occur at a U.S. nuclear power plant," though they may be ill-defined, can be read to be more stringent than the plainly stated criteria suggested above.

offsite consequences deserves careful thought. Is it reasonable that Zion and Palo Verde, for example, be assigned the same theoretical "standard person" risk, even though they pose considerably different risks for the U.S. population as a whole? As they stand, these 0.1 percent goals do not explicitly include population density considerations; a power plant could be located in Central Park and still meet the Commission's quantitative offsite release standard.

I believe the Commission's standards should preserve the important principle that site-specific population density be quantitatively considered in formulating the Commission's societal risk objective; e.g., by requiring that for the *entire* U.S. population, the risk of fatal injury as a consequence of U.S. nuclear power plant operations should not exceed some appropriate specified fraction of the sum of the expected risk of fatality from all other hazards to which members of the U.S. population are generally exposed.

I am further concerned by the arbitrary nature of the 0.1 percent incremental "societal" health risk standard adopted by the Commission, a concept grounded in a purely subjective assessment of what the public might accept. The Commission should seriously consider a more rational standard, tied statistically to the average variations in natural exposure to radiation from all other sources.

Finally, as noted in its introductory comments, the Commission long ago committed to "move forward with an explicit policy statement on safety philosophy and the role of safety-cost tradeoffs in NRC safety decisions." While this policy statement may not be very "explicit", as discussed above, it contains nothing at all on the subject of "safety-cost" tradeoffs in NRC safety decisions." For example, is \$1,000 per person-rem an appropriate cost-benefit standard for NRC regulatory action? While I have long argued that such fundamental decisions are more rightly the responsibility of Congress, the NRC staff continues to use its own ad-hoc judgment in lieu of either the Commission or the Congress speaking to the issue.

In summary, while the Commission has produced a document which is not in conflict with my broad philosophy in such matters, I doubt that the public expected a philosophical dissertation, however erudite. It is a tribute to Chairman Palladino's efforts that the Commission has come this far. But the task remains unfinished.



UNITED STATES  
**NUCLEAR REGULATORY COMMISSION**  
ADVISORY COMMITTEE ON NUCLEAR WASTE  
WASHINGTON, D.C. 20555

October 31, 1997

The Honorable Shirley Ann Jackson  
Chairman  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555-0001

Dear Chairman Jackson:

**SUBJECT: RECOMMENDATIONS REGARDING THE IMPLEMENTATION OF THE DEFENSE-  
IN-DEPTH CONCEPT IN THE REVISED 10 CFR PART 60**

This letter communicates the recommendations of the Advisory Committee on Nuclear Waste (ACNW) for adopting a revised approach to the existing subsystem performance criteria in 10 CFR Part 60, "Disposal of High-Level Radioactive Wastes in Geologic Repositories," to implement the defense-in-depth (DID) concept.

**RECOMMENDATIONS**

1. The Committee endorses the concept of defense in depth, including institutional as well as structural aspects. In particular, we recognize the benefit of multiple barriers of protection. The Committee recommends that sound principles be set forth guiding the implementation of the concept of defense in depth. The Committee, however, does not endorse the establishment of rule-based subsystem requirements as exist in 10 CFR Part 60.

We believe that guidance will depend to a large extent on proper construction of a performance assessment (PA) to expose the role of design elements, operational elements, and multiple barriers, including interdependency of the multiple barriers. The regulations should be clear on how the DID concept should be implemented. The Department of Energy (DOE) (or any future license applicant) should be directed to furnish documentation that shows how the DID concept has been implemented in meeting the overall performance goal.

2. The Committee recommends that NRC performance assessment procedures be structured so that the effectiveness of individual barriers can be identified explicitly in the total system performance.

The PA should clearly expose the effectiveness and role of selected individual barriers such as the engineered systems and the natural geological setting. The assessment of individual barriers should include a quantification of the uncertainties involved and the inter-relationships among barriers. The Committee believes that there are methods for quantifying the role of individual engineered barriers and the containment capability of the natural setting. To achieve the capability to assess the effectiveness of individual barriers, both geological

and engineered, it may be necessary to modify the analysis methods, including the PA models, and to enhance the database to reveal the performance of individual barriers. The Committee also believes that exposure of the public to a PA process that is sufficiently transparent could lead to improved public confidence in the ability of the repository to isolate waste effectively.

This letter is one in a series of letters to the Commission conveying the ACNW's views on aspects of the NRC staff's strategy for revising 10 CFR Part 60. Previous letters on the staff's strategy for revising 10 CFR Part 60 include "Issues and NRC Activities Associated with the National Research Council's Report, 'Technical Bases for Yucca Mountain Standards,' " February 9, 1996; "Time Span for Compliance of the Proposed High-Level Waste Repository at Yucca Mountain, Nevada," June 7, 1996; and the "Reference Biosphere and Critical Group Issues and Their Application to the Proposed HLW Repository at Yucca Mountain, Nevada," April 3, 1997. Our recommendations are formulated on the basis of presentations made to the Committee during the 90th, 91st, 92nd, and 93rd meetings by the NRC staff, the DOE staff and its contractors, the State of Nevada, the National Research Council, and representatives from industry, as well as on the basis of the Commission's policy on risk-informed, performance-based regulation.

The Nuclear Waste Policy Act of 1982, as amended, mandates NRC to develop technical criteria for HLW disposal that are consistent with the Environmental Protection Agency (EPA) generic standards and provide for a system of multiple barriers. The Energy Policy Act of 1992 mandates that NRC conform its regulation to the final EPA standards for Yucca Mountain, the latter of which are to be based on and consistent with recommendations made by the National Academy of Sciences' Committee on Technical Bases for Yucca Mountain Standards (TBYMS). As directed by the Commission, the NRC staff is currently pursuing development of site-specific regulations for Yucca Mountain to implement the forthcoming EPA site-specific standards for Yucca Mountain.

In this letter, the concept of DID refers to the methods of design, construction, and operation of a geological repository for HLW in ways that aim to ensure safety in the face of considerable uncertainty in our knowledge of various processes. The implementation of DID in the repository context entails an analysis that exposes the contribution of each design element, each process (or set of processes) in the natural geological setting, and each operational technique to the safety of the repository. The DID concept includes (but is not identical to) the notion of multiple barriers that act to isolate the waste. One of the major issues regarding regulation within the DID framework is whether and how prescriptive requirements (so-called subsystem requirements) should be placed on classes of these barriers. As discussed below, the Committee believes that the adoption of a risk-informed approach eliminates the need for prescriptive subsystem requirements for Yucca Mountain.

The present form of 10 CFR Part 60 partly implements the DID approach by prescribing performance requirements of particular barriers.<sup>1</sup> As noted in the Statement of Considerations to 10 CFR Part 60, in addition to the natural barrier provided by the geological setting, this multiple barrier approach identifies two engineered barriers: the waste package and the underground facility. The Statement of Considerations notes that the multiple barrier concept is implemented by the performance objectives or requirements, as well as by more detailed siting and design criteria. The Committee

---

<sup>1</sup>Paraphrasing the regulation, the performance requirements specify substantially complete containment of waste packages for 300 to 1,000 years after permanent closure, release rates of radionuclides from the engineered barrier system less than one part in 100,000 per year at 1,000 years after closure, and a prewaste-emplacment groundwater travel time of at least 1,000 years.

recognizes that inclusion of the quantitative subsystem performance requirements in the rule was thought to provide additional confidence to compensate for uncertainties associated with predicting the behavior of a repository over thousands of years and for the general lack of experience and confidence in analyzing repository performance.

The Committee supports the NRC's view expressed in the Statement of Considerations to 10 CFR Part 60 that the performance of the engineered portion of the repository and the geological system must each make a definite contribution to waste isolation. The Committee recognizes the need for reliance on multiple and diverse barriers as part of the DID concept. However, we do not endorse the implementation of the DID concept through inclusion of prescriptive subsystem criteria in the revised 10 CFR Part 60.

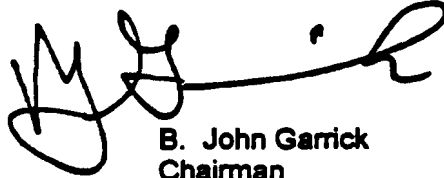
Current thinking, which is supported by much experience and empirical evidence in both probabilistic performance assessment and site characterization is that performance-based regulations are much more efficient and effective in protecting health, safety, and the environment than are "command-and-control" approaches. Focusing on quantitative subsystem requirements for the proposed repository at Yucca Mountain would run counter to this thinking because it potentially could force a design that would increase overall risk even though all subsystem requirements were met. A hypothetical example may clarify: a requirement that backfill in the repository be capable of substantially retaining all radionuclides leached from the waste package for 1000 years might be imposed. Such a requirement, which on the surface could be seen as beneficial, might force a design that would diminish significantly the lifetime of the waste canister by changing geochemical conditions in the near field. The outcome could be an increased risk to affected populations relative to a repository without backfill. It is this type of potentially adverse effect from subsystem requirements that an overall performance-based regulation would avoid. Consideration of such hypothetical examples supports our main conclusion that an overall performance-based regulation in the context of a risk-based standard is a superior tool for promoting safety relative to imposed subsystem requirements.

A major problem with the current version of 10 CFR 60.113, "Performance of Particular Barriers After Permanent Closure," which prescribes performance of particular barriers, is that it is not clear just how relevant any subsystem performance requirement is to the overall safety performance of the repository. Furthermore, in the analysis of repository performance, interdependency of barriers makes it difficult to assess precisely the role of individual barriers. For example, the assumed rate of percolation of water through the repository affects the performance of all subsystems. The connection between barrier performance and overall performance is very site- and design-specific. Prescribing individual barrier performance may create a design that is imbalanced in terms of individual barrier effectiveness. Subsystem requirements may also result in very poor designs from an economic standpoint. The ACNW's view is consistent with the TBYMS report, which cautioned against imposing subsystem requirements that may inadvertently result in a suboptimal repository design.

The primacy of an overall performance-based regulation does not imply that DOE, as the license applicant for Yucca Mountain, would not have to demonstrate convincingly to the NRC that both the geological system and multiple aspects of the engineered system were effective in providing waste isolation capacity. The NRC should insist that the applicant's PA clearly and quantitatively indicates how each barrier contributes to meeting the overall safety objective. This information should provide the basis for an informed decision on the license application.

The approach that we recommend offers many advantages over prescriptive subsystem requirements. First, it allows taking maximum advantage of site- and design-specific properties and features. Second, it is a clear example of risk-informed, performance-based regulation. The important contributors to risk can be ranked, thus providing a basis for prioritizing design changes and risk management activities. Third, it clarifies the degree of dependence of overall repository performance on individual barriers. In a sense, the safety margins of the various barriers are made more explicit through quantification.

Sincerely,

A handwritten signature in black ink, appearing to read "B. John Garrick". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

B. John Garrick  
Chairman



# REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

## REGULATORY GUIDE 1.174

(Draft was issued as DG-1061)

### AN APPROACH FOR USING PROBABILISTIC RISK ASSESSMENT IN RISK-INFORMED DECISIONS ON PLANT-SPECIFIC CHANGES TO THE LICENSING BASIS

#### 1. PURPOSE AND SCOPE

##### 1.1 INTRODUCTION

The NRC's policy statement on probabilistic risk assessment (PRA) (Ref. 1) encourages greater use of this analysis technique to improve safety decisionmaking and improve regulatory efficiency. The NRC staff's PRA Implementation Plan (Ref. 2) describes activities now under way or planned to expand this use. These activities include, for example, providing guidance for NRC inspectors on focusing inspection resources on risk-important equipment, as well as reassessing plants with relatively high core damage frequencies for possible backfits.

Another activity under way in response to the policy statement is using PRA to support decisions to modify an individual plant's licensing basis (LB).<sup>1</sup> This regulatory guide provides guidance on the use of PRA findings and risk insights in support of licensee requests for changes to a plant's LB, as in requests for license amendments and technical specification changes under Sections 50.90-92 of 10 CFR Part 50, "Domestic

<sup>1</sup>These are modifications to a plant's design, operation, or other activities that require NRC approval. These modifications could include items such as exemption requests under 10 CFR 50.11 and license amendments under 10 CFR 50.90.

Licensing of Production and Utilization Facilities." It does not address licensee-initiated changes to the LB that do NOT require NRC review and approval (e.g., changes to the facility as described in the final safety analysis report (FSAR), the subject of 10 CFR 50.59).

Licensee-initiated LB changes that are consistent with currently approved staff positions (e.g., regulatory guides, standard review plans, branch technical positions, or the Standard Technical Specifications) are normally evaluated by the staff using traditional engineering analyses. A licensee would not be expected to submit risk information in support of the proposed change.

Licensee-initiated LB change requests that go beyond current staff positions may be evaluated by the staff using traditional engineering analyses as well as the risk-informed approach set forth in this regulatory guide. A licensee may be requested to submit supplemental risk information if such information is not submitted by the licensee. If risk information on the proposed LB change is not provided to the staff, the staff will review the information provided by the licensee to determine whether the application can be approved. Based on the information provided, using traditional

#### USNRC REGULATORY GUIDES

Regulatory Guides are issued to describe and make available to the public such information as methods acceptable to the NRC staff for implementing specific parts of the Commission's regulations, techniques used by the staff in evaluating specific problems or postulated accidents, and data needed by the NRC staff in its review of applications for permits and licenses. Regulatory guides are not substitutes for regulations, and compliance with them is not required. Methods and solutions different from those set out in the guides will be acceptable if they provide a basis for the findings requisite to the issuance or continuance of a permit or license by the Commission.

This guide was issued after consideration of comments received from the public. Comments and suggestions for improvements in these guides are encouraged at all times, and guides will be revised, as appropriate, to accommodate comments and to reflect new information or experience.

Written comments may be submitted to the Rules Review and Directives Branch, ADM, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

The guides are issued in the following ten broad divisions:

- |                                   |                                   |
|-----------------------------------|-----------------------------------|
| 1. Power Reactors                 | 6. Products                       |
| 2. Research and Test Reactors     | 7. Transportation                 |
| 3. Fuels and Materials Facilities | 8. Occupational Health            |
| 4. Environmental and Siting       | 9. Antitrust and Financial Review |
| 5. Materials and Plant Protection | 10. General                       |

Single copies of regulatory guides may be obtained free of charge by writing the Reproduction and Distribution Services Section, Office of the Chief Information Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; or by fax at (301)415-2289; or by e-mail to GRW1@NRC.GOV.

Issued guides may also be purchased from the National Technical Information Service on a standing order basis. Details on this service may be obtained by writing NTIS, 5285 Port Royal Road, Springfield, VA 22161.



methods, the NRC staff will either approve or reject the application.

This regulatory guide describes an acceptable method for assessing the nature and impact of LB changes by a licensee when the licensee chooses to support (or is requested by the staff to support) these changes with risk information. The NRC staff would review these changes by considering engineering issues and applying risk insights. Licensees submitting risk information (whether on their own initiative or at the request of the staff) should address each of the principles of risk-informed regulation discussed in this regulatory guide. Licensees should identify how their chosen approaches and methods (whether quantitative or qualitative, deterministic or probabilistic), data, and criteria for considering risk are appropriate for the decision to be made.

The guidance provided here does not preclude other approaches for requesting changes to the LB. Rather, this regulatory guide is intended to improve consistency in regulatory decisions in areas in which the results of risk analyses are used to help justify regulatory action. As such, the principles, process, and approach discussed herein also provide useful guidance for the application of risk information to a broader set of activities than plant-specific changes to a plant's LB (i.e., generic activities), and licensees are encouraged to use this guidance in that regard.

## 1.2 BACKGROUND

During the last several years, both the NRC and the nuclear industry have recognized that PRA has evolved to the point that it can be used increasingly as a tool in regulatory decisionmaking. In August 1995, the NRC adopted the following policy statement (Ref. 1) regarding the expanded use of PRA.

- The use of PRA technology should be increased in all regulatory matters to the extent supported by the state of the art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy
- PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state of the art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and

staff practices. Where appropriate, PRA should be used to support the proposal of additional regulatory requirements in accordance with 10 CFR 50.109 (Backfit Rule). Appropriate procedures for including PRA in the process for changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations shall be complied with unless these rules and regulations are revised.

- PRA evaluations in support of regulatory decisions should be as realistic as practicable and appropriate supporting data should be publicly available for review.
- The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments on need for proposing and backfitting new generic requirements on nuclear power plant licensees.

In its approval of the policy statement, the Commission articulated its expectation that implementation of the policy statement will improve the regulatory process in three areas: foremost, through safety decision-making enhanced by the use of PRA insights; through more efficient use of agency resources; and through a reduction in unnecessary burdens on licensees.

In parallel with the publication of the policy statement, the staff developed an implementation plan to define and organize the PRA-related activities being undertaken (Ref. 2). These activities cover a wide range of PRA applications and involve the use of a variety of PRA methods (with variety including both types of models used and the detail of modeling needed). For example, one application involves the use of PRA in the assessment of operational events in reactors. The characteristics of these assessments permit relatively simple PRA models to be used. In contrast, other applications require the use of detailed models.

The activities described in the PRA Implementation Plan (Ref. 2), which is updated quarterly, relate to a number of agency interactions with the regulated industry. With respect to reactor regulation, activities include, for example, developing guidance for NRC inspectors on focusing inspection resources on risk-important equipment and reassessing plants with

relatively high core-damage frequencies (CDF) for possible backfit.

This regulatory guide focuses on the use of PRA in a subset of the applications described in the staff's implementation plan. Its principal focus is the use of PRA findings and risk insights in decisions on proposed changes to a plant's LB.

This regulatory guide also makes use of the NRC's Safety Goal Policy Statement (Ref. 3). As discussed below, one key principle in risk-informed regulation is that proposed increases in CDF and risk are small and are consistent with the intent of the Commission's Safety Goal Policy Statement. The safety goals (and associated quantitative health objectives (QHOs)) define an acceptable level of risk that is a small fraction (0.1%) of other risks to which the public is exposed. The acceptance guidelines defined in this regulatory guide (in Section 2.2.4) are based on subsidiary objectives derived from the safety goals and their QHOs.

### **1.3 PURPOSE OF THIS REGULATORY GUIDE**

Changes to many of the activities and design characteristics in a nuclear power plant's LB require NRC review and approval. This regulatory guide provides the staff's recommendations for using risk information in support of licensee-initiated LB changes requiring such review and approval. The guidance provided here does not preclude other approaches for requesting LB changes. Rather, this regulatory guide is intended to improve consistency in regulatory decisions in areas in which the results of risk analyses are used to help justify regulatory action. As such, this regulatory guide, the use of which is voluntary, provides general guidance concerning one approach that the NRC has determined to be acceptable for analyzing issues associated with proposed changes to a plant's LB and for assessing the impact of such proposed changes on the risk associated with plant design and operation. This guidance does not address the specific analyses needed for each nuclear power plant activity or design characteristic that may be amenable to risk-informed regulation.

### **1.4 SCOPE OF THIS REGULATORY GUIDE**

This regulatory guide describes an acceptable approach for assessing the nature and impact of proposed LB changes by considering engineering issues and applying risk insights. Assessments should consider relevant safety margins and defense-in-depth attributes, including consideration of success criteria as well as equipment functionality, reliability, and availability. The analyses should reflect the actual design, construction, and operational practices of the plant. Acceptance

guidelines for evaluating the results of such assessments are provided. This guide also addresses implementation strategies and performance monitoring plans associated with LB changes that will help ensure that assumptions and analyses supporting the change are verified.

Consideration of the Commission's Safety Goal Policy Statement (Ref. 3) is an important element in regulatory decisionmaking. Consequently, this regulatory guide provides acceptance guidelines consistent with this policy statement.

In theory, one could construct a more generous regulatory framework for consideration of those risk-informed changes that may have the effect of increasing risk to the public. Such a framework would include, of course, assurance of continued adequate protection (that level of protection of the public health and safety that must be reasonably assured regardless of economic cost). But it could also include provision for possible elimination of all measures not needed for adequate protection, which either do not effect a substantial reduction in overall risk or result in continuing costs that are not justified by the safety benefits. Instead, in this regulatory guide, the NRC has chosen a more restrictive policy that would permit only small increases in risk, and then only when it is reasonably assured, among other things, that sufficient defense in depth and sufficient margins are maintained. This policy is adopted because of uncertainties and to account for the fact that safety issues continue to emerge regarding design, construction, and operational matters notwithstanding the maturity of the nuclear power industry. These factors suggest that nuclear power reactors should operate routinely only at a prudent margin above adequate protection. The safety goal subsidiary objectives are used as an example of such a prudent margin.

Finally, this regulatory guide indicates an acceptable level of documentation that will enable the staff to reach a finding that the licensee has performed a sufficiently complete and scrutable analysis and that the results of the engineering evaluations support the licensee's request for a regulatory change.

### **1.5 RELATIONSHIP TO OTHER GUIDANCE DOCUMENTS**

Directly relevant to this regulatory guide is the Standard Review Plan (SRP) designed to guide the NRC staff evaluations of licensee requests for changes to the LB that apply risk insights (Ref. 4), as well as guidance that is being developed in selected application-specific regulatory guides and the corresponding standard review plan chapters. Related

regulatory guides are being developed on inservice testing, inservice inspection, graded quality assurance, and technical specifications (Refs. 5-8). An NRC contractor report (Ref. 9) is also available that provides a simple screening method for assessing one measure used in the regulatory guide—large early release frequency. The staff recognizes that the risk analyses necessary to support regulatory decisionmaking may vary with the relative weight that is given to the risk assessment element of the decisionmaking process. The burden is on the licensee who requests a change to the LB to justify that the chosen risk assessment approach, methods, and data are appropriate for the decision to be made.

The information collections contained in this regulatory guide are covered by the requirements of 10 CFR Part 50, which were approved by the Office of Management and Budget, approval number 3150-0011. The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

## 2. AN ACCEPTABLE APPROACH TO RISK-INFORMED DECISIONMAKING

In its approval of the policy statement on the use of PRA methods in nuclear regulatory activities (Ref. 1), the Commission stated an expectation that "the use of PRA technology should be increased in all regulatory matters...in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy." The use of risk insights in licensee submittals requesting LB changes will assist the staff in the disposition of such licensee proposals.

The staff has defined an acceptable approach to analyzing and evaluating proposed LB changes. This approach supports the NRC's desire to base its decisions on the results of traditional engineering evaluations, supported by insights (derived from the use of PRA methods) about the risk significance of the proposed changes. Decisions concerning proposed changes are expected to be reached in an integrated fashion, considering traditional engineering and risk information, and may be based on qualitative factors as well as quantitative analyses and information.

In implementing risk-informed decisionmaking, LB changes are expected to meet a set of key principles. Some of these principles are written in terms typically used in traditional engineering decisions (e.g., defense in depth). While written in these terms, it should be understood that risk analysis techniques can be, and are

encouraged to be, used to help ensure and show that these principles are met. These principles are:

1. The proposed change meets the current regulations unless it is explicitly related to a requested exemption or rule change, i.e., a "specific exemption" under 10 CFR 50.12 or a "petition for rulemaking" under 10 CFR 2.802.
2. The proposed change is consistent with the defense-in-depth philosophy.
3. The proposed change maintains sufficient safety margins.
4. When proposed changes result in an increase in core damage frequency or risk, the increases should be small and consistent with the intent of the Commission's Safety Goal Policy Statement (Ref. 3).<sup>2</sup>
5. The impact of the proposed change should be monitored using performance measurement strategies.

Each of these principles should be considered in the risk-informed, integrated decisionmaking process, as illustrated in Figure 1.

The staff's proposed evaluation approach and acceptance guidelines follow from these principles. In implementing these principles, the staff expects that:

- All safety impacts of the proposed change are evaluated in an integrated manner as part of an overall risk management approach in which the licensee is using risk analysis to improve operational and engineering decisions broadly by identifying and taking advantage of opportunities to reduce risk, and not just to eliminate requirements the licensee sees as undesirable. For those cases when risk increases are proposed, the benefits should be described and should be commensurate with the proposed risk increases. The approach used to identify changes in requirements should be used to identify areas where requirements should be increased<sup>3</sup> as well as where they can be reduced.
- The scope and quality of the engineering analyses (including traditional and probabilistic analyses) conducted to justify the proposed LB change should be appropriate for the nature and scope of the change, should be based on the as-built and as-operated and maintained plant, and should reflect operating experience at the plant.

<sup>2</sup>For purposes of this guide, a proposed LB change that meets the acceptance guidelines discussed in Section 2.2.4 is considered to have met the intent of the policy statement.

<sup>3</sup>The NRC staff is aware of but does not endorse guidelines that have been developed (e.g., by NEI/NUMARC) to assist in identifying potentially beneficial changes to requirements.

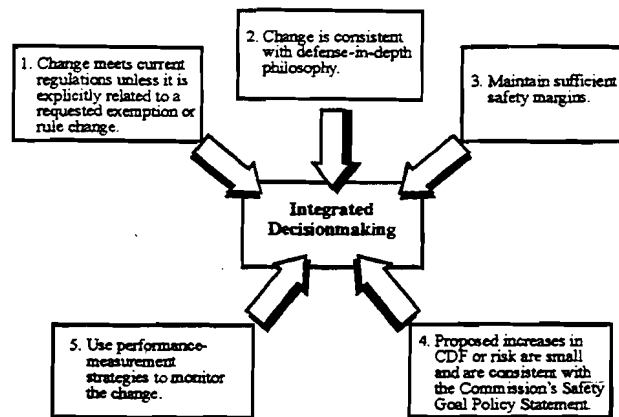


Figure 1. Principles of Risk-Informed Integrated Decisionmaking

- The plant-specific PRA supporting the licensee's proposals has been subjected to quality controls such as an independent peer review or certification.<sup>4</sup>
- Appropriate consideration of uncertainty is given in analyses and interpretation of findings, including using a program of monitoring, feedback, and corrective action to address significant uncertainties.
- The use of core damage frequency (CDF) and large early release frequency (LERF)<sup>5</sup> as bases for PRA acceptance guidelines is an acceptable approach to addressing Principle 4. Use of the Commission's Safety Goal QHOs in lieu of LERF is acceptable in principle, and licensees may propose their use. However, in practice, implementing such an approach would require an extension to a Level 3 PRA, in which case the methods and assumptions used in the Level 3 analysis, and associated uncertainties, would require additional attention.
- Increases in estimated CDF and LERF resulting from proposed LB changes will be limited to small increments. The cumulative effect of such changes should be tracked and considered in the decision process.
- The acceptability of proposed changes should be evaluated by the licensee in an integrated fashion that ensures that all principles are met.<sup>6</sup>
- Data, methods, and assessment criteria used to support regulatory decisionmaking must be well documented and available for public review.

Given the principles of risk-informed decisionmaking discussed above, the staff has identified a four-element approach to evaluating proposed LB changes. This approach, which is presented graphically in Figure 2, acceptably supports the NRC's decisionmaking process. This approach is not sequential in nature; rather it is iterative.

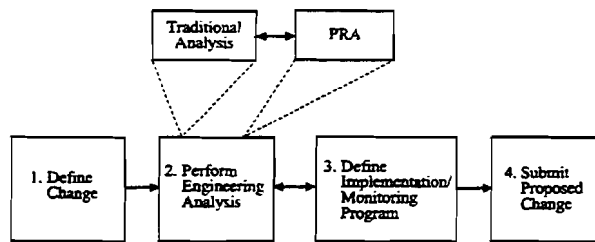
## 2.1 ELEMENT 1: DEFINE THE PROPOSED CHANGE

Element 1 involves three primary activities. First, the licensee should identify those aspects of the plant's licensing bases that may be affected by the proposed change, including but not limited to rules and regulations, final safety analysis report (FSAR), technical specifications, licensing conditions, and licensing commitments. Second, the licensee should identify all

<sup>4</sup>As discussed in Section 2.2.2 below, such a peer review or certification is not a replacement for NRC review. Certification is defined as a mechanism for assuring that a PRA, and the process of developing and maintaining that PRA, meets a set of technical standards established by a diverse group of personnel experienced in developing PRA models, performing PRAs, and performing quality reviews of PRAs. Such a process has been developed and integrated with a peer review process by, for example, the BWR Owners Group and implemented for the purpose of enhancing the quality of PRAs at several BWR facilities.

<sup>5</sup>In this context, LERF is being used as a surrogate for the early fatality QHO. It is defined as the frequency of those accidents leading to significant, unmitigated releases from containment in a time frame prior to effective evacuation of the close-in population such that there is a potential for early health effects. Such accidents generally include unscrubbed releases associated with early isolation. This definition is consistent with accident analyses used in the safety goal screening criteria discussed in the Commission's regulatory analysis guidelines. An NRC contractor's report (Ref. 9) describes a simple screening approach for calculating LERF.

<sup>6</sup>One important element of integrated decisionmaking can be the use of an "expert panel." Such a panel is not a necessary component of risk-informed decisionmaking; but when it is used, the key principles and associated decision criteria presented in this regulatory guide still apply and must be shown to have been met or to be irrelevant to the issue at hand.



**Figure 2. Principal Elements of Risk-Informed, Plant-Specific Decisionmaking**

structures, systems, and components (SSCs), procedures, and activities that are covered by the LB change being evaluated and should consider the original reasons for including each program requirement.

When considering LB changes, a licensee may identify regulatory requirements or commitments in its LB that it believes are overly restrictive or unnecessary to ensure safety at the plant. Note that the corollary is also true; that is, licensees are also expected to identify design and operational aspects of the plant that should be enhanced consistent with an improved understanding of their safety significance. Such enhancements should be embodied in appropriate LB changes that reflect these enhancements.

Third, with this staff expectation in mind, the licensee should identify available engineering studies, methods, codes, applicable plant-specific and industry data and operational experience, PRA findings, and research and analysis results relevant to the proposed LB change. With particular regard to the plant-specific PRA, the licensee should assess the capability to use, refine, augment, and update system models as needed to support a risk assessment of the proposed LB change.

The above information should be used collectively to describe the LB change and to outline the method of analysis. The licensee should describe the proposed change and how it meets the objectives of the NRC's PRA Policy Statement (Ref. 1), including enhanced decisionmaking, more efficient use of resources, and reduction of unnecessary burden. In addition to improvements in reactor safety, this assessment may consider benefits from the LB change such as reduced fiscal and personnel resources and radiation exposure. The licensee should affirm that the proposed LB change meets the current regulations unless the proposed change is explicitly related to a proposed exemption or rule change (i.e., a "specific exemption" under 10 CFR

50.12 or a "petition for rulemaking" under 10 CFR 2.802).

### 2.1.1 Combined Change Requests

Licensee proposals may include several individual changes to the LB that have been evaluated and will be implemented in an integrated fashion. The staff expects that, with respect to the overall net change in risk, combined change requests (CCRs) will fall in one of two broad categories, each of which may be acceptable:

1. CCRs in which any individual change increases risk;
2. CCRs in which each individual change decreases risk.

In the first category, the contribution of each individual change in the CCR must be quantified in the risk assessment and the uncertainty of each individual change must be addressed. For CCRs in the second category, qualitative analysis may be sufficient for some or all individual changes. Guidelines for use in developing CCRs are discussed below.

### 2.1.2 Guidelines for Developing CCRs

The changes that make up a CCR should be related to one another, for example, by affecting the same single system or activity, by affecting the same safety function or accident sequence or group of sequences, or by being of the same type (e.g., changes in outage time allowed by technical specifications). However, this does not preclude acceptance of unrelated changes. When CCRs are submitted to the NRC staff for review, the relationships among the individual changes and how they have been modeled in the risk assessment should be addressed in detail, since this will control the characterization of the net result of the changes. Licensees should evaluate not only the individual changes but also the changes taken together against the safety principles and qualitative acceptance guidelines in Sections 2 and 2.2.1, respectively, of this regulatory guide.

In addition, the acceptability of the cumulative impact of the changes that make up the CCR with respect to the quantitative acceptance guidelines discussed in Section 2.2.4 of this guide should be assessed.

In implementing CCRs in the first category, it is expected that the risk from significant accident sequences will not be increased and that the frequencies of the lower ranked contributors will not be increased so that they become significant contributors to risk. It is expected that no significant new sequences or cutsets will be created. In assessing the acceptability of CCRs, (1) risk increases related to the more likely initiating events (e.g., steam generator tube ruptures) should not be traded against improvements related to unlikely events (e.g., earthquakes) even if, for instance, they involve the same safety function, and (2) risk should be considered in addition to likelihood. The staff also expects that CCRs will lead to safety benefits such as simplifying plant operations or focusing resources on the most important safety items.

Proposed changes that modify one or more individual components of a previously approved CCR must also address the impact on the previously approved CCR. Specifically, the question to be addressed is whether the proposed modification would cause the previously approved CCR to not be acceptable. If the answer is yes, the submittal should address the actions the licensee is taking with respect to the previously approved CCR.

## **2.2 Element 2: Perform Engineering Analysis**

The staff expects that the scope and quality of the engineering analyses conducted to justify the proposed LB change will be appropriate for the nature and scope of the change. The staff also expects that appropriate consideration will be given to uncertainty in the analysis and interpretation of findings. The licensee is expected to use judgment on the complexity and difficulty of implementing the proposed LB change to decide upon appropriate engineering analyses to support regulatory decisionmaking. Thus, the licensee should consider the appropriateness of qualitative and quantitative analyses, as well as analyses using traditional engineering approaches and those techniques associated with the use of PRA findings. Regardless of the analysis methods chosen, the licensee must show that the principles set forth in Section 2 have been met through the use of scrutable acceptance guidelines established for making that determination.

Some proposed LB changes can be characterized as involving the categorization of SSCs according to

safety significance. An example is grading the application of quality assurance controls commensurate with the safety significance of equipment. Like other applications, the staff's review of LB change requests for applications involving safety categorization will be according to the acceptance guidelines associated with each key principle presented in this regulatory guide, unless equivalent guidelines are proposed by the licensee. Since risk importance measures are often used in such categorizations, guidance on their use is provided in Appendix A to this regulatory guide. Other application-specific guidance documents address guidelines associated with the adequacy of programs (in this example, quality controls) implemented for different safety-significant categories (e.g., more safety significant and less safety significant). Licensees are encouraged to apply risk-informed findings and insights to decisions (and potential LB requests).

As part of the second element, the licensee will evaluate the proposed LB change with regard to the principles that adequate defense-in-depth is maintained, that sufficient safety margins are maintained, and that proposed increases in core damage frequency and risk are small and are consistent with the intent of the Commission's Safety Goal Policy Statement.

### **2.2.1 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. 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 influence plant design and operation. Margins and defenses associated with these considerations may be affected by the licensee's proposed LB change and, therefore, should be reevaluated 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.

#### **2.2.1.1 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 the 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. 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. If a comprehensive risk analysis is done, it can be used to help determine the appropriate extent of defense in depth (e.g., balance among core damage prevention, containment failure, and consequence mitigation) to ensure protection of public health and safety. When a comprehensive risk analysis is not or cannot be done, traditional defense-in-depth considerations should be used or maintained to account for uncertainties. The evaluation should consider the intent of the general design criteria, 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 meets the defense-in-depth principle. Defense in depth consists of a number of elements, as summarized below. These elements can be used as guidelines for making that assessment. Other equivalent acceptance guidelines may also be used.

Consistency with the defense-in-depth philosophy is maintained if:

- A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.
  - Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided.
  - System redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties (e.g., no risk<sup>0</sup> outliers).
  - Defenses against potential common cause failures are preserved, and the potential for the introduction of new common cause failure mechanisms is assessed.
- Independence of barriers is not degraded.
  - Defenses against human errors are preserved.
  - The intent of the General Design Criteria in Appendix A to 10 CFR Part 50 is maintained.

#### 2.2.1.2 Safety Margins

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 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:

- 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.

Application-specific guidelines reflecting this general guidance are being developed and may be found in the application-specific regulatory guides (Refs. 5-8).

#### 2.2.2 Evaluation of Risk Impact, Including Treatment of Uncertainties

The licensee's risk assessment may be used to address the principle that proposed increases in CDF and risk are small and are consistent with the intent of the NRC's Safety Goal Policy Statement (Ref. 3). For purposes of implementation, the licensee should assess the expected change in CDF and LERF. The necessary sophistication of the evaluation, including the scope of the PRA (e.g., internal events only, full power only), depends on the contribution the risk assessment makes to the integrated decisionmaking, which depends to some extent on the magnitude of the potential risk impact. For LB changes that may have a more substantial impact, an in-depth and comprehensive PRA analysis, one appropriate to derive a quantified estimate of the total impact of the proposed LB change, will be necessary to provide adequate justification. In other applications, calculated risk importance measures or bounding estimates will be adequate. In still others, a qualitative assessment of the impact of the LB change on the plant's risk may be sufficient.

The remainder of this section discusses the use of quantitative PRA results in decisionmaking. This discussion has three parts:

- A fundamental element of NRC's risk-informed regulatory process is a PRA of sufficient quality and scope for the intended application. Section 2.2.3 discusses the staff's expectations with respect to the needed PRA's scope, level of detail, and quality.
- PRA results are to be used in this decisionmaking process in two ways—to assess the overall baseline CDF/LERF of the plant and to assess the CDF/LERF impact of the proposed change. Section 2.2.4 discusses the acceptance guidelines to be used by the staff for each of these measures.
- One of the strengths of the PRA framework is its ability to characterize the impact of uncertainty in the analysis, and it is essential that these uncertainties be recognized when assessing whether the principles are being met. Section 2.2.5 provides guidelines on how the uncertainty is to be addressed in the decisionmaking process.

The staff's decision on the proposed LB change will be based on its independent judgment and review of the entire application.

### **2.2.3 Scope, Level of Detail, and Quality of the PRA**

The scope, level of detail, and quality of the PRA is to be commensurate with the application for which it is intended and the role the PRA results play in the integrated decision process. The more emphasis that is put on the risk insights and on PRA results in the decisionmaking process, the more requirements that have to be placed on the PRA, in terms of both scope and how well the risk and the change in risk is assessed.

Conversely, emphasis on the PRA scope and quality can be reduced if a proposed change to the LB results in a risk decrease or is very small, or if the decision could be based mostly on traditional engineering arguments, or if compensating measures are proposed such that it can be convincingly argued that the change is very small.

Since this Regulatory Guide 1.174 is intended for a variety of applications, the required quality and level of detail may vary. One over-riding requirement is that the PRA should realistically reflect the actual design, construction, operational practices, and operational experience of the plant and its owner. This should include the licensee's voluntary actions as well as regulatory re-

quirements, and the PRA used to support risk-informed decisionmaking should also reflect the impact of previous changes made to the LB.

#### **2.2.3.1 Scope**

Although the assessment of the risk implications in light of the acceptance guidelines discussed in Section 2.2.4 requires that all plant operating modes and initiating events be addressed, it is not necessary to have a PRA that treats all these modes and initiating events. A qualitative treatment of the missing modes and initiators may be sufficient in many cases. Section 2.2.5 discusses this further.

#### **2.2.3.2 Level of Detail Required To Support an Application**

The level of detail required of the PRA is that which is sufficient to model the impact of the proposed change. The characterization of the problem should include establishing a cause-effect relationship to identify portions of the PRA affected by the issue being evaluated. Full-scale applications of the PRA should reflect this cause-effect relationship in a quantification of the impact on the PRA elements. For applications like component categorization, sensitivity studies on the effects of the change may be sufficient. For other applications it may be adequate to define the qualitative relationship of the impact on the PRA elements or only identify which elements are impacted.

If the impacts of a change to the plant cannot be associated with elements of the PRA, the PRA should be modified accordingly or the impact of the change should be evaluated qualitatively as part of the decisionmaking process (or expert panel process). In any case, the effects of the changes on the reliability and unavailability of systems, structures, and components or on operator actions should be appropriately accounted for.

#### **2.2.3.3 PRA Quality**

In the current context, quality will be defined as measuring the adequacy of the actual modeling. A PRA used in risk-informed regulation should be performed correctly, in a manner that is consistent with accepted practices, commensurate with the scope and level of detail required as discussed above. One approach a licensee could use to ensure quality is to perform a peer review of the PRA. In this case, the submittal should document the review process, the qualification of the reviewers, the summarized review findings, and resolutions to these findings where applicable. Industry PRA certification programs and PRA cross-comparison studies could also be used to help ensure appropriate



scope, level of detail, and quality of the PRA. If such programs or studies are to be used, a description of the program, including the approach and standard or guidelines to which the PRA is compared, the depth of the review, and the make-up and qualifications of the personnel involved should be provided for NRC review. Based on the peer review or certification process and on the findings from this process, the licensee should justify why the PRA is adequate for the present application in terms of scope and quality. A staff review cannot be replaced in its entirety by a peer review, a certification, or cross-comparison, although the more confidence the staff has in the review that has been performed for the licensee, the less rigor should be expected in the staff review.

The NRC has not developed its own formal standard nor endorsed an industry standard for a PRA submitted in support of applications governed by this regulatory guide. However, the NRC supports ongoing initiatives to develop a standard and expects that one will be available in the future. In the interim, the NRC staff will evaluate PRAs submitted in support of specific applications using the guidelines given in Chapter 19 of its Standard Review Plan (Ref. 4). The staff expects to feed back the experience gained from these reviews into the standards development process so that ultimately a standard can be developed that is suitable for regulatory decisionmaking as described in this guide. In addition, the references and bibliography provide information that licensees may find useful in deciding on the acceptability of their PRA.

#### 2.2.4 Acceptance Guidelines

The risk-acceptance guidelines presented in this regulatory guide are based on the principles and expectations for risk-informed regulation discussed in Section 2, and they are structured as follows. Regions are established in the two planes generated by a measure of the baseline risk metric (CDF or LERF) along the x-axis, and the change in those metrics ( $\Delta$ CDF or  $\Delta$ LERF) along the y-axis (Figures 3 and 4), and acceptance guidelines are established for each region as discussed below. These guidelines are intended for comparison with a full-scope (including internal events, external events, full power, low power, and shutdown) assessment of the change in risk metric, and when necessary, as discussed below, the baseline value of the risk metric (CDF or LERF). However, it is recognized that many PRAs are not full scope and PRA information of less than full scope may be acceptable as discussed in Section 2.2.5 of this regulatory guide.

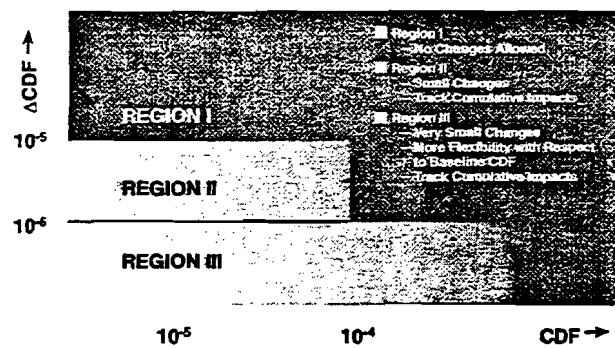


Figure 3. Acceptance Guidelines\* for Core Damage Frequency (CDF)

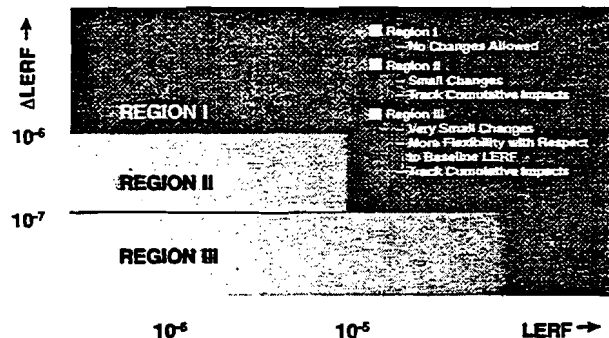


Figure 4. Acceptance Guidelines\* for Large Early Release Frequency (LERF)

\*The analysis will be subject to increased technical review and management attention as indicated by the darkness of the shading of the figure. In the context of the integrated decisionmaking, the boundaries between regions should not be interpreted as being definitive; the numerical values associated with defining the regions in the figure are to be interpreted as indicative values only.

There are two sets of acceptance guidelines, one for CDF and one for LERF, and *both* sets should be used.

- If the application clearly can be shown to result in a decrease in CDF, the change will be considered to have satisfied the relevant principle of risk-informed regulation with respect to CDF. (Because Figure 3 is drawn on a log scale, this region is not explicitly indicated on the figure.)
- When the calculated increase in CDF is very small, which is taken as being less than  $10^{-6}$  per reactor year, the change will be considered regardless of whether there is a calculation of the total CDF (Region III). While there is no requirement to calculate the total CDF, if there is an indication that the CDF

may be considerably higher than  $10^{-6}$  per reactor year, the focus should be on finding ways to decrease rather than increase it. Such an indication would result, for example, if (1) the contribution to CDF calculated from a limited scope analysis, such as the individual plant examination (IPE) or the individual plant examination of external events (IPEEE), significantly exceeds  $10^{-4}$ , (2) a potential vulnerability has been identified from a margins-type analysis, or (3) historical experience at the plant in question has indicated a potential safety concern.

- When the calculated increase in CDF is in the range of  $10^{-6}$  per reactor year to  $10^{-5}$  per reactor year, applications will be considered only if it can be reasonably shown that the total CDF is less than  $10^{-4}$  per reactor year (Region II).
- Applications that result in increases to CDF above  $10^{-5}$  per reactor year (Region I) would not normally be considered.

#### AND

- If the application clearly can be shown to result in a decrease in LERF, the change will be considered to have satisfied the relevant principle of risk-informed regulation with respect to LERF. (Because Figure 4 is drawn with a log scale, this region is not explicitly indicated on the figure.)
- When the calculated increase in LERF is very small, which is taken as being less than  $10^{-7}$  per reactor year, the change will be considered regardless of whether there is a calculation of the total LERF (Region III). While there is no requirement to calculate the total LERF, if there is an indication that the LERF may be considerably higher than  $10^{-5}$  per reactor year, the focus should be on finding ways to decrease rather than increase it. Such an indication would result, for example, if (1) the contribution to LERF calculated from a limited scope analysis, such as the IPE or the IPEEE, significantly exceeds  $10^{-5}$ , (2) a potential vulnerability has been identified from a margins-type analysis, or (3) historical experience at the plant in question has indicated a potential safety concern.
- When the calculated increase in LERF is in the range of  $10^{-7}$  per reactor year to  $10^{-6}$  per reactor year, applications will be considered only if it can be reasonably shown that the total LERF is less than  $10^{-5}$  per reactor year (Region II).

- Applications that result in increases to LERF above  $10^{-6}$  per reactor year (Region I) would not normally be considered.

These guidelines are intended to provide assurance that proposed increases in CDF and LERF are small and are consistent with the intent of the Commission's Safety Goal Policy Statement.

As indicated by the shading on the figures, the change request will be subject to an NRC technical and management review that will become more intensive when the calculated results are closer to the region boundaries.

The guidelines discussed above are applicable for full power, low power, and shutdown operations. However, during certain shutdown operations when the containment function is not maintained, the LERF guideline as defined above is not practical. In those cases, licensees may use more stringent baseline CDF guidelines (e.g.,  $10^{-5}$  per reactor year) to maintain an equivalent risk profile or may propose an alternative guideline to LERF that meets the intent of Principle 4 (see Figure 1).

The technical review that relates to the risk evaluation will address the scope, quality, and robustness of the analysis, including consideration of uncertainties as discussed in the next section. Aspects covered by the management review are discussed in Section 2.2.6, Integrated Decisionmaking, and include factors that are not amenable to PRA evaluation.

#### 2.2.5 Comparison of PRA Results with the Acceptance Guidelines

This section provides guidance on comparing the results of the PRA with the acceptance guidelines described in Section 2.2.4. In the context of integrated decisionmaking, the acceptance guidelines should not be interpreted as being overly prescriptive. They are intended to provide an indication, in numerical terms, of what is considered acceptable. As such, the numerical values associated with defining the regions in Figures 3 and 4 of this regulatory guide are approximate values that provide an indication of the changes that are generally acceptable. Furthermore, the state of knowledge, or epistemic, uncertainties associated with PRA calculations preclude a definitive decision with respect to which region the application belongs in based purely on the numerical results.

The intent of comparing the PRA results with the acceptance guidelines is to demonstrate with reasonable assurance that Principle 4, discussed in Section 2, is being met. This decision must be based on a full un-

derstanding of the contributors to the PRA results and the impacts of the uncertainties, both those that are explicitly accounted for in the results and those that are not. This is a somewhat subjective process, and the reasoning behind the decisions must be well documented. Guidance on what should be addressed follows in Section 2.2.5.4; but first, the types of uncertainty that impact PRA results and methods typically used for their analysis are briefly discussed. More information can be found in some of the publications in the Bibliography.

### **2.2.5.1 Types of Uncertainty and Methods of Analysis**

There are two facets to uncertainty that, because of their natures, must be treated differently when creating models of complex systems. They have recently been termed aleatory and epistemic uncertainty. The aleatory uncertainty is that addressed when the events or phenomena being modeled are characterized as occurring in a "random" or "stochastic" manner, and probabilistic models are adopted to describe their occurrences. It is this aspect of uncertainty that gives PRA the probabilistic part of its name. The epistemic uncertainty is that associated with the analyst's confidence in the predictions of the PRA model itself, and it reflects the analyst's assessment of how well the PRA model represents the actual system being modeled. This has been referred to as state-of-knowledge uncertainty. In this section, it is the epistemic uncertainty that is discussed; the aleatory uncertainty is built into the structure of the PRA model itself.

Because they are generally characterized and treated differently, it is useful to identify three classes of uncertainty that are addressed in and impact the results of PRAs: parameter uncertainty, model uncertainty, and completeness uncertainty. Completeness uncertainty can be regarded as one aspect of model uncertainty, but because of its importance, it is discussed separately. The Bibliography may be consulted for additional information on definitions of terms and approaches to the treatment of uncertainty in PRAs.

### **2.2.5.2 Parameter Uncertainty**

Each of the models that is used, either to develop the PRA logic structure or to represent the basic events of that structure, has one or more parameters. Typically, each of these models (e.g., the Poisson model for initiating events) is assumed to be appropriate. However, the parameter values for these models are often not known perfectly. Parameter uncertainties are those associated with the values of the fundamental parameters of the PRA model, such as equipment failure rates, ini-

tiating event frequencies, and human error probabilities that are used in the quantification of the accident sequence frequencies. They are typically characterized by establishing probability distributions on the parameter values. These distributions can be interpreted as expressing the analyst's degree of belief in the values these parameters could take, based on his state of knowledge and conditional on the underlying model being correct. It is straightforward and within the capability of most PRA codes to propagate the distribution representing uncertainty on the basic parameter values to generate a probability distribution on the results (e.g., CDF, accident sequence frequencies, LERF) of the PRA. However, the analysis must be done to correlate the sample values for different PRA elements from a group to which the same parameter value applies (the so-called state-of-knowledge dependency; see Ref. 10).

### **2.2.5.3 Model Uncertainty**

The development of the PRA model is supported by the use of models for specific events or phenomena. In many cases, the industry's state of knowledge is incomplete, and there may be different opinions on how the models should be formulated. Examples include approaches to modeling human performance, common cause failures, and reactor coolant pump seal behavior upon loss of seal cooling. This gives rise to model uncertainty. In many cases, the appropriateness of the models adopted is not questioned and these models have become, de facto, the standard models to use.

Examples include the use of Poisson and binomial models to characterize the probability of occurrence of component failures. For some issues with well-formulated alternative models, PRAs have addressed model uncertainty by using discrete distributions over the alternative models, with the probability associated with a specific model representing the analyst's degree of belief that that model is the most appropriate. A good example is the characterization of seismic hazard as different hypotheses lead to different hazard curves, which can be used to develop a discrete probability distribution of the initiating event frequency for earthquakes. Other examples can be found in the Level 2 analysis.

Another approach to addressing model uncertainty has been to adjust the results of a single model through the use of an adjustment factor. However it is formulated, an explicit representation of model uncertainty can be propagated through the analysis in the same way as parameter uncertainty. More typically, however, particularly in the Level 1 analysis, the use of different models would result in the need for a different structure

(e.g., with different thermal hydraulic models used to determine success criteria). In such cases, uncertainties in the choice of an appropriate model are typically addressed by making assumptions and, as in the case of the component failure models discussed above, adopting a specific model.

PRA's model the continuum of possible plant states in a discrete way, and are, by their very nature, approximate models of the world. This results in some random (aleatory) aspects of the 'world' not being addressed except in a bounding way, e.g., different realizations of an accident sequence corresponding to different LOCA sizes (within a category) are treated by assuming a bounding LOCA, time of failure of an operating component assumed to occur at the moment of demand. These approximations introduce biases (uncertainties) into the results.

In interpreting the results of a PRA, it is important to develop an understanding of the impact of a specific assumption or choice of model on the predictions of the PRA. This is true even when the model uncertainty is treated probabilistically, since the probabilities, or weights, given to different models would be subjective. The impact of using alternative assumptions or models may be addressed by performing appropriate sensitivity studies, or they may be addressed using qualitative arguments, based on an understanding of the contributors to the results and how they are impacted by the change in assumptions or models. The impact of making specific modeling approximations may be explored in a similar manner.

### 2.2.5.3 Completeness Uncertainty

Completeness is not in itself an uncertainty, but a reflection of scope limitations. The result is, however, an uncertainty about where the true risk lies. The problem with completeness uncertainty is that, because it reflects an unanalyzed contribution, it is difficult (if not impossible) to estimate its magnitude. Some contributions are unanalyzed not because methods are not available, but because they have not been refined to the level of the analysis of internal events. Examples are the analysis of some external events and the low power and shutdown modes of operation. There are issues, however, for which methods of analysis have not been developed, and they have to be accepted as potential limitations of the technology. Thus, for example, the impact on actual plant risk from unanalyzed issues such as the influences of organizational performance cannot now be explicitly assessed.

The issue of completeness of scope of a PRA can be addressed for those scope items for which methods are in principle available, and therefore some understanding of the contribution to risk exists, by supplementing the analysis with additional analysis to enlarge the scope, using more restrictive acceptance guidelines, or by providing arguments that, for the application of concern, the out-of-scope contributors are not significant. Approaches acceptable to the NRC staff for dealing with incompleteness are discussed in the next section.

### 2.2.5.4 Comparisons with Acceptance Guidelines

The different regions of the acceptance guidelines require different depths of analysis. Changes resulting in a net decrease in the CDF and LERF estimates do not require an assessment of the calculated baseline CDF and LERF. Generally, it should be possible to argue on the basis of an understanding of the contributors and the changes that are being made that the overall impact is indeed a decrease, without the need for a detailed quantitative analysis.

If the calculated values of CDF and LERF are very small, as defined by Region III in Figures 3 and 4, a detailed quantitative assessment of the baseline value of CDF and LERF will not be necessary. However, if there is an indication that the CDF or LERF could considerably exceed  $10^{-4}$  and  $10^{-5}$  respectively, in order for the change to be considered, the licensee may be required to present arguments as to why steps should not be taken to reduce CDF or LERF. Such an indication would result, for example, if (1) the contribution to CDF or LERF calculated from a limited scope analysis, such as the IPE or the IPEEE, significantly exceeds  $10^{-4}$  and  $10^{-5}$  respectively, (2) there has been an identification of a potential vulnerability from a margins-type analysis, or (3) historical experience at the plant in question has indicated a potential safety concern.

For larger values of  $\Delta$ CDF and  $\Delta$ LERF, which lie in the range used to define Region II, an assessment of the baseline CDF and LERF is required.

To demonstrate compliance with the numerical guidelines, the level of detail required in the assessment of the values and the analysis of uncertainty related to model and incompleteness issues will depend on both (1) the LB change being considered and (2) the importance of the demonstration that Principle 4 has been met. In Region III of Figures 3 and 4, the closer the estimates of  $\Delta$ CDF or  $\Delta$ LERF are to their corresponding acceptance guidelines, the more detail will be required. Similarly, in Region II of Figures 3 and 4, the closer the estimates of  $\Delta$ CDF or  $\Delta$ LERF and CDF and LERF are

to their corresponding acceptance guidelines, the more detail will be required. In a contrasting example, if the estimated value of a particular metric is very small compared to the acceptance goal, a simple bounding analysis may suffice with no need for a detailed uncertainty analysis.

Because of the way the acceptance guidelines were developed, the appropriate numerical measures to use in the initial comparison of the PRA results to the acceptance guidelines are mean values. The mean values referred to are the means of the probability distributions that result from the propagation of the uncertainties on the input parameters and those model uncertainties explicitly represented in the model. While a formal propagation of the uncertainty is the best way to correctly account for state-of-knowledge uncertainties that arise from the use of the same parameter values for several basic event probability models, under certain circumstances, a formal propagation of uncertainty may not be required if it can be demonstrated that the state-of-knowledge correlation is unimportant. This will involve, for example, a demonstration that the bulk of the contributing scenarios (cutsets or accident sequences) do not involve multiple events that rely on the same parameter for their quantification.

Consistent with the viewpoint that the guidelines are not to be used prescriptively, even if the calculated  $\Delta$ CDF and  $\Delta$ LERF values are such that they place the change in Region I or II, it may be possible to make a case that the application should be treated as if it were in Region II or III if, for example, it is shown that there are unquantified benefits that are not reflected in the quantitative risk results. However, care should be taken that there are no unquantified detrimental impacts of the change, such as an increase in operator burden. In addition, if compensatory measures are proposed to counter the impact of the major risk contributors, even though the impact of these measures may not be estimated numerically, such arguments will be considered in the decision process.

While the analysis of parametric uncertainty is fairly mature, and is addressed adequately through the use of mean values, the analysis of the model and completeness uncertainties cannot be handled in such a formal manner. Whether the PRA is full scope or only partial scope, and whether it is only the change in metrics or both the change and baseline values that need to be estimated, it will be incumbent on the licensee to demonstrate that the choice of reasonable alternative hypotheses, adjustment factors, or modeling approximations or methods to those adopted in the PRA model

would not significantly change the assessment. This demonstration can take the form of well formulated sensitivity studies or qualitative arguments. In this context, "reasonable" is interpreted as implying some precedent for the alternative, such as use by other analysts, and also that there is a physically reasonable basis for the alternative. It is not the intent that the search for alternatives should be exhaustive and arbitrary. For the decisions that involve only assessing the change in metrics, the number of model uncertainty issues to be addressed will be smaller than for the case of the baseline values, when only a portion of the model is affected. The alternatives that would drive the result toward unacceptableness should be identified and sensitivity studies performed or reasons given as to why they are not appropriate for the current application or for the particular plant. In general, the results of the sensitivity studies should confirm that the guidelines are still met even under the alternative assumptions (i.e., change generally remains in the appropriate region). Alternatively, this analysis can be used to identify candidates for compensatory actions or increased monitoring. The licensee should pay particular attention to those assumptions that impact the parts of the model being exercised by the change.

When the PRA is not full scope, it is necessary for the licensee to address the significance of the out-of-scope items. The importance of assessing the contribution of the out-of-scope portions of the PRA to the base case estimates of CDF and LERF is related to the margin between the as-calculated values and the acceptance guidelines. When the contributions from the modeled contributors are close to the guidelines, the argument that the contribution from the missing items is not significant must be convincing, and in some cases may require additional PRA analyses. When the margin is significant, a qualitative argument may be sufficient. The contribution of the out-of-scope portions of the model to the change in metric may be addressed by bounding analyses, detailed analyses, or by a demonstration that the change has no impact on the unmodeled contributors to risk. In addition, it should also be demonstrated that changes based on a partial PRA do not disproportionately change the risk associated with those accident sequences that arise from the modes of operation not included in the PRA.

One alternative to an analysis of uncertainty is to design the proposed LB change such that the major sources of uncertainty will not have an impact on the decisionmaking process. For example, in the region of the acceptance guidelines where small increases are allowed regardless of the value of the baseline CDF or

LERF, the proposed change to the LB could be designed such that the modes of operation or the initiating events that are missing from the analysis would not be affected by the change. In these cases, incompleteness would not be an issue. Similarly, in such cases, it would not be necessary to address all the model uncertainties, but only those that impact the evaluation of the change.

If only a Level 1 PRA is available, in general, only the CDF is calculated and not the LERF. An approach is presented in Reference 9 that allows a subset of the core damage accidents identified in the Level 1 analysis to be allocated to a release category that is equivalent to a LERF. The approach uses simplified event trees that can be quantified by the licensee on the basis of the plant configuration applicable to each accident sequence in the Level 1 analysis. The frequency derived from these event trees can be compared to the LERF acceptance guidelines. The approach described in Reference 9 may be used to estimate LERF only in those cases when the plant is not close to the CDF and LERF benchmark values.

### 2.2.6 Integrated Decisionmaking

The results of the different elements of the engineering analyses discussed in Sections 2.2.1 and 2.2.2 must be considered in an integrated manner. None of the individual analyses is sufficient in and of itself. In this way, it can be seen that the decision will not be driven solely by the numerical results of the PRA. They are one input into the decisionmaking and help in building an overall picture of the implications of the proposed change on risk. The PRA has an important role in putting the change into its proper context as it impacts the plant as a whole. The PRA analysis is used to demonstrate that Principle 4 has been satisfied. As the discussion in the previous section indicates, both quantitative and qualitative arguments may be brought to bear. Even though the different pieces of evidence used to argue that the principle is satisfied may not be combined in a formal way, they need to be clearly documented.

In Section 2.2.4, it was indicated that the application would be given increased NRC management attention when the calculated values of the changes in the risk metrics, and their baseline values when appropriate, approached the guidelines. Therefore, the issues in the submittal that are expected to be addressed by NRC management include:

- The cumulative impact of previous changes and the trend in CDF (the licensee's risk management approach);

- The cumulative impact of previous changes and the trend in LERF (the licensee's risk management approach);
- The impact of the proposed change on operational complexity, burden on the operating staff, and overall safety practices;
- Plant-specific performance and other factors (for example, siting factors, inspection findings, performance indicators, and operational events), and Level 3 PRA information, if available;
- The benefit of the change in relation to its CDF/ LERF increase;
- The practicality of accomplishing the change with a smaller CDF/ LERF impact; and
- The practicality of reducing CDF/ LERF when there is reason to believe that the baseline CDF/ LERF are above the guideline values (i.e.,  $10^{-4}$  and  $10^{-5}$  per reactor year).

### 2.3 ELEMENT 3: DEFINE IMPLEMENTATION AND MONITORING PROGRAM

Careful consideration should be given to implementation and performance-monitoring strategies. The primary goal for this element is to ensure that no adverse safety degradation occurs because of the changes to the LB. The staff's principal concern is the possibility that the aggregate impact of changes that affect a large class of SSCs could lead to an unacceptable increase in the number of failures from unanticipated degradation, including possible increases in common cause mechanisms. Therefore, an implementation and monitoring plan should be developed to ensure that the engineering evaluation conducted to examine the impact of the proposed changes continues to reflect the actual reliability and availability of SSCs that have been evaluated. This will ensure that the conclusions that have been drawn from the evaluation remain valid. Further details of acceptable processes for implementation in specific applications are discussed in application-specific regulatory guides (Refs. 5-8).

Decisions concerning the implementation of changes should be made in light of the uncertainty associated with the results of the traditional and probabilistic engineering evaluations. Broad implementation within a limited time period may be justified when uncertainty is shown to be low (data and models are adequate, engineering evaluations are verified and validated, etc.), whereas a slower, phased approach to implementation (or other modes of partial implementation) would be expected when uncertainty in evaluation

findings is higher and where programmatic changes are being made that could impact SSCs across a wide spectrum of the plant, such as in inservice testing, inservice inspection, and graded quality assurance (IST, ISI, and graded QA). In such situations, the potential introduction of common cause effects must be fully considered and included in the submittal.

The staff expects licensees to propose monitoring programs that include a means to adequately track the performance of equipment that, when degraded, can affect the conclusions of the licensee's engineering evaluation and integrated decisionmaking that support the change to the LB. The program should be capable of trending equipment performance after a change has been implemented to demonstrate that performance is consistent with that assumed in the traditional engineering and probabilistic analyses that were conducted to justify the change. This may include monitoring associated with non-safety-related SSCs, if the analysis determines those SSCs to be risk significant. The program should be structured such that (1) SSCs are monitored commensurate with their safety importance, i.e., monitoring for SSCs categorized as having low safety significance may be less rigorous than that for SSCs of high safety significance, (2) feedback of information and corrective actions are accomplished in a timely manner, and (3) degradation in SSC performance is detected and corrected before plant safety can be compromised. The potential impact of observed SSC degradation on similar components in different systems throughout the plant should be considered.

The staff expects that licensees will integrate, or at least coordinate, their monitoring for risk-informed changes with existing programs for monitoring equipment performance and other operating experience on their site and throughout the industry. In particular, monitoring that is performed in conformance with the Maintenance Rule can be used when the monitoring performed under the Maintenance Rule is sufficient for the SSCs affected by the risk-informed application. If an application requires monitoring of SSCs that are not included in the Maintenance Rule, or have a greater resolution of monitoring than the Maintenance Rule (component vs. train or plant-level monitoring), it may be advantageous for a licensee to adjust the Maintenance Rule monitoring program rather than to develop additional monitoring programs for risk-informed purposes. In these cases, the performance criteria chosen should be shown to be appropriate for the application in question. It should be noted that plant or licensee performance under actual design conditions may not be

readily measurable. When actual conditions cannot be monitored or measured, whatever information most closely approximates actual performance data should be used. For example, establishing a monitoring program with a performance-based feedback approach may combine some of the following activities.

- Monitoring performance characteristics under actual design basis conditions (e.g., reviewing actual demands on emergency diesel generators, reviewing operating experience)
- Monitoring performance characteristics under test conditions that are similar to those expected during a design basis event
- Monitoring and trending performance characteristics to verify aspects of the underlying analyses, research, or bases for a requirement (e.g., measuring battery voltage and specific gravity, inservice inspection of piping)
- Evaluating licensee performance during training scenarios (e.g., emergency planning exercises, operator licensing examinations)
- Component quality controls, including developing pre- and post-component installation evaluations (e.g., environmental qualification inspections, reactor protection system channel checks, continuity testing of boiling water reactor squib valves).

As part of the monitoring program, it is important that provisions for specific cause determination, trending of degradation and failures, and corrective actions be included. Such provisions should be applied to SSCs commensurate with their importance to safety as determined by the engineering evaluation that supports the LB change. A determination of cause is needed when performance expectations are not being met or when there is a functional failure of an application-specific SSC that poses a significant condition adverse to quality. The cause determination should identify the cause of the failure or degraded performance to the extent that corrective action can be identified that would preclude the problem or ensure that it is anticipated prior to becoming a safety concern. It should address failure significance, the circumstances surrounding the failure or degraded performance, the characteristics of the failure, and whether the failure is isolated or has generic or common cause implications (as defined in Ref. 11).

Finally, in accordance with Criterion XVI of Appendix B to 10 CFR Part 50, the monitoring program should identify any corrective actions to preclude the recurrence of unacceptable failures or degraded performance. The circumstances surrounding the failure may

indicate that the SSC failed because of adverse or harsh operating conditions (e.g., operating a valve dry, overpressurization of a system) or failure of another component that caused the SSC failure. Therefore, corrective actions should also consider SSCs with similar characteristics with regard to operating, design, or maintenance conditions. The results of the monitoring need not be reported to the NRC, but should be retained on-site for inspection.

#### **2.4 ELEMENT 4: SUBMIT PROPOSED CHANGE**

Requests for proposed changes to the plant's LB typically take the form of requests for license amendments (including changes to or removal of license conditions), technical specification changes, changes to or withdrawals of orders, and changes to programs pursuant to 10 CFR 50.54 (e.g., QA program changes under 10 CFR 50.54(a)). Licensees should (1) carefully review the proposed LB change in order to determine the appropriate form of the change request, (2) ensure that information required by the relevant regulations in support of the request is developed, and (3) prepare and submit the request in accordance with relevant procedural requirements. For example, license amendments should meet the requirements of 10 CFR 50.90, 50.91, and 50.92, as well as the procedural requirements in 10 CFR 50.4. Risk information that the licensee submits in support of the LB change request should meet the guidance in Section 3 of this regulatory guide.

Licensees are free to decide whether to submit risk information in support of their LB change request. If the licensee's proposed change to the LB is consistent with currently approved staff positions, the staff's determination will be based solely on traditional engineering analyses without recourse to risk information (although the staff may consider any risk information submitted by the licensee). However, if the licensee's proposed change goes beyond currently approved staff positions, the staff normally will consider both information based on traditional engineering analyses and information based on risk insights. If the licensee does not submit risk information in support of an LB change that goes beyond currently approved staff positions, the staff may request the licensee to submit such information. If the licensee chooses not to provide the risk information, the staff will review the proposed application using traditional engineering analyses and determine whether sufficient information has been provided to support the requested change.

In developing the risk information set forth in this regulatory guide, licensees will likely identify SSCs with high risk significance that are not currently subject to regulatory requirements, or are subject to a level of regulation that is not commensurate with their risk significance. It is expected that licensees will propose LB changes that will subject these SSCs to an appropriate level of regulatory oversight, consistent with the risk significance of each SSC. Specific information on the staff's expectations in this regard are set forth in the application-specific regulatory guides (Refs. 5-8).

#### **2.5 QUALITY ASSURANCE**

As stated in Section 2.2, the staff expects that the quality of the engineering analyses conducted to justify proposed LB changes will be appropriate for the nature of the change. In this regard, it is expected that for traditional engineering analyses (e.g., deterministic engineering calculations) existing provisions for quality assurance (e.g., Appendix B to 10 CFR Part 50, for safety-related SSCs) will apply and provide the appropriate quality needed. Likewise, when a risk assessment of the plant is used to provide insights into the decisionmaking process, the staff expects that the PRA will have been subject to quality control.

To the extent that a licensee elects to use PRA information to enhance or modify activities affecting the safety-related functions of SSCs, the following, in conjunction with the other guidance contained in this guide, describes methods acceptable to the NRC staff to ensure that the pertinent quality assurance requirements of Appendix B to 10 CFR Part 50 are met and that the PRA is of sufficient quality to be used for regulatory decisions.

- Use personnel qualified for the analysis.
- Use procedures that ensure control of documentation, including revisions, and provide for independent review, verification, or checking of calculations and information used in the analyses (an independent peer review or certification program can be used as an important element in this process).
- Provide documentation and maintain records in accordance with the guidelines in Section 3 of this guide.
- Provide for an independent audit function to verify quality (an independent peer review or certification program can be used for this purpose).
- Use procedures that ensure appropriate attention and corrective actions are taken if assumptions,



analyses, or information used in previous decision-making is changed (e.g., licensee voluntary action) or determined to be in error.

When performance monitoring programs are used in the implementation of proposed changes to the LB, it is expected that those programs will be implemented by using quality assurance provisions commensurate with the safety significance of affected SSCs. An existing PRA or analysis can be utilized to support a proposed LB change, provided it can be shown that the appropriate quality provisions have been met.

### 3. DOCUMENTATION AND SUBMITTAL

#### 3.1 INTRODUCTION

To facilitate the NRC staff's review to ensure that the analyses conducted were sufficient to conclude that the key principles of risk-informed regulation have been met, documentation of the evaluation process and findings are expected to be maintained. Additionally, the information submitted should include a description of the process used by the licensee to ensure quality and some specific information to support the staff's conclusion regarding the acceptability of the requested LB change.

#### 3.2 ARCHIVAL DOCUMENTATION

Archival documentation should include a detailed description of engineering analyses conducted and the results obtained, irrespective of whether they were quantitative or qualitative, or whether the analyses made use of traditional engineering methods or probabilistic approaches. This documentation should be maintained by the licensee, as part of the normal quality assurance program, so that it is available for examination. Documentation of the analyses conducted to support changes to a plant's LB should be maintained as lifetime quality records in accordance with Regulatory Guide 1.33 (Ref. 12).

#### 3.3 LICENSEE SUBMITTAL DOCUMENTATION

To support the NRC staff's conclusion that the proposed LB change is consistent with the key principles of risk-informed regulation and NRC staff expectations, the staff expects the following information will be submitted to the NRC:

- A description of how the proposed change will impact the LB (relevant principle: LB changes meet regulations).

- A description of the components and systems affected by the change, the types of changes proposed, the reason for the changes, and results and insights from an analysis of available data on equipment performance (relevant staff expectation: all safety impacts of the proposed LB change must be evaluated).
- A reevaluation of the LB accident analysis and the provisions of 10 CFR Parts 20 and 100, if appropriate (Relevant principles: LB changes meet the regulations, sufficient safety margins are maintained, defense-in-depth philosophy).
- An evaluation of the impact of the LB change on the breadth or depth of defense-in-depth attributes of the plant (relevant principle: defense-in-depth philosophy).
- Identification of how and where the proposed change will be documented as part of the plant's LB (e.g., FSAR, technical specifications, licensing conditions). This should include proposed changes or enhancements to the regulatory controls for high-risk-significant SSCs that are not subject to any requirements or the requirements are not commensurate with the SSC's risk significance.

The licensee should also identify:

- Key assumptions in the PRA that impact the application (e.g., voluntary licensee actions), elements of the monitoring program, and commitments made to support the application.
- SSCs for which requirements should be increased.
- The information to be provided as part of the plant's LB (e.g., FSAR, technical specifications, licensing condition).

As discussed in Section 2.5 of this guide, if a licensee elects to use PRA as an element to enhance or modify its implementation of activities affecting the safety-related functions of SSCs subject to the provisions of Appendix B to 10 CFR Part 50, the pertinent requirements of Appendix B will also apply to the PRA. In this context, therefore, a licensee would be expected to control PRA activity in a manner commensurate with its impact on the facility's design and licensing basis and in accordance with all applicable regulations and its QA program description. An independent peer review can be an important element of ensuring this quality. The licensee's submittal should discuss measures used to ensure adequate quality, such as a report of a peer review (when performed) that addresses the appropriateness of the PRA model for supporting a risk assessment of the LB change under consideration.

The report should address any analysis limitations that are expected to impact the conclusion regarding acceptability of the proposed change.

The licensee's resolution of the findings of the peer review, certification, or cross comparison, when performed, should also be submitted. For example, this response could indicate whether the PRA was modified or could justify why no change was necessary to support decisionmaking for the LB change under consideration. As discussed in Section 2.2.2, the staff's decision on the proposed license amendment will be based on its independent judgment and review, as appropriate, of the entire application.

### 3.3.1 Risk Assessment Methods

In order to have confidence that the risk assessment conducted is adequate to support the proposed change, a summary of the risk assessment methods used should be submitted. Consistent with current practice, information submitted to the NRC for its consideration in making risk-informed regulatory decisions will be made publicly available, unless such information is deemed proprietary and justified as such. The following information should be submitted and is intended to illustrate that the scope and quality of the engineering analyses conducted to justify the proposed LB change are appropriate to the nature and scope of the change.

- A description of risk assessment methods used,
- The key modeling assumptions that are necessary to support the analysis or that impact the application,
- The event trees and fault trees necessary to support the analysis of the LB change, and
- A list of operator actions modeled in the PRA that impact the application and their error probabilities.

The submitted information that summarizes the results of the risk assessment should include:

- The effects of the change on the dominant sequences (sequences that contribute more than five percent to the risk) in order to show that the LB change does not create risk outliers and does not exacerbate existing risk outliers.
- An assessment of the change to CDF and LERF, including a description of the significant contributors to the change.
- Information related to assessment of the total plant CDF—the extent of the information required will depend on whether the analysis of the change in CDF is in Region II or Region III of Figure 3. The

information could include quantitative (e.g., IPE or PRA results for internal initiating events, external event PRA results if available) and qualitative or semi-quantitative information (results of margins analyses, outage configuration studies).

- Information related to assessment of total plant LERF—the extent of the information required will depend on whether the analysis of the change in LERF is in Region II or Region III of Figure 4. The information could include quantitative (e.g., IPE or PRA results for internal initiating events, external event PRA results if available) and qualitative or semi-quantitative information (results of margins analyses, outage configuration studies).
- Results of analyses that show that the conclusions regarding the impact of the LB change on plant risk will not vary significantly under a different set of plausible assumptions.
- A description of the licensee process to ensure PRA quality and a discussion as to why the PRA is of sufficient quality to support the current application.

### 3.3.2 Cumulative Risks

As part of evaluation of risk, licensees should understand the effects of the present application in light of past applications. Optimally, the PRA used for the current application should already model the effects of past applications. However, qualitative effects and synergistic effects are sometimes difficult to model. Tracking changes in risk (both quantifiable and nonquantifiable) that are due to plant changes would provide a mechanism to account for the cumulative and synergistic effects of these plant changes and would help to demonstrate that the proposing licensee has a risk management philosophy in which PRA is not just used to systematically increase risk, but is also used to help reduce risk where appropriate and where it is shown to be cost effective. The tracking of cumulative risk will also help the NRC staff in monitoring trends.

Therefore, as part of the submittal, the licensee should track and submit the impact of all plant changes that have been submitted for NRC review and approval. Documentation should include:

- The calculated change in risk for each application (CDF and LERF) and the plant elements (e.g., SSCs, procedures) affected by each change,
- Qualitative arguments that were used to justify the change (if any) and the plant elements affected by these arguments,

- Compensatory measures or other commitments used to help justify the change (if any) and the plant elements affected, and
- Summarized results from the monitoring programs (where applicable) and a discussion of how these results have been factored into the PRA or into the current application.

As an option, the submittal could also list (but not submit to the NRC) past changes to the plant that reduced the plant risk, especially those changes that are related to the current application. A discussion of

whether these changes are already included in the base PRA model should also be included.

#### **3.4 IMPLEMENTATION PLAN AND PERFORMANCE MONITORING DOCUMENTATION**

As described in Section 2.3, a key principle of risk-informed regulation is that proposed performance implementation and monitoring strategies reflect uncertainties in analysis models and data. Consequently, the submittal should include a description and rationale for the implementation and performance monitoring strategy for the proposed LB change.

## REFERENCES

1. USNRC, "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," *Federal Register*, Vol. 60, p. 42622 (60 FR 42622), August 16, 1995.
2. "Quarterly Status Update for the Probabilistic Risk Assessment Implementation Plan," SECY-97-234, October 14, 1997.<sup>1</sup>
3. USNRC, "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement," *Federal Register*, Vol. 51, p. 30028 (51 FR 30028), August 4, 1986.
4. USNRC, "Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decisionmaking: General Guidance," Chapter 19 of the Standard Review Plan, July 1998.<sup>2</sup>
5. USNRC, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Inservice Testing," Draft Regulatory Guide DG-1062, June 1997.<sup>2</sup> (To be issued as Regulatory Guide 1.175)
6. USNRC, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Inservice Inspection

of Piping," Draft Regulatory Guide DG-1063, October 1997.<sup>2</sup> (To be issued as Regulatory Guide 1.178)

7. USNRC, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Graded Quality Assurance," Draft Regulatory Guide DG-1064, June 1997.<sup>2</sup> (To be issued as Regulatory Guide 1.176)
8. USNRC, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications," Draft Regulatory Guide DG-1065, June 1997.<sup>2</sup> (To be issued as Regulatory Guide 1.177)
9. W.T. Pratt et al., "An Approach for Estimating the Frequencies of Various Containment Failure Modes and Bypass Events," Draft NUREG/CR-6595, December 1997.<sup>2</sup>
10. G. Apostolakis and S. Kaplan, "Pitfalls in Risk Calculations," *Reliability Engineering*, Vol. 2, pages 135-145, 1981.
11. A. Mosleh et al., "Procedures for Treating Common Cause Failures in Safety and Reliability Studies," NUREG/CR-4780, Vol. 2, January 1989.<sup>3</sup>
12. USNRC, "Quality Assurance Program Requirements," Regulatory Guide 1.33, Revision 2, February 1978.<sup>2</sup>

<sup>1</sup>Copies are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW, Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555; telephone (202)634-3343.

<sup>2</sup>Single copies of regulatory guides, both active and draft, and draft NUREG documents may be obtained free of charge by writing the Reproduction and Distribution Services Section, OCIO, USNRC, Washington, DC 20555-0001, or by fax to (301)415-2289, or by email to GRW1@NRC.GOV. Active guides may be also purchased from the National Technical Information Service on a standing order basis. Details of this service may be obtained by writing NTIS, 5285 Port Royal Road, Springfield, VA 22161. Copies of active and draft guides are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street, NW, Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555; telephone (202)634-3273; fax (202)634-3343.

<sup>3</sup>Copies are available at current rates from the U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20402-9328 (telephone (202)512-2249); or from the National Technical Information Service by writing NTIS at 5285 Port Royal Road, Springfield, VA 22161. Copies are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW, Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555; telephone (202)634-3273; fax (202)634-3343.



# **RULEMAKING ISSUE**

(Notation Vote)

September 28, 1998

SECY-98-225

FOR: The Commissioners

FROM: L. Joseph Callan  
Executive Director for Operations

SUBJECT: PROPOSED RULE: 10 CFR PART 63---"DISPOSAL OF HIGH-LEVEL  
RADIOACTIVE WASTES IN A PROPOSED GEOLOGIC REPOSITORY AT  
YUCCA MOUNTAIN, NEVADA"

PURPOSE:

To request Commission approval to publish a notice of proposed rulemaking.

CATEGORY:

This paper covers a policy question.

BACKGROUND:

The staff submitted its proposed strategy for development of regulations governing disposal of high-level radioactive wastes in a proposed geologic repository at Yucca Mountain, Nevada, in SECY-97-300. The Staff Requirements Memorandum (SRM), issued March 6, 1998 (Attachment 1), approved the strategy, directing the staff to develop a draft proposal for a new, separate part of the regulations that would apply solely to the proposed Yucca Mountain repository.

This paper responds to that direction; it contains a draft Federal Register notice with a proposed 10 CFR Part 63-- regulations that would apply solely to a proposed geologic repository at Yucca Mountain (Attachment 2). The draft notice also contains corresponding

**CONTACTS:** Timothy J. McCartin, NMSS/DWM  
(301) 415-6681

Janet Kotra, NMSS/DWM  
(301) 415-6674

Clark W. Prichard, NMSS/IMNS  
(301) 415-6203

amendments to 10 CFR Parts 2, 19, 20, 21, 30, 40, 51, 60, and 61, needed to make appropriate sections of these regulations applicable to the proposed Part 63, as well as to Part 60, and to indicate that Part 60 criteria do not apply, nor may they be the subject of litigation, in any U.S. Nuclear Regulatory Commission licensing proceeding for a repository at Yucca Mountain.

#### DISCUSSION:

The proposed Part 63 follows the guidance to the staff, contained in the SRM, regarding general consistency with, and implementability of, National Academy of Sciences recommendations, establishment of an all-pathways dose standard, and avoidance of separate groundwater criteria. The proposed Part 63 regulations include emergency planning requirements, that were reserved in Part 60 for promulgation at a later date. These would require the U.S. Department of Energy to develop, and be prepared to implement, an emergency plan that is based on the Commission's emergency planning requirements for monitored retrievable storage facilities at § 72.32 (b).

As discussed in SECY-97-300, the staff's strategy included plans to "Adopt, as much as possible, definitions, administrative, preclosure, retrievability, and quality assurance portions of Part 60, with minor revisions for purposes of clarity and simplification (emphasis added)." In the course of implementing the Commission's direction for post-closure requirements for a repository at Yucca Mountain, however, it became clear that a risk-informed, more performance-based approach could be applied as well to the development of criteria governing activities at the repository before permanent closure. The staff elected to draft Part 63 with a risk-informed, performance-based approach to preclosure activities, including, at § 63.111, "Performance objectives for the geologic repository operations area through permanent closure," and, at § 63.112, "Requirements for integrated safety analysis of the geologic repository operations area."

The staff recognizes that this treatment of preclosure operation, in the proposed Part 63, as drafted, deviates from the strategy approved by the Commission, and has evaluated two approaches for treating pre-closure technical criteria in the proposed Part 63, as follows:

#### Alternative 1:

The Commission could approve the draft proposed rule, as written, including risk-informed, performance-based criteria for both pre-closure operations and post-closure performance of the proposed repository at Yucca Mountain.

- PRO:
- a. Is consistent with Commission philosophy supporting risk-informed, performance-based regulation of licensed facilities.
  - b. Creates a parallel regulatory framework for evaluation of pre-closure and post-closure performance. Performance objectives for pre- and post-closure performance are stated at §§ 63.111 and 63.113, respectively, followed by requirements for compliance demonstration, using an integrated safety analysis for pre-closure performance (§ 63.112); and a performance assessment for post-closure performance (§63.114).

- CON: a. Is inconsistent with updated generic criteria at Part 60 for pre-closure activities at repository sites, promulgated in December 1996. These criteria were modified, in part, to achieve greater consistency with NRC licensing requirements for independent storage of spent fuel and high-level waste, as codified at 10 CFR Part 72.
- b. Is not needed for compliance with statutory direction compelling consistency with site-specific environmental standards for repository performance after permanent closure.

Alternative 2:

The Commission could direct the staff to redraft the Federal Register notice and proposed Part 63 to incorporate Part 60 requirements for activities at the geologic repository operations area before closure.

- PRO: a. Is consistent with recently revised, generic criteria at Part 60.
- b. Is consistent with existing design and operations criteria specified at Part 72 for independent spent fuel storage and monitored retrievable storage installations.
- CON: a. Is inconsistent with risk-informed, performance-based approach taken for post-closure criteria in proposed rule.
- b. Is inconsistent with Commission policy for more risk-informed, performance-based regulation of licensed facilities. Generic revision of NRC regulations for operating materials facilities, which would include those applicable to a repository before closure, could take years.

The staff recognizes that the Commission has under review two proposed rulemakings, one containing amendments to 10 CFR Parts 50, 52 and 72 (SECY-98-171) and one containing proposed amendments to 10 CFR Part 70 (SECY-98-185). Both of these proposed rules include, among other things, requirements concerning changes, tests, and experiments that do not require prior Commission approval. The Part 63 requirements proposed herein include a § 63.44, modeled on the existing § 60.44, that contains language similar to the existing § 50.59. This section allows DOE to make changes in the geological repository operations area as described in the license application, make changes in the procedures, and conduct tests or experiments without Commission approval, absent a change in a license condition or an unreviewed safety question. If the Commission approves changes to § 50.59, or to Part 70 relevant to this issue, the staff will evaluate their applicability for incorporation into the proposed Part 63.

Lastly, the staff notes that, historically, the Commission has expressed its intent to convene an adjudicatory, trial-type (i.e., formal) hearing for licensing of a HLW repository. The Commission's generic regulations for HLW disposal at 10 CFR Part 60 were established with the expectation that licensing would be conducted using a formal adjudicatory process and the proposed Part 63 regulations have been drafted to be consistent with such a process.

Nonetheless, the staff recognizes that the Commission is exploring ways to streamline its hearing process, and may elect to fashion a less formal, legislative hearing process to apply to the licensing of a repository at Yucca Mountain.

Because there is no legal requirement to provide a formal (i.e., on-the-record) hearing for the repository, the Commission is free to hold either a formal hearing or an informal hearing. However, changing the present formal hearing process will require rulemaking to change Part 2. The current formal hearing provides an opportunity for cross-examination, which some participants would regard as a valuable feature. Therefore, a change to the current process, that eliminated this feature, could be highly controversial. However, in accordance with the governing statute for EPA's certification of the Waste Isolation Pilot Project (WIPP), the WIPP certification process used informal procedures (i.e., rulemaking) that did not include cross-examination. Thus, use of informal procedures in this general area is not unprecedented.

Recognizing that the NRC's broader efforts to improve the effectiveness of its programs and processes have touched on the process used for licensing actions, the staff believes it may be appropriate for the Commission to include a statement in this Part 63 rulemaking about the repository hearing process. For example, depending on the Commission's policy perspective, the Part 63 rulemaking might include a statement that the Commission has the repository hearing process under review. (In this regard, the proposed Part 63 regulations attached to this paper notify readers that the repository hearing process is under review and that if any changes are warranted, they will be adopted in a separate notice and comment rulemaking.) Further, the statement could go on to address the Commission's present inclination, such as to adopt an informal hearing in place of the current formal hearing, or to maintain the present formal hearing subject to Commission oversight to assure its functioning.

If the Commission, as a policy matter, is inclined to provide an informal, rather than the current formal, hearing for repository licensing, then the staff recommends that OGC be directed specifically to develop an informal hearing process for repository licensing. The OGC work would be carried out in the context of its on-going study of the NRC hearing process.

In the future event that the Commission amends its regulations, at 10 CFR Part 2, governing the hearing process, as they apply to the proposed repository at Yucca Mountain, the staff is confident that the proposed Part 63 regulations, with, at most, minor amendments, can be accommodated in a less formal process.

#### COORDINATION:

The Office of the General Counsel has no legal objection to this paper. The Office of the Chief Financial Officer has reviewed this Commission Paper for resource implications and has no objections. The Office of the Chief Information Officer has reviewed the rule for information technology and information management implications and concurs in the rulemaking.

Consistent with Commission direction to consult with the Advisory Committee on Nuclear Waste as early as possible in the rulemaking process, the Committee was provided a working draft of the proposed rule, and was briefed on the major technical questions associated with the draft on July 22, 1998.

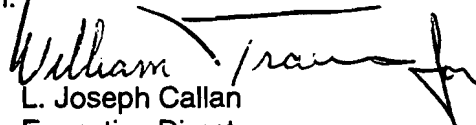


Unless otherwise directed by the Commission, staff intends to place the Commission paper and draft Federal Register Notice on NRC's Technical Conference Forum website within five working days.

RECOMMENDATIONS:

That the Commission:

1. Approve the Notice of Proposed Rulemaking, which applies the strategy of alternative 1, for publication (Attachment 2).
2. Certify that this rule, if promulgated, will not have a negative economic impact on a substantial number of small entities to satisfy requirements of the Regulatory Flexibility Act, 5 U.S.C. 605(b).
3. Note:
  - a. The proposed rule would be published in the Federal Register for a 75-day comment period;
  - b. A draft regulatory analysis will be available in the Public Document Room (Attachment 3);
  - c. The Chief Counsel for Advocacy of the Small Business Administration will be informed of the certification regarding economic impact on small entities and the reasons for it as required by the Regulatory Flexibility Act;
  - d. A press release will be issued (Attachment 4);
  - e. The appropriate Congressional committees will be informed (Attachment 5);
  - f. This proposed rule contains a new information collection requirement subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501, et seq.).
  - g. Commission direction is needed by October 28, 1998 in order not to delay NRC's target in its FY99 Performance Plan.

  
L. Joseph Callan  
Executive Director  
for Operations

Attachments:

1. SRM dtd 3/6/98
2. Draft Federal Register Notice + disk
3. Draft Regulatory Analysis
4. Draft Press Release
5. Draft Congressional Letters

Commissioners' completed vote sheets/comments should be provided directly to the Office of the Secretary by COB Thursday, October 15, 1998.

Commission Staff Office comments, if any, should be submitted to the Commissioners NLT October 7, 1998, with an information copy to the Office of the Secretary. If the paper is of such a nature that it requires additional review and comment, the Commissioners and the Secretariat should be apprised of when comments may be expected.

DISTRIBUTION:

Commissioners

OGC

OCAA

OIG

OPA

OCA

ACNW

CIO

CFO

EDO

REGIONS

SECY

**ATTACHMENT 1**

**SRM DATED, MARCH 6, 1998**

March 6, 1998

MEMORANDUM TO: L. Joseph Callan  
Executive Director for Operations

FROM: John C. Hoyle, Secretary /s/

SUBJECT: STAFF REQUIREMENTS - SECY-97-300 - PROPOSED  
STRATEGY FOR DEVELOPMENT OF REGULATIONS  
GOVERNING DISPOSAL OF HIGH-LEVEL  
RADIOACTIVE WASTES IN A PROPOSED  
REPOSITORY AT YUCCA MOUNTAIN, NEVADA

The Commission has approved the staff's proposed general strategy for developing site-specific regulations for Yucca Mountain while deferring the updating of Part 60 generic requirements to a later date. The Commission also approved Alternative 1, to implement the proposed strategy by drafting a new, separate part of the regulations that would apply solely to the proposed Yucca Mountain repository. The approval of Alternative 1 was based, in part, on concerns regarding current resource and time constraints.

In developing regulations specific to Yucca Mountain, the staff should:

- o omit the preparation of a formal rulemaking plan for this rulemaking because of time constraints.
- o develop rule language (in both the new rule and the Part 60 purpose and scope sections) to explicitly state that the purpose of the new rule is to provide specific criteria applicable to Yucca Mountain and that the more generic requirements in the existing Part 60 do not apply and can not be the subject of litigation in any NRC licensing proceeding for Yucca Mountain.
- o develop radiation standards in the form of an overall facility performance standard that is generally consistent with the 1995 National Academy of Sciences report, "Technical Bases for Yucca Mountain Standards" as required by the 1992 Energy Policy Act, in the absence of Environmental Protection Agency (EPA) standards and with due consideration given to the implementability of the NAS recommendations under NRC's regulatory process.
- o also consider the recommendations of the International Commission on Radiation Protection (ICRP) for use of an all-pathways limit and no collective dose as a basis for the overall facility performance standard. To be consistent with these NAS and ICRP recommendations and NRC's current clean-up standards, the staff should consider an all pathways dose standard in the

range of 25 to 30 millirem per year to the average member of the critical group.

- o continue to steadfastly oppose the implementation of a separate groundwater standard and keep the Commission informed of developments in this area.
- o immediately inform the Commission of any delays to the schedule shown in Attachment 4, including future EPA or Congressional actions that may result in a potential delay in the schedule.
- o consult with the Advisory Committee on Nuclear Waste (ACNW) as early as possible in the rulemaking process so the ACNW can fulfill its chartered role to advise the Commission on this important waste disposal rulemaking.

(EDO)

(SECY Suspense:

9/30/98)

Since this rulemaking will further the NRC's use of risk-informed methods in the regulatory process all NRC offices that have responsibilities in developing and implementing regulatory policies should monitor this rulemaking for applicability to other regulatory programs.

cc: Chairman Jackson  
Commissioner Dicus  
Commissioner Diaz  
Commissioner McGaffigan  
OGC  
CIO  
CFO  
OCA  
OIG  
Office Directors, Regions, ACRS, ACNW, ASLBP (via E-Mail)  
PDR  
DCS

**ATTACHMENT 2**

**FEDERAL REGISTER NOTICE**

**NUCLEAR REGULATORY COMMISSION**

**10 CFR Parts 2, 19, 20, 21, 30, 40, 51, 60, 61, and 63**

**RIN 3150-AG04**

**Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca  
Mountain, Nevada**

**AGENCY:** Nuclear Regulatory Commission.

**ACTION:** Proposed Rule.

**SUMMARY:** The U.S. Nuclear Regulatory Commission (NRC) is proposing licensing criteria for disposal of spent nuclear fuel and high-level radioactive wastes in the proposed geologic repository at Yucca Mountain, Nevada. These criteria will address the performance of the repository system at Yucca Mountain, a system that must comprise both natural and engineered barriers. Also included are licensing procedures, criteria for public participation, records and reporting, monitoring and testing programs, performance confirmation, quality assurance, personnel training and certification, and emergency planning. The proposed criteria will apply specifically and exclusively to the proposed repository at Yucca Mountain. Consistent with this intent, the Commission proposes to modify its generic criteria for disposal of spent nuclear fuel and high-level radioactive wastes in geologic repositories at 10 CFR Part 60 to make clear that they do not apply, nor may they be the subject of litigation, in any NRC licensing proceeding for a repository at Yucca Mountain.

**DATES:** Submit comments by [insert date 75 days after publication]. Comments received after this date will be considered if it is practical to do so, but the NRC is able to assure consideration only for comments received on or before this date.

**ADDRESSES:** Comments may be sent by mail to the Secretary, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, Attention: Rulemakings and Adjudications Staff.

Hand deliver comments to 11555 Rockville Pike, Rockville, Maryland, between 7:30 am and 4:15 pm on Federal workdays.

You may also provide comments via the NRC's interactive rulemaking web site through the NRC home page (<http://www.nrc.gov>). This site provides the availability to upload comments as files (any format), if your web browser supports that function. For information about the interactive rulemaking site, contact Ms. Carol Gallagher (301) 415-5905; e-mail [CAG@nrc.gov](mailto:CAG@nrc.gov).

Certain documents related to this rulemaking, including comments received and the regulatory analysis, may be examined at the NRC Public Document Room, 2120 L Street NW. (Lower Level), Washington, DC. These same documents also may be viewed and downloaded electronically via the interactive rulemaking website established by NRC for this rulemaking.

**FOR FURTHER INFORMATION CONTACT:** Timothy McCartin, Office of Nuclear Material Safety and Safeguards, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, telephone (301) 415-6681; e-mail [tjm3@nrc.gov](mailto:tjm3@nrc.gov), or Clark Prichard, Office of Nuclear Material Safety and Safeguards, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, telephone (301) 415-6203; e-mail [cwp@nrc.gov](mailto:cwp@nrc.gov).



**SUPPLEMENTARY INFORMATION:**

- I. Background.
- II. NAS Conclusions and Recommendations for Yucca Mountain.
- III. Development of a New 10.CFR Part 63.
- IV. Part 63 Technical Criteria.
- V. Individual Protection Standard for Postclosure Repository Performance.
- VI. Reference Biosphere and Critical Group for Yucca Mountain.
- VII. Compliance Period.
- VIII. Multiple Barriers and Defense in Depth.
- VIX. Performance Assessment.
- X. Institutional Controls.
- XI. Human Intrusion.
- XII. Preclosure Performance Objective.
- XIII. Integrated Safety Analysis of Activities at the Geologic Repository Operations Area.
- XIV. Quality Assurance.
- XV. Emergency Planning.
- XVI. Relationship to Generic Criteria at Part 60.
- XVII. Section-by-Section Analysis of Part 63.
- XVIII. Section-by Section Analysis of Corresponding Changes to Other Parts.
- XIX. Finding of No Significant Environmental Impact: Availability.
- XX. Paperwork Reduction Act Statement.
- XXI. Regulatory Analysis.
- XXII. Regulatory Flexibility Certification.

overall performance. Irrespective of the projected lifetime of the waste package design, the capability of the natural barriers to limit exposures would need to be evaluated in the context of the multiple barrier requirement.

Finally, from a policy perspective, EPA has already codified a 10,000-year compliance period at 40 CFR 191 applicable to the Waste Isolation Pilot Plant (WIPP), a similar type of disposal system as that proposed at Yucca Mountain. A 10,000-year performance period is also referenced in EPA guidance on no-migration petitions for facilities seeking exemption from certain land-disposal restrictions for long-lived hazardous, nonradioactive materials. Additionally, a 10,000-year compliance period is specified in NRC's Draft Technical Position on a Performance Assessment Methodology for Low-Level Radioactive Waste Disposal Facilities (62 FR 29164). All of these land disposal situations, like HLW disposal, involve disposed wastes containing long-lived, hazardous materials which are of concern, because they can become mobile in the groundwater pathway.

The Commission proposes that a 10,000-year compliance period is appropriate for evaluating a Yucca Mountain repository because it: 1) includes the period when the waste is inherently most hazardous; 2) is sufficiently long, such that a wide range of conditions will occur which will challenge the natural and the engineered barriers, providing a reasonable evaluation of the robustness of the geologic repository; and 3) is consistent with other regulations involving geologic disposal of long-lived hazardous materials, including radionuclides.

### **VIII. Multiple Barriers and Defense in Depth**

The defense-in-depth principle has served as a cornerstone of NRC's deterministic regulatory framework for nuclear reactors, and it provides an important tool for making

regulatory decisions, with regard to complex facilities, in the face of significant uncertainties. NRC also has applied the concept of defense-in-depth elsewhere in its regulations to ensure safety of licensed facilities through requirements for multiple, independent barriers, and, where possible, redundant safety systems and barriers. Traditionally, the reliance on independence and redundancy of barriers has been used to provide assurance of safety when reliable, quantitative assessments of barrier reliability are unavailable. The Commission maintains, as it has in the past, that the application of the defense-in-depth concept to a geologic repository is appropriate and reasonable. The Commission now believes, however, that its implementation, in the context of a geologic repository, should be reexamined, in light of the advancement in methods to quantitatively assess the components of a geologic repository system and with due consideration of the Commission's goal of a regulatory program and associated requirements that are risk-informed and performance-based.

Development of NRC's regulations for geologic disposal in 1983 represented a unique application of the defense-in-depth philosophy to a first-of-a-kind type of facility. While waste is being emplaced, and before a geologic repository is closed, its operation may be amenable to regulation comparable to other operating nuclear fuel cycle facilities licensed by NRC. Application of defense-in-depth principles for regulation of repository performance, for long time periods following closure, however, must account for the difference between a geologic repository and an operating facility with active safety systems and the potential for active control and intervention. A closed repository is essentially a passive system, and assessment of its safety over long timeframes is best evaluated through consideration of the relative likelihood of threats to its integrity and performance. Although it is relatively easy to identify multiple, diverse barriers that comprise the engineered and geologic systems, the performance of any of these systems and their respective subsystems cannot and should not be considered either truly

independent or totally redundant.

As stated earlier, NWPA mandated that technical criteria developed by the Commission "...shall provide for the use of a system of multiple barriers in the design of the repository." How the performance of those barriers should be assessed, consistent with the Commission's policy of defense-in-depth, was a major issue throughout the development and promulgation of the Commission's generic regulations at 10 CFR Part 60 and continues to be of concern as the Commission contemplates new regulations for Yucca Mountain.

Well before NWPA was enacted, the Commission had considered the appropriate bases for establishing regulations for HLW disposal. In developing proposed generic technical criteria for Part 60, the Commission placed primary emphasis on the need to compensate for the large uncertainty that is inherent in the assessment of the long-term performance of HLW disposal systems. The Commission expressed its view, then, that the state-of-the-art in the earth sciences was such that all the uncertainties related to predicting long-term performance of a repository could not be resolved through consideration of the geologic setting alone.

It should be noted that during the late 1970s and early 1980s, when the Commission was first considering the development of proposed technical criteria for geologic repositories, quantitative techniques for assessing repository performance were in their infancy. The lack of experience with, and confidence in, quantitative methods for addressing the uncertainties associated with estimates of repository performance weighed heavily as the Commission considered options for formulating generic regulations for HLW disposal. As will be discussed later in this statement, the Commission now believes that the application of such methods has matured sufficiently to move away from its earlier approach.

As Part 60 was being developed, the Commission gave serious consideration to a "systems approach," that is, regulation of a repository system through a single figure of merit,

that of overall system performance, leaving maximum flexibility for determining the extent and focus of site characterization, and for the designer to make trade-offs among components of the system. It was noted that this approach could include a requirement that the system design incorporate multiple barriers to compensate for uncertainty in overall system performance. It was believed, at the time, however, that compensation for uncertainties in assessing the system's overall performance could only be achieved by introducing conservatism. Intentional addition of conservatism, either by making the measure of performance unduly stringent or by using worst-case, bounding assumptions in the evaluation, was argued to be impractical from a regulatory point of view.

Instead, the Commission opted to prescribe minimum performance standards for each of the major system elements (as they were envisioned at the time) as well as to require the overall system to comply with the primary performance objective, namely, whatever standards EPA would eventually establish. This approach was thought to have two advantages over the systems approach, if the barriers were chosen judiciously. It was argued that barriers could be prescribed, generically, which act "independently," and that generic performance measures for these "independent" barriers could be selected that would reduce calculational uncertainty. Identification of such subsystem performance measures was expected to be helpful input to DOE's design process, without being overly restrictive. It is now recognized that NRC attempted to define such criteria on the basis of limited, existing knowledge, without benefit of research and site-specific information that only later was acquired during characterization of a specific site at Yucca Mountain.

The vast majority of comments received on the proposed Part 60 favored a "systems approach." Nevertheless, in publishing its final rule (48 FR 28194), the Commission elected to retain the proposed approach, stating that "...in simply adopting the EPA standard as the sole

measure of performance, it [the Commission] would have failed to convey in any meaningful way the degree of confidence which it expects must be achieved in order for it to be able to make the required licensing decisions” and, further that “...The Commission firmly believes that the performance of the engineered and natural barriers must each make a definite contribution in order for the Commission to be able to conclude that the EPA standard will be met.”

In support of the final rule, the Commission examined how particular values for the performance of the proposed barriers would assist in concluding that compliance with the EPA standards had been demonstrated, given an assumed set of anticipated processes and events. Final EPA standards still had not been promulgated, so analyses were conducted based on NRC staff assumptions regarding the final standards. These analyses, based on a simplified modeling study for a hypothetical repository located in a variety of saturated geologic media, were documented as NUREG-0804 -- “Staff Analyses of Public Comments on Proposed Rule 10 CFR Part 60, Disposal of High-Level Radioactive Wastes in Geologic Repositories.” For many, but by no means all, of the cases examined, compliance with the proposed subsystem performance objectives did increase the probability of meeting the assumed EPA standards. NRC was not able to demonstrate, however, that compliance with the subsystem criteria alone was sufficient to meet the assumed EPA standards, nor that compliance with the assumed EPA standards would suffice to assure compliance with the subsystem criteria. For the cases analyzed, however, it was asserted that the analyses “...demonstrate that compliance with 10 CFR Part 60 can substantially increase confidence that the assumed EPA standard[s] will be met.”

Lastly, in order to address concerns that quantitative subsystem performance criteria may unduly restrict the applicant’s flexibility, the Commission modified the proposed rule to explicitly recognize the potential need to change the subsystem objectives to account for unique,

features of a specific site or design. This flexibility was provided at § 60.113 (b).

Since their promulgation, the subsystem criteria in § 60.113, in particular, have not gained broad acceptance in the technical community. These criteria have been criticized as

overly prescriptive, lacking in both a strong technical basis and a clear technical nexus to the overall performance objective (*i.e.*, the EPA standards), and unclear in their wording.

In contrast to the state of performance assessment technology assumed at the time Part 60 criteria were put in place, the NAS Committee on Technical Bases for Yucca Mountain Standards found, in 1995, that the physical and geologic processes relevant to a Yucca Mountain repository: "...are sufficiently quantifiable and the related uncertainties sufficiently boundable that the performance [of a repository] can be assessed over timeframes during which the geological system is relatively stable or varies in a boundable manner." As has been described earlier, it was a lack of confidence in this capability to quantify overall performance and adequately bound uncertainty that factored prominently in the Commission's decision to include quantitative subsystem requirements in the Part 60 regulations. Also, as discussed earlier, NAS cautioned against implementation of multiple barriers through the use of subsystem performance requirements. In addition, the Commission's Advisory Committee on Nuclear Waste (ACNW) recently recommended that the Commission implement the concept of defense in depth by ensuring that the effectiveness of individual barriers be identified explicitly in the total system performance assessment (TSPA), but specifically did not endorse the establishment of rule-based subsystem requirements for Yucca Mountain. The ACNW noted that "...an overall performance-based regulation in the context of a risk-based standard is a superior tool for promoting safety relative to imposed subsystem requirements. (see letters dated October 31, 1997 and March 6, 1998)."

Upon review of this regulatory history, the Commission is persuaded that much of the basis for NRC's initial development of the specific numerical values for the subsystem criteria was generic judgment with regard to what was (and was not) feasible with regard to the quantitative assessment of long-term repository performance. Because the stated goal was to compensate for uncertainty, there was never any attempt to derive the subsystem performance criteria from a specified dose or risk level or from some projected dose or risk reduction expected to be achieved by their application. Furthermore, after 15 years of experience in working with the requirements of Part 60, the Commission is concerned that, for the Yucca Mountain site, the application of the subsystem performance criteria at § 60.113 may impose significant additional expenditure of resources on the nation's HLW program, without producing any commensurate increase in the protection of public health and safety.

Specifically, when the Part 60 subsystem criteria were selected, they were intended to be separate, "independent," easily-determined measures of subsystem performance, determination of which would require only application of technology that was readily available. Extensive experience with site-specific performance assessment has shown them to be none of these. For example, because container performance, release rate, and ground-water travel time will be derived from the same general data and knowledge base as the TSPA, they are subject to many, if not all, of the same uncertainties. Furthermore, waste package performance and release rate are both a function of available water; therefore, it is arguable whether the existing (or any other) subsystem measures can provide truly independent assurance of total system performance.

Nevertheless, despite its reconsideration of the merits of establishing quantitative criteria for the performance of repository subsystems, the Commission continues to believe that multiple barriers, as required by NWPA, must each make a definite contribution to the isolation



of waste at Yucca Mountain, so that the Commission may find, with reasonable assurance, that the repository system will be able to achieve the overall safety objective over timeframes of thousands of years. Geologic disposal of HLW is predicated on the expectation that a portion of the geologic setting will act as a barrier, both to water reaching the waste, and to dissolved radionuclides migrating away from the repository, and thus, contribute to the isolation of radioactive waste. Although there exists an extensive geologic record ranging from thousands to millions of years, this record is subject to interpretation and includes many uncertainties. These uncertainties can be quantified generally and are addressed by requiring the use of a multiple barrier approach; specifically, an engineered barrier system, consisting of one or more distinct engineered barriers, is required in addition to the natural barriers implicit in a geologic setting. Similarly, although the composition and configuration of engineered structures, as well as their capacity to function as barriers, can be defined with a degree of precision not possible for natural barriers, it is recognized that except for a few archaeological analogues, there is no experience base for the performance of complex, engineered structures over periods longer than a few hundred years. It is expected that DOE will demonstrate that the natural barriers and the engineered barrier system will work in combination to enhance overall performance of the geologic repository.

The Commission believes that this approach to multiple barriers is consistent with the NAS conclusions and recommendations cited above. The Commission also recognizes, and believes, it is important to acknowledge that experience and improvements in the technology of performance assessment, acquired over more than 15 years, now provide significantly greater confidence in the technical ability to assess comprehensively overall repository performance, and to address and quantify the corresponding uncertainty. In addition to extensive reviews of evolving TSPAs produced by DOE and its contractors, the Commission, itself, has developed

and exercised its own technical capability in the field of repository performance assessment (See, for example, Bonano, E. J., *et al.*, "Demonstration of a Performance Assessment Methodology for High-Level Waste Disposal in Basalt Formation," NUREG/CR-4759, U.S. Nuclear Regulatory Commission, Washington, DC, 1989; "Initial Demonstration of the NRC's Capability to Conduct a Performance Assessment for a High-Level Waste Repository," NUREG-1327, Division of Waste Management, NUREG-1327, 1992; "NRC Iterative Performance Assessment Phase 2 - Development of Capabilities for Review of a Performance Assessment for a High-Level Waste Repository," NUREG-1464, 1995).

Drawing from this experience, the Commission is now proposing to require that DOE evaluate the behavior of barriers important to waste isolation in the context of the performance of the geologic repository. The Commission does not intend to specify numerical goals for the performance of individual barriers. Such an approach will require DOE to provide an analysis that: 1) identifies those design features of the engineered barrier system, and natural features of the geologic setting, that are considered barriers important to waste isolation; 2) describes the capability of these barriers to isolate waste, taking into account uncertainties in characterizing and modeling the barriers; and 3) provides the technical basis for the description of the capability of these barriers. In implementing this approach, the Commission proposes to incorporate flexibility into its regulations by requiring DOE to demonstrate that the geologic repository comprises multiple barriers but not prescribe which barriers are important to waste isolation or the methods to describe their capability to isolate waste.

DOE could select from a variety of methods in order to demonstrate the capability of barriers to isolate waste. Regardless of the method and the level of quantification, it is expected that the capability of individual barriers to perform their intended function and the relationship of that function to limiting radiological exposure would be described. In parallel with

this rulemaking, NRC staff is developing guidance in the form of a Yucca Mountain Review Plan. In this review plan, guidance will be provided on acceptable methods for demonstrating compliance with the multiple barrier requirement that could include, but not necessarily be limited to, performing sensitivity analyses, modeling the behavior of individual barriers, quantifying how individual barriers contribute to performance, and delineating the capabilities of the barriers to isolate waste. The Commission believes that it is appropriate to afford DOE flexibility in selecting the methods to demonstrate the waste isolation capability of the multiple barriers that must comprise its repository design. The proposed requirements will provide for a system of multiple barriers and an understanding of the resiliency of the geologic repository provided by the barriers important to waste isolation to ensure defense in depth and increase confidence that the postclosure performance objective will be achieved.

## **IX. Performance Assessment**

Demonstration of compliance with the postclosure performance objective specified at § 63.113(b) requires a performance assessment that quantitatively estimates the expected annual dose, over the compliance period and weighted by probability of occurrence, to the average member of the critical group. Performance assessment is a systematic analysis of what can happen at the repository after permanent closure, how likely it is to happen, and what can result, in terms of dose to the average member of the critical group. Taking into account, as appropriate, the uncertainties associated with data, methods, and assumptions used to quantify repository performance, the performance assessment is expected to provide a quantitative evaluation of the overall system's ability to achieve the performance objective (§ 63.113 (b)). Consistent with EnPA and the NAS recommendations, the Commission

proposes that the results of performance assessment shall be the sole quantitative measure used to demonstrate compliance with the postclosure individual dose limit.

In order to find that issuance of a license will not constitute an unreasonable risk to the health and safety of the public, the Commission must have reasonable assurance that the required performance assessment has demonstrated that, following permanent closure, for the duration of the compliance period and considering the likelihood of occurrence of adverse natural events, annual exposures to the average member of the critical group will not exceed the individual dose limit of .25 mSv (25 mrem) TEDE. Although the performance objective for the geologic repository after permanent closure (§ 63.113) is generally stated in unqualified terms, it is not expected that complete assurance that the requirement will be met can be presented. A reasonable assurance, on the basis of the record before the Commission, that the performance objective will be met is the general standard that is required. Proof that the geologic repository will be in conformance with the objective for postclosure performance is not to be had in the ordinary sense of the word because of the uncertainties inherent in the understanding of the evolution of the geologic setting, biosphere, and engineered barrier system. For such long-term performance, what is required is reasonable assurance, making allowance for the time period, hazards, and uncertainties involved, that the outcome will be in conformance with the objective for postclosure performance of the geologic repository. Demonstrating compliance, by necessity, will involve the use of complex predictive models that are supported by limited data from field and laboratory tests, site-specific monitoring, and natural analog studies that may be supplemented with prevalent expert judgment. Further, in reaching a determination of reasonable assurance, the Commission may supplement numerical analyses with qualitative judgments including, for example, consideration of the degree of diversity or redundancy among the multiple barriers of the geologic repository.

Because of the significance of the performance assessment as the sole quantitative measure of compliance, it is essential that the performance assessment be scientifically defensible and transparent. For this reason, the Commission considers it important to specify, at § 63.114, requirements for a complete and high-quality performance assessment. A defensible performance assessment should contain a technical rationale for those features, events, and processes that have been included in the performance calculation, as well as those that have been considered but were excluded. The features, events, and processes (i.e., specific conditions or attributes of the geologic setting; degradation, deterioration, or alteration of the engineered barriers; and interactions between the natural and engineered barriers) considered for inclusion in the assessment should represent a wide range of beneficial and detrimental effects on performance. Features, events, and processes should be considered in light of available data and current scientific understanding, and alternative conceptual models that are consistent with such data and understanding should be evaluated. Inclusion of alternative models should be based, however, on reasonable interpretation of available information, and should not be driven by open-ended speculation. To this end, the Commission is proposing to constrain speculation by defining a lower limit on the probability of events and processes that need to be considered and requiring inclusion of only those features and processes, and higher probability events that significantly change the expected annual dose.

The performance assessment will rely, by necessity, on computer modeling to determine whether a proposed geologic repository meets the performance objectives. Such reliance on computer simulation has become commonplace for determining the likely performance of complex engineered systems. In most applications, it is accompanied by a rigorous testing program, involving model "validation" and "verification," to ensure that the simulated system behavior is sufficiently consistent with empirically observed behavior to meet

the need of the application at hand. The Commission expects that DOE will take reasonable and practical measures to ensure that its performance assessment provides a credible representation of a geologic repository at Yucca Mountain. For example, assurance of the soundness of the performance assessment cannot and will not involve the comparison of simulated behavior of a geologic repository with empirical observation over tens of kilometers and tens of thousands of years. At best, assurance for the performance assessment will involve comparison of simulations with observations drawn from an integrated program of laboratory tests, field tests, and analog studies that starts with site characterization and continues, as appropriate, through the performance confirmation period. To the extent that DOE's performance assessment provides a credible representation of a geologic repository, the Commission expects no more than that and believes that no more is needed. When the NWSA became law in 1982, and when it was revisited in 1987, and again in 1992, the limits on human knowledge that are attendant to confirming performance of a geologic repository were well known. The Commission does not believe that these laws were passed with the intention of creating an impossible task. Accordingly, the Commission has included, at §§ 63.101(a)(2) and 63.101(b), explanations regarding the purpose and nature of the findings it will make.

To be transparent, DOE's performance assessment must contain an evaluation of the performance of the geologic repository relative to compliance with the individual dose limit and an explanation of how the estimated performance was achieved. Section 63.113(b) requires that compliance with the individual dose limit be demonstrated through the calculation of an expected annual dose. The expected annual dose is the expected value of the annual dose considering the probability of the occurrence of the events and the uncertainty, or variability, in parameter values used to describe the behavior of the geologic repository (the expected annual dose is calculated by accumulating the dose estimates for each year, where the dose estimates

are weighted by the probability of the events and the parameters leading to the dose estimate). Demonstration of compliance with the individual dose limit will need to include an estimate of the expected annual dose to the average member of the critical group that, for any single year within the compliance period, is below the limit. Explanation of how the estimated performance was achieved should reveal an understanding of the relationship between the performance of individual components or subsystems of the geologic repository and the total system performance. Such understanding would be used to build confidence that the expected annual dose, as asserted in the license application, is a reasonable estimate of the performance of the geologic repository. Consistent with a performance-based philosophy, the Commission proposes to permit DOE the flexibility to select the approach for demonstrating this relationship that is most appropriate to its analysis.


#### **X. Institutional Controls**

The Commission is proposing to require DOE to institute active, as well as passive, control measures to reduce the potential for inadvertent human intrusion into the site. Reasonably prudent, active institutional controls, consistent with the requirements of Section 801(c) of EnPA, should be maintained at the site for as long as possible. The Commission is also proposing that DOE's passive control measures should be designed to serve their intended purpose for as long as practicable.

Section 801(b) of EnPA requires that:

...the Commission's requirements assume, to the extent consistent with the findings and recommendations of the National Academy of Sciences, that following repository closure, the inclusion of engineered barriers and the Secretary's postclosure oversight

## MEMORANDUM

TO: Andrew C. Campbell  
FROM: J. N. Sorensen   
DATE: February 11, 1999  
SUBJECT: Defense in Depth in the Geologic Repository

Introduction

Defense in depth is a safety strategy which provides successive protective measures to guard against unwanted events. In the field of nuclear safety, the term is commonly used in two different senses. The first is to denote an overall safety philosophy such as: (1) prevent accident initiators from occurring, (2) terminate accident sequences quickly, and (3) mitigate accidents that are not successfully terminated. The second usage is to denote multiple physical barriers preventing the release of radioactive materials. In the case of a radioactive waste repository, the term defense in depth is usually understood to mean the multiple engineered and geologic barriers established between the waste and the human environment.

Although there is no preferred definition in the regulatory context, there seems to be general agreement on a few essential attributes. The first such attribute is the idea of successive barriers; if one barrier fails, another barrier is available to perform nearly the same function. The second attribute is that the barriers provided should be independent of one another, and not be subject to a common failure mode. The third attribute is the concept of providing a suitable balance between the prevention of unwanted events, and mitigating the consequences of such events.

Department of Energy's Treatment of Defense in Depth

A preliminary review of the "Repository Safety Strategy," (RSS, YMP/96-01, Revision 2), relevant parts of the TSPA-VA Technical Basis Document (TBD, Chapter 11) and the Viability Assessment of a Repository at Yucca Mountain (VA), reveals frequent references to defense in depth as an essential element of ensuring satisfactory post-closure performance. At this stage in the evolution of the design, however, the analysis<sup>s</sup> which will establish the degree of defense in depth that can be achieved have not been done.



The RSS identifies five elements of a competent postclosure safety case:

- Assessment of expected postclosure performance and supporting evidence
- Design margin and defense in depth
- Consideration of disruptive processes and events
- Insights from natural and man-made analogs
- A performance confirmation plan.

The document then defines design margin as the ". . . margin of safety incorporated in specifications for engineered components in order to account for uncertainty in the conditions and variability in the material properties." Defense in depth is defined as ". . . the use of multiple barriers to mitigate uncertainties in conditions, processes and events." The brief discussion which follows these definitions treats "design margin and defense in depth" together, and does not distinguish one from the other. The RSS states that the repository system ". . . will rely on multiple engineered and natural barriers against the movement of water and radionuclides and invoke other measures beyond those that can be explicitly demonstrated in a total system performance assessment." It goes on to say, "Explicit analyses to address design margin and defense in depth have not yet been conducted." This is followed by a discussion of the nature of the work needed to complete the safety case, which again does not separate design margin from defense in depth.

The RSS concludes the discussion of defense in depth by saying "The system evaluations of design margin and defense in depth will evaluate system performance for the designs under consideration, and assess both the uncertainty in that estimate and the degree of margin in meeting performance criteria. They will evaluate design margin in particular by considering the effect of neutralizing each of the barriers that contribute to performance. These analyses will transparently display the degree of reliance on individual elements of the system and the degree to which lower than expected performance of one barrier may be compensated for the performance of another."

In a December 1998 presentation to the ACNW, the CRWMS M&O Contractor discussed postclosure defense in depth. In that presentation it was stated that "defense in depth [is] needed to assure safety when quantitative assessment

includes significant uncertainties." Defense in depth was then described as a ". . . safety philosophy that employs multiple protective measures to ensure that failure in any one of them does not imply failure of the entire system." The concept was further amplified by stating that, "In general, defense in depth means

- Multiple physical barriers to assure safety in design basis events
- Conservatism, redundancy, and diversity in system design
- Other measures (e.g., QA, emergency plans)."

The process for evaluating defense in depth was described as:

- "Evaluate expected performance and identify principal barriers
- Determine threats to performance -- select neutralizations
- Neutralize barriers reflecting threats -- determine contribution of each barrier to total system performance
- Evaluate overall postclosure defense in depth provided by system."

The presentation included two examples of the above process, one evaluating the contribution of overlying rock units and one evaluating the contribution of the drift invert. Neither example included quantitative results.

The development and evaluation of defense in depth is not carried any farther in the Viability Assessment published in December 1998. The concept of defense in depth is discussed, along with its role in establishing the repository design, but no systematic evaluation of defense in depth for a conceptual design has been undertaken. As a result, it is not yet possible to arrive at a judgement that the repository design is likely to meet NRC expectations with respect to defense in depth.

### Current Regulatory Requirements

For the geologic repository, defense in depth has been firmly identified with multiple physical barriers, and possibly with the provisions that might be made to protect those barriers. Attributes ascribed to defense in depth in active systems (redundancy, diversity and independence) may not be truly achievable in a completely passive system.

This may be true especially where some of the key parameters (those associated with the geologic setting) cannot be controlled.

The proposed 10 CFR 63 does not define defense in depth, nor does the term appear in the rule itself. The supplementary information to be published with the proposed rule contains a discussion of multiple barriers and defense in depth. That discussion states, in part, "The defense-in-depth principle has served as a cornerstone of NRC's deterministic regulatory framework for nuclear reactors, and it provides an important tool for making regulatory decisions, with regard to complex facilities, in the face of significant uncertainties." This is followed by a discussion of the relationship between multiple barriers and defense in depth in the context of a geologic repository, and ultimately concludes, "The Commission does not intend to specify numerical goals for the performance of individual barriers. Such an approach will require DOE to provide an analysis that: 1) identifies those design features . . . that are considered important to waste isolation; 2) describes the capabilities of these barriers to isolate waste . . . and 3) provides the technical basis for the description of the capability of these barriers." The requirement for defense in depth is thus limited to a requirement for multiple barriers and a requirement to display the contribution of each barrier to the waste isolation function.

Although no judgements can yet be made on the ease or difficulty of incorporating adequate provisions for defense in depth in the geologic repository, the regulatory context described above suggests some observations on DOE's discussion of defense in depth. The first observation is that DOE has not clearly differentiated the concept of defense in depth from the concept of design margin and other contributors to meeting the overall system performance standard. Normal engineering practice includes conservative design, appropriate margins of safety, and assurance of the quality of design, fabrication and installation. Defense in depth, which DOE often mentions in the same sentence with design margin, is fundamentally different. Defense in depth incorporates the concepts of redundancy, diversity, and independence. Design margin is the concept of providing more of something that is already present, such as greater material thickness or more heat transfer capacity.

The overall impression from the DOE discussions of defense in depth is that everything that somehow increases the probability of meeting the performance standard is part of defense in depth. One example is DOE's inclusion of quality assurance as an element of defense in depth. Some authorities (for example, the International Safety Advisory Group of the IAEA) do not consider QA to be an element of defense in depth. Within the context created by the proposed Part 63, quality assurance is neither a physical nor a systematic barrier. Rather, it is an integral component of all barriers or lines of defense. In particular, it is difficult to see how the contribution of QA to overall system performance can be isolated and displayed as contemplated by Part 63.

#### Guidance on Defense in Depth in Reactor Regulation

In 1998, the reactor regulatory staff published Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis." This guide establishes an approach to risk-informed decision making, acceptable to the staff, which includes the provision that proposed changes to the current licensing basis be must consistent with the defense in depth philosophy. The guide then states that consistency with the defense in depth philosophy is maintained if:

- a reasonable balance among prevention of core damage, prevention of containment failure, and consequence mitigation is preserved
- over-reliance on programmatic activities to compensate for weakness in plant design is avoided
- system redundancy, independence, and diversity are preserved commensurate with the expected frequency, and consequences of challenges to the system and uncertainties . . .
- defenses against potential common cause failures are preserved and the potential for introduction of new common cause failure mechanisms is assessed
- independence of barriers is not degraded
- defenses against human error are preserved

- the intent of the General Design Criteria in 10 CFR Part 50, Appendix A, is maintained.

It is apparent that these seven attributes of defense in depth have little applicability to a passive system such as the repository. The idea of balance, avoiding over reliance on a single barrier, has meaning in the repository. The concepts of redundancy, diversity, and independence also are meaningful, but they may not be achievable in a system that partially depends on the natural setting.

It is not unreasonable to contemplate that guidance, similar to that described above for reactors, may be required for the repository. Both the NRC staff and the applicant may require some criteria for judging the acceptability of provisions for defense in depth.

c: R. P. Savio  
J. T. Larkins

February 24, 1999

**MEMORANDUM TO:** William D. Travers  
Executive Director for Operations

**FROM:** Annette L. Vietti-Cook, Secretary /s/

**SUBJECT:** STAFF REQUIREMENTS - SECY-98-144 - WHITE PAPER ON  
RISK-INFORMED AND PERFORMANCE-BASED REGULATION

The Commission has approved the issuance of the white paper which defines the terms and Commission expectations for risk-informed and performance-based regulation. The paper should be prepared for issuance by the Commission for use by the NRC and interested parties.

**Attachment:**  
As stated

**cc:** Chairman Jackson  
Commissioner Dicus  
Commissioner Diaz  
Commissioner McGaffigan  
Commissioner Merrifield  
OGC  
CIO  
CFO  
OCA  
OIG  
OPA  
Office Directors, Regions, ACRS, ACNW, ASLBP (via E-Mail)  
PDR  
DCS

### Risk-Informed and Performance-Based Regulation

The NRC has established its regulatory requirements, in both reactor and materials applications, to ensure that “no undue risk to public health and safety” results from licensed uses of Atomic Energy Act (AEA) materials and facilities. The objective of these requirements has always been to assure that the probabilities of accidents with the potential for adversely affecting public health and safety are low. For reactors, these probabilities were not quantified in a systematic way until 1975 when the Reactor Safety Study (WASH-1400) was published. For non-reactor activities, the situation is more complex. In some areas, high-level waste disposal and transportation, risk assessment has been in use since the 1970s; in others, such quantification is still evolving. Consequently, most of NRC’s regulations were developed without the benefit of quantitative estimates of risk. The perceived benefits of the deterministic and prescriptive regulatory requirements were based mostly on experience, testing programs and expert judgment, considering factors such as engineering margins and the principle of defense-in-depth.

There have been significant advances in and experience with risk assessment methodology since 1975. Thus, the Commission is advocating certain changes to the development and implementation of its regulations through the use of risk-informed, and ultimately performance-based approaches. The Probabilistic Risk Assessment (PRA) Policy Statement (60 FR 42622, August 16, 1995) formalized the Commission’s commitment to risk-informed regulation through the expanded use of PRA. The PRA Policy Statement states, in part, “The use of PRA technology should be increased in all regulatory matters to the extent supported by the state of the art in PRA methods and data, and in a manner that complements the NRC’s deterministic approach and supports the NRC’s traditional defense-in-depth philosophy.”

The transition to a risk-informed regulatory framework is expected to be incremental. Many of the present regulations are based on deterministic and prescriptive requirements that cannot be quickly replaced. Therefore, the current requirements will have to be maintained while risk-informed and/or performance-based regulations are being developed and implemented.

To understand and apply the commitment expressed in the PRA Policy Statement, it is important that the NRC, the regulated community, and the public at large have a common understanding of the terms and concepts involved; an awareness of how these concepts (in both reactor and materials arenas) are to be applied to NRC rulemaking, licensing, inspection, assessment, enforcement, and other decision-making; and an appreciation of the transitional period in which the agency and industry currently operate.

1. Risk and Risk Assessment: This paper defines risk in terms that can be applied to the entire range of activities involving NRC licensed use of AEA materials. The risk definition takes the view that when one asks, “What is the risk?” one is really asking three questions: “What can go wrong?” “How likely is it?” and “What are the consequences?” These three questions can be referred to as the “risk triplet.” The traditional definition of risk, that is, probability times consequences, is fully embraced by the “triplet” definition of risk.

The first question, "What can go wrong?" is usually answered in the form of a "scenario" (a combination of events and/or conditions that could occur) or a set of scenarios.

The second question, "How likely is it?" can be answered in terms of the available evidence and the processing of that evidence to quantify the probability and the uncertainties involved. In some situations, data may exist on the frequency of a particular type of occurrence or failure mode (e.g., accidental overexposures). In other situations, there may be little or no data (e.g., core damage in a reactor) and a predictive approach for analyzing probability and uncertainty will be required.

The third question, "What are the consequences?" can be answered for each scenario by assessing the probable range of outcomes (e.g., dose to the public) given the uncertainties. The outcomes or consequences are the "end states" of the analyses. The choice of consequence measures can be whatever seems appropriate for reasonable decision-making in a particular regulated activity and could involve combinations of end states.

A risk assessment is a systematic method for addressing the risk triplet as it relates to the performance of a particular system (which may include a human component) to understand likely outcomes, sensitivities, areas of importance, system interactions and areas of uncertainty. From this assessment the important scenarios can be identified.

2. Deterministic and Probabilistic Analyses: All safety regulation ultimately is concerned with risk and addresses the three questions discussed in item 1 above. In practice, NRC addresses these three questions through the body of regulations, guidance, and license conditions that it uses to regulate the many activities under its jurisdiction. The current body of regulations, guidance and license conditions is based largely on deterministic analyses and implemented by prescriptive requirements. As described in the PRA Policy Statement, the deterministic approach to regulation establishes requirements for engineering margin and for quality assurance in design, manufacture, and construction. In addition, it assumes that adverse conditions can exist and establishes a specific set of design basis events (i.e., what can go wrong?). The deterministic approach involves implied, but unquantified, elements of probability in the selection of the specific accidents to be analyzed as design basis events. It then requires that the design include safety systems capable of preventing and/or mitigating the consequences (i.e., what are the consequences?) of those design basis events in order to protect public health and safety. Thus, a deterministic analysis explicitly addresses only two questions of the risk triplet. In addition, traditional regulatory analyses do not integrate results in a comprehensive manner to assess the overall safety impact of postulated initiating events.

PRA and other risk assessment methods (also described in the PRA Policy Statement) considers risk (i.e., all three questions) in a more coherent, explicit, and quantitative manner. Risk assessment methodology examines systems and their interactions in a integrated, comprehensive manner. Probabilistic analysis explicitly addresses a broad spectrum of initiating events and their event frequency. It then analyzes the consequences of those event scenarios and weights the consequences by the frequency, thus giving a measure of risk.

Since risk assessment methods were first used to gain a better understanding of the risk



associated with some of the activities and facilities that NRC regulates, substantial event data and increased sophistication and experience in the use of certain risk assessment methods (e.g., Probabilistic Risk Assessment (PRA), Integrated Safety Assessment (ISA), and Performance Assessment (PA)) has been acquired. Accordingly, there is now the opportunity to enhance the traditional approach by more explicitly addressing risk and incorporating the insights thus gained.

While the traditional deterministic approach to regulation has been successful in ensuring no undue risk to public health and safety in the use of nuclear materials, opportunities for improvement exist. Given the broad spectrum of equipment and activities covered, the regulations can be strengthened and resources allocated to ensure that they are focused on the most risk-significant equipment and activities, and to ensure a consistent and coherent framework for regulatory decision-making. The different “risk-informed” and/or “performance-based” approaches to regulation described below, if properly applied singly or in combination, would provide such a framework.

3. **“Risk Insights”**: The term “risk insights”, as used here, refers to the results and findings that come from risk assessments. The end results of such assessments may relate directly to public health effects as in the Commission’s Safety Goals for the Operations of Nuclear Power Plants. For specific applications the results and findings may take other forms. For example, for reactors these include such things as identification of dominant accident sequences, estimates of core damage frequency (CDF)<sup>1</sup> and large early release frequency (LERF)<sup>2</sup>, and importance measures of structures, systems, and components. On the other hand, in other areas of NRC regulation, findings and results include risk curves<sup>3</sup> for disposal facilities for radioactive wastes, frequency of and costs associated with accidental smelting of sealed sources at steel mills, frequency of occupational exposures, predicted dose from decommissioned sites and many others.

Risk insights have already been incorporated successfully into numerous regulatory activities, and have proven to be a valuable complement to traditional deterministic approaches. Given the current maturity of some risk assessment methodologies and the current body of event data, risk insights can be incorporated more explicitly into the regulatory process in a manner that will improve both the efficiency and effectiveness of current regulatory requirements.

4. **“Risk-Based Approach”**: Regulatory decision-making is required in both the development of regulations and guidance and the determination of compliance with those regulations and guidance. A “risk-based” approach to regulatory decision-making is one in which such decision-making is solely based on the numerical results of a risk assessment. This places heavier reliance on risk assessment results than is currently

---

<sup>1</sup> CDF is the frequency of the combinations of initiating events, hardware failures, and human errors leading to core uncovering with reflooding of the core not imminent.

<sup>2</sup> LERF is the frequency of those accidents leading to significant, unmitigated releases from containment in a time-frame prior to effective evacuation of the close-in population such that there is a potential for early health effects.

<sup>3</sup> Risk curves (also known as Complementary Cumulative Distribution Functions (CCDFs) or Farmer curves) are estimates of the probability that a given consequence will be exceeded.

practicable for reactors due to uncertainties in PRA such as completeness. Note that the Commission does not endorse an approach that is “risk-based”; however, this does not invalidate the use of probabilistic calculations to demonstrate compliance with certain criteria, such as dose limits.

5. **“Risk-Informed” Approach:** A “risk-informed” approach to regulatory decision-making represents a philosophy whereby risk insights are considered together with other factors to establish requirements that better focus licensee and regulatory attention on design and operational issues commensurate with their importance to public health and safety. A “risk-informed” approach enhances the deterministic approach by: (a) allowing explicit consideration of a broader set of potential challenges to safety, (b) providing a logical means for prioritizing these challenges based on risk significance, operating experience, and/or engineering judgment, (c) facilitating consideration of a broader set of resources to defend against these challenges, (d) explicitly identifying and quantifying sources of uncertainty in the analysis (although such analyses do not necessarily reflect all important sources of uncertainty), and (e) leading to better decision-making by providing a means to test the sensitivity of the results to key assumptions. Where appropriate, a risk-informed regulatory approach can also be used to reduce unnecessary conservatism in purely deterministic approaches, or can be used to identify areas with insufficient conservatism in deterministic analyses and provide the bases for additional requirements or regulatory actions. “Risk-informed” approaches lie between the “risk-based” and purely deterministic approaches. The details of the regulatory issue under consideration will determine where the risk-informed decision falls within the spectrum.
6. **Risk-Informed and Defense-in-Depth Approach:** The concept of defense-in-depth<sup>4</sup> has always been and will continue to be a fundamental tenet of regulatory practice in the nuclear field, particularly regarding nuclear facilities. Risk insights can make the elements of defense-in-depth more clear by quantifying them to the extent practicable. Although the uncertainties associated with the importance of some elements of defense may be substantial, the fact that these elements and uncertainties have been quantified can aid in determining how much defense makes regulatory sense. Decisions on the adequacy of or the necessity for elements of defense should reflect risk insights gained through identification of the individual performance of each defense system in relation to overall performance.
7. **“Performance-Based Approach”:** A regulation can be either prescriptive or performance-based. A prescriptive requirement specifies particular features, actions, or programmatic elements to be included in the design or process, as the means for achieving a desired objective. A performance-based requirement relies upon measurable (or calculable) outcomes (i.e., performance results) to be met, but provides more flexibility to the licensee as to the means of meeting those outcomes. A performance-based regulatory approach is one that establishes performance and results

---

<sup>4</sup>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.

as the primary basis for regulatory decision-making, and incorporates the following attributes: (1) measurable (or calculable) parameters (i.e., direct measurement of the physical parameter of interest or of related parameters that can be used to calculate the parameter of interest) exist to monitor system, including facility and licensee performance, (2) objective criteria to assess performance based on risk insights, deterministic analyses and/or performance history, (3) licensees have flexibility to determine how to meet the established performance criteria in ways that will encourage and reward improved outcomes; and (4) a framework exists in which the failure to meet a performance criterion, while undesirable, will not in and of itself constitute or result in an immediate safety concern. The measurable (or calculable) parameters may be included in the regulation itself or in formal license conditions, including reference to regulatory guidance adopted by the licensee. This regulatory approach is not new to the NRC. For instance, the Commission previously has approved performance-based approaches in 10 CFR Parts 20, 50 (Option B, Appendix J and the Maintenance Rule, 10 CFR 50.65), 60, and 61. In particular, the Commission weighed the relative merits of prescriptive and performance-based regulatory approaches in issuing 10 CFR Part 60.

A performance-based approach can be implemented without the use of risk insights. Such an approach would require that objective performance criteria be based on deterministic safety analysis and performance history. This approach would still provide flexibility to the licensee in determining how to meet the performance criteria. Establishing objective performance criteria for performance monitoring may not be feasible for some applications and, in such cases, a performance-based approach would not be feasible.

As applied to inspection, a performance-based approach tends to emphasize results (e.g., can the pump perform its intended function?) over process and method (e.g., was the maintenance technician trained?). Note that a performance-based approach to inspection does not supplant or displace the need for compliance with NRC requirements, nor does it displace the need for enforcement action, as appropriate, when non-compliance occurs.<sup>5</sup>

As applied to licensee assessment, a performance-based approach focuses on a licensee's actual performance results (i.e., desired outcomes), rather than on products (i.e., outputs). In the broadest sense, the desired outcome of a performance-based approach to regulatory oversight will be to focus more attention and NRC resources on those licensees whose performance is declining or less than satisfactory.

8. **"Risk-Informed, Performance-Based"**: A risk-informed, performance-based approach to regulatory decision-making combines the "risk-informed" and "performance-based" elements discussed in Items 3 and 6, above, and applies these concepts to NRC rulemaking, licensing, inspection, assessment, enforcement, and other decision-making. Stated succinctly, a risk-informed, performance-based regulation is an approach in

---

<sup>5</sup>Not every aspect of licensed activities can or should be inspected using this approach. For example, if a licensee is unsuccessful in meeting the criteria defined by a performance-based regulation, the inspector should then focus on the licensee's process and method, to understand the root cause of the breakdown in performance, and to understand how future poor performance may be avoided.

which risk insights, engineering analysis and judgment including the principle of defense-in-depth and the incorporation of safety margins, and performance history are used, to (1) focus attention on the most important activities, (2) establish objective criteria for evaluating performance, (3) develop measurable or calculable parameters for monitoring system and licensee performance, (4) provide flexibility to determine how to meet the established performance criteria in a way that will encourage and reward improved outcomes, and (5) focus on the results as the primary basis for regulatory decision-making.

The definitions and concepts in this paper have proven suitable for application to nuclear power plants and certain non-reactor activities (e.g., PA of geologic repositories). While different in detail, these activities are similar in terms of system complexity and the application of probabilistic methods to the determination of safety. In simpler situations, the concepts and definitions should prove equally suitable provided that NRC adopts a flexible framework for the implementation of risk-informed, and ultimately performance-based regulation across the full spectrum of the materials, processes, and facilities regulated by the NRC.

May 19, 1999

The Honorable Shirley Ann Jackson  
Chairman  
U. S. Nuclear Regulatory Commission  
Washington, D.C. 20555-0001

Dear Chairman Jackson:

**SUBJECT: THE ROLE OF DEFENSE IN DEPTH IN A RISK-INFORMED REGULATORY SYSTEM**

During the 462<sup>nd</sup> and 461<sup>st</sup> meetings of the Advisory Committee on Reactor Safeguards, May 5-8 and April 7-10 1999, we discussed issues identified in the Staff Requirements Memorandum dated March 5, 1999, concerning the appropriate relationship and balance between probabilistic risk assessment (PRA) and defense in depth in the context of risk-informed regulation. We previously discussed this matter with the Commission during our meeting on February 3, 1999.

We are attempting to identify pitfalls that may exist along the path the Commission is taking toward risk-informed regulation so they may be addressed in a timely manner. We have communicated previously on the need for plant-specific safety goals that are practical for licensees to evaluate, the need for risk assessments for all modes of plant operation, and the need for research to support further use of risk information in regulatory activities. Several ACRS members, working with an ACRS Senior Fellow, have produced the attached paper in which two views of defense in depth are discussed along with a preliminary proposal regarding its role. Here, we further discuss the role that defense in depth should have in a risk-informed regulatory scheme.

Our motivation for this report has arisen because of instances in which seemingly arbitrary appeals to defense in depth have been used to avoid making changes in regulations or regulatory practices that seemed appropriate in the light of results of quantitative risk analyses. Certainly, we have seen defense in depth used as a basis for delaying changes in the existing regulatory practices:

- there has been reluctance to develop new, risk-informed limits on leakage from steam generator tubes because these are part of the defense-in-depth barriers,
- the development of extensions of the Regulatory Guide 1.174 process to define criteria for risk-informed revisions to 10 CFR 50.59 has been delayed because of defense in depth issues,

- the development of graded quality assurance measures has been overly conservative because of concerns about the imputed importance of quality assurance to defense in depth, and
- the development of regulatory requirements on software-based digital instrumentation and control systems was delayed because of concerns related to defense in depth.

We are concerned that arbitrary appeals to defense in depth could inhibit the effective use of risk information in the regulatory process. At the same time, we are mindful that risk analyses are not perfect. Defense in depth can be an effective means for compensating for any weaknesses in our ability to understand the risks posed by nuclear power plants.

As discussed in the attached paper, the defense-in-depth approach to safety arose in an earlier time when there was less capability to analyze a nuclear power plant as an integrated system. Subsystems were designed such that the necessity and sufficiency of defense in depth could be determined from experience and through exercising engineering judgment. Defense in depth was a design and operational philosophy that called for multiple layers of protection to prevent and mitigate accidents. Its practical implementation was most often associated with control of initiating event frequencies, redundancy and diversity in key safety functions, multiple physical barriers to fission-product release, and emergency response measures. This philosophy has been invoked primarily to compensate for uncertainty in our knowledge of the progression of accidents at nuclear power plants.

Improved capability to analyze nuclear power plants as integrated systems is leading us to reconsider the role of defense in depth. Defense in depth can still provide needed safety assurance in areas not treated or poorly treated by modern analyses or when results of the analyses are quite uncertain. To avoid conflict between the useful elements of defense in depth and the benefits that can be derived from quantitative risk assessment methods, constraints of necessity and sufficiency must be imposed on the application of defense in depth and these must somehow be related to the uncertainties associated with our ability to assess the risk.

We believe that two different perceptions of defense in depth are prominent. In one view (the "structuralist" view as described in the attached paper), defense in depth is considered to be the application of multiple and redundant measures to identify, prevent, or mitigate accidents to such a degree that the design meets the safety objectives. This is the general view taken by the plant designers. The other view (the "rationalist"), sees the proper role of defense in depth in a risk-informed regulatory scheme as compensation for inadequacies, incompleteness, and omissions of risk analyses. We choose here to refer to the inadequacies, incompleteness, and omissions collectively as uncertainties. Defense-in-depth measures are those that are applied to the design or operation of a plant in order to reduce the uncertainties in the determination of the overall regulatory objectives to acceptable levels. Ideally then, there would be an inverse correlation between the uncertainty in the results of risk assessments and the extent to which defense in depth is applied. For those uncertainties that can be directly evaluated, this inverse correlation between defense in depth and the uncertainty should be manifest in a sophisticated PRA uncertainty analysis.

When defense in depth is applied, a justification is needed that is as quantitative as possible of both the necessity and sufficiency of the defense-in-depth measures. Unless defense-in-depth measures are justified in terms of necessity and sufficiency, the full benefits of risk-informed regulation cannot be realized.

The use of quantitative risk-assessment methods and the proper imposition of defense-in-depth measures would be facilitated considerably by the availability of risk-acceptance criteria applicable at a greater level of detail than those we now have. Development of the additional risk-acceptance criteria would have to take into consideration safety objectives embodied in the existing regulations. For example, risk-acceptance criteria are needed to meet the Commission's safety objectives with respect to worker health and environmental contamination and to meet additional public health and safety objectives [e.g., total fatalities, land interdiction]. All of these may not be currently reflected in conventional risk assessments.

We believe that a key missing ingredient needed to place quantitative limits on defense-in-depth measures is acceptance values on the level of uncertainty for each safety objective. Setting such acceptance values is a policy role, very much like setting safety goal values. The uncertainties that are intended to be compensated for by defense in depth include all uncertainties (epistemic and aleatory). Not all of these are directly assessed in a normal PRA uncertainty analysis. Therefore, when acceptance values are placed on uncertainty, these would have to appropriately incorporate consideration of the additional uncertainties not subject to direct quantification by the PRA. These considerations would have to be determined by judgment and expert opinion. As a practical matter, we suggest that the acceptance values be placed on only those epistemic uncertainties quantifiable by the PRA but that these be set sufficiently low to accommodate the unquantified aleatory uncertainties.

When acceptance values have been chosen as policy for the regulatory objectives and their associated uncertainties, it would be possible to develop objective limits on the amount of defense in depth required for those design and operational elements that are subject to evaluation by PRA. To do this, it is necessary to incorporate the effects of the defense-in-depth measures into the PRA uncertainty analysis and the designer or regulator must be able to adjust the defense in depth until the acceptance levels for the regulatory objectives and the acceptance values for the associated uncertainties have both been achieved.

The balance between core damage frequency (CDF) and conditional containment failure probability (CCFP) can serve as an example of this defense-in-depth concept. We have previously recommended that CDF be elevated to a fundamental safety goal. Let us suppose, for example sake, that our acceptance value on this is  $10^{-4}$  per reactor year. If that is the value actually achieved by the design, then a CCFP of about 0.5 has been shown (NUREG-1150) to be generally sufficient to meet the safety goal regulatory objective of individual risk of prompt fatality [which can be adequately represented by an acceptance value of  $10^{-5}$  per reactor year on large, early release frequency (LERF) as noted in Regulatory Guide 1.174]. Does this CCFP provide sufficient defense in depth?

In our view, three acceptance criteria must be satisfied -- one each on CDF, LERF, and the epistemic uncertainty associated with LERF. The Safety Goal Policy Statement suggests

candidate acceptance values on CDF and LERF. In addition to these, we must establish the acceptance value on the uncertainty associated with LERF. For the particular value of LERF achieved, let's say that the acceptance value has been set by policy to be on the epistemic uncertainty that can be directly developed from the PRA [but which properly reflects the unquantified aleatory uncertainties]. Now suppose our PRA uncertainty analysis tells us that the quantified uncertainty for this design is greater than the acceptance value. Employing our concept, the design with the 0.5 CCFP does not have sufficient defense in depth. The design must, then, include provisions for more defense in depth [e.g., a better containment perhaps] or reduction of the LERF to values for which the achieved uncertainty is acceptable. The acceptance value on uncertainty for any given regulatory objective could be a function of the absolute value achieved for the regulatory objective. That is, as the achieved mean value for LERF gets further below the acceptance value, the acceptable level of uncertainty on its determination can be greater.

We believe this concept of defense in depth can provide a rational way to develop sufficiency limits wherever the defense-in-depth measures can be directly evaluated by PRA. We acknowledge however, that considerable judgment will have to be exercised to set limits on uncertainty, especially uncertainties not quantified by the PRA. Our preceding example suggests one approach to managing these uncertainties.

For those regulatory functions that are not well suited for PRA or where the current capabilities of PRAs are not sufficient, we suggest that the limits on application of defense in depth be placed at levels lower than the top-level safety objectives (see Figure 1 of attached paper). We emphasize that, even under these circumstances, the PRA can still dictate when defense in depth is needed. Let us illustrate how we envision defense in depth to be applied under these circumstances with an example. Fire is one of the initiating events of interest. PRAs quantify the occurrence of fires in nuclear power plants and, among other things, their impact on control and power cables. The plant response to the loss of the relevant systems (due to the loss of these cables) is also analyzed.

The frequency of fires in specific critical locations, that is, locations in which cables of redundant systems may be damaged, is estimated in the PRA using experience-based rates of occurrence of fires, multiplied by subjective estimates of the fraction of fires that are large enough to have the potential to cause damage and the fraction of those fires that occur in the specified critical locations. This is a highly subjective part of the risk assessment (therefore, highly uncertain). It is, therefore, a suitable area to invoke defense in depth and to impose prescriptive requirements regarding the prevention of fires in those critical locations [e.g., strict administrative controls and periodic inspections]. Thus, the relative inadequacy of the PRA model suggests how defense in depth should be applied at levels lower than the top-level safety objectives.

We further realize that the fire risk assessment does not include the damaging effects of the smoke generated by a fire. This is a case of omission of a potentially significant effect. Therefore, we would, again, resort to defense in depth and may demand barriers to limit the spread of smoke and to protect sensitive equipment.

Since the impact on the risk metrics of these lower-level defense-in-depth measures cannot be quantified, nor can the uncertainties, the necessity and sufficiency of the defense-in-depth



measures will have to be simply prescribed and that prescription would constitute the acceptance criteria.

We note that our first example dealing with CDF and CCFP addresses the top level of Figure 1 of the attached paper. If one adopts the structuralist viewpoint at that level, as the paper's preliminary proposal suggests, then the tradeoffs of our example between CDF and CCFP will have to be performed under the assumption that at least some level of defense in depth will be required. If, on the other hand, one adopts the rationalist view even at that level, it is conceivable that the LERF objectives could be satisfied without a containment. Our second example dealing with fires exemplified the rationalist view at lower levels, as the preliminary proposal recommends.

We acknowledge that these preliminary thoughts on the role of defense in depth in a risk-informed regulatory system identify a direction but fall short of closing the issue. We recommend that the Commission give further consideration to this matter.

Sincerely,

Dana A. Powers  
Chairman

References:

1. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," July 1998.
2. U. S. Nuclear Regulatory Commission, NUREG-1150, Vols. 1-3, "Severe Accident Risks: An Assessment for Five U. S. Nuclear Power Plants," December 1990.
3. Report dated August 15, 1996, from T. S. Kress, Chairman, ACRS, to Shirley A. Jackson, Chairman, NRC, Subject: Risk-Informed, Performance-Based Regulation and Related Matters.
4. Memorandum dated March 5, 1999, from Annette Vietti-Cook, Secretary of the NRC, to John T. Larkins, Executive Director, ACRS, Subject: Staff Requirements - Meeting with the Advisory Committee on Reactor Safeguards, February 3, 1999.

Attachment:

U. S. Nuclear Regulatory Commission, Advisory Committee on Reactor Safeguards, J. N. Sorensen, G. E. Apostolakis, T. S. Kress, D. A. Powers, "On the Role of Defense in Depth in Risk-Informed Regulation," to be presented at PSA 1999, August 22-25, 1999.

# **ON THE ROLE OF DEFENSE IN DEPTH IN RISK-INFORMED REGULATION**

**To be presented at PSA '99  
Washington, D.C.  
August 22-25, 1999**

**J. N. Sorensen, Senior Fellow  
G. E. Apostolakis, Member  
T. S. Kress, Member  
D. A. Powers, Member**

**Advisory Committee on Reactor Safeguards  
U. S. Nuclear Regulatory Commission  
Washington, D.C. 20555-0001**

## **ABSTRACT**

The nascent implementation of risk informed regulation in the United States suggests a need for reexamination of the Nuclear Regulatory Commission's (NRC) defense in depth philosophy and its impact on the design, operation, and regulation of nuclear power plants. This reexamination is motivated by two opposing concerns: (1) that the benefits of risk informed regulation might be diminished by arbitrary appeals to defense in depth, and (2) that the implementation of risk informed regulation could undermine the defense in depth philosophy. From either perspective, two questions are suggested: (1) How is defense in depth defined? (2) How should the implementation of risk informed regulation alter our view of defense in depth? A preliminary proposal for the role of defense in depth in a risk-informed regulatory system is presented.

## **HISTORICAL DEVELOPMENT**

Defense in depth is a nuclear industry safety strategy that began to develop in the 1950s. A review of the history of the term indicates that there is no official or preferred definition. Where the term is used, if a definition is needed, one is created consistent with the intended use of the term. Such definitions are often made by example.

In a 1967 statement<sup>1</sup> submitted to the Joint Committee on Atomic Energy by Clifford Beck, then Deputy Director of Regulation for the Atomic Energy Commission, three basic lines of defense for nuclear power reactor facilities were described. The first line was the prevention of accident initiators through superior quality of design, construction and operation. The second line was engineered safety systems designed to prevent mishaps from escalating into major accidents. The third line was consequence-limiting safety systems designed to confine or minimize

the escape of fission products to the environment.

A 1969 paper<sup>2</sup> by an internal study group of the Atomic Energy Commission identified the issue of balance among accident prevention, protection, and mitigation, with the conclusion that the greatest emphasis should be put on prevention, the first line of defense.

A 1994 NRC document<sup>3</sup> identifies the elements of the defense in depth safety strategy as accident prevention, safety systems, containment, accident management, and siting and emergency plans. Other interpretations of defense in depth can be found in INSAG-3<sup>4</sup> and INSAG-10<sup>5</sup>

The historical record indicates an evolution of the term from a narrow application to the multiple barrier concept to an expansive application as an overall safety strategy. The term has increased in scope and gained stature over time. The history also indicates that defense in depth is considered to be a concept, an approach, a principle or a philosophy, as opposed to being a regulatory requirement per se.

Currently the term is commonly used in two different senses. The first is to denote the philosophy of high level lines of defense, such as prevent accident initiators from occurring, terminate accident sequences quickly, and mitigate accidents that are not successfully terminated. The second is to denote the multiple physical barrier approach, most often exemplified

by the fuel cladding, primary system, and containment.

One of the essential properties of defense in depth is the concept of successive barriers or levels. This concept applies equally well to multiple physical barriers and to high level lines of defense. A closely related attribute would be requiring a reasonable balance among prevention, protection and mitigation.

## EMERGING REGULATORY PRACTICE

The most recent NRC policy statement that deals with defense in depth is the Probabilistic Risk Assessment (PRA) Policy statement<sup>6</sup> published in 1995, which states, in part:

“The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC’s deterministic approach and supports the NRC’s traditional defense-in-depth philosophy.”

The policy statement, thus, places PRA in a subsidiary role to defense in depth.

In 1998, the NRC published Regulatory Guide 1.174.<sup>7</sup> This guide establishes an approach to risk-informed decision making, acceptable to the NRC staff, which includes the provision that proposed changes to the current licensing basis must be consistent with the defense in depth philosophy. The RG 1.174

discussion states that, "The defense in depth philosophy . . . has been and continues to be an effective way to account for uncertainties in equipment and human performance." The discussion goes on to say that PRA can be used to help determine the appropriate extent of defense in depth, which, by example, is equated to balance among core damage prevention, containment failure prevention and consequence mitigation. The regulatory guide thus addresses the concern of preventing risk-informed regulation from undermining defense in depth. Defense in depth is primary, with PRA available to measure how well it has been achieved.

### STRUCTURALIST MODEL

We have identified two different schools of thought (models) on the scope and nature of defense in depth. These models came to be labeled "structuralist" and "rationalist."

The structuralist model asserts that defense in depth is embodied in the structure of the regulations and in the design of the facilities built to comply with those regulations. The requirements for defense in depth are derived by repeated application of the question, "What if this barrier or safety feature fails?" The results of that process are documented in the regulations themselves, specifically in Title 10, Code of Federal Regulations. In this model, the necessary and sufficient conditions are those that can be derived from Title 10. It is also a

characteristic of this model that balance must be preserved among the high-level lines of defense, e.g., preventing accident initiators, terminating accident sequences quickly, and mitigating accidents that are not successfully terminated. One result is that certain provisions for safety, for example reactor containment and emergency planning, must be made regardless of our assessment of the probability that they may be required. Accident prevention alone is not relied upon to achieve an adequate level of protection.

There does not appear to be any question that the implementation of defense in depth up to the present time reflects the structuralist model. While this philosophy has served the industry well from the safety perspective, it is now realized that, in some instances, it has led to excessive regulatory burden. Furthermore, the lack of an integrated view of the reactor systems has resulted in some significant accident sequences not being identified until PRA was developed, e.g., the interfacing-systems LOCA sequence.

The next issue, then, becomes how should the insights from PRA be integrated into this structure to reduce unnecessary burden and make it more rational? In the structuralist model, defense in depth is primary, with PRA available to measure how well it has been achieved.

## THE RATIONALIST MODEL

The rationalist model asserts that defense in depth is the aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression. This model is made practical by the development of the ability to quantify risk and estimate uncertainty using probabilistic risk assessment techniques. The process envisioned by the rationalist is: (1) establish quantitative acceptance criteria, such as the quantitative health objectives, core damage frequency and large early release frequency, (2) analyze the system using PRA methods to establish that the acceptance criteria are met, and (3) evaluate the uncertainties in the analysis, especially those due to model incompleteness, and determine what steps should be taken to compensate for those uncertainties. In this model, the purpose of defense in depth is to increase the degree of confidence in the results of the PRA or other analyses supporting the conclusion that adequate safety has been achieved.

The underlying philosophy here is that the probability of accidents must be acceptably low. Provisions made to achieve sufficiently low accident probabilities are defense in depth. It should be noted that defense in depth may be manifested in safety goals and acceptance criteria which are input to the design process. In choosing goals for core damage frequency and conditional containment failure probability, for

example, a judgement is made on the balance between prevention and mitigation.

What distinguishes the rationalist model from the structural model is the degree to which it depends on establishing quantitative acceptance criteria, and then carrying formal analyses, including analysis of uncertainties, as far as the analytical methodology permits. The exercise of engineering judgement, to determine the kind and extent of defense in depth measures, occurs after the capabilities of the analyses have been exhausted.

## A PRELIMINARY PROPOSAL

The structuralist and rationalist models are not generally in conflict. Both can be construed as a means of dealing with uncertainty. Neither incorporates any reliable means of determining when the degree of defense in depth achieved is sufficient. In the final analysis, they both depend on knowledgeable people discussing the risks and uncertainties and ultimately agreeing on the provisions that must be made in the name of defense in depth. The fundamental difference is that the structural model accepts defense in depth as the fundamental value, while the rationalist model would place defense in depth in a subsidiary role.

The remaining question is which model provides the better basis for moving forward with risk-informed regulation. How can capricious imposition of

defense-in-depth be prevented from undermining the focus that can be provided by risk-informed methods of regulation? PRA methods have identified gaps in the regulations and in the safety profiles of individual plants. They have also identified regulations and plant systems that do not make a significant contribution to safety. Typically, however, regulatory reactions to findings that regulations or plant systems are superfluous to safety have been less aggressive than reactions to apparent safety deficiencies.

Two options can be identified:

- (1) Recommend defense in depth as a supplement to risk analysis (the rationalist view)
- (2) Recommend a high-level structuralist view and a low-level rationalist view.

Option (1) requires a significant change in the regulatory structure. The place of defense in depth in the regulatory hierarchy would have to change. The PRA policy statement could no longer relegate PRA to a position of supporting defense in depth. Defense in depth would become an element of the overall safety analysis.

Option (2) is to a large degree compatible with the current regulatory structure. The structuralist model of defense in depth would be retained as the high-level safety philosophy, but the rationalist model would be used at lower levels in the safety

hierarchy. An example is shown in Figure 1.

The PRA uncertainties increase as we move from the initiating events to risk (from left to right). The structuralist view dictates that intermediate goals be set, such as core damage frequency (CDF), large early release frequency (LERF) or conditional containment failure probability (CCFP), or frequency-consequence (F-C) curves. This would satisfy the requirement of balance between prevention and mitigation. We note that the actual numerical value chosen for core damage frequency can express a preference for prevention, and such a preference is unrelated to defense in depth. One could proceed and set goals at the "cornerstone" level, i.e., one level below. This could include goals on initiating-event frequencies, safety-function or safety-system unavailabilities, and so on. How far down one would go would be a policy issue. The structuralist view would not be applied at lower levels.

The rationalist model would be applied at levels lower than the cornerstones of Figure 1. Defense in depth would be used only to address uncertainties in PRA at the lower levels, thus becoming an element of the overall safety analysis. For events or processes that are not modeled in PRA, defense in depth would play its traditional role. Such is the case with the impact of smoke from fires on plant safety. Current fire risk assessments do not account for the effects of smoke, therefore, prescriptive defense-in-depth based

measures would be taken to limit this impact.

We view Option (2) as a pragmatic approach to reconciling defense in depth with risk-informed regulation. There can be little doubt, however, that the rationalist model, Option (1), will ultimately provide the strongest theoretical foundation for risk-informed regulation. When more experience has been gained with the application of PRA in the design and regulation of nuclear power plants, when PRA models can adequately treat most of the phenomena of interest, the role of defense in depth can and should be changed to one of supporting the risk analyses. This transition will need to be supported by the development of subsidiary principles from which necessary and sufficient conditions could be derived.

#### Note

The views expressed in this paper are the authors' and do not necessarily represent the views of the Advisory Committee on Reactor Safeguards

#### REFERENCES

1. C. Beck, "Basic Goals of Regulatory Review: Major Considerations Affecting Reactor Licensing," Statement submitted to the Joint Committee on Atomic Energy, Congress of the United States, Hearings on Licensing and

Regulation of Nuclear Reactors, April 4,5,6,20, and May 3, 1967.

2. Internal Study Group, "Report to the Atomic Energy Commission on the Reactor Licensing Program," submitted to the Joint Committee on Atomic Energy, Congress of the United States, Hearings on AEC Licensing Procedure and Related Legislation, June 1969.
3. F. E. Haskin, and A. L. Camp,, "Perspectives on Reactor Safety," NUREG/CR-6042, Nuclear Regulatory Commission, Washington, DC, March 1994.
4. International Nuclear Safety Advisory Group, "Basic Safety Principles for Nuclear Power Plants," Safety Series No. 75-INSAG-3, International Atomic Energy Agency, Vienna, Austria, 1988
5. International Nuclear Safety Advisory Group, "Defense in Depth in Nuclear Safety," INSAG-10, International Atomic Energy Agency, Vienna, Austria, 1996
6. U. S. Nuclear Regulatory Commission, "Use of Probabilistic Risk Assessment in Nuclear Regulatory Activities; Final Policy Statement," Federal Register, 60 FR 42622

7. U. S. Nuclear Regulatory Commission, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis," Regulatory Guide 1.174, June 1998



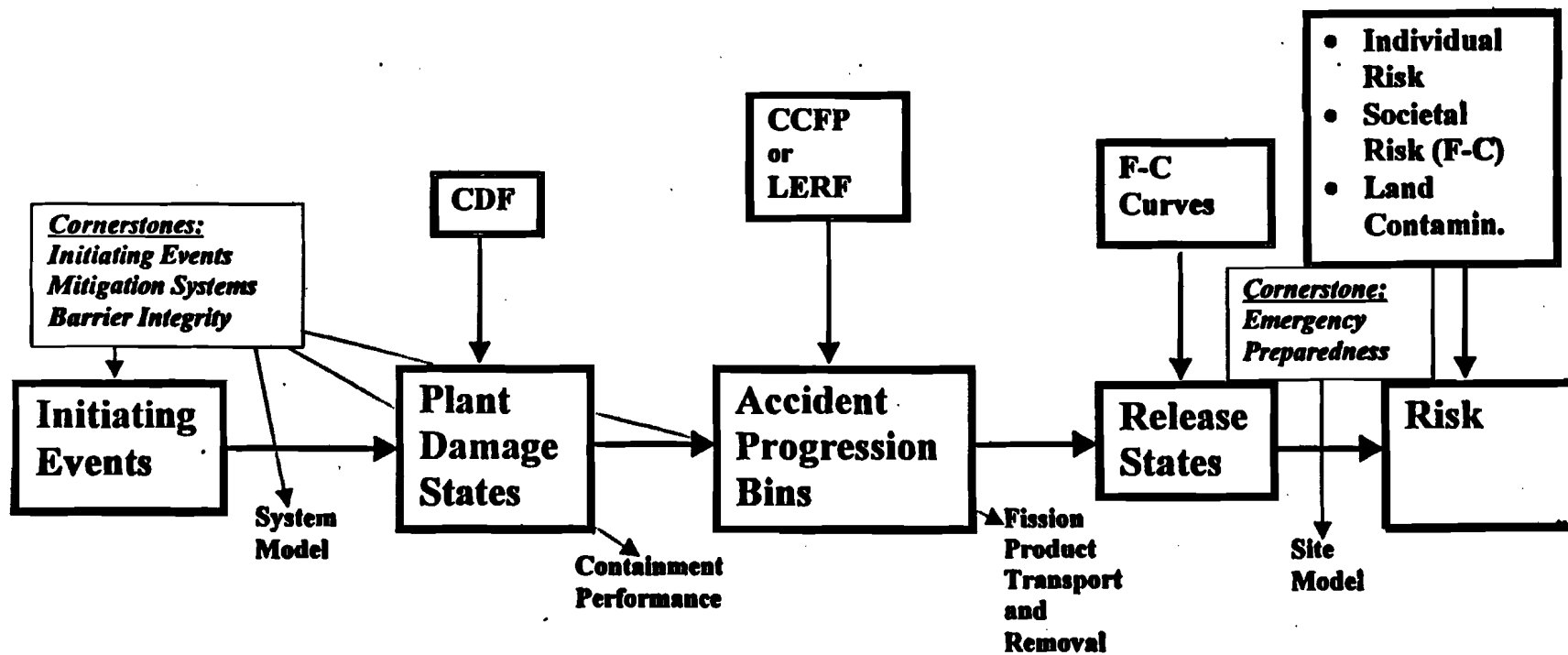


Figure 1. Possible implementation of the structural model at a high level.

June 8, 1999

MEMORANDUM TO: William D. Travers  
Executive Director for Operations

FROM: Annette Vietti-Cook, Secretary /s/

SUBJECT: STAFF REQUIREMENTS - SECY-98-300 - OPTIONS FOR  
RISK-INFORMED REVISIONS TO 10 CFR PART 50 -  
"DOMESTIC LICENSING OF PRODUCTION AND  
UTILIZATION FACILITIES"

#### Option 1

The Commission has approved the staff's recommendation that current rulemaking activities identified under Option 1 continue unimpeded (50.59, 50.72, 50.73, 50.55a, and the new 50.67).

#### Option 2

The Commission has approved implementation of Option 2 to develop risk-informed definitions for "safety-related" and "important to safety" SSCs. This option would make changes to the scope of systems, structures, and components covered by those sections of Part 50 requiring special treatment (e.g., Quality Assurance, Environmental Qualification, Technical Specifications, 50.59, ASME code, 50.72, and 50.73). This effort should proceed with early internal and external stakeholder discussions and utilization of industry pilot studies involving the use of exemptions to assist in the development of the Part 50 modifications.

Regarding the overall scope of the Maintenance Rule (50.65), the Commission has approved changing the existing scope to conform to the risk-informed regulatory framework being developed as part of Option 2. A rulemaking plan should be developed for Option 2 which reflects the incorporation of the Maintenance Rule activities.

(EDO)

(SECY Suspense:

10/31/99)

#### Option 3

The Commission has approved the staff's recommendation to study Option 3. The staff should pursue this study on an aggressive timetable and provide, for Commission approval, a schedule for this activity. The staff should periodically inform the Commission on progress made in the study. The study should determine how best to proceed with risk-informing the remaining sections of Part 50. During this study, if the staff identifies a regulatory requirement which warrants prompt revision because such a change would significantly enhance safety or significantly reduce unnecessary regulatory burden, the Commission should be notified and

provided with a recommended course of action. Otherwise, once this study phase is completed, the staff should provide, for Commission approval, a detailed plan outlining its recommendations regarding specific regulatory changes that should be pursued.

(EDO)

(SECY Suspense:

9/30/99)

## **Policy Issues**

### **1. Voluntary vs. Mandatory Conformance with Modified 10 CFR Part 50**

The Commission has approved the staff's recommendation that risk-informed implementation of Part 50 should be voluntary for licensees. As the staff proceeds with its efforts to risk-inform Part 50, it should provide the Commission with additional information regarding how it will manage voluntary implementation. The Commission has disapproved the staff's recommendation that selective implementation not be allowed. This issue is prematurely before the Commission. A future Commission will be better able to judge the issue of selective implementation after rules are drafted and rulemakings provide comment on this issue as it affects that rule. A "no selective implementation" approach will adversely affect NRC's ability to solicit industry pilot participants.

### **2. Industry Pilot Studies with Selected Exemptions to Part 50**

The Commission has approved the staff's recommendation regarding the use of industry pilot studies involving the use of exemptions to assist in the development of the Part 50 modifications.

### **3. Modification of the Scope of the Maintenance Rule Section (a)(3)/(a)(4).**

The Commission has approved continuation of the expeditious revision of 50.65(a)(3)/(a)(4), as discussed at the Commission meeting of May 5, 1999. Specific Commission direction regarding the rule language and development of the regulatory guidance was provided in the SRM on the Maintenance Rule Commission briefing of May 5, 1999, which was issued on May 13, 1999.

### **4. Clarification of Staff Authority for Applying Risk-Informed Decision Making**

The Commission has approved the staff's recommendation that additional guidance be developed to provide clarification on staff authority for applying risk-informed processes in regulatory activities beyond risk-informed licensing actions. This clarifying guidance should be submitted for Commission approval.

(EDO)

(SECY Suspense:

9/30/99)

The staff should: 1) continue to work with stakeholders in risk-informing Part 50; 2) provide sufficient staff resources and management oversight to these high priority initiatives to ensure effective development of the risk-informed regulatory structure and timely completion of pilot plant applications; and 3) bring policy issues promptly to the attention of the Commission.

While moving towards a risk-informed regulatory framework, the staff should keep in mind that the use of quantitative risk analyses may not be appropriate for all applications, and therefore, should not be force-fit into areas that are not amenable to such an approach.

As we proceed with risk-informing Part 50, the Executive Council should take an active leadership role and ensure that the Planning, Budgeting, and Performance Management process is effectively utilized to allocate agency resources to this effort.

cc: Chairman Jackson  
Commissioner Dicus  
Commissioner Diaz  
Commissioner McGaffigan  
Commissioner Merrifield  
OGC  
CIO  
CFO  
OCA  
OIG  
OPA  
Office Directors, Regions, ACRS, ACNW, ASLBP (via E-Mail)  
PDR  
DCS

December 23, 1998

SECY-98-300

FOR: The Commissioners

FROM: William D. Travers /s/  
Executive Director for Operations

SUBJECT: OPTIONS FOR RISK-INFORMED REVISIONS TO 10 CFR PART 50 -  
"DOMESTIC LICENSING OF PRODUCTION AND UTILIZATION FACILITIES"

PURPOSE:

This paper proposes high-level options for modifying regulations in 10 CFR Part 50 to make them risk-informed and to delineate associated policy issues for Commission consideration. The staff seeks guidance on the Commission's preferred approach in order to develop a detailed rulemaking plan.

SUMMARY:

The staff has proposed a high level approach for incorporating risk-informed attributes into the Part 50 regulations, and is seeking Commission approval to proceed with a phased implementation strategy. After receiving Commission guidance, the staff will develop a rulemaking plan which includes more complete resource and schedule estimates. Two primary objectives of this effort are to develop a risk-informed regulatory framework that will enhance safety as well as reducing unnecessary staff and licensee burden. To initiate this phased effort, the staff is recommending (Option 2) changes to the regulatory scope of SSCs needing special

CONTACT:

M. Rubin, NRR  
415-3234

M. Cunningham, RES  
415-6292

treatment in such areas as quality assurance, environmental qualification, Technical Specifications, 10 CFR 50.59 and ASME code. This will be accomplished, in part, by developing risk-informed definitions for safety-related and safety important SSCs. While this approach would allow "grading" of special treatment requirements on SSCs based upon their risk importance, system functional capabilities would not be removed. Rather, the SSC functional capabilities (for low risk important SSCs) would remain in the plant and be expected to perform their design function but without additional margin, assurance or documentation associated with high safety significant SSCs.

The staff is also planning to undertake a study (Option 3) to explore changes to the body of the Part 50 regulations, to incorporate risk-informed attributes. These changes could involve such actions as developing a new set of design-basis accidents, adding provision to Part 50 allowing for risk-informed alternatives to the present requirements, revising specific requirements to reflect risk-informed considerations, or deleting unnecessary or ineffective regulations. After the completion of this study, the staff will make recommendations to the Commission on any specific regulatory changes that should be pursued, and the corresponding schedules and resource needs.

In addition, the staff has identified four policy issues for Commission consideration and guidance. Direction with respect to these issues would be needed to proceed with a risk-informed Part 50 program. The staff has recommended that: 1) Licensee conformance with a modified Part 50 should be voluntary rather than mandatory, 2) Industry pilot studies with selected exemptions to Part 50 should be utilized as part of the risk-informed development process, 3) The scope of the maintenance rule should be changed as an early part of the risk-informed program, and 4) The staff should develop clarification of its authority for applying risk-informed decision making in areas beyond those associated with licensee initiated risk-informed licensing actions.

#### BACKGROUND:

In 1995, the Commission published a Policy Statement on the Use of Probabilistic Risk Assessment (PRA). Since then, the staff has developed guidance on the use of risk information for reactor license amendments and is currently processing license amendment applications that use risk information as part of their technical justification. However, the fundamental reactor regulations remain largely deterministic. In addition, in recent meetings between the Commission and various stakeholders, the concern was expressed that the NRC is not placing enough emphasis on risk-informing its reactor requirements with the results of risk assessments. It is generally believed that our current reactor regulatory framework (based largely upon design-basis events rather than on core-damage-accident scenarios) results in sufficient safety regulation but in some cases also results in unnecessary regulatory burden. In its September 2, 1998, briefing to the Commission on the status of the PRA Implementation Plan, the staff discussed this issue with the Commission and proposed the development and assessment of various options for making requirements in 10 CFR Part 50 risk-informed. In a staff requirements memorandum dated September 14, 1998, the Commission asked the staff to present a set of options that contain an assessment of the implications of each option, and to also present resource impacts and the role pilot studies would play in the development of new or modified requirements.

In developing the options discussed below, the staff met with the public, the Nuclear Energy Institute (NEI), nuclear utilities, and other representatives of industrial groups on several occasions, including a 2-day public workshop<sup>1</sup>, for the purpose of discussing the objectives of revising Part 50, different approaches for incorporating risk information into the regulations in Part 50, and issues that the staff should consider in evaluating the options for the Commission. These stakeholder activities produced significant information for developing the implementation options given below. A general consensus was also reached regarding the overall objectives of risk-informed modifications to Part 50. These include the following:

- Enhance safety by focusing NRC and licensee resources in areas commensurate with their importance to health and safety.
- Provide NRC with the framework to use risk information to take action in reactor regulatory matters.
- Allow use of risk information to provide flexibility in plant operation and design, which can result in burden reduction without compromising safety.

This paper discusses options and a phased approach for their implementation such that, when completed, the staff envisions that Part 50 would have the following characteristics:

- In concert with other NRC regulations, it would continue to provide reasonable assurance of adequate protection of public health and safety.
- It would contain requirements on specific attributes of nuclear power plant design and operations commensurate with their safety significance. This safety significance would be assessed using principles of risk-informed regulation including the following:
  - consistency with the defense-in-depth philosophy
  - maintenance of sufficient safety margins
  - consistency with the intent of the Safety Goal Policy Statement
- The requirements would be written in a manner that would accommodate the plant-specific nature of the safety significance of design and operational attributes.

---

<sup>1</sup>The transcript of the 10/27-28/98 Public Workshop on Risk-Informing Part 50 are available on the NRC public website (<http://www.nrc.gov>).

At the NRC public homepage ([www.nrc.gov](http://www.nrc.gov)),  
Click on [News & Info](#) Icon  
Click on [Public Meetings](#)  
Click on [Meeting Transcripts](#)  
Click on [Public Meeting on Making 10 CFR Part 50 Risk-Informed](#)  
To read the transcript, choose and click on either of the two days

- It would provide a clear, consistent, and coherent set of requirements that would also facilitate consistency in treatment among the assessment, inspection and enforcement programs.
- It would provide a regulatory basis for all NRC reactor-related activities, including licensing, inspection, enforcement, and assessment.
- It would be performance-based to the extent practical.
- It would be practical to implement for both licensees and the NRC.

These characteristics reflect the long term holistic vision for a risk-informed Part 50.

## DISCUSSION:

### High-Level Options

As a result of our preliminary assessments and stakeholder activities, the staff has identified the following three options for risk-informed modifications of 10 CFR Part 50: (1) make no changes to current Part 50, (2) make changes to the overall scope of systems, structures, and components (SSCs) covered by those sections of Part 50 requiring special treatment (such as quality assurance, technical specifications, environmental qualification, and 50.59 by formulating new definitions of safety-related and important-to-safety SSCs)<sup>2</sup>, and (3) make changes to specific requirements in the body of regulations, including general design criteria (GDCs). Options 2 and 3 could be implemented individually or in combination, since in many aspects they are complementary. The three options are discussed next.

#### Option 1. Make No Change to Current Part 50

This option would terminate staff action to develop comprehensive risk-informed changes to the current Part 50. Risk-informed approaches specified in Regulatory Guide (RG) 1.174, and associated application-specific RGs would continue to be implemented subject to existing regulatory limitations. One example of these limitations is in the area of graded quality assurance (GQA), where requirements other than those that govern QA (10 CFR 50.54 and Appendix B to Part 50 directly govern QA) limit the degree to which the risk informed process can be implemented. See Attachment 1 regarding the Graded QA implementation experiences at South Texas project (STP). This impediment could, if the Commission agrees, be eliminated by granting 10 CFR 50.12 exemptions on the basis of risk information. This approach, however, would be very resource intensive in the long term, assuming that many exemptions would be requested.

---

<sup>2</sup>Changes to these definitions will have to be carefully assessed with respect to potential impact on the underlying definition of "basic component," which have specific requirement imposed as provided in Section 223.10 of the Atomic Energy Act. Modifying the treatment of safety-related and safety important SSCs without necessitating a change to the Atomic Energy Act would be desirable.



Under Option 1, ongoing Part 50 rulemaking activities, which have risk informed elements, would continue on their current schedules rather than be subsumed into an overall Part 50 revision process. These would include ongoing activities related to 50.65, 50.59, 50/72.50.73 and 50.55a as well as the revised source term rulemaking that will, if approved, create a new Section 50.67. Currently, the staff is going forward with each of these programs separately from the proposed Part 50 process.

Meetings with stakeholders have indicated the industry's desire that ongoing activities proceed on their current schedule, with the exception of the Maintenance Rule (10 CFR 50.65) rulemaking where the Nuclear Energy Institute (NEI) has indicated it will respond to proposed rulemaking with comments suggesting broader changes to the Rule's scope as part of current rulemaking. Discussions on various Maintenance Rule approaches, with associated advantages and disadvantages, are presented as a policy issue in a later section of this paper. The assessment of the advantages and disadvantages of risk-informing the Maintenance Rule (in Attachment 4) also addresses the possibility of developing more risk-informed guidance on application of the Maintenance Rule within the context of the existing rule without further modifications to the rule itself.

Ongoing rulemaking activities associated with 50.59 will provide increased clarity and implementation stability by defining a minimal (but non-zero) threshold for licensees to make changes to their facility without prior staff review and approval. The changes to the reporting requirements in 50.72 and 50.73 are intended to provide a better safety and risk focus to the reporting process and avoid unnecessary burden. The ongoing Inservice Inspection (ISI) code case endorsement process will incorporate staff guidance directly into the ASME code cases, allowing for more efficient implementation. The proposed 50.67 would enable operating reactors to voluntarily implement a more representative source term that would be used in assessing design-basis accident response against revised dose acceptance criteria. (A similar change in 50.34 in January 1997 enabled the use of revised source terms by applicants for Construction Permit, Combined Operating License, or Design Certification.) These alternative source terms reflect the release of fission products during design-basis accidents more accurately than does the current source term, making it possible for operating reactors to implement cost-beneficial plant modifications, thereby reducing unnecessary regulatory burden.

None of the ongoing revisions are anticipated to be inconsistent or incompatible with future Part 50 risk informed revisions. However the more extensive Part 50 revision process identified in Options 2 and 3 below, would likely identify additional refinements in some of the above regulations. For example, more specific risk-informed decision criteria may be developed for 50.59. Allowing these separate efforts to continue could necessitate revisiting some of the above regulations at a later date.

Option 2. Make Changes to the Scope of Systems, Structures, and Components Covered by Those Sections of Part 50 Requiring Special Treatment

The current scope of SSCs covered by most sections of Part 50 is based primarily on the evaluation of selected design-basis events, as described in final safety analysis reports (FSARs). These postulated events represent a small fraction of the potential accident sequences treated in risk assessments. As the primary part of this option, risk-informed

definitions of “safety-related” and “important to safety” could be developed. This would lead to changes in the scope of what receives special operational and qualification treatment.

This option only addresses implementing changes to the regulatory scope for SSCs needing special treatment in terms of quality (e.g., quality assurance, environmental qualification, Tech Specs, 50.59, ASME Code). It does not address changing the design of the plant or the design-basis accidents, which establishes the physical complement of plant systems included in the design. Under this option, SSCs of low safety significance (from a risk-informed assessment) would move from “special treatment” to normal industrial (sometimes called “commercial” treatment), but would remain in the plant and be expected to perform their design function but without additional margin, assurance or documentation associated with high safety significant SSCs.

As discussed in Option 1, one area that the industry has identified for early consideration of a revised regulatory scope is the Maintenance Rule (10 CFR 50.65). Revisions to the scope of this rule could be undertaken as part of Option 2 activities, or could be undertaken as part of the ongoing 50.65 rulemaking, which currently only address the 50.65(a)(3)/(a)(4) pre-maintenance safety assessment process. It should be noted however, that applying such changes would modify the original scope of the rule as intended by the Commission. A discussion on the intent and implications of the present Maintenance Rule scope is provided in Attachment 2. The question of whether the scope of the Maintenance Rule should be revised is discussed below as a Commission policy issue, as is consideration of alternative approaches that could reduce unnecessary burden without a rule revision.

Under implementation of Option 2, there could be extensive changes to treatment of SSCs, as those with low risk importance have their regulatory requirements reduced and others not currently regulated have requirements added. To prevent excessive industry and staff burden, it is essential that an efficient regulatory process be employed as part of any implementation process. That process should be structured to eliminate unnecessary prior staff review and approval as licensees implement the operational changes allowed by the changes in Part 50 scope. Therefore, as part of this option, the staff could place specific regulatory requirements in a revised Part 50 (and associated guidance in a regulatory guide) on what provisions and criteria should be utilized by licensees to implement these changes without having to submit them to the staff for prior review and approval. Since changes to requirements in the revised regulations would apply to those SSCs of low risk importance, it is anticipated that such an approach could be accomplished with no significant safety impact. However, as part of this process, the staff would have to ensure that the licensee had appropriate assessment and feedback programs in place to reflect SSC performance degradation back into the PRA and to modify SSC risk importance as necessary.

Additionally, in the time period before the Part 50 scope changes take final form, the staff believes that the current provisions of 50.12 would permit the Commission to approve regulatory exemptions that allow for early implementation of risk-informed reductions to operational and qualification requirements. An exemption to operational requirements that involve, in toto, no change or a decrease in risk could be granted pursuant to paragraph (a)(2)(iv) of Section 50.12. An exemption that involves an increase in risk could potentially be granted under paragraph (a)(2)(vi) if the Commission were able to find that quantitative risk

information was not considered in the establishment of the regulatory requirement which is the subject of the exemption. The rationale for granting an exemption under paragraph (a)(2)(vi) would be that quantitative risk information constitutes a "material circumstance" not considered when the regulation was adopted. The grant of limited exemptions to a limited number of plants for purposes of pilot testing does not pose any special problems but the repeated issuance of a large number of exemptions which, considered together, represent a fundamental alteration of the conceptual nature of the licensing basis, to more than a limited number of plants essentially constitutes a generic change to the regulatory requirements in Part 50. Such generic changes should be adopted through rulemaking, rather than the case-by-case approach inherent in the regulatory approach embodied in the issuance of exemptions. Similarly, the granting of a large number of exemptions to a single plant, should not be so extensive that the validity of the original license is called into question (i.e., grant wholesale exemptions to all GDC, and regulations for an extensive subset of SSCs.

### Option 3. Changes to Specific Regulatory Requirements

Under this option, changes would be made to the body of the Part 50 regulations to include risk-informed attributes in the requirements. Approaches to revising the body of the regulations could include the following:

- adding provisions to Part 50 allowing the staff to approve risk-informed alternatives to current regulations,
- revising specific requirements to reflect risk-informed considerations,
- deleting unnecessary or ineffective regulations.

This approach could be as broad as a complete rewrite of 10 CFR Part 50, or it could be more limited in scope, focusing on the regulations that have the most significant potential for improving safety and efficiency and reducing unnecessary burden. A process that results in a comprehensive reassessment of the Part 50 requirements would offer the ability to develop a coherent risk-informed regulatory framework that can be propagated throughout the regulations. It is especially important that the process results in consistent requirements among the assessment, inspection, and enforcement programs. In addition to benefits to currently operating reactors, such a framework would be of benefit for future reactors, and potential impact on Part 52 should be considered in developing this option.

Changes to specific design provisions of the general design criteria (GDCs) in Appendix A to 10 CFR Part 50 or development of a revised set of design-basis events based upon risk significance are potential areas for action under this option. The changes envisioned under Option 3 would be necessary to accomplish the long term vision for a risk-informed Part 50 discussed earlier in this paper. Changes of this magnitude would involve extensive public comment and participation. Use of industry pilot programs would be helpful for selecting, prioritizing, and implementing such changes.

### Assessment of Benefits/Impacts For Various Options

The staff has assessed each of the options for risk-informing Part 50 with respect to the following factors to determine the implications of pursuing them:

- potential for improving safety decisions and increasing public confidence
- potential for reducing unnecessary licensee and NRC burdens
- the anticipated complexity of changes
- NRC resources needed for putting changes in place
- licensee resources needed for putting changes in place
- calendar time for full implementation<sup>3</sup> (NRC and licensee)

These assessments are, for the most part, qualitative, although preliminary estimates or estimated ranges have been made for resources, burden reduction, and an implementation schedule. In addition, magnitudes of the impacts of the other factors have been judged in relative terms as either high, moderate, or low. The results of the staff's assessment are summarized below and presented in both a narrative and tabular form in Attachment 3.

### RECOMMENDATIONS:

The staff recommends adopting a phased approach to making 10 CFR Part 50 more risk-informed by proceeding initially with Option 2. However, the staff acknowledges that the options developed here have not had the benefit of full internal and external stakeholder involvement and that additional discussions on the formulation of these issues and their costs and benefits are needed in the process of developing a rulemaking package for the Commission. A phased approach appears to be consistent with comments received from stakeholders and would allow for achieving meaningful benefits in the early stages, while additional study is conducted to identify where additional risk-informed insights can be factored into more extensive regulatory changes in later phases. The staff also recommends that the current rulemaking activities identified in Option 1 continue unimpeded.

The staff also recommends that pilot plants be solicited (1) to assist in the development of scope and definition changes to Part 50 and (2) to test proposed changes during the development and comment period. The staff seeks guidance from the Commission on whether the scope of the Maintenance Rule should be revised and included as an early part of Option 2 (see associated issue under "Policy Issues" below). With Commission approval (see associated issue under "Policy Issues" below), the staff would consider exemption requests from pilot plants related to risk-informed scope modifications for such operational and qualification requirements that could be justified by applying the guidelines of RG 1.174 or supplemental criteria developed as part of the rulemaking effort.

---

<sup>3</sup>Full implementation means that all NRC and licensee actions needed to make the option become part of day-to-day operations have been completed. This includes rule changes, guidance documents, staff and licensee program and procedure changes and training.

The staff additionally recommends that Option 3 be studied further and that the industry and staff continue with such pilot programs as the NEI Whole Plant study, to identify specific requirements meriting change and possible risk-informed alternatives to the body of Part 50. At the conclusion of this study, the staff would make recommendations to the Commission on any specific regulatory changes that should be pursued and the corresponding schedules and resource needs. During this study phase, the staff would be receptive to identifying specific regulatory changes that provide very beneficial risk-informed enhancements. These could include identifying requirements that are not risk- or safety-effective (for deletion consideration) as well as identifying areas in which very well-focused revisions could significantly enhance safety and/or effectiveness. When such issues are identified, they will be brought to the Commission's attention on a priority basis along with staff recommendations for action.

#### POLICY ISSUES:

The policy issues for Commission consideration include the following:

- (1) voluntary vs. mandatory conformance with modified 10 CFR Part 50,
- (2) industry pilot studies with selected exemptions to Part 50,
- (3) modification of scope of the Maintenance Rule,
- (4) clarification of staff authority for applying risk-informed decision making.

An assessment of the advantages and disadvantages of these issues is discussed in detail in Attachment 4 to this paper.

In summary, (1) the staff recommends that risk-informed implementation of Part 50 should be voluntary for licensees; (2) the staff recommends allowing pilot plants to implement changes using exemptions, because it will provide a significant benefit to the process of developing risk-informed revisions to Part 50; (3) the staff recommends that the current rulemaking initiatives associated with paragraphs (a)(3)/(a)(4) of 50.65 continue and that the scope of the Maintenance Rule be revised to one that is risk-informed and that this activity be an early activity in support of the overall Part 50 revision process; and (4) the staff recommends that additional guidance be developed, such as in a regulatory guide, to provide clarification on staff authority for applying risk-informed processes in regulatory activities beyond risk-informed licensing actions.

#### IMPLEMENTATION ISSUES:

The modification of 10 CFR Part 50 to make it more risk-informed requires the resolution of a set of implementation issues as well as the policy issues identified previously in this paper. These implementation issues are described in Attachment 5, and are provided for the Commission's information at this time. Resolution of these issues will be addressed during the development of the rulemaking process.

#### REQUESTED COMMISSION ACTION:

The staff requests that the Commission (1) approve implementation of Option 2 (including additional early internal and external stakeholder discussion) with utilization of industry pilot

studies, and allow ongoing rulemaking actions identified in Option 1 to continue unimpeded; (2) note that the staff will initiate a study of Option 3; (3) approve the use of industry pilot studies involving the use of exemptions to assist in the development of the Part 50 modifications; (4) endorse using the Maintenance Rule (10 CFR 50.65) as part of the Option 2 effort, as an initial step in revising the scope to be risk-informed and to facilitate scope revisions being developed for other Part 50 operational requirements (Option 2); (5) approve work to develop regulatory guide or other staff guidance clarifying staff approaches for applying risk-informed decision making; and (6) provide guidance on the remaining policy issues discussed in Attachment 4.

After the Commission issues its guidance, the staff will develop another Commission paper (including a Rulemaking Activities Plan, as appropriate) to address in more detail a plan of action for implementing the guidance provided by the Commission.

#### COORDINATION:

The Office of the General Counsel has reviewed this paper and has no legal objections. The Office of the Chief Financial Officer has reviewed this paper for resource implications and has no objections.

#### RESOURCES:

On the basis of experience with developing such programs as standard technical specifications, Maintenance Rule, and risk-informed regulatory guidance, the staff has made some preliminary estimates of NRC resources needed to implement the various options. These estimates, which the staff believes are the best possible at this point in time, are shown in Attachment 3. Also provided are preliminary estimates of the potential benefits from the various options with respect to decision making and burden reduction. Although these estimates vary among options, in all cases they are considered substantial in an environment of declining resources. Current Operating Plan budgets for FY 1999 and FY 2000 do not reflect the resources (dollars or FTE) needed to pursue Options 2 or 3 or the study of Option 3. Therefore, implementing these options would necessitate reprogramming resources from other activities from within the NRR and RES budgets. More specifically, this would have implications for the NRR operating plan and budget for undertaking rulemaking and review of exemptions, and the RES operating plan and budget for support of the development of technical bases and study of Option 3 alternatives. The staff proposes to make more refined resource estimates and identify adjustments in office operating plans after receiving guidance and direction from the Commission regarding specific options. The staff's initial judgment is that the resource

requirements for the recommended options could be accommodated without compromising the high priority issues of risk-informed licensing actions and risk-informing the inspection, assessment and enforcement processes.

William D. Travers  
Executive Director  
for Operations

Attachments:

1. Insights From Graded Quality Assurance Implementation at South Texas
2. Supplementary Information on Maintenance Rule Scope
3. Preliminary Assessment of Impacts of Various Options for Risk-Informing Part 50
4. Discussion of Policy Issues

cc: SECY  
OGC  
OCA  
OPA  
CFO  
CIO

requirements for the recommended options could be accommodated without compromising the high priority issues of risk-informed licensing actions and risk-informing the inspection, assessment and enforcement processes.

William D. Travers  
Executive Director  
for Operations

Attachments:

1. Insights From Graded Quality Assurance Implementation at South Texas
2. Supplementary Information on Maintenance Rule Scope
3. Preliminary Assessment of Impacts of Various Options for Risk-Informing Part 50
4. Discussion of Policy Issues

cc: SECY  
OGC  
OCA  
OPA  
CFO  
CIO

DISTRIBUTION:

File Center	GHolahan	TKing	SPSB R/F	BSheron	WTravers
MRubin	SCollins	RBarrett	OGC	MCaruso	SBlack
NRR Mailroom (W9800152)		PMagnanelli			

\*See previous concurrence.

G:\PT50R108.WPD

SPSB:DSSA	SPSB:DSSA	TECH. ED	D:DSSA	ADT:NRR
MRubin*	RBarrett*	RSanders*	GHolahan*	BSheron*
12/11 /98	12/11 /98	11/24/98	12/11 /98	12/11 /98

D:NRR	OGC	OD:RES	D:DST	CFO	EDO
SCollins*	JGray*	AThadani*	TKing*	JFunches (TP)*	WTravers
12/11/98	12/16/98	12/11/98	12/14/98	12/17/98	12/ /98

OFFICIAL RECORD COPY



## INSIGHTS FROM GRADED QUALITY ASSURANCE IMPLEMENTATION AT SOUTH TEXAS PROJECT (STP)

In March 1996, the STP licensee asked NRC to approve a revised Operations Quality Assurance Program (OQAP) for STP, incorporating the methodology for graded quality assurance (QA), which was also based on probabilistic safety assessment (PSA) risk insights. Following extensive discussions with the licensee and substantial review, the staff approved the proposed revision to the OQAP by letter dated November 6, 1997. In its letter and accompanying safety evaluation, the staff concluded that the licensee's methodology for determining the relative safety significance of plant structures, systems, and components (SSCs) was acceptable; that appropriate QA controls had been defined for the established categories of SSCs; that adequate feedback mechanisms had been established to adjust the graded QA program if operational performance indicated such a need; and that all pertinent regulatory requirements continued to be satisfied.

Subsequent to NRC approval, the licensee has identified implementation difficulties associated with the graded QA program. For a number of low-risk-significant SSCs, for which the licensee has reduced the QA requirement, other regulatory requirements such as environmental qualification and American Society of Mechanical Engineers Code seismic requirements continue to impose substantial requirements. This has prevented the licensee from reducing additional burdens on these SSCs that have low importance.

The licensee has indicated its desire to solicit additional regulatory relief, to achieve its originally envisioned graded QA program benefits. As discussed with the staff at several meetings, the licensee would propose exemptions to 10 CFR 50.2 and 10 CFR 50.59, so that some components currently considered as "safety-related" or "important to safety" could be reclassified as non-risk-significant and low-risk-significant components, consistent with the NRC-approved graded QA process. This STP initiative could reduce the complexity and resources required for routine maintenance and replacement for specifically identified systems or components by removing them from the scope of specific regulations, such as those governing seismic and other qualification requirements. Commission approval of the policy issue allowing risk-informed exemptions would clarify the staff's ability to proceed with this pilot.

## SUPPLEMENTARY INFORMATION ON MAINTENANCE RULE SCOPE

### Scope Issues Related to Risk-Informing the Maintenance Rule

The staff has received comments from the Nuclear Energy Institute (NEI) that the industry intends to propose narrowing the Maintenance Rule (10 CFR 50.65) scope as part of the current Maintenance Rule revision.<sup>4</sup> It should be noted that the scope of the Maintenance Rule was intentionally broader than the scope of other regulations. In 1991, when the rule was written, the Commission specifically included non-safety-related structures, systems, and components (SSCs) in order to apply the NRC's authority to take action against poor maintenance practices in the balance of plant. The purpose of the Maintenance Rule is to "provide reasonable assurance that (1) intended safety, accident mitigation, and transient mitigation functions of the SSCs [in scope via (b)(1) and (b)(2)(I)] can be performed, and (2) failure of SSCs [in scope via (b)(2)(ii) and (b)(iii) ] will not occur which prevent the fulfillment of safety-related functions, and failures resulting in scrams and unnecessary actuation of safety-related systems are **minimized**." The staff's current thinking on a risk-informed Part 50 is in conflict with the present scope of the Maintenance Rule, in that SSCs whose failures could result in transients and scrams are currently captured but would not necessarily be captured by a risk-informed scope. Also, equipment that is used to mitigate accidents and transients as well as equipment whose failure could prevent a safety-related SSC from fulfilling its intended function would not necessarily (dependent on their risk importance) remain in a risk-informed scope. Since risk-informing Part 50, including the Maintenance Rule, would change a previous Commission policy, a related policy issue has been included in the "Policy Issues" section of this paper. This policy issue addresses whether a scope change on the Maintenance Rule should be implemented, and possible alternatives to a rule change that offer potential reductions in implementation burden.

---

<sup>4</sup>The current rulemaking is limited to the safety assessment (a)(3) recommendation; a separate proposed rule change (including scope revisions) would have to be issued for public comment.

**PRELIMINARY ASSESSMENT OF IMPACTS OF VARIOUS OPTIONS FOR RISK-  
INFORMING PART 50**

	<b>Option 2</b>	<b>Option 3</b>
	<b>Change Scope of SSCs Requiring Special Treatment</b>	<b>Change Specific Safety Requirements</b>
<b>Improved safety decisions and public confidence</b>	High	Moderate to High
<b>Implementation costs NRC<sup>5</sup></b>	25 to 50 NRR FTE over 4 to 8 years; NRR tech. assistance \$250K/yr  2 to 3 Research FTE and 500K/yr for approximately 2 to 3 years	100 RES/NRR FTE over not less than 5 years; RES tech. assistance of \$1 million/yr <sup>6</sup>
<b>Implementation costs licensees</b>	High	High
<b>Burden reduction NRC</b>	Moderate <sup>7</sup>	Less than Option 2 but dependent upon specific changes implemented
<b>Burden reduction licensees</b>	Very High <sup>8</sup>	Potentially high
<b>Complexity</b>	Moderately high	High
<b>Time to full implementation</b>	4 to 8 years	Not less than 5 years after completion of Option 3 study

<sup>5</sup>Estimated direct FTE assuming that all policy issue recommendations are endorsed by the Commission. Industry implementation being mandatory or voluntary (i.e., policy Option 1) would not appreciably affect these estimates.

<sup>6</sup>Preliminary estimates for full Option 3 implementation, including rulemaking. Resources to conduct the study of Option 3 are in addition to the full implementation costs and are estimated to be approximately 5 RES/NRR FTE spread over 2-3 years, and RES technical assistance of \$500k/yr.

<sup>7</sup>Once fully implemented, this option is estimated to result in increased staff efficiencies in the area of licensing reviews, inspection and enforcement to correspond to a net reduction in staffing levels of approximately 10-20 direct FTE per year.

<sup>8</sup>Reduction of 1 to 10 % of current operations and maintenance (O&M) cost assumed (~\$100 million to 1 billion/year).

## Assessment of the Implications of Pursuing Various Options

The staff has made a very preliminary assessment of each of the options for risk-informing Part 50 with respect to the following factors to determine the implications of pursuing them:

- potential for improving safety decisions
- potential for reducing unnecessary licensee and NRC burdens
- the anticipated complexity of changes
- licensee and NRC resources needed for putting changes in place
- calendar time for full implementation<sup>9</sup> (licensee and NRC)

Although the assessments are, for the most part qualitative, some preliminary estimates have been made for NRC resources, burden reduction on the part of NRC and licensees, and the schedules for implementation. In addition, magnitudes of the impacts of the other factors have been judged in relative terms as either very high, high or moderate, or low.

The results of the staff's assessment are discussed below and summarized in the table on the preceding page.

### **Option 2. Changing the Scope of SSCs Requiring Special Treatment**

Changing the scope of SSC operational and qualification treatment requirements to be risk-informed would lead to better safety decisions in one of the most important areas with respect to safety at nuclear power plants-plant operations. Indeed, operating experience, research, and analyses of severe accidents have shown plant designs to be generally robust; also, with the completion of the individual plant examinations, plant-specific design vulnerabilities have been addressed. Consequently, the risk at plant sites is controlled on a day-to-day basis by decisions pertaining to operations. For this reason, the staff believes that this option would have the highest safety impact with respect to the regulatory decision making process, as well as offering the greatest potential for reducing unnecessary burden.

Changing the scope of operational and qualification treatment involves fundamental changes to a significant number of diverse requirements that would lead to many changes in procedures and practices for the licensees and NRC. Because of this, the staff believes that NRC and its licensees would face a significant number of complex issues in implementing this option. Along with resolving difficult issues, significant effort by both the NRC and licensees would be required to make changes to their respective "infrastructures" (e.g., procedures, training, regulatory guides) dictated by this option. Consequently, the staff expects that this option would require significant resource commitments from the NRC and licensees to develop and implement the option fully. The staff estimates 25 to 50 direct FTE expended over a 4-8 year period and \$250K per year would be needed to implement this option. At the public workshop on risk-informing Part 50, industry representatives also expressed their expectation that this option could lead to significant reductions in operating costs (burden), especially when the changes lead to reductions in occupational exposure to radiation. The staff believes that a

---

<sup>9</sup>Full implementation means all licensee and NRC actions needed to make the option become part of day-to-day operations have been completed.

1 percent to 10 percent reduction in current operations and maintenance (O&M) costs per plant per year following implementation of the option ( $\leq$ \$100 million to 1 billion/year for the entire population of operating plants) is a reasonable figure to use for the purpose of considering options. This estimate is consistent with the views of senior nuclear industry executives. In a November 10, 1998 e-mail to Annette L. Vietti-Cook, Mr. Harold B. Ray, Executive Vice President, Southern California Edison Company, submitted information in preparation of the planned November 13, 1998 Stakeholders meeting. In that e-mail, Mr. Ray stated in response, "In contrast, savings of at least 1 percent of annual O&M should certainly be achievable over the long term, and far more than this would be a reasonable goal. On another basis, only a few hours of avoided, market-based revenue loss per year, as a result of fully risk-informed regulation, would offset the assumed cost of plan implementation by any one unit. In our experience, this should certainly be achievable."

In regard to schedule, one licensee representative at the workshop who is a participant in the NEI Whole Plant initiative on Part 50 expressed his belief that this option could be fully implemented in approximately 5 years. Given the time it has taken to develop the Maintenance Rule and put it in place, and the lessons learned from Maintenance Rule implementation, the staff believes that a reasonable estimate is on the order of 4-8 years.

### **Option 3. Changes in Safety Requirements**

Changes to safety requirements can vary substantially in cost and burden reduction, depending on the number of requirements being changed, the nature of each specific requirement being changed, and the complexity of the change being made to the regulation. Fundamental and far-reaching changes to cornerstone safety requirements such as 10 CFR 50.46 (emergency core cooling) or 10 CFR Part 50, Appendix A (General Design Criteria) would have a cost and schedule much higher than that associated with changes that simply permit licensees to propose an alternative risk-informed method for satisfying an existing Part 50 requirement. Resources needed on the part of the NRC and licensees to make substantive changes to safety requirements are expected to be large. In many cases such changes would include changes in codes, standards, NRC regulatory guides, NRC standard review plans, FSARs, and design-basis documents that implement the requirements in Part 50. For this reason, the staff believes this option would be the most difficult, most expensive, most time-consuming (no fewer than 5 years) to implement. The staff's preliminary estimate for NRC resources needed to implement this option is a total of 100 direct FTE with technical assistance of \$1 million/yr. This estimate will be refined after the Option 3 study is finished. These are preliminary estimates for full Option 3 implementation, including rulemaking. The estimated resources to conduct the study of Option 3 are approximately 5 direct FTE spread over 2-3 years and technical assistance of \$500k/yr.

Changes in safety requirements that eliminate the need for some systems, structures, and components, or that allow substantial flexibility in such areas as reactor fuel design, would lead to a reduction in the unnecessary burden to licensees. The staff estimates a reduction that could be potentially high, but that there is more uncertainty regarding the potential benefit, which will be dependent upon what rule revisions are actually implemented.

## DISCUSSION OF POLICY ISSUES

The Commission is requested to provide guidance on the following policy issues in order to develop specific implementation approaches for the options discussed above. These include the following:

- voluntary vs. mandatory conformance with modified 10 CFR Part 50,
- industry pilot studies with selected exemptions to Part 50,
- modification of scope of the Maintenance Rule,
- clarification of staff authority for applying risk-informed decision making.

### 1. Mandatory versus Voluntary Implementation of Risk-informed Part 50

For any proposed risk-informed changes to Part 50, a fundamental policy question is whether all licensees would be required to implement the revised regulations, or whether the revised regulations would offer licensees an optional alternative set of requirements that each individual licensee can choose to adopt, (changes to the current Part 50) or not adopt (remain with the current Part 50). If the Commission directs that implementation of a risk-informed Part 50 modification be voluntary, a related policy question arises: can a licensee choose which elements of the revised Part 50 to follow, or does selection of the risk-informed track require utilization of the entire set of revised requirements.

#### Advantages of Mandatory Implementation

Requiring the mandatory implementation of a risk-informed Part 50 has a number of advantages. Regulatory clarity and stability would be enhanced since there would be a single set of regulatory requirements. The Commission's objective stated in the PRA Policy Statement, to increase use of PRA, would be furthered. The safety benefit and burden-reduction benefits of risk-informed regulation would be uniformly achieved throughout the industry as regulatory requirements would be more properly risk-focused. Problems inherent in having two classes of licensees, risk-informed and not risk-informed, would be avoided. The staff is currently committed to check on implementation of more than 500 safety enhancements identified by the IPE and IPEEE program and to consider the need for regulatory oversight of such safety enhancements to the extent that they meet the backfit rule. Under a mandatory, risk-informed program, important safety enhancements would receive appropriate regulatory oversight, reducing the need for staff IPE followup.

#### Disadvantages of Mandatory Implementation

Mandatory application of risk-informed changes to Part 50 could have a detrimental effect on the schedule, resources, and extent to which Part 50 could be risk-informed. This is because many in the nuclear industry oppose any mandatory application of risk-informed initiatives and would likely work to limit changes if they are mandatory. More fundamentally, it may be very difficult to show that the risk informed changes, in any form, either: (i) will result in a substantial increase in overall protection of the public health and safety or common defense and security, the initial backfit threshold finding; or (ii) are *necessary* for adequate protection. In the latter regard, it must be shown that the existing regulatory approach no longer provides reasonable assurance of adequate protection, such that mandatory imposition of the new regulatory scheme is necessary to provide such reasonable assurance. While there are several options

open to the Commission with respect to addressing the Backfit Rule, it is likely that the industry would oppose Commission adoption of any of those options.

Also, licensees that have limited in-house PRA capability, and who may not have anticipated using the optional risk-informed approaches of RG 1.174, will have to expend start-up resources to ensure that they have adequate technical capability and an adequate quality PRA to properly implement the revised regulatory framework. Licensees that have shorter remaining license periods or those that anticipate early decommissioning would have less time to gain the benefits from a reduced regulatory burden. Also, the implications for those plants currently seeking license renewal would need to be determined.

Finally, current requirements have led to plants that are judged safe. Mandatory application of sweeping changes to Part 50 could send a signal that current plants are less safe than desired. If the risk-informed changes to Part 50 do represent an improvement, the staff expects that licensees would eventually change voluntarily.

If the Commission does direct the staff to proceed with risk-informed Part 50 revisions on a voluntary basis as the chosen option, the policy issue that remains is whether licensees that wish to use risk-informed options can implement selected elements, or whether they should employ the entire complement of risk-informed regulatory requirements. For example, could a licensee reduce quality assurance (QA), operational requirements, and equipment qualification requirements (EQ, and code class) on low risk important SSCs in the emergency ac power system, even though risk-important elements in non-safety-related gas turbine generators or startup feedpumps are not identified for additional attention?

This approach would allow licensees to be selective about what systems or programs are targeted for risk-informed implementation, thereby reducing implementation costs, and possibly allowing for earlier implementation, but in a more limited scope. However, partial implementation, sometimes known as "cherry picking" would tend to reduce burden in areas that are over regulated, but without the commensurate benefit of additional quality or performance requirements where SSC risk importance has not been fully recognized by the current regulatory framework. Such selective implementation is not compatible with the intent of risk-informed regulation.

#### Staff Recommendation

The staff recommends that implementation be voluntary, but that selective implementation not be allowed.

#### 2. Industry Pilot Studies With Selected Exemptions to Part 50 in Advance of Rulemaking

The rulemaking process associated with a structured phased approach to risk-informing Part 50 would likely require several years before significant changes are issued. As the staff develops proposed regulatory revisions and works with pilot participants, the policy question arises as to whether pilot plant licensees may implement risk-informed alternatives through exemptions.

### Advantages of Industry Pilot Studies With Exemptions

Industry pilot programs would be a very useful vehicle to develop and test approaches for risk-informed revisions to our regulatory requirements. They also would offer the opportunity to explore the detailed impact on design and operational requirements. Allowing exemptions in advance of final rulemaking would offer an incentive for industry pilot participants to justify the resource costs of pilot cooperation. This would serve to increase the potential pool of risk-informed pilot programs, which would benefit the risk-informing process. Even without formal pilot programs, stating the Commission's receptiveness to risk-informed exemption requests would demonstrate the agency's commitment to be forward-looking in allowing appropriate use of risk-informed approaches in the most timely manner. Additionally, Commission endorsement of this approach would clarify the ability of the staff to respond to the South Texas Project initiatives for resolving problems associated with Graded QA implementation (discussed in Attachment 1).

### Disadvantages of Industry Pilot Studies With Exemptions

Since the rulemaking process would not have been fully completed when some exemptions would be issued, there is a possibility that details of a licensee risk-informed implementation might not be identical with the final rule. However, once the rulemaking process is completed, the pilot plants could be required to comply with the final rule(s) if the exemptions authorizing each plant's pilot approach include a provision requiring the plants to comply with the requirements in the final rulemaking(s).

### Staff Recommendation

The staff recommends that industry pilot programs be undertaken in all appropriate areas including, but not limited to, the Maintenance Rule scope (see policy issue #3 below) and NEI Whole Plant study, and that exemptions be granted to pilot participants in cases in which the staff has determined that adequate risk-informed bases have been provided and the provisions of 10 CFR 50.12 are met.

### 3. Modification of Scope of the Maintenance Rule

As discussed in Attachment 2, the intent of the Maintenance Rule was that licensee's maintenance of important SSCs is effective to assure the functional capability of a broad range of plant SSCs and to reduce (or minimize) safety challenges such as reactor scrams. If the scope of the Maintenance Rule were to be modified in a risk-informed manner, much of the current scope could be eliminated since many of the SSCs currently monitored have little impact on core damage frequency or large early release frequency. One of the proposed risk-informed assessment program cornerstones includes all plant scrams regardless of their safety significance. The impact of modifying the rule on the regulatory basis for inspection and enforcement related to those initiators should be carefully assessed and considered. Modifying the scope of the Maintenance Rule could also impact the implementation of the license renewal rules in 10 CFR Part 54. If the Commission directs the staff to modify the scope of the Maintenance Rule, the remaining issue is: should the present rulemaking (requiring assessment prior to taking equipment out of service for maintenance) continue on its present schedule, or should this rulemaking be suspended, and its content included in a later



rulemaking package which includes the scope changes. As an alternative for rulemaking to revise the scope of 10 CFR 50.65, the staff could revise its guidance to reduce the scope of non-safety-related SSCs and the implementation requirements for SSCs that are of low risk importance.

#### Advantages of Revising Maintenance Rule Scope

Modifying the scope of the Maintenance Rule along with other regulations to be risk-informed would result in a coherent and consistent scope of all operation-related requirements. In addition, the overall intent of risk-informing the regulations (i.e., to better focus NRC and licensee resources on issues commensurate with safety) would be better served. Having a common scope of all operationally oriented rules would also contribute to improved clarity and communications. The inspection and enforcement programs are clear areas that would benefit from a reduced Maintenance Rule scope by more closely focusing on risk-significant SSCs and activities. Additionally, risk-informing the scope of the Maintenance Rule could relieve licensee burden without significantly affecting plant safety. The process would also provide the staff and industry with an excellent pilot activity that could serve as a basis for scope development for other rule revisions.

If the Commission does direct the staff to implement a revised scope to the Maintenance Rule, the remaining policy question is whether the current rulemaking should continue and the scope changes be conducted as an early part of Option 2, or should current 50.65 rulemaking be suspended and the proposed (a)(3)/(a)(4) changes be incorporated into a single rulemaking which includes the scope revisions.

The advantage of continuing with the current rulemaking is that it allows for earlier implementation of the requirement for licensees to assess the safety impact of taking equipment out of service for maintenance, which is voluntary in the existing rule.

The disadvantage of continuing with the current rulemaking activities is that it will necessitate two separate rulemakings, one dealing with the assessment requirement and a later effort directed towards the scope change. This would likely result in a small overall increase in staff resources, versus a single rulemaking effort that included both elements.

#### Disadvantages of Revising Maintenance Rule Scope

Modifying the scope of the Maintenance Rule would eliminate one mechanism for getting early predictive information on licensees' performance and on equipment reliability and availability; therefore, such scope changes would have to be assessed relative to their impact on the reactor assessment process currently under development to ensure design consistency. Also, the Commission's longstanding desire to reduce challenges, such as reactor scrams, could be eroded to some extent, especially as related to performance of balance-of-plant (BOP) systems.

The Maintenance Rule was credited (along with the entire regulatory process) in establishing the scope and objective of the license renewal rule in 10 CFR Part 54. Prior to changing the scope of the Maintenance Rule, the potential impact of the proposed changes on license renewal must be carefully considered.

If the Commission directs the staff not to revise the scope of the Maintenance Rule to be risk-informed, the remaining policy question is whether revised guidance should be issued to remove some less risk significant non-safety-related SSCs from scope and to allow less monitoring and assessment for those in-scope low risk standby SSCs which are of low risk importance. A revised regulatory guide could be developed which outlines such reductions in implementation burden for low importance SSCs.

The advantages of issuing such guidance is that it would provide some amount of burden reduction for licensees on an expedited basis, without requiring the staff resources necessary to conduct additional rulemaking on 10 CFR 50.65.

The disadvantage of utilizing regulatory guidance documents, rather than a rule change, is that some monitoring and assessment burden would still remain on low risk importance SSCs due to the current scope definition in the rule. Therefore, this approach would only partially improve the risk-informed focus of the Maintenance Rule.

#### Staff Recommendation

The staff recommends that the present rulemaking effort on 10 CFR 50.65 continue unimpeded. The staff also recommends that the scope of the Maintenance Rule be revised to be risk-informed and that this effort be conducted in an early stage of Option 2 implementation. If the Commission directs the staff not to revise the scope of the Maintenance Rule, then the staff recommends that implementation guidance be revised to reduce the monitoring and assessment requirements on low risk important SSCs.

#### 4. Clarification of Staff Authority for Applying Risk-Informed Decision making

Commission guidance presented in the final risk-informed regulatory guidance e.g., RG 1.174 and standard review plans, documents the process and criteria for licensees to use in justifying licensee-initiated (voluntary) risk-informed licensing actions. Although the Commission's 1995 PRA Policy Statement indicated that the staff should increase the use of PRA in its regulatory activities, no specific requirement exists for licensees to perform risk analyses in support of licensing actions.

#### Advantages of Clarification of Staff Authority

This action would clarify the staff's authority to question the risk implications of, and potentially reject proposed changes to, the license or licensing basis for specific instances where risk considerations indicate the change would be unacceptable, (i.e., would not ensure adequate protection). This guidance would specifically state the staff's responsibilities to consider risk in regulatory decision making where the staff has information that leads it to question whether there is adequate protection. Section 182.a of the Atomic Energy Act of 1954, as amended (AEA) provides the NRC the authority to require the submission of information in connection with a license application (including an application for a license amendment) and this includes requesting risk information where NRC has reason to question adequate protection in a specific case. In cases where the risk information raises a concern with respect to adequate protection, the Commission could deny the application or condition its approval upon a showing that the applicant has addressed the risk information such that there is reasonable assurance of

adequate protection. However, if the risk information does not raise a concern with respect to adequate protection, then the Commission could: grant the license subject to conditions or requirements beyond those required in the Commission's regulations if a backfit analysis pursuant to 10 CFR 50.109 were performed to demonstrate that the additional conditions or requirements represent a substantial increase in protection of public health and safety whose costs are justified in view of the increased level of protection. In either case, however, the NRC bears the burden of demonstrating that the additional conditions and requirements are justified.

Therefore, additional direct authority does not need to be stated in Part 50 itself. However, to provide clarity and consistency, additional guidance in such supporting documents as a regulatory guide could be established to assist the staff in identifying circumstances in which the relationship between meeting the regulation and demonstrating adequate protection should be further explored. The staff would utilize such guidance in deciding "if undue risk exists" (i.e., there is no adequate protection), even when all other regulatory requirements appear to be satisfied.

#### Disadvantages of Clarification of Staff Authority

Issuing staff guidance, rather than undertaking a rulemaking, to clarify the responsibility of the staff to apply risk-informed concepts in regulatory activities would rely upon our regulatory authority to take appropriate action whenever adequate protection is called into question. Absent rulemaking severe accident risk will be considered only in those instances where the staff believes adequate protection may be in question, or the backfit provisions of 50.109 can be satisfied. This sets a high threshold that the staff must achieve in pursuing severe-accident issues with licensees, who are not in the process of supporting risk-informed licensing actions. Pursuing the clarification approach discussed above would put the additional burden on the staff to demonstrate lack of adequate protection, where the staff would wish to take regulatory action based upon risk insights.

#### Staff Recommendation

The staff recommends that the Commission approve development of clarification guidance with respect to the staff's authority to use risk-informed approaches in appropriate regulatory activities. However, should the Commission decide to initiate rulemaking to go further and require licensees to consider severe accident risk in all licensing activities, the staff recommends that this issue be included into the scope of Option 3 for further study.

## IMPLEMENTATION ISSUES FOR RISK-INFORMING 10 CFR PART 50

Issue	Description
Metrics and acceptance guidelines	What metrics are needed for the traditional engineering and risk parts of specific risk-informed regulations? What are the associated acceptance guidelines? Should the categorization of SSCs with respect to safety importance be graded? How should currently "non-safety-related" SSCs that are risk-important be captured in the new categorization scheme?
Required NRC review and approval	What risk-informed decisions can be made by licensees without NRC advance review and approval? What decisions will require such advance approval?
PRA quality	What is the required scope, level of detail, and quality of risk information needed for using PRA to support decisions for specific regulations?
Required documentation	What documentation is needed on site and is submitted to NRC for plant design and operational changes made as a result of the modifications to Part 50? Should the PRA be required to be docketed? How do potential changes to Part 50 to make it more risk-informed affect the ongoing process to make FSAR updates risk-informed?
Conforming regulatory guide and standard review plan changes	What regulatory guides (RGs) and standard review plan (SRP) sections need to be modified to reflect changes to Part 50? Should these modifications be made in parallel with or subsequent to rule changes?
Integration with risk-informed oversight	How do changes to make the oversight process more risk-informed affect potential changes to Part 50? How do changes to Part 50 affect the oversight process?
Integration with ongoing rule changes	Which ongoing rule changes should be combined with potential rule changes to Part 50 to make it more risk-informed?

**Future Resources Associates, Inc.**

2039 Shattuck Avenue, Suite 402, Berkeley, California 94704  
(510) 644-2700 FAX (510) 644-1117  
e-mail: BUDNITZ @ PACBELL.NET

25 June 1999

Dr. B. John Garrick  
Chair, Advisory Committee on Nuclear Waste  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555

Dear Dr. Garrick:

Recently, I served as a member of the "Performance Assessment Peer Review Panel" that TRW and DOE assembled to review the most recent performance assessment for the proposed repository at Yucca Mountain. During that work, I had occasion to give some thought to the relative roles of realistic (probabilistic) performance assessment and defense-in-depth in NRC's overall scheme for regulation of Yucca Mountain, in light of both the obvious strengths and advantages of probabilistic performance-assessment methods and their equally obvious limitations.

The draft version of NRC's proposed Part 63 to Title 10 contains some words about defense-in-depth that seem to me ambiguous concerning its potential role in the overall regulatory approach. The principal discussion is found in the "Supplementary Information", Section VIII, "Multiple Barriers and Defense in Depth", page 8647 ff., Federal Register of February 22, 1999. Here NRC describes how it has decided to back away from the subsystem performance requirements of the old Part 60, based on advances in analysis technology and certain other considerations that are discussed extensively. The text cites the ACNW's recommendation on this question as follows: "....the ACNW recently recommended that the Commission implement the concept of defense in depth by ensuring that the effectiveness of individual barriers be identified explicitly in the total system performance assessment (TSPA), but specifically did not endorse the establishment of rule-based subsystem requirements for Yucca Mountain." The NRC then goes on essentially to endorse this ACNW recommendation, and seems to ask the applicant (DOE) only to "....demonstrate that the natural barriers and the engineered barrier system will work in combination to enhance overall performance of the geologic repository." Specifically, "....the Commission is now proposing to require that DOE evaluate the behavior of barriers important to waste isolation in the context of the performance of the geologic repository. The Commission does not intend to specify numerical goals

for the performance of individual barriers .... The Commission proposes to incorporate flexibility into its regulations by requiring DOE to demonstrate that the geologic repository comprises multiple barriers but not prescribe which barriers are important to waste isolation or the methods to describe their capability to isolate waste."

So far, so good — this text is quite clear to me. But then, at the very end of this Section VIII, comes the kicker: "The proposed requirements will provide for a system of multiple barriers and an understanding of the resiliency of the geologic repository provided by the barriers important to waste isolation to ensure defense in depth and increase confidence that the postclosure performance objective will be achieved." [emphasis added].

The thrust of this letter is an inquiry as to the operational meaning of those words, in the context of NRC's upcoming review of how DOE accomplishes "defense in depth" in the Yucca Mountain license application.

One interpretation of how NRC will review the Yucca Mountain design vis-a-vis defense-in-depth is that the DOE design for Yucca Mountain absolutely must take defense-in-depth into account (somehow! — apparently DOE gets to decide how!), and if it does not do so then a license will not be granted even if the other requirements are met. A second and alternate interpretation is that, if DOE can demonstrate that the repository design can meet the probabilistic criteria (the vehicle for such a demonstration would be a high-quality probabilistic performance assessment), then meeting those probabilistic criteria would be sufficient, without the need to demonstrate the efficacy of any specific design features to address defense-in-depth. In this latter interpretation, the defense-in-depth "requirement" might be met by the rather simple observation that both engineered and natural "barriers" will exist (as they manifestly do — several of each!) at Yucca Mountain, but the regulations would not demand any specific performance from any of the specific barriers. This would mean, in effect, that defense-in-depth would be formally cited as an important part of the regulatory philosophy underlying Part 63, but would be accorded only "lip service" in the actual implementation of the regulation itself, given the observation that the Yucca Mountain design will surely have both several engineered barriers and several natural barriers.

The two above interpretations aren't all that different in practice, although in philosophy they are quite different. In either of them, no further regulatory guidance from the NRC staff is apparently needed: DOE will simply need to show that several barriers exist, and will need to analyze the effectiveness of each, but will not need to compare them to any criteria, fixed or floating. Thus, either way, as a practical matter DOE could not "flunk" this defense-in-depth "requirement."

Still a third possibility is that NRC will specify later (through regulatory guides, branch technical positions, etc.) an acceptable way for DOE to address defense-in-depth, but that as of now the specific details of such a future NRC staff position have not yet been worked out. The text of draft Part 63 hints at this, in a way, but gives no clue as to which of the two possible approaches I mentioned above will govern as a matter of philosophy, and also doesn't indicate whether the philosophy to be used will have any practical impacts during NRC's regulatory review.

I cannot resolve this dilemma myself: no amount of staring at the conflicting sections of NRC text vis-a-vis the proposed Part 63 has been sufficient. I decided, charitably, that there must be more background that I am not aware of.

A few weeks ago, and I believe just by coincidence, the ACRS shined a light on this problem with their letter to Chairman Jackson: "The Role of Defense in Depth in a Risk-Informed Regulatory System", May 19, 1999. This ACRS letter was accompanied by an attached paper by J. N. Sorensen et al. ("On the Role of Defense in Depth in Risk-Informed Regulation"). Together, the ACRS letter and Sorensen's paper describe well the historical role of defense-in-depth in nuclear-reactor regulation. They observe that defense-in-depth has never been a regulatory requirement per se in reactor regulation, but instead has historically been a philosophy that the specific regulations embed all-over-the-place to accomplish the stated defense-in-depth goal(s). They also highlight that over the decades there have been many different interpretations of what defense-in-depth actually means for power-reactor regulation, both in terms of the underlying philosophy, and in terms of specific layers of "defense" that have been cited as manifestations of defense-in-depth.

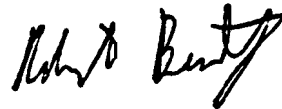
Turning back to Yucca Mountain and the proposed Part 63, I am writing to ask if the ACNW has given thought to (i) just what role the notion of defense-in-depth ought to play in NRC's regulatory scheme for Yucca Mountain; and to (ii) what the NRC staff really is seeking in its use of defense-in-depth language along with TSPA-performance-criteria language in Part 63. Also, I am writing to ascertain whether the ambiguities that I seem to find in the current draft language bother ACNW. Perhaps the language is clearer to the ACNW than it is to me, because the ACNW has had opportunities not available to me to delve more deeply into the staff's thinking and the regulatory background. (I modestly point out, though, that if I find the language ambiguous then perhaps others will also.)

On the specific issue of how the philosophy of defense-in-depth might be used at Yucca Mountain, I believe that a major contribution has been made by the ACRS when they distinguish between the "rationalist view" (in which defense-in-depth is a supplement to risk analysis) and the "structural view" (in which defense-in-depth plays a primary role in regulation and risk assessment supports it through analysis only). When I apply these ideas to Yucca Mountain, I stumble principally because the notion

of so-called independent barriers (one of which can fail without compromising the overall system), which notion has been so useful conceptually for achieving and demonstrating power-reactor safety, seems not to apply to the Yucca Mountain repository system. As I understand the Yucca Mountain design concept, one cannot assume total failure of any of the so-called "barriers" without seriously compromising the overall performance!

So what might the NRC have in mind when discussing defense-in-depth in their draft Part 63? I am writing to ask if the ACNW can cast light on this question for me, and by extension for the broader community.

Sincerely yours,

A handwritten signature in black ink, appearing to read "Robert J. Budnitz". The signature is written in a cursive, somewhat stylized font.

Robert J. Budnitz

**Note:** In parallel with this letter, I have sent a letter to the Part 63 docket with a "public comment", discussing this defense-in-depth issue. All of the thinking and much of the text in that public-comment letter are identical to the thoughts herein.





## **POLICY ISSUE** **(Information)**

July 16, 1999

SECY-99-186

**FOR:** The Commissioners

**FROM:** William D. Travers  
Executive Director for Operations

**SUBJECT:** STAFF PLAN FOR CLARIFYING HOW DEFENSE-IN-DEPTH APPLIES  
TO THE REGULATION OF A POSSIBLE GEOLOGIC REPOSITORY AT  
YUCCA MOUNTAIN, NEVADA

**PURPOSE:**

To inform the Commission of the staff's plans to more clearly address the Commission's defense-in-depth philosophy as it pertains to the proposed 10 CFR Part 63 and to the disposal of high-level radioactive wastes in a possible geologic repository at Yucca Mountain, Nevada.

**SUMMARY:**

This paper provides the staff's plan to address more clearly the U.S. Nuclear Regulatory Commission's (NRC's) defense-in-depth philosophy as it relates to disposal of high-level radioactive wastes. The plan describes a 6-month staff effort that includes conducting an interactive dialogue with stakeholders. The staff plan culminates with a formal response to the Commission on the implementation of defense-in-depth in the NRC's repository regulatory program on November 30, 1999, as part of the package transmitting the proposed final rule at 10 CFR Part 63. Additional milestones beyond November 30, 1999, are identified in the plan for development of more detailed guidance pending Commission approval.

**CONTACT:** Keith I. McConnell, NMSS/DWM  
(301) 415-7289

**BACKGROUND:**

The Staff Requirements Memorandum, issued on April 12, 1999, directed the staff to evaluate how the NRC could more clearly address repository defense-in-depth to foster a common understanding of this concept, and to inform the Commission of its findings. This paper responds to that direction and provides the staff's plan to clarify its expectations for a demonstration of defense-in-depth for a geologic repository. The staff intends to accomplish this through responses to public comments in the draft final rule for Part 63 and through development of the Yucca Mountain Review Plan (YMRP). In completing Part 63 and the YMRP, the staff will incorporate the Commission's defense-in-depth philosophy as elaborated in the White Paper on Risk-Informed and Performance-Based Regulation, issued on March 1, 1999, and has identified specific activities to involve stakeholders.

**DISCUSSION:**

The Nuclear Waste Policy Act of 1982 mandated that technical criteria developed by the Commission provide for a system of multiple barriers in the design of the geologic repository. To fulfill this statutory requirement, the Commission, in promulgating its generic regulations at Part 60 (final rule published on June 21, 1983), specified three numerical subsystem performance objectives for repository performance after closure:

- 1) The length of time radionuclides should be contained in the waste packages (300-1000 years);
- 2) The rate of subsequent releases from the engineered system (one part in 100,000 per year of the inventory present at 1000 years after permanent closure); and
- 3) The pre-placement ground-water travel time to the accessible environment (at least 1000 years).

Under Part 60, demonstrating compliance with these numerical objectives would constitute compliance with the multiple barrier provision.

In proposing revisions to these objectives in the proposed Part 63<sup>1</sup>, 15 years after Part 60 was promulgated, the staff noted that risk-informed, performance-based regulation of geologic disposal, together with advances in performance assessment methods, called for reexamining the imposition of specific numerical subsystem requirements as was done in Part 60. Further, it should be noted that the National Academy of Sciences (NAS) report on the "Technical Bases for Yucca Mountain Standards," published in 1995, opposed the inclusion of subsystem performance objectives. To maintain the Commission's defense-in-depth philosophy, but avoid incorporation of numerical subsystem performance objectives in its site-specific regulation, the staff recommended (SECY-97-300), and the Commission accepted, a proposed regulatory approach that includes assessment of repository barrier performance, without specifying numerical goals for subsystem performance.

---

<sup>1</sup>A comprehensive review of the Commission's consideration of multiple barriers and "defense-in-depth" for Part 63 was provided as Attachment 3 to SECY-97-300, "Proposed Strategy for Development of Regulations Governing Disposal of High-Level Radioactive Wastes in a Proposed Repository at Yucca Mountain, Nevada."

Such an approach will require the U.S. Department of Energy (DOE) to provide greater transparency of how multiple barriers contribute to overall performance, and associated uncertainty. The approach does not require compliance with separate performance objectives for individual barriers that are unrelated to the U.S. Environmental Protection Agency standards. As proposed at Part 63.114, DOE must:

- 1) Identify the design features of the engineered barrier system (e.g., waste package, backfill), and natural features of the geologic setting (e.g., unsaturated zone, saturated zone), that are considered barriers important to waste isolation (63.114(h));
- 2) Describe the capability of barriers, identified as important to waste isolation, to isolate wastes, taking into account uncertainties in characterizing and modeling the barriers (63.114(i)); and
- 3) Provide the technical basis for the description of the capability of barriers, identified as important to waste isolation, to isolate waste (63.114(j)).

The staff believes that these requirements for multiple barriers, when combined with requirements for active and passive institutional control, are sufficient to provide for defense-in-depth for post-closure repository performance<sup>2</sup>. However, the staff anticipated that comments would be received on the requirements for defense-in-depth in the proposed Part 63, because they represent a substantially different approach from that taken in Part 60.

In the statement of considerations for the proposed rule, the staff noted that, in parallel with the rulemaking, staff was developing review guidance in the form of a YMRP. The purpose of these statements was to recognize the need to develop additional guidance on how to evaluate compliance with these requirements. Also noted in the proposed rule was the fact that the staff was considering a number of approaches to evaluating DOE's license application including, but not limited to: (1) sensitivity analyses; (2) modeling the behavior of individual barriers; (3) quantifying how individual barriers contribute to performance; and (4) delineating the capability of barriers to isolate waste. Although various approaches exist for aiding the definition of the capability of individual barriers to isolate waste, the identification of which approach or combination of approaches is acceptably transparent in defining the waste isolation attributes of the repository system, without placing undue or non-productive burdens on DOE, is inherently complex. Consequently, developing a common understanding of these complex issues within a risk-informed, performance-based framework will require considerable deliberation and interaction with stakeholders. Therefore, to facilitate development of a common understanding on an acceptable approach(es), the staff has planned a program that includes substantial stakeholder involvement.

The staff's plan focuses on developing detailed guidance for conducting its review of a geologic repository at Yucca Mountain in the YMRP. Interaction with the DOE, the Advisory Committee on Nuclear Waste (ACNW), the Office of Nuclear Reactor Regulation, the Office of Nuclear

---

<sup>2</sup>It is expected that defense-in-depth for pre-closure operations would be achieved in a manner similar to that for other operating nuclear facilities.

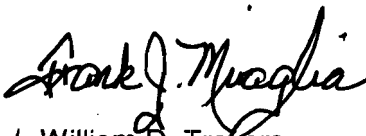
Regulatory Research, the State of Nevada and Affected Units of Local Government, possibly the Joint Advisory Committee on Reactor Safeguards (ACRS)/ACNW Subcommittee on Risk-Informed Regulation in NMSS, and other stakeholders will occur as the YMRP is developed. The staff intends to include the annotated outline of the review plan when the proposed final Part 63 is submitted to the Commission.

RESOURCES:

The activities described above are part of the efforts to finalize Part 63 and complete Rev. 0 of the YMRP in FY1999 and beyond. Resources to accomplish these activities are included in the current budget.

COORDINATION:

The Office of the General Counsel has reviewed this paper and has no legal objection. The Office of the Chief Financial Officer has reviewed this paper for resource implications and has no objection.

  
for William D. Travers  
Executive Director  
for Operations

Attachment: As stated

DISTRIBUTION:

Commissioners  
OGC  
OCAA  
OIG  
OPA  
OCA  
ACNW  
CIO  
CFO  
EDO  
REGIONS  
SECY

## **STAFF APPROACH TO CLARIFYING DEFENSE-IN-DEPTH FOR THE POSSIBLE GEOLOGIC REPOSITORY AT YUCCA MOUNTAIN, NEVADA**

### **WHAT ARE THE UNDERLYING BASES FOR IMPLEMENTING DEFENSE-IN-DEPTH?**

- The Commission's "White Paper on Risk-Informed and Performance-Based Regulation," (issued on March 11, 1999) defined the concept of defense-in-depth as follows:

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.

- The Proposed 10 CFR Part 63:

As reflected in the statement accompanying proposed 10 CFR Part 63, DOE will demonstrate that the natural barrier and the engineered barrier system will work in combination to enhance overall performance of the repository.

In Part 63, a barrier is defined as any material or structure that prevents or substantially delays movement of water or radioactive materials.

Requirements in Part 63 are that the U.S. Department of Energy (DOE) must: 1) identify those design features of the engineered barrier system, and natural features of the geologic setting, that are considered barriers important to waste isolation (e.g., waste package, drip shield, unsaturated zone limiting moisture flux, and saturated zone retarding radionuclide migration); 2) describe the capability of these barriers to isolate waste, taking into account uncertainties in characterizing and modeling the barriers; and 3) provide the technical basis for the description of the capability of these barriers.

### **HOW WILL STAFF CLARIFY ITS EXPECTATIONS FOR DEMONSTRATING MULTIPLE BARRIERS?**

- Based on public comments, we will consider refining regulatory requirements, as needed, to show that multiple barriers are acceptably covered by 10 CFR Part 63 (described under the second bullet under "Proposed 10 CFR Part 63"). However, the goal of avoiding imposition of numerical subsystem performance objectives will be maintained.
- We will describe an acceptable approach(es) for demonstrating the capabilities of multiple barriers to isolate waste in the Yucca Mountain Review Plan (YMRP). Specific

quantitative approaches that will be considered include, but are not limited to: sensitivity analyses, importance analysis, and presentation of intermediate modeling results (e.g., model results that are calculated in support of dose estimates such as waste package lifetime).

**WHEN AND HOW WILL CLARIFICATIONS BE MADE AVAILABLE TO STAKEHOLDERS?**

- We have presented information on the defense-in-depth regulatory requirements in Part 63 at the DOE/U.S. Nuclear Regulatory Commission (NRC) Technical Exchange (public meeting) on May 26, 1999. The DOE is currently working on approaches to meeting the multiple barriers requirements in Part 63 and presented some of their ideas at the technical exchange.
- We will coordinate with the Advisory Committee on Nuclear Waste (ACNW) on this topic, as we did in briefing the Committee in June of this year on this plan. We will also coordinate with the Offices of Nuclear Reactor Regulation and Nuclear Regulatory Research, and the Joint ACRS/ACNW Subcommittee on Risk-Informed Regulation in NMSS.
- We will hold a public meeting in Las Vegas. In the meeting, we will further clarify the requirements of Part 63 by: 1) discussing our proposed resolution of public comments on defense-in-depth; and 2) presenting example calculations that demonstrate the effectiveness of multiple barriers.
- Based on these interactions, we will finalize guidance in Rev. 0 of the YMRP, due to be completed in March 2000.

**WHAT IS THE SCHEDULE OF PLANNED ACTIVITIES FOR CLARIFYING REPOSITORY DEFENSE-IN-DEPTH?**

Activity	Completion Date	Purpose
1. DOE/NRC Total System Performance Assessment Technical Exchange at the Center for Nuclear Waste Regulatory Analyses	May 25 - 27, 1999	Preliminary discussion with DOE on the proposed regulatory requirements for multiple barriers (other stakeholders present as observers)
2. Concept Paper on Defense-in-Depth (this Commission Paper)	July 2, 1999	To present the staff's plan for the repository defense-in-depth concept as proposed in Part 63 (in response to the SRM dated April 12, 1999)

Activity	Completion Date	Purpose
3. Presentation to the ACNW	June 28 - 30, 1999	To brief the ACNW on the staff's proposed plan for clarifying the acceptance criteria and review plans for the license application
4. Interactions with the Office of Nuclear Reactor Regulation, Office of Nuclear Regulatory Research, and possibly Joint ACRS/ACNW Subcommittee on Risk-Informed Regulation	July/August 1999	To ensure an appropriately consistent approach for risk-informed and performance-based requirements
5. Meetings with DOE and Public Meetings on Repository Defense-in-Depth in Nevada	August/September 1999	To solicit comments on the staff's approach to repository defense-in-depth; to present possible technical approaches
6. Total System Performance Assessment and Integration Issue Resolution Status Report	September 30, 1999	To provide preliminary draft guidance on possible technical approaches to demonstrate repository design meets applicable regulatory requirements. This guidance will become part of the Yucca Mountain Review Plan (YMRP) or be referenced by the YMRP.
7. Presentation to ACNW	September (after public comment period is over, but before Part 63 is finalized)	To brief the ACNW on staff's proposed positions and strategies on addressing public comments and on the annotated outline of the YMRP
8. Draft final 10 CFR Part 63 to Commission along with Annotated Outline of YMRP	November 30, 1999	To finalize the rule and summarize the approach to defense-in-depth in the YMRP
9. Public meetings in Nevada after finalizing Part 63	January 2000	To present and clarify the final Part 63 and the YMRP, including the requirements for repository defense-in-depth
10. Interactions with DOE	January 2000	To present and clarify the final Part 63 and the YMRP, including requirements for repository defense-in-depth

Activity	Completion Date	Purpose
11. YMRP Rev. 0 (postclosure only)	To the Commission March 31, 2000	To submit to the Commission a risk-informed performance-based YMRP which includes technical guidance and acceptance criteria for conducting the review
12. Future Revisions of YMRP	September 30, 2000; September 30, 2001	To update the YMRP on an annual basis. The last revision would be published 5 months before the current expected Yucca Mountain License Application submission date (March 1, 2002).





UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

RELEASED TO THE PDR

10/28/99      DW  
date                      initials

October 28, 1999

SECRETARY

MEMORANDUM TO: William D. Travers  
Executive Director for Operations

FROM: Annette Vietti-Cook, Secretary *Annette Vietti-Cook*

SUBJECT: STAFF REQUIREMENTS - SECY-99-191 - MODIFICATIONS  
TO THE SAFETY GOAL POLICY STATEMENT

The Commission has disapproved the staff's recommendation to proceed with a study of the feasibility of developing overarching safety principles as being premature in light of the ongoing efforts to transition to more risk-informed regulation. This effort should be delayed until experience is gained from the current changes to our regulatory structure so that we can build on a robust foundation. This approach should build on our experience with operational safety, deterministic analysis, and risk-informed methods. Instead of using a top-down approach to develop the overarching safety principles and define adequate protection, we should use a bottom-up approach. This guidance is not meant to supercede previous Commission guidance associated with SECY-99-100. However, in implementing this guidance, should the staff identify areas where this guidance cannot be reconciled with previous Commission guidance on SECY-99-100, the staff should forward the issue to the Commission for resolution. The staff should work to bolster and clarify how it makes its findings of reasonable assurance and should enhance and verify the bases and premises for its determinations as new methodologies and technology permit. This process should not only improve the Commission's specific findings but, lead to a more refined description of the meaning of "reasonable assurance" of adequate protection.

The staff should still provide a recommendation to the Commission on whether to modify the current Safety Goal Policy Statement.

(EDO)

(SECY Suspense:

3/30/2000)

290085

*DF03/0*  
*OTM-6*  
*Sam*

cc: Chairman Dicus  
Commissioner Diaz  
Commissioner McGaffigan  
Commissioner Merrifield  
OGC  
CIO  
CFO  
OCA  
OIG  
OPA  
Office Directors, Regions, ACRS, ACNW, ASLBP (via E-Mail)  
PDR  
DCS



## **POLICY ISSUE** **(Notation Vote)**

July 22, 1999

SECY-99-191

**FOR:** The Commissioners

**FROM:** William D. Travers  
Executive Director for Operations

**SUBJECT:** MODIFICATIONS TO THE SAFETY GOAL POLICY STATEMENT

**PURPOSE:**

To inform the Commission of staff progress in developing recommendations regarding possible modifications of the reactor Safety Goal Policy Statement in response to the Commission's Staff Requirements Memoranda on SECY-97-208 (October 16, 1997) and on SECY-98-101 (June 30, 1998). We also propose beginning a feasibility study of the development of overarching safety principles for the agency.

**BACKGROUND:**

As discussed in SECY-98-101, the Commission's Safety Goal Policy Statement, issued in 1986, should be modified to make the statement consistent with current practices as stated in Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," to reflect Commission guidance received since the 1986 Policy Statement was issued, and to clarify the role of safety goals in NRC's regulatory process.

By a Staff Requirements Memorandum dated June 30, 1998, the Commission approved the staff's plans and cautioned that "The revised policy statement should remain a high-level document describing the principles consistent with the Commission's views on 'how safe is safe enough.' The staff should be mindful that the revised Safety Goal Policy Statement needs to be consistent with the PRA Policy Statement, and should not include too many quantitative guidelines which would make the Safety Goal Policy Statement overly prescriptive."

Contact:  
Joseph A. Murphy, RES  
301-415-5670

## DISCUSSION:

### 1.0 Reactor Safety Goal Policy

The staff is proceeding with the review of the eleven issues identified in SECY-98-101 and in March 2000 will recommend to the Commission whether or not to modify the current Safety Goal Policy Statement. This delay will provide time for coordination with a study on the development of overarching safety principles (discussed later in this paper), permit integration with the other ongoing risk-informed initiatives, and provide for stakeholder, ACRS and CRGR feedback. The NRC Steering Committee for Risk-Informed Activities has reviewed the concepts and recommendations contained in this paper and their guidance has been incorporated into the paper. As work proceeds on the Safety Goal Policy issues, the overarching safety principles, as well as the other items in the PRA Implementation Plan, the Steering Committee will continue to review and provide integrated guidance on these activities. The status of our evaluation of each of the issues is provided below. Two of the eleven issues (definition of adequate protection and consideration of defense in depth) have been combined in the discussion which follows.

### Plant Specific Usage of Safety Goals

The present Policy Statement restricts the use of the safety goals to generic applications. We intend to recommend amending the Safety Goal Policy Statement, consistent with Commission guidance on Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis" to indicate that safety goals can be considered as part of a risk-informed evaluation of individual reactor regulatory actions, in addition to consideration in generic agency actions, subject to the adequacy of the underlying probabilistic risk analysis. This will make the Policy Statement consistent with existing guidance. The five general principles on the use of risk information in making regulatory changes, stated in Regulatory Guide 1.174, may be appropriate for inclusion into the Safety Goal Policy to provide guidance for such plant-specific use.

### Subsidiary Objectives Including Elevation of Core Damage Frequency as Fundamental Goal

Considering the uncertainties associated with predicting severe accidents, the staff believes that additional emphasis should be placed on accident prevention in the Policy Statement. This should be done in a qualitative fashion so that it is clear that accident prevention should receive priority over mitigation. However, a quantitative accident prevention goal does not appear necessary, since it is currently adequately covered by the existing subsidiary objective for core damage frequency (CDF) and related regulatory guidance documents, such as Regulatory Guide 1.174, and in the Regulatory Analysis Guidelines (NUREG/BR-0058). It may be reasonable, however, to include in the Policy Statement a discussion of the subsidiary objectives (CDF and large early release frequency, LERF) as well as any additional subsidiary objectives that may result from further study (e.g., temporary changes in risk).

We will include a discussion of the pros and cons associated with elevation of the core damage frequency to the level of a fundamental goal in our final paper.

### Treatment of Uncertainty

The existing Safety Goals consider uncertainties implicitly by setting the goals in terms of the mean of the probability distribution for the qualitative health objectives (QHOs). Guidance is provided in Regulatory Guide 1.174 on the importance of consideration of not only parameter uncertainty, but also model uncertainty and completeness uncertainty in risk-informed decisions. Guidance is also being developed by international bodies. We believe it would be desirable to amend the Safety Goal Policy Statement to make clear that all types of uncertainty must be considered when making a safety decision.

### Use of Safety Goals to Define "How safe is safe enough"

The guidance provided to the staff in the June 15, 1990, SRM on safety goals articulates that it is the intent of the Safety Goal Policy Statement to define "how safe is safe enough." The SRM guidance should be incorporated into the Policy Statement.

### Definition of Adequate Protection and Defense-in-Depth

Several stakeholders have called for a definition of "adequate protection." For example, the Center for Strategic and International Studies in their draft report on "Nuclear Regulatory Process Review," noted the importance of a clear definition of adequate protection and a consistent application of safety requirements. The concept of adequate protection has multiple attributes and both legal and technical considerations. Therefore, it is not clear if the reactor Safety Goal Policy is the correct vehicle for exploring this issue. For example, it may be more appropriate to address this issue as part of a broader set of safety principles as discussed later in this paper.

As stated in its June 15, 1990, SRM the Commission did not consider it necessary to create a generic definition of adequate protection. However, use of a three-tiered regulatory philosophy (a region where adequate protection is required regardless of cost, a region where cost-beneficial actions are considered provided they pass the Backfit Rule, and a region below the safety goals where additional requirements would not be justified) could benefit from a definition of adequate protection.

As an alternative to "defining" adequate protection, there may be benefit in defining a "zone of presumptive adequate protection," as an extension of the "presumptive" approach to adequate protection for the current set of deterministic regulations as articulated in Maine Yankee, ALAB-161, 6 AEC 1003 (1973). Under this approach, qualitative and/or quantitative elements and threshold values would be identified which, if met, would be regarded as presumptively providing adequate protection. However, failure to meet the threshold values would not per se be regarded as a failure to provide adequate protection. Rather, the failure to meet the threshold values would require more detailed consideration of relevant factors, including risk, to determine whether adequate protection would be provided.

If it is decided to pursue a definition of adequate protection, defense in depth will be defined and placed in context in the regulatory framework as part of that discussion. If not, it will be considered separately in formulating recommended changes to the Policy Statement. The Staff will also determine the feasibility of establishing a concept of adequate protection for non-power facilities and materials users. This will likely pose the same issues that were identified in SECY-99-100 with respect to establishing a safety goal (or goals) for materials users.

#### Societal Risk

Societal risk is currently addressed through a qualitative statement and a QHO on latent cancer fatalities. Comparisons to the QHO are calculated based on the individual risk of latent cancer fatality, averaged over 10 miles. This averaging process, expressed in terms of average individual risk, does not explicitly limit societal risk. However, since new rule changes are subjected to backfit analysis using the regulatory analysis guidelines, societal risk (in person-rem) is explicitly considered when determining if the cost of safety improvements is commensurate with societal risk averted. Therefore, the policy statement should be expanded to acknowledge this approach in implementing the existing qualitative societal risk goal, but additional quantitative goals are not necessary.

#### Land Contamination

The Commission's Strategic Plan calls for protection of the environment in a manner that is responsive to environmental concerns and is consistent with the Commission's responsibility for protecting the radiological health and safety of the public. Risk analyses indicate that, in case of a severe accident involving large off-site releases, most of the population dose associated with the latent cancer fatalities (or cancer incidence) comes from ground shine and ingestion dose, rather than from a cloud inhalation dose. The magnitude of this dose, thus, is strongly affected by protective measures employed after an accident. However, decisions associated with recommending land interdiction following an accident are directly dependent on protective action guidelines and actions taken by others (e.g., States, EPA). Given these concerns, we are evaluating the pros and cons associated with a separate goal in this area. Such a goal would need to consider the differences between land interdiction following an accident and the criteria in the License Termination Rule. We note that in the recent revision to Part 100, the Low Population Zone distance was evaluated to ensure it was sufficient to keep the likelihood of contaminating a large population center, such that it is uninhabitable, at a very low value. Thus, land contamination has, to some extent, been considered in developing the siting regulations.

#### Temporary Changes in Risk

We believe that the Safety Goal Policy should address in general terms the Commission's policy regarding temporary changes in risk as a result of equipment failures, maintenance activities, and human actions. We are evaluating the pros and cons of various approaches. It may be appropriate to consider the impact of temporary changes on defense in depth. This evaluation is being coordinated with the treatment of configuration control in the pending amendments to the Maintenance Rule.

### Update Policy Statement To Reflect Recent Guidance and Current Use of Risk Information

The policy statement will be updated to reflect the use of a risk-informed approach to implement regulatory requirements.

### General Performance Guideline for Frequency of a Large Release of Radioactive Material

SECY-93-138 concluded that a guideline of  $1 \times 10^{-6}$  for the frequency of a large release of radioactive material could not be developed without being significantly more restrictive than the QHOs and recommended that work on such a guideline be terminated. Consistent with the related SRM, dated June 10, 1993, which approved that termination, statements in the policy statement on the frequency of a large release of  $1 \times 10^{-6}$  per year will be deleted.

### 2.0 Overarching Safety Principles

Several factors have emerged over the past year that suggest consideration should be given to developing a high level "safety policy" that would describe those overarching safety principles that apply to all agency safety activities. These factors include the following:

- The criticism received in the context of our Congressional hearings in July 1998, regarding the lack of consistency and transparency in our safety decisions,
- Similar feedback received in reviews by the General Accounting Office in their reports on "Major Management Challenges and Program Risks - Nuclear Regulatory Commission" (GAO/OCG-99-19) and "Strategy Needed to Regulate Safety Using Information on Risk" (GAO/RCED-99-95) and the Center for Strategic and International Studies in their draft report on "Nuclear Regulatory Process Review,"
- The fact that many of the issues discussed in SECY-98-101 are agency- wide issues, not just reactor issues, and should be addressed in an overall agency context. These include the following issues:
  - Role and use of an adequate protection definition and safety goals to express a basic safety philosophy,
  - Plant specific usage of safety goals,
  - Treatment of uncertainty,
  - Appropriate application of defense in depth, and
  - Use of risk-informed and performance based regulation.

- The submission of SECY-99-100, which recommends actions to risk-inform NMSS activities and the Commission's response in a June 28, 1999, SRM. Implementation of the direction provided in the June 28, 1999, SRM, would benefit from articulation of these overarching safety principles. Further, the development of these principles will benefit from NMSS input by helping to assure that there is an appropriate level of generality.

These principles could be qualitative and would address items such as:

- Qualitative goals for public, worker, and environmental protection,
- Description of the approach to regulation and a statement that changes to rules and regulations will be made consistent with Regulatory Analysis Guidelines. The consideration of the cost-benefit relationship will be made in context of the various activities regulated,
- Role and definition of adequate protection,
- The role and definition of risk-informed and performance-based requirements, expanding on the guidance given in the Commission's White Paper,
- Role and definition of defense in depth, recognizing the insights in the White Paper, in comments from ACRS in this regard, and expanding on the discussion in the Strategic Plan,
- Other considerations such as treatment of uncertainty, population at risk, temporary risk increases, and the different time scale of risk considerations between reactor considerations and those associated with high level waste, and
- The need for consistency and integration among these principles and other NRC regulatory principles such as the Severe Accident Policy Statement, Regulatory Analysis Guidelines, and the Backfit Rule.

Attachment 1 illustrates, in concept, examples of the types of principles that we might explore in this high level policy. We are proposing a small feasibility study to explore the viability of developing such principles.

The objective of developing a set of integrated high level safety principles is to document in a hierarchical fashion those high level objectives, goals, and practices that shape regulatory requirements and decision-making and ensure compliance with the Atomic Energy Act. Their development will require substantial stakeholder involvement. However, once developed, they will help promote regulatory stability, consistency, and public confidence by consolidating and clearly stating the Commission's philosophy and approach to safety and regulatory actions. These principles should also provide the public with a better understanding of how NRC's regulatory actions are developed and what our regulatory actions are trying to achieve, thus facilitating communication with our stakeholders and enhancing public confidence. These principles will also provide the NRC staff with the framework to develop and take regulatory actions and facilitate the move to risk-informed regulation by providing a foundation for making risk-informed decisions with respect to the scope of and objectives for regulation. Ultimately, such high level principles would facilitate and could be included in an overall agency strategy to



risk-inform its activities, as proposed by GAO in its report, GAO/RCED- 99-95, and discussed in the Chairman's response to GAO. They could also become part of the Agency's Strategic Plan. However, it should be recognized that principles are not enforceable, and our ability to apply them to the regulatory process may involve the need for rulemaking.

COORDINATION:

The Office of the General Counsel has reviewed this paper and has no legal objection. The Office of the Chief Financial Officer has reviewed this Commission paper for resource implications and has no objections. The Office of the Chief Information Officer has reviewed the Commission Paper for information technology and information management implications and concurs in it. The NRC Steering Committee for Risk-Informed Activities has reviewed the concepts and recommendations contained in this paper and their guidance has been incorporated into the paper. As work proceeds on the Safety Goal Policy issues and the overarching safety principles, the Steering Committee will continue to review and provide guidance on these activities.

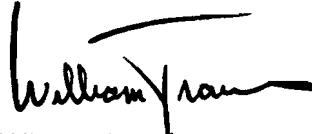
RESOURCES:

The staff proposes a small effort, in parallel with continuing evaluation of the reactor Safety Goal issues, to draft a set of high level safety principles. This effort would build upon and complement the work on the reactor Safety Goal issues by helping to ensure that these issues are addressed in an agency-wide fashion. This effort would also involve obtaining feedback from stakeholders and additional interaction with ACRS and ACNW. A report to the Commission on the feasibility and usefulness of continuing this effort would be prepared and provided to the Commission after the preliminary work is completed. This approach is consistent with feedback received from ACRS in their letter of April 19, 1999. It is estimated that this effort to evaluate feasibility would take approximately 9 months and would be done with in-house resources (1-2 FTE combined from RES, NMSS, OGC and NRR) that would be reprogrammed from other lower priority work (NMSS resources are discussed in SECY-99-100).

RECOMMENDATION:

1. That the Commission authorize the staff to proceed with a study of the feasibility of developing overarching safety principles,
2. That the Commission note that a recommendation will be provided by March 30, 2000, regarding the need to modify the current Safety Goal Policy Statement. This represents a delay of eight months from that previously reported, but is necessary recognizing the

complexity of the issues involved, the need to ensure coordination and consistency with the feasibility study on overarching safety principles and with those risk-informed initiatives already underway under the PRA Implementation Plan, and the need for stakeholder, ACRS and CRGR review.



William D. Travers  
Executive Director  
for Operations

Attachment:

1. Conceptual Outline for Proposed High Level Safety Principles

Commissioners' completed vote sheets/comments should be provided directly to the Office of the Secretary by COB Friday, August 6, 1999.

Commission Staff Office comments, if any, should be submitted to the Commissioners NLT July 30, 1999, with an information copy to the Office of the Secretary. If the paper is of such a nature that it requires additional review and comment, the Commissioners and the Secretariat should be apprised of when comments may be expected.

DISTRIBUTION:

Commissioners  
OGC  
OCAA  
OIG  
OPA  
OCA  
ACRS  
ACNW  
CIO  
CFO  
EDO  
REGIONS  
SECY

## Conceptual Outline for Proposed High Level Safety Principles

(The concepts presented here are provisional and are subject to review as the staff develops these safety principles.)

- **OBJECTIVE:**

To document in a hierarchical fashion those high level objectives, principles, and practices that shape regulatory requirements and decision-making and ensure compliance with the Atomic Energy Act. Such high level principles will help promote regulatory stability, consistency, and public confidence by consolidating and clearly stating the Commission's philosophy and approach to safety and regulatory actions. This will provide the public with a better understanding of how NRC's regulatory actions are developed and what they are trying to achieve, as well as provide the NRC staff with the framework to develop and take those actions. It will also facilitate the move to risk-informed regulation by providing a foundation for making risk-informed decisions with respect to the scope of and objectives for regulation. Rule changes associated with later implementation of the principles would be subject to the Backfit Rule and evaluated using the Regulatory Analysis Guidelines, as appropriate.

- **SCOPE:**

High level principles and practices that apply to all NRC activities (reactor and non-reactor), including normal and off-normal operation.

- **PRINCIPLES AND PRACTICES THAT APPLY TO ALL NRC ACTIVITIES**

- A. **Qualitative Goals for Public, Worker, and Environmental Protection**

- Individual members of the public should be provided a level of protection from the use of radioactive material such that individuals bear no significant additional risk to life and health.<sup>1</sup>
- Individual workers who are exposed to radiation or handle radioactive materials as part of their occupation should be provided a level of protection from the consequences of such exposures commensurate with the risks to life and health<sup>1</sup> and the cost of preventing such exposure. Adequate protection should be provided regardless of costs, with further reductions in exposures in accordance with an ALARA (as low as reasonably achievable) principle.
- Societal risk to life and health from the use of radioactive materials should be comparable to or less than the risks from other similar activities and should not be a significant addition to other societal risks.

---

<sup>1</sup>Life and health refers to early and latent fatalities

B. Regulatory Approach To Meet Public, Worker Protection Goals

- A level of protection (safety) provided to the public and workers should be established such that a sufficient level is provided without regard to cost (adequate protection<sup>2</sup>) and additional protection is provided where the benefits of such protection outweigh the costs (cost-beneficial) and result in a substantial improvement in protection. Risk to workers should be comparable to or lower than the risk to workers in comparable industries.
- Safety decisions and regulatory actions must be commensurate with the levels of protection achieved in the design and operation of regulated activities. In general, regulated activities will not take place unless adequate protection is achieved and will comply with all cost-beneficial requirements unless special circumstances permit an exception to the cost-beneficial requirements.

C. Implementation of Regulatory Approach

- Wherever practical, regulatory requirements will be risk-informed and performance-based.<sup>3</sup>
- Regulatory requirements are to provide a balance between prevention and mitigation, as appropriate.
- Regulatory requirements will address uncertainties by application of sound principles. These may include considerations such as defense in depth,<sup>4</sup> safety margins, and the use of appropriate codes and standards, depending on the nature of the issue at hand.

Consideration will be given to the ICRP Principles of Radiation Protection.

- Regulatory requirements will address long term (high level waste) as well as short term (temporary conditions) risks.
- Regulatory requirements will reflect due consideration of the population at risk, the time scale of the regulated activity, and the various modes of operation of the regulated activity.
- Regulatory requirements will consider accident initiators caused by equipment error, human error, and natural hazards.

---

<sup>2</sup>A definition of adequate protection will be needed.

<sup>3</sup>Use definitions from Risk Informed Performance Based white paper (Yellow Announcement-019, dated 3/11/99).

<sup>4</sup>A definition of defense in depth will be needed.



# **RULEMAKING ISSUE**

(Notation Vote)

October 29, 1999

SECY-99-256

**FOR:** The Commissioners

**FROM:** William D. Travers  
Executive Director for Operations

**SUBJECT:** RULEMAKING PLAN FOR RISK-INFORMING SPECIAL TREATMENT  
REQUIREMENTS

**PURPOSE:**

To obtain the Commission's approval of a rulemaking plan and issuance of an Advance Notice of Proposed Rulemaking for risk-informing special treatment requirements.

**SUMMARY:**

The staff has prepared a rulemaking plan (Attachment 1) that describes an alternative risk-informed approach to special treatment requirements.<sup>1</sup> These alternative requirements would vary the treatment applied to structures, systems, and components (SSCs) on the basis of their safety significance using a risk-informed categorization method. SSCs that are safety significant would be subject to greater regulatory control than SSCs of low safety significance. This

**CONTACT:**  
Thomas A. Bergman, NRR  
301-415-1021

---

<sup>1</sup>Special treatment requirements are current requirements imposed on structures, systems, and components that go beyond industry-established requirements for equipment classified as commercial grade that provide additional confidence that the equipment is capable of meeting its functional requirements under design basis conditions. These additional special treatment requirements include additional design considerations, qualification, change control, documentation, reporting, maintenance, testing, surveillance, and quality assurance requirements.

approach differs from the current special treatment requirements, which are based on those SSCs that are determined to be safety-related or important to safety based on deterministic considerations. This alternative approach would maintain safety while reducing unnecessary regulatory burden to licensee's and improving the staff's regulatory effectiveness and efficiency. The rulemaking plan implements the approach described under Option 2 in SECY-98-300, "Options for Risk-Informed Revisions to 10 CFR Part 50 - 'Domestic Licensing of Production and Utilization Facilities,'" dated December 23, 1998.

Four issues that represent significant challenges to completing this rulemaking have been identified: (1) selective implementation (discussed in SECY-98-300), (2) potential impact of these rule changes on other rules (e.g., 10 CFR Part 19, 10 CFR 50.120, 10 CFR Part 54, 10 CFR Part 55), (3) the type and amount of staff review required before licensees can implement the alternative requirements, and (4) the level of regulatory treatment required for SSCs based on their safety-significance.

The rulemaking plan includes six major efforts: (1) review of the South Texas Project (STP) exemption request;<sup>2</sup> (2) issuance of an advanced notice of proposed rulemaking (ANPR, Attachment 2); (3) a categorization pilot program; (4) review of a Nuclear Energy Institute (NEI) guideline on SSC categorization; (5) issuance of a proposed rulemaking; and (6) issuance of a final rulemaking. Some of these efforts are ongoing.

If Commission approval of the rulemaking plan is granted within 6 weeks of the date of this Commission paper, the staff estimates that the final rule can be submitted to the Commission for approval in October 2001. Licensee implementation could then begin in March 2002. Execution of the rulemaking plan is estimated to require 47 full-time equivalent (FTE) staff, and \$3.0 million of technical assistance over FY 2000, 2001, and 2002.

#### **BACKGROUND:**

In SECY-98-300, the staff presented three options for risk-informed modifications of 10 CFR Part 50: (1) continue ongoing rulemaking activities and risk-informed approaches making no changes to the current Part 50; (2) change the special treatment rules in Part 50 to modify their scopes to be risk informed; and (3) make changes to specific requirements in the body of regulations, including general design criteria (GDC).

Under Option 2 of SECY-98-300, it was recommended that risk-informed approaches to the application of special treatment requirements be developed. This option of SECY-98-300 only addressed implementing changes to the regulatory scope for SSCs needing special treatment in terms of providing assurance that the SSCs will perform their functions. It did not address changing the design of the plant or the design basis accidents, which establish the physical complement of plant systems included in the design. SECY-98-300 indicated that safety related SSCs that are of low safety significance would move from special treatment to normal industrial (sometimes called commercial grade) treatment. They would, however, remain in the plant and

---

<sup>2</sup>STP has requested an exemption to a subset of the special treatment requirements included in the rulemaking plan to allow use of a risk-informed approach similar to that proposed in this rulemaking plan. This exemption request was submitted to the NRC on July 13, 1999.

be expected to perform their design function, although without the additional margin, assurance, or documentation required for current safety-related SSCs. Conversely, SSCs that are currently not safety-related but that are determined to be safety significant would move from normal industrial to regulatory treatment. The staff recommended proceeding with Option 2.

The staff also addressed three policy issues related to Option 2 in SECY-98-300: (1) voluntary versus mandatory conformance with the modified Part 50, (2) use of industry pilot studies with selected exemptions to facilitate implementation of Options 2 and 3, and (3) modification of the scope of the maintenance rule.

With respect to Option 2, in the staff requirements memorandum (SRM) for SECY-98-300 dated June 8, 1999, the Commission approved (1) implementing Option 2, including incorporation of the maintenance rule into Option 2; (2) voluntary implementation of the risk-informed alternative requirements, but deferred judgment on the issue of selective implementation; and (3) use of industry pilot studies.

The staff's rulemaking plan for implementing Option 2 is summarized below. The staff's effort regarding Option 3 of SECY-98-300 will be provided in another Commission paper. The two regulatory efforts are being coordinated and it is expected that the Option 3 effort will be able to build upon the framework discussed below.

#### DISCUSSION:

In response to the June 8, 1999 SRM, this paper provides a rulemaking plan as one of the following three attachments:

Attachment 1 is the rulemaking plan.

Attachment 2 is the ANPR.

Attachment 3 is the methodology and criteria for selecting candidate rules.

In the course of preparing the rulemaking plan, the staff (1) developed guiding principles in the form of a mission statement; (2) developed a general scheme to categorize SSCs and vary their treatment by overlaying a risk-informed approach onto the current deterministic framework; (3) identified the preferred rulemaking approach; (4) identified the rules to be considered for inclusion in the rulemaking; (5) developed an ANPR; (6) established the framework for an acceptable categorization pilot program; and (7) identified policy and implementation issues that present significant challenges to completing the rulemaking. The results of these efforts are summarized below and discussed in more detail in the attachments.

#### Mission Statement

The mission statement is described in Section 1.2 of the rulemaking plan (Attachment 1). The mission statement provides the strategies and objectives for the effort. Its purpose is to provide overall guidance in determining what issues and approaches are appropriate and it contains measures for determining whether the rulemaking effort is successful.

### General Scheme for Categorization and Treatment

The purpose of this rulemaking is to develop an alternative regulatory framework that enables licensees, using a risk-informed process for categorizing SSCs according to their safety significance (i.e., a decision that considers both traditional deterministic insights and risk insights), to reduce unnecessary regulatory burden for SSCs of low safety significance by removing these SSCs from the scope of special treatment requirements. In the process, both the NRC staff and industry should be able to better focus their resources on regulatory issues of greater safety significance. This framework should improve regulatory effectiveness and efficiency, and contribute to enhanced plant safety. To accomplish this goal, it is necessary to amend the governing regulations. The current regulations use terms such as "safety-related," "important to safety," and "basic component" to identify the groups of SSCs and associated activities that require "special treatment." This rulemaking will build into the regulations an alternative that offers licensees the flexibility of utilizing a risk-informed process to evaluate the need for special treatment. This risk-informed process will ensure that risk insights will be used in a manner that complements the NRC's traditional deterministic approach. The risk-informed approach will be consistent with the defense-in-depth philosophy, will maintain sufficient safety margins, will ensure that any increase in core damage frequency or risk is small and consistent with the safety goal policy statement, and will include a performance measurement strategy. The risk-informed framework will also be aligned to the NRC Reactor Inspection Oversight process by incorporating the cornerstones from the reactor safety and radiation protection safety areas into the SSC categorization process.

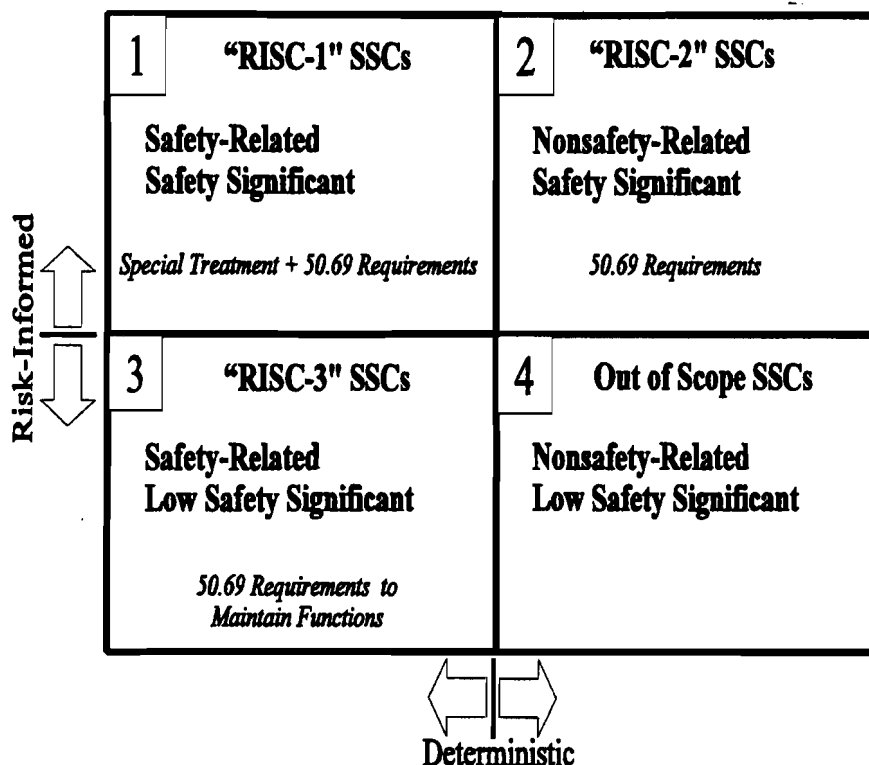
A graphical depiction of the changes that are expected to result from a risk-informed re-categorization of SSCs is illustrated in Figure 1. The figure is only intended to provide a conceptual understanding of the new SSC categorization process. The staff's thinking is continuing to evolve on this matter and as suggested in the Advisory Committee on Reactor Safeguards (ACRS) letter of October 12, 1999, the staff will explore whether more than two levels of safety significance is a better approach. The staff is requesting stakeholder feedback regarding safety significance categories in question C.3 of the ANPR. The figure depicts the current safety-related versus nonsafety-related SSC categorization scheme with an overlay of the new risk-informed categorization. The risk-informed categorization would group SSCs into one of the four boxes in Figure 1.

Box 1 of Figure 1 contains safety-related SSCs that a risk-informed categorization process concludes are significant contributors to plant safety. These SSCs are termed risk-informed safety class 1 (RISC-1) SSCs. SSCs in this box would continue to be subject to the current special treatment requirements. In addition, it is possible that some of these SSCs may have additional requirements concerning reliability and availability, if attributes which cause an SSC to be safety significant are not sufficiently controlled by current special treatment requirements. However, the staff is not currently aware of any examples of this situation.

Box 2 depicts the SSCs that are nonsafety-related, and that the risk-informed categorization concludes make a significant contribution to plant safety. These SSCs are termed RISC-2 SSCs. Examples of RISC-2 SSCs could include the station blackout emergency diesel, startup feedwater pumps, or SSCs that function for pressurized water reactor (PWR) "feed and bleed" capability. For RISC-2 SSCs, there will probably need to be requirements to maintain the reliability and availability of the SSCs consistent with the probabilistic risk assessment (PRA). As discussed below, it is currently envisioned that 10 CFR 50.69 (i.e., the new rule) would



**Figure 1: Diagram of Categorization and Treatment**



contain the regulatory treatment requirement for RISC-1 and RISC-2 SSCs regarding the reliability and availability of these SSCs.

Box 3 depicts the currently safety-related SSCs that a risk-informed categorization process determines are not significant contributors to plant safety. These SSCs are termed RISC-3 SSCs. The rulemaking would revise Part 50 to contain alternative requirements (per §50.69) such that RISC-3 SSCs would no longer be subject to the current special treatment requirements. For RISC-3 SSCs, it is not the intent of this rulemaking to allow such SSCs to be removed from the facility, or to have their functional capability lost. Instead, the RISC-3 SSCs will need to receive sufficient regulatory treatment such that these SSCs are still expected to meet functional requirements, albeit at a reduced level of assurance. The staff may determine that this level of assurance can be provided by licensee's commercial grade programs. As discussed below, it is currently envisioned that §50.69 would contain the regulatory treatment requirements for RISC-3 SSCs.

Box 4 depicts SSCs that are nonsafety-related and continue to be categorized as not being significant contributors to plant safety. These SSCs are out of scope of both current special treatment and any future regulatory controls of §50.69. The functional performance of these SSCs is controlled under the licensee's commercial grade program (no change from the current requirements).

### Rulemaking Approach

As described in Section 4.1 “Selection of the Rulemaking Approach” of the rulemaking plan, the staff is recommending a rulemaking approach that would include development of a new Part 50 rule. This rule would be supported with an appendix that utilizes new terminology as presented in Figure 1. The staff is recommending this approach in lieu of modifying the definition of “safety-related” and defining “important to safety” as was suggested in SECY-98-300 because if the current terminology is redefined to include a risk-informed part and voluntary and selective implementation is allowed, the meaning of “safety-related” and “important to safety” would be licensee and rule-specific. The staff believes that this outcome would result in confusion among both the staff and industry. With the use of new terminology, it would be immediately apparent whether a licensee was using the risk-informed alternative or the current requirement. The staff’s proposed terminology, as previously described, is risk-informed safety class (RISC)1, 2, and 3.

The rulemaking approach includes two parts. The first part is a new rule, 10 CFR 50.69, that will allow the use of the new risk-informed categorization for the regulations identified within that rule.<sup>3</sup> Section 50.69 will require that licensees use a method that complies with criteria in a new Appendix T “Categorization of SSCs Into Risk-Informed Safety Classes,” or is otherwise found acceptable by the staff, to identify the appropriate SSCs for each risk-informed safety class. Section 50.69 will also provide requirements for regulatory treatment depending on the risk-informed safety class. Licensees would be allowed to use the risk-informed approach for any of the rules, or sets of rules as appropriate, that are identified in §50.69. The second part is a new 10 CFR Part 50 Appendix T that provides the criteria and categorization processes to properly identify safety significant SSCs that require special treatment. An objective of this rulemaking is to attempt to establish criteria in Appendix T such that licensee’s who satisfy those requirements will be able to implement the risk-informed alternative with little or no prior staff review of the categorization process. The staff will not be able to determine the feasibility of this approach until after both the South Texas Project (STP) exemption effort and the categorization pilot program are complete.

### Candidate Rules

The staff’s methodology for determining the set of rules that should be considered for modification includes (1) a review of the regulations to identify those that use a scope based on terminology such as “safety-related,” “important to safety,” or a similar construct; (2) development of criteria for establishing which rules belong in this effort; and (3) evaluation of the rules identified in the first step against the criteria. A fourth step, which would be accomplished as part of the proposed rulemaking, would be to review other regulations that do not have a safety-related or important-to-safety type scope to identify any requirement that may be affected by the modifications to the special treatment requirements. This method is described in detail in Attachment 3.

---

<sup>3</sup>This approach assumes that identifying in §50.69 the set of regulations to which the risk-informed categorization can be applied will be a sufficient regulatory modification. It is possible that some rule-specific issues may also need to be addressed in this new rule. If these rule-specific issues become excessive, the staff may alternatively modify some individual rules.

The staff's preliminary assessment using this method identified the following rules for consideration in this rulemaking (**bold** means the rule was discussed as an example of a special treatment rule in SECY-98-300):

- 50.34, Contents of applications; technical information (FSAR)
- 50.36, Technical specifications**
- 50.44, Combustible gas control
- 50.48, Fire protection
- 50.49, Environmental qualification**
- 50.54(a)(3), Conditions of licenses (in reference to Quality Assurance Programs only)
- 50.55, Conditions of construction permits
- 50.55a, Codes and standards**
- 50.59, Changes, tests and experiments<sup>4</sup>**
- 50.65, Monitoring effectiveness of maintenance**
- 50.71(e), Maintenance of records, making of reports
- 50.72/50.73, Reporting**
- Appendix A, General Design Criteria
  - GDC 1, Quality standards and records
  - GDC 2, Design bases for protection against natural phenomena
  - GDC 3, Fire protection
  - GDC 4, Environmental and dynamic effects design bases
  - GDC 37, Testing of emergency core cooling system
  - GDC 40, Testing of containment heat removal system
  - GDC 42, Inspection of containment atmosphere cleanup systems
  - GDC 43, Testing of containment atmosphere cleanup systems
  - GDC 45, Inspection of cooling water system
  - GDC 46, Testing of cooling water system
- Appendix B, Quality Assurance**
- Appendix J, Containment leakage
- Appendix R, Fire Protection
- Appendix S, Seismic
- Part 21, Reporting of defects and noncompliance
- Part 52, Advanced Reactors
- Part 54, License Renewal
- Part 100, Appendix A, Seismic

#### Advanced Notice of Proposed Rulemaking

The ANPR (Attachment 2) provides a description of, and requests that the public comment on: (1) the alternative new terminology and proposed criteria (the proposed Appendix T); (2) the staff's proposed approach for modifying the special treatment requirements; (3) the staff's expectations with respect to conduct of the pilot program; (4) the staff's proposed activities and

---

<sup>4</sup>Although §50.59 is considered a special treatment requirement, the change to §50.59 is proposed to be limited to obviating the need for an evaluation of the change in special treatment for a safety-related SSC that is of low safety significance (see rulemaking plan Section 4.3).

schedules for completion; and (5) certain policy and implementation issues. The staff believes that the ANPR provides the following benefits:

1. It is consistent with the strategy in the mission statement to use processes that maximize the opportunity for public participation. The ANPR does not preclude the use of meetings and workshops, both of which are planned. The effectiveness of the meetings and workshops may be improved by providing preliminary staff positions in the ANPR.
2. As a formal request for comments, the ANPR will receive high visibility within the industry and from other external stakeholders and establishes a timetable by which comments must be received. The schedule assumes that this exchange of information will reduce the time required to address comments on the proposed rulemaking because many issues may be resolved on the basis of public comments received on the ANPR.
3. By describing the contemplated new terminology and acceptance criteria for the proposed Appendix T, the ANPR would facilitate early implementation of the categorization pilot program and may encourage additional licensees to participate in this program.
4. It provides an early basis for evaluating the draft NEI categorization guideline, which is expected to be submitted for staff review in December 1999.
5. The ANPR does not commit the NRC to implement the contemplated rulemaking; it is only a mechanism for receiving stakeholder input. In the event the staff determined that this rulemaking was not feasible, the staff could discontinue its efforts.

#### Pilot Program

The proposed approach includes two distinct pilot activities as part of the pilot program. They are (1) review of the STP exemptions as a proof-of-concept prototype pilot and (2) a categorization pilot program to demonstrate the acceptability of the contemplated new Appendix T and the NEI guideline.

The staff's review of the STP exemption request will address many of the same issues as this rulemaking. It may establish the type of staff review necessary to allow implementation of risk-informed alternatives and will address the regulatory treatment associated with maintaining the functionality of RISC-3 SSCs. It is not expected, however, that the STP exemption will demonstrate whether the contemplated Appendix T or the NEI guideline is adequate.

The categorization pilot program will be conducted to demonstrate the adequacy of the contemplated new terminology and categorization acceptance criteria in the proposed Appendix T. The staff further recommends that final rulemaking be deferred until the staff has confirmed the acceptability of the proposed rule language and the NEI guideline. Under the proposed schedule, the staff would complete this evaluation in July 2001. The staff could then issue exemptions to the pilot program participants at that time.

---

## Policy and Implementation Issues

The staff is evaluating a number of issues to determine their effect on the scope and character of this rulemaking. These issues are summarized below, and additional details are provided in the ANPR.

### 1. Selective Implementation

Selective implementation is defined as either implementing a subset of alternative regulatory treatment requirements or implementing those requirements for a subset of SSCs at a facility, or both. In SECY-98-300, the staff stated that if selective implementation is allowed, some licensees could focus their efforts in areas where unnecessary regulatory burden could be reduced, and may not focus in areas where it would be appropriate to place additional regulatory controls on SSCs given their safety significance. Therefore, selective implementation was judged incompatible with the intent of risk-informed regulation. However, the Commission determined that a decision on this topic was premature. The staff now believes that selective implementation for a subset of alternative special treatment requirements should be accommodated. The staff has not reached a conclusion regarding selective implementation for a subset of SSCs, but acknowledges that implementation of this framework would likely be through a phased approach by licensees. Selective implementation of alternative regulatory treatment requirements would introduce additional complexity into the regulatory process and the staff will need to assess the practicality of the approach. In addressing this issue, the staff will need to establish an implementation approach which recognizes all of the NRC's outcome oriented goals, not just reducing unnecessary regulatory burden. The staff is continuing to evaluate this issue and thus is seeking stakeholder feedback through the ANPR.

### 2. Effect on Other Regulations

The staff has determined that implementation of risk-informed alternatives in Part 50 may affect implementation of other regulations (e.g., Part 21, Part 55, and Part 54). In some cases, such as operator licensing (Part 55), rule changes may not be necessary; however, licensees may need to make changes to programs implementing these regulations in order to ensure compliance. In other cases such as Part 21 and Part 54, it appears that changes may be needed (Refer to Section 4.3 of the rulemaking plan).

### 3. Staff Review Requirement

As described in SECY-98-300 and in the mission statement objectives, the preferred approach is to avoid the need for prior staff review and approval of either the licensee's PRA and SSC categorization process (other than confirmation that it meets the criteria in the proposed Appendix T) or the results of that process (i.e., the list of SSCs of safety significance). This approach may not be feasible. In that event, the staff will need to determine what level of review would be necessary.

By providing detailed categorization requirements in the proposed Appendix T, it is the staff's intent to provide a regulatory framework supporting implementation of risk-informed alternative requirements without prior NRC review and approval. Appendix T

will be developed, in part, from existing guidance such as RG 1.174, and from experience gained by review of the South Texas Project (STP) Graded Quality Assurance methodology. Several significant aspects of the proposed categorization technique rely upon subjective and qualitative judgement. For example, it is expected that an expert panel will consider defense-in-depth as part of the assessment of SSC risk significance. Terms such as defense-in-depth and margin of safety are often defined only in qualitative, not quantitative, terms. Such terms are difficult to translate into inspectable and enforceable regulations yielding consistent, objective results. Therefore, application of these concepts within Appendix T creates a significant challenge for the staff. It should be noted that work to risk-inform the technical requirements of 10 CFR 50 (Option 3) must also address the defense-in-depth and safety margin issue and the work in this area will be closely coordinated between Options 2 and 3. To support a "no prior approval" approach, Appendix T will need to be constructed such that expert panels will reach sound and consistent judgements. It is important to note that SSCs categorized as RISC-3 are not being removed from regulatory treatment (i.e., there will be some requirements in 50.69 to address functionality). If the staff cannot develop criteria that result in consistent, objective results, then some level of prior NRC review and approval will be necessary.

The "no prior staff approval" approach puts increased emphasis on the quality of the underlying PRA. It is currently the staff's intention that the issue of PRA quality will be addressed through the staff's endorsement of national consensus standards on PRA quality.

#### 4. Identification and Control of Attributes Requiring Special Treatment

The staff anticipates development of regulatory controls for RISC-1 and RISC-2 SSCs to ensure the attributes of these SSCs that make them safety significant are adequately preserved. For RISC-1 SSCs, it is possible that existing special treatment requirements do not adequately address these attributes. For RISC-2 SSCs, the safety significant attributes are probably not subject to regulatory control in the existing deterministic framework. Therefore, for these components, the staff is considering what are the appropriate regulatory controls that should be applied.

For RISC-3 SSCs, appropriate controls must be established to preserve functional performance. For example, safety-related hydrogen recombiners installed in large dry containments may be determined to be of low safety significance. Nonetheless, the hydrogen recombiner's function must be preserved until such time that 10 CFR 50.44 criteria are revised under Option 3. It is expected that criteria for preservation of functional capability (at a reduced level of assurance) will be developed and incorporated into 10 CFR 50.69. Defining the controls that are appropriate for maintaining functionality of RISC-3 SSCs will be a significant challenge.

Regarding the appropriate level of regulatory controls to be placed on RISC-1, RISC-2, and RISC-3 SSCs, the staff expects that it will receive significant stakeholder feedback through the ANPR. Refer to questions E.1 through E.4 of the ANPR.

**LEGAL ANALYSIS AND BACKFIT ANALYSIS:**

The Office of the General Counsel (OGC) has not identified any bases for legal objection to the contemplated rulemaking approach. The rulemaking provides an alternative method for ensuring that the requirements of the Atomic Energy Act (AEA) of 1954 as amended are complied with, that there can be reasonable assurance of adequate protection to public health and safety, that the operation of a nuclear power plant will not impose an undue risk to public health and safety, and that appropriate levels of protection are provided to minimize danger to life and property. Accordingly, OGC believes that the AEA provides the Commission with sufficient authority to promulgate the contemplated rule. OGC has concluded that the contemplated rulemaking appears to comply with rulemaking requirements.

OGC has also determined that the contemplated rulemaking would not constitute a backfit as defined in Section 50.109(a)(1). This determination is made on the basis that each of the rules being modified in this rulemaking would provide a voluntary alternative to licensees that wish to utilize risk-informed methods for selecting the SSCs that are subject to special treatment requirements. Licensees that choose not to use such an approach can continue to rely upon their existing designations of safety-related and important to safety.

**SCHEDULE:**

The proposed schedule, described in Section 17 of the rulemaking plan, includes six major efforts: (1) the STP exemption; (2) the ANPR; (3) the categorization pilot program; (4) the NEI guideline review; (5) the proposed rulemaking; and (6) the final rulemaking. Assuming that the staff requirements memorandum (SRM) for this rulemaking plan paper is issued within 6 weeks of the date of this Commission paper, the staff's proposed schedule would result in the following projected milestone dates:

1. A proposed rulemaking package submitted to the Commission for approval in September 2000.
2. A final rulemaking package submitted to the Commission for approval in October 2001.
3. Licensee implementation could begin in March 2002.

The proposed schedule, while achievable, does assume that all issues can be resolved promptly. As described in the rulemaking plan, even short delays in many of the tasks could delay the project as a whole. In addition, since this rulemaking represents a developmental activity, it is possible that extensive public comments or unforeseen issues could arise that may be difficult to resolve and thus delay the schedule.

**RESOURCES:**

As described in Section 17 of the rulemaking plan, the total resources estimated for this effort are 47 FTE and \$3.0 million in technical assistance, as illustrated in the following table. The resource estimates are consistent with each office's budget, except for the FY 2000 technical assistance estimate for NRR.

	FY 2000		FY 2001		FY 2002	
	FTE	\$ (000s)	FTE	\$ (000s)	FTE	\$ (000s)
<b>NRR</b>	22*	1,350	12	150	3	0
<b>RES</b>	2	500	3	500	3	500

\*This includes 3 FTE to review the STP exemption.

In addition to the program office resources, OGC will require approximately 1 FTE total over the three fiscal years, and other offices (Administration, OCIO, OCFO) should require less than 1 FTE combined in support of this effort. None of these offices will require technical assistance funds.

During the staff's interactions with industry, the public, ACRS and other stakeholders in September and October 1999, the difficulty of the task of identifying the appropriate level of assurance for each safety class became apparent. Thus, additional effort may be necessary to establish the impact of removing equipment from the scope of the current special treatment requirements, and to assess the appropriate level of assurance in the proposed §50.69. For NRR, the preliminary technical assistance estimate for this effort is that it could be as much as \$1.1 million more than budgeted for FY 2000. At this time the staff plans to move ahead using internal resources. At mid-year the staff will reassess using the PBPM process to identify whether additional resources are needed. The staff will then provide the results of the PBPM assessment for the agency mid-year review to identify whether resources should be reallocated.

These estimates are tentative and may change as better information is developed as a result of public comments on the ANPR, and as the staff addresses the technical and policy issues associated with the rulemaking. In the event schedule delays occur, substantial revisions to the estimated resources would be necessary, in particular for FY 2002. In the event reprogramming is necessary as a result of issues that are raised or schedule delays, the staff will use the PBPM process to reallocate resources as necessary at that time.

These estimates only encompass the effort associated with the rulemaking, including development of appropriate regulatory and inspection guidance. It does not include resources necessary to implement the final rules, such as staff training or review and inspection of licensee programs (except for the effort to review the STP exemption and pilot plant program and exemptions). The implementation resources can be better estimated once a final decision on the regulatory approach has been made (e.g., whether prior staff review and approval is required).

**COORDINATION:**

The staff conducted three information briefings with the ACRS, and provided an information briefing for the Committee to Review Generic Requirements (CRGR). By letter dated October 12, 1999, the ACRS indicated its general agreement with staff's proposal to develop a new rule and supporting appendix to risk-inform special treatment requirements. OGC has reviewed this paper and has no legal objection. The Office of the Chief Financial Officer has reviewed this paper for resource implications and has no objections. The Office of the Chief



Information Officer has reviewed the rulemaking plan for information technology and information management-implications and concurs in it. However, the plan suggests changes in information collection requirements that must be submitted to the Office of Management and Budget at the same time the rule is forwarded to the Federal Register for publication.

The staff is also developing an internal and external communications plan regarding the rulemaking. The objective will be to engage internal (e.g., NRC staff, ACRS, CRGR) and external (e.g., NEI, licensees, members of the public) during the rulemaking process.

RECOMMENDATIONS:

The staff recommends that:

1. The staff issue the ANPR in Attachment 2. The staff requests action within 10 days. Action will not be taken until the SRM is received. We consider this action to be within the delegated authority of the EDO.
2. The Commission approve the rulemaking plan as described in Attachment 1.



William D. Travers  
Executive Director  
for Operations

- Attachments: 1. Rulemaking plan for Risk-Informing Special Treatment Requirements  
2. Proposed ANPR  
3. Rule selection methodology

Commissioners' completed vote sheets/comments should be provided directly to the Office of the Secretary by COB Monday, November 15, 1999.

Commission Staff Office comments, if any, should be submitted to the Commissioners NLT November 5, 1999, with an information copy to the Office of the Secretary. If the paper is of such a nature that it requires additional review and comment, the Commissioners and the Secretariat should be apprised of when comments may be expected.

DISTRIBUTION:

Commissioners  
OGC  
OCAA  
OIG  
OPA  
OCA  
ACRS  
CIO  
CFO  
EDO  
REGIONS  
SECY



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS  
WASHINGTON, D.C. 20555-0001

October 12, 1999

The Honorable Greta Joy Dicus  
Chairman  
U.S. Nuclear Regulatory Commission  
Washington, D.C. 20555-0001

Dear Chairman Dicus:

**SUBJECT: PROPOSED PLANS FOR DEVELOPING RISK-INFORMED REVISIONS TO 10 CFR PART 50, "DOMESTIC LICENSING OF PRODUCTION AND UTILIZATION FACILITIES"**

During the 466<sup>th</sup> meeting of the Advisory Committee on Reactor Safeguards, September 30-October 2, 1999, we met with representatives of the NRC staff and Nuclear Energy Institute to discuss proposed plans for developing risk-informed revisions to 10 CFR Part 50. We also met with a representative of Public Citizen, Critical Mass Energy Project, to discuss these matters and a recent report issued by Public Citizen. Our Subcommittees on Reliability and Probabilistic Risk Assessment and on Regulatory Policies and Practices met on July 13 and September 24, 1999, to discuss these matters. We had the benefit of the documents referenced.

Conclusions and Recommendations

1. We agree with the staff's proposal to develop a new regulatory section 10 CFR 50.69 and associated Appendix T to implement Option 2 (changing the special treatment rules in 10 CFR Part 50) of SECY-98-300.
2. We agree that the current terminology of safety-related structures, systems, and components (SSCs) should be preserved and that additional terminology referring to the safety significance of SSCs should be considered. We recommend that the staff explore the potential benefits of defining more than two categories of safety significance.
3. The determination of the safety significance of SSCs relies heavily on the use of importance measures. These measures are strongly affected by the scope and quality of the probabilistic risk assessment (PRA). For example, incomplete assessments of risk contributions from low-power and shutdown operations, fires, and human performance will distort the importance measures.

4. Even with a full-scope, high-quality PRA, the importance measures have limitations. The guidance to be provided in the proposed Appendix T for the categorization of SSCs should clarify the proper roles of (a) importance measures, (b) sensitivity and uncertainty analysis, (c) baseline core damage frequency (CDF) and large, early release frequency (LERF), and (d) the changes in CDF and LERF (i.e.,  $\Delta$ CDF and  $\Delta$ LERF).
5. It is essential that the implementation of Option 2 be scrutable and auditable. The staff should have access to the risk assessments and technical bases documents (e.g., inputs to and deliberations of the expert panel) that licensees use to justify requests.
6. The guidance to be provided in the proposed Appendix T for the expert panel should include insights gained from the implementation of recommendation 4 above. The staff should include guidance for conducting expert panel sessions and training of the panel members on the use of importance measures.
7. We agree with the staff's plan for implementing Option 3 (changing specific requirements in the body of 10 CFR Part 50 and associated regulations) of SECY-98-300. Policy issues regarding the role of defense in depth in a risk-informed regulatory system should be resolved before the plan is fully implemented.

### Discussion

In a Staff Requirements Memorandum dated June 8, 1999, the Commission directed the staff to make risk-informed changes to the scope of SSCs covered by regulations that provide special treatment requirements (e.g., quality assurance, environmental qualification, technical specifications, 10 CFR 50.59, ASME Code, 10 CFR 50.72, and 10 CFR 50.73). 10 CFR 50.2 defines safety-related SSCs as those SSCs that "are relied upon to remain functional during and following design basis events to assure: (1) The integrity of the reactor coolant 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...."

To date, the determination of whether an SSC is safety related has been based largely on deterministic analyses that include engineering judgment. Advances in PRAs have made it possible to quantify the degree to which SSCs are relied upon to ensure that the requirements in 10 CFR 50.2 are met. For example, using a combination of deterministic and PRA insights, the South Texas Project Nuclear Operating Company has concluded that many SSCs currently categorized as safety-related contribute very little to CDF and LERF, while a few SSCs currently categorized as nonsafety-related are significant from a risk perspective.

The staff proposes to develop a new rule, 10 CFR 50.69, and an associated Appendix T. The new rule will explicitly allow the use of a new risk-informed scope. Appendix T will provide the criteria for the new categorization process. We agree with this approach.

The current "safety-related" and "nonsafety-related" categories will be retained. Two new categories that consider risk information, i.e., high safety significance and low safety significance, will be developed. Appendix T will provide criteria for the new categorization process. The staff proposes to use a 2x2 matrix where SSCs are to be placed in one of the four categories according to safety significance and safety-related status. Introducing these new categories while preserving the safety-related and nonsafety-related terminology should help to avoid the confusion that could result from a redefinition of the safety-related concept. We agree that such an approach is preferable to redefining "safety-related" and "important to safety."

At this early stage, the staff has not decided what special treatment the SSCs in each of the four categories of the 2x2 matrix will receive. The staff has indicated that this decision may require a finer treatment of safety significance than the two groups to be proposed in Appendix T. The South Texas Project Nuclear Operating Company has chosen to consider four groups for safety significance instead of the two that will be proposed for Appendix T. They are: 1) high safety/risk significant (HSS), 2) medium safety/risk significant (MSS), 3) low safety/risk significant (LSS), and 4) non-risk significant (NRS). LSS and NRS SSCs support ancillary functions (e.g., vents and drains) for safety-related systems, but do not affect the primary functions of these systems. LSS SSCs may be included in the PRA while NRS SSCs are not.

We believe that the staff should further evaluate the various options for partitioning the range of safety significance before it settles on a grouping that it considers optimum.

Appendix T will include requirements for categorizing SSCs using PRA. We offer the following comments and suggestions for inclusion in the development of Appendix T:

1. The screening criteria are based primarily on two importance measures: Fussell-Vesely (FV) and Risk Achievement Worth (RAW). The criteria are:  $FV > 0.005$  and  $RAW > 2$  based on either CDF or LERF. It is important to fully understand what information these measures convey as well as their limitations. Detailed discussions on these matters are available in References 9, 12, and 13.

As an example, consider a very simple case in which the risk metric, e.g., the CDF due to internal events, is a function of a single accident sequence. We have

$$CDF^E = fq = 10^{-4} \text{ per reactor-year} \quad (1)$$

where

- f: frequency of the initiating event (say,  $10^{-2}$  per reactor-year)  
 q: unavailability of the protection system (say,  $10^{-2}$  per demand)

The importance measures for the system are

$$FV = \frac{fq}{fq} = 1 \quad (2)$$

$$RAW = \frac{CDF^{E,+}}{CDF^E} = \frac{f}{fq} = \frac{1}{q} = 100 \quad (3)$$

where  $CDF^{E,+}$  is the new value of CDF with the protection system assumed unavailable.

Suppose that several protection systems are added, each of unavailability  $q_j$ . The new importance measures for the system are

$$FV' = \frac{fq \prod q_j}{fq \prod q_j} = 1 \quad (4)$$

$$RAW' = \frac{f \prod q_j}{fq \prod q_j} = \frac{1}{q} = 100 \quad (5)$$

Even though several protection systems have been added thereby reducing reliance on the original system and reducing the overall risk, the importance measures have not changed. We believe that this insensitivity should be better understood and communicated to the expert panel and that insights from this discussion need to be incorporated into the rule or the associated guidance documents.

2. Suppose that the CDF estimate of Equation (1) is expanded to include the contribution from external events. We assume that this contribution is  $10^{-3}$  per reactor-year, i.e., it dominates the risk due to internal events, as is often the case with the seismic contribution. The new CDF is

$$CDF = CDF^E + CDF^{EE} = 10^{-4} + 10^{-3} = 1.1 \times 10^{-3} \text{ per reactor-year} \quad (6)$$

A calculation of the new importance measures provides:

$$FV'' = \frac{10^{-4}}{1.1 \times 10^{-3}} = 0.09 \quad (7)$$

$$RAW'' = \frac{10^{-2} + 10^{-3}}{1.1 \times 10^{-3}} = 10 \quad (8)$$

As expected, the importance measures of the protection system have been reduced drastically. The question is whether including the dominant seismic contribution results in meaningful importance measures, especially within the context of the proposed new

reactor oversight process where the frequency of initiating events and the unavailability of the protection systems are cornerstones of the assessment process.

In a PRA, the additional terms in the equation may be the products of analyses that are not as rigorous as those for the terms in which a particular system appears. For example, some terms may contain probabilities of recovery actions or damage caused by "external" events, such as fires and tornadoes. The current assessment of risk contributions from low-power and shutdown operations, fires, and human performance is incomplete. Because the PRA technology for such assessments is not as well developed as that for "internal" events, the analyses may contain many overly conservative assumptions, thus artificially increasing these contributions. Inconsistencies in the analysis of the various contributions to risk distort the importance measures.

It is evident that the absolute value of the baseline risk metric is a critical element in these evaluations and that the importance measures contain only relative information with respect to a given risk metric.

The change in risk depends on this absolute value also, i.e.,  $\Delta CDF$  at two plants with different baseline CDFs, will be different for the same change in the unavailability of a component whose importance measures have the same value at these plants. Reference 9 states that "if we are interested in controlling the change in risk in an absolute sense, it does not make sense to have a universally fixed value of FV as a criterion for risk significance," and "it is clear that it does not make much sense to define a universal criterion based on RAW."

3. The calculation of RAW in Equation (3) requires the estimation of  $CDF^{E+}$ , i.e., the CDF assuming that the protection system is unavailable. This assessment may be much more involved than simply setting the unavailability of the system equal to unity. The assumption of a system being unavailable may affect several terms in the PRA. For example, in a two-train redundant system, the PRA contains terms representing the "random" independent failure of the two trains, the probability of a common-cause failure, and the probability that coupled human errors after test and maintenance may disable both trains. All of these terms are affected by the assumption of one train being unavailable. Recovery actions may also be affected (see Reference 11).

We question whether these considerations are adequately taken into account when RAW is calculated for hundreds of components.

4. The current practice of calculating FV and RAW is to use the mean epistemic values of the parameters in the ratios appearing in Equations (2) and (3). The more rigorous way is to first find the ratios and then to average them over the epistemic distributions of the parameters (Reference 10). The current practice is an approximation that is usually reasonable, unless the epistemic uncertainties of the parameters are very large (Reference 9). The section on sensitivity analysis in the proposed Appendix T should reflect this observation.

The preceding paragraphs are not intended to discourage the use of importance measures. Although our example is a simple one, it does illustrate that FV and RAW values must be carefully calculated and interpreted. We do believe that a good understanding of the limitations of importance measures is essential to their proper use.

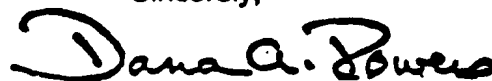
The issues discussed above, as well as the detailed investigations in the cited references, suggest that the members of the expert panel that determines the categorization of SSCs need to be aware of these limitations and constraints. We believe that there is a need to ensure that members of expert panels have formal training in the properties of importance measures. Similar training sessions are provided in other contexts, e.g., before quantitative judgments are elicited from engineers and scientists who are not familiar with the cognitive issues associated with the elicitation of expert opinion.

Option 3 of SECY-98-300 deals with changes in specific requirements in 10 CFR Part 50, including general design criteria. The staff's high-level plan for implementing this option and associated study is acceptable. We note, however, that defense in depth plays a critical role in this plan.

The PRA Policy Statement of 1995 and subsequent agency documents such as Regulatory Guide 1.174 for risk-informed changes to the licensing basis place defense in depth at the level of a principle whereby PRA should be used in "a manner that supports the NRC's traditional defense-in-depth philosophy." As noted in our May 19, 1999 report, this may create conflicts between risk-informed insights and defense in depth. Since the staff's plan includes defense-in-depth considerations in several key areas, e.g., the identification of candidate requirements to be revised and the determination of the revisions, it is very important for the Commission to clarify the proper role of defense in depth.

We look forward to working with the staff to resolve the significant technical issues associated with the implementation of Options 2 and 3 of SECY-98-300.

Sincerely,



Dana A. Powers  
Chairman

References:

1. Memorandum dated September 16, 1999, from David B. Matthews, Office of Nuclear Reactor Regulation, to John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards, Subject: ACRS Preliminary Review of the Draft SECY Paper for Risk-Informing Special Treatment Regulations.
2. Memorandum dated September 23, 1999, from Thomas L. King, Office of Nuclear Regulatory Research, to John T. Larkins, Advisory Committee on Reactor Safeguards, Subject: ACRS Review of Proposed Staff Plan for Risk-Informing Technical Requirements in 10 CFR Part 50

3. Memorandum dated June 8, 1999, from Annette Vietti-Cook, Secretary, NRC, to William D. Travers, Executive Director for Operations, Subject: Staff Requirements - SECY-98-300 - Options for Risk-Informed Revisions to 10 CFR Part 50 - "Domestic Licensing of Production and Utilization Facilities."
4. Letter dated December 14, 1998, from R. L. Seale, Chairman, ACRS, to William D. Travers, Executive Director for Operations, NRC, Subject: Proposed Commission Paper Concerning Options for Risk-Informed Revisions to 10 CFR Part 50 - "Domestic Licensing of Production and Utilization Facilities."
5. Report dated May 19, 1999, from Dana A. Powers, Chairman, Advisory Committee on Reactor Safeguards, to Shirley Ann Jackson, Chairman, U.S. Nuclear Regulatory Commission, Subject: *The Role of Defense in Depth in a Risk-Informed Regulatory System.*
6. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," July 1998.
7. Letter dated July 13, 1999, from J.J. Sheppard, South Texas Nuclear Operating Company, to U.S. Nuclear Regulatory Commission, Subject: Request for Exemption to Exclude Certain Components from the Scope of Special Treatment Requirements Required by Regulations.
8. Title 10: Code of Federal Regulations, Part 50, Domestic Licensing of Production and Utilization Facilities, Section 50.2, Definitions.
9. M.C. Cheok, G.W. Parry, and R.R. Sherry, "Use of importance measures in risk-informed regulatory applications," *Reliability Engineering and System Safety* 60, 213-226, 1998.
10. G. Apostolakis, "The distinction between aleatory and epistemic uncertainties is important: An example from the inclusion of aging effects into PSA," American Nuclear Society Conference, PSA '99, Washington, DC, August 22-25, 1999.
11. C.L. Smith, "Calculating conditional core damage probabilities for nuclear plant operations," *Reliability Engineering and System Safety* 59, 299-307, 1998.
12. W.E. Vesely, "Reservations on 'ASME Risk-Based Inservice Inspection and Testing: An Outlook to the Future,'" *Risk Analysis* 18, 423-425, 1998.
13. W.E. Vesely, "Supplemental viewpoints on the use of importance measures in risk-informed regulatory applications," *Reliability Engineering and System Safety* 60, 257-259, 1998.
14. Report entitled, "Amnesty Irrational -- How the Nuclear Regulatory Commission Fails to Hold Nuclear Reactors Accountable for Violations of Its Own Safety Regulations," by James P. Riccio, Public Citizen, August 1999.
15. U.S. Nuclear Regulatory Commission, "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," dated August 16, 1995.





UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS  
ADVISORY COMMITTEE ON NUCLEAR WASTE  
WASHINGTON, D.C. 20555

November 17, 1999

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

Dear Chairman Meserve:

**SUBJECT: IMPLEMENTING A FRAMEWORK FOR RISK-INFORMED REGULATION IN  
THE OFFICE OF NUCLEAR MATERIAL SAFETY AND SAFEGUARDS**

During the 113th meeting of the Advisory Committee on Nuclear Waste (ACNW), October 12-13, 1999, and the 467<sup>th</sup> meeting of the Advisory Committee on Reactor Safeguards (ACRS), November 4-6, 1999, the Committees considered the staff's proposed framework for risk-informed and performance-based regulation in the Office of Nuclear Material Safety and Safeguards (NMSS), as articulated in SECY-99-100 and an associated Staff Requirements Memorandum dated June 28, 1999. A meeting of the ACRS/ACNW Joint Subcommittee was held on May 11, 1999, to discuss these matters. We had the benefit of the documents referenced.

**Recommendations**

1. NMSS should develop a set of principles and a safety goal approach for each of its regulated activities to guide its implementation of risk-informed and performance-based regulation.
2. NMSS should identify the analytical methods to be applied to implement risk-informed and performance-based regulation on an application-specific basis.

**Discussion**

The NMSS staff is examining the use of risk information in four major categories of regulated activities: (1) long-term commitment of a site to the presence of nuclear material (e.g., high-level waste disposal); (2) use of engineered casks to isolate nuclear material under a variety of conditions (e.g., transportation and storage); (3) physical and chemical processing and possession of nuclear material at a large-scale facility (e.g., fuel fabrication); and (4) use of sealed or unsealed byproduct material in industrial and medical applications. The objectives of

this examination are to focus regulatory activities on matters that are important to safety and avoid unnecessary burdens on licensees and the NRC staff.

The diversity of the four categories of activities listed above indicates that the risk assessment methods for material licensees are likely to be different from those for nuclear power plants. While quantitative risk assessment is a well-developed and utilized tool for nuclear power plant licensees, it may be unnecessarily complex for the NMSS regulated activities. The performance assessments (PAs) done for waste repositories are conceptually similar to probabilistic risk assessments (PRAs) for reactors. Recently, there have been developments for simplified approaches to quantitative risk analysis, e.g., integrated safety assessments (ISAs), that are less rigorous than PRAs or PAs.

The staff must address two crucial issues as it considers risk methods in the regulation of material licensees:

1. What criteria should be used to decide whether the regulations for a specific nuclear materials activity should be changed to a risk-informed regulation? Can the current deterministic criteria, accounting methods, or proposed approaches such as ISA accomplish risk-informed objectives?
2. What risk analysis methods (and scope) and risk acceptance criteria should be applied to the operations that merit risk-informed regulation?

To address the first question, we believe that the staff will need to develop a set of principles for risk-informed regulation. Such a set of principles is important to guide the need for and change from a prescriptive form of regulation to a less prescriptive, but risk-informed, method of regulation. In developing these principles, the staff should take full advantage of the knowledge base unique to materials and waste disposal regulation, as well as the staff's experience in developing principles for other regulatory applications, such as Regulatory Guide 1.174.

Some of the characteristics of nuclear materials regulation that differ from reactor regulation include: (1) experience in regulating to radiation exposure standards, as opposed to surrogate measures such as facility damage, (2) diversity of types of licensee activities involving major differences in materials, facilities, and practices, (3) activities not dominated by a clear-cut feature such as core damage, and (4) activities where the operational risk, as opposed to the accident risk, may be the central issue of risk regulation. Although these characteristics distinguish materials regulation from reactor regulation, the Committees believe that the approach to regulatory decisionmaking for the NMSS activities should have a basis that is consistent with the approach for reactor regulation.

An important element introduced in Regulatory Guide 1.174 and that should be investigated in the present context of materials regulation is that regulatory decisionmaking should be based on an analytic and deliberative process. Analytical results from risk assessments and other engineering analyses are only part of the input to this process. Qualitative inputs, e.g., the preservation of the defense-in-depth philosophy, may be considered by an expert panel or other decisionmaking entity. In developing the new principles, the staff should consider this approach and its applicability to the various NMSS activities. If qualitative information is to be used in the

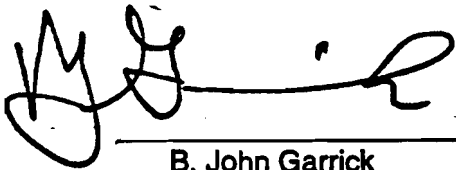
decisionmaking process, then the reason(s) should be explained. If there is a need for an expert panel for some activities, its form and composition should be discussed.<sup>1</sup>

Consideration should be given to developing variations on the safety goal approach to risk acceptance. One variation may be to include uncertainty directly in the risk acceptance criteria via required confidence levels in their determination. Another may be to define acceptance criteria that are either met or not, i.e., the range of risk is partitioned into two regions, the acceptable and unacceptable regions. Another might be to adopt a three-region approach. In this concept, there is a range of acceptability with an upper and lower bound. The lower bound constitutes the level below which no further action is required. The upper bound constitutes a level above which definitive action to control the risk is required. The middle region is the region in which cost-benefit tradeoffs can be made. These are a few concepts that should be investigated by the staff for materials regulation. There may be others.

The Committees believe that, just as "guiding principles" are important to establishing a well-founded philosophy of risk-informed regulation, so are certain risk assessment concepts. The representation of risk as a triplet set is such a guiding concept. The triplet consists of accident scenarios (what can go wrong?), probabilities of these scenarios (how likely is each scenario?), and the consequences (what are the consequences?). We view the various risk (or safety) assessment methods that exist in the literature as dealing with these three elements of the risk triplet in different ways. PRAs for reactors and PAs for HLW repositories offer the most complete treatment of the triplet, and they require the most resources. We believe that the staff should clarify how any chosen method deals with the risk triplet (either quantitatively or qualitatively) and justify the appropriateness of the selected scopes as differentiated among the four major categories of NMSS licensees. If methods that are less rigorous than PRAs or PAs are judged to be appropriate for certain applications, their treatment of the triplet should be explicitly identified. The reasons for resorting to these less rigorous methods should be carefully justified. We are especially concerned about the completeness of the scenario list and the analysis of uncertainties.

We look forward to reviewing staff activities on these matters during future meetings.

Sincerely,



B. John Garrick  
Chairman, ACNW



Dana A. Powers  
Chairman, ACRS

---

<sup>1</sup> This concept of an expert panel refers to the discussion on integrated decisionmaking in Regulatory Guide 1.174. The purpose of such an expert panel is to evaluate multiple sources of information to make decisions in an integrated manner. This is different from the guidance in the "Branch Technical Position on the Use of Expert Elicitation in the High-Level Radioactive Waste Program," NUREG-1563, that refers to a specific formalized process for developing information and "data" to be used in a performance assessment.

**References:**

1. Memorandum dated June 28, 1999, from Annette Vietti-Cook, Secretary, NRC, to William D. Travers, Executive Director for Operations, NRC, and John T. Larkins, Advisory Committee on Reactor Safeguards, Subject: Staff Requirements - SECY-99-100 - Framework for Risk-Informed Regulation in the Office of Nuclear Material Safety and Safeguards.
2. SECY-99-100, Memorandum dated March 31, 1999, from William D. Travers, Executive Director for Operations, NRC, to the Commissioners, Subject: Framework for Risk-Informed Regulation in the Office of Nuclear Material Safety and Safeguards.
3. Memorandum dated February 24, 1999, from Annette Vietti-Cook, Secretary, NRC, to William D. Travers, Executive Director for Operations, NRC, Subject: Staff Requirements - SECY-99-144 - White Paper on Risk-Informed and Performance-Based Regulation.
4. Report dated April 19, 1999, from Dana A. Powers, Chairman, Advisory Committee on Reactor Safeguards, to Shirley Ann Jackson, Chairman, NRC, Subject: Status of Efforts on Revising the Commission's Safety Goal Policy Statement.
5. U.S. Nuclear Regulatory Commission, Regulatory Guide 1:174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," July 1998.
6. U.S. Nuclear Regulatory Commission, NUREG-1563, "Branch Technical Position on the Use of Expert Elicitation in the High-Level Radioactive Waste Program," November 1996.