POLICY ISSUE
(Notation Vote)

March 28, 1994 SECY-94-084

FOR: The Commissioners

FROM: James M. Taylor
Executive Director of Operations

SUBJECT: POLICY AND TECHNICAL ISSUES ASSOCIATED WITH THE REGULATORY TREATMENT OF NON-SAFETY SYSTEMS IN PASSIVE PLANT DESIGNS

PURPOSE:

To present the Commission with recommended positions pertaining to policy and technical issues affecting passive advanced light water reactor (ALWR) designs and to request that the Commission approve the underlined staff positions presented in this paper.

SUMMARY:

In the enclosure, the U. S. Nuclear Regulatory Commission (NRC) staff discusses eight technical and policy issues pertaining to the regulatory treatment of non-safety systems (RTNSS) for passive ALWRs. The staff previously identified these issues in the draft Commission papers, "Issues Pertaining to Evolutionary and Passive Light-Water Reactors and Their Relationship to Current Regulatory Requirements," February 20, 1992, and "Design Certification Licensing Policy Issues Pertaining to Passive and Evolutionary Advanced Light-Water Reactor Designs," June 25, 1992; and in SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," April 2, 1993. After extensive dialogue with the Electric Power Research Institute (EPRI), the vendors, and the Advisory Committee on Reactor Safeguards (ACRS), the staff proposed its position on these technical and policy issues in a draft Commission paper issued September 7, 1993. Subsequently, comments were received from EPRI and from

CONTACT:
James H. Wilson, NRR
504-1108

NOTE: TO BE MADE PUBLICLY AVAILABLE IN 3 WORKING DAYS FROM THE DATE OF THIS PAPER

Westinghouse. The staff briefed the ACRS in August and November on these issues. The ACRS comments on the eight policy and technical issues associated with RTNSS were provided to the Chairman in a letter dated November 10, 1993. After considering industry, vendor, and ACRS comments, the staff has reached a final position on the RTNSS issues. The staff has underlined the positions for which it is requesting the Commission's approval.

BACKGROUND:

In the staff requirements memorandum (SRM) dated August 24, 1989, the Commission instructed the staff to provide an analysis detailing where the staff proposes departure from current regulations or where the staff is substantially supplementing or revising interpretive guidance applied to currently-licensed light water reactors (LWRs). The staff considers these to be policy issues fundamental to agency decisions on the acceptability of ALWR designs.

As described in the summary above, the eight technical and policy issues associated with RTNSS have been previously identified to the Commission.

In SECY-93-087, the staff indicated that it would be discussing control room habitability in a Commission paper on the subject of source term. Although control room habitability is linked to passive plant policy and source term issues, the staff believes that it was more appropriate to discuss control room habitability as a passive plant issue; hence, recommendations on control room habitability are presented in this paper.

In SECY-93-087, the staff also provided the Commission its interim position on the reliability assurance program (RAP) applicable to design certification. The staff stated that the final position on RAP would be included in a future Commission paper on the regulatory treatment of non-safety systems. This paper provides the staff's position on RAP for both the evolutionary and passive ALWRs.

DISCUSSION:

The regulatory treatment of non-safety-related systems in advanced reactor passive designs will have wide-ranging effects on both the design and licensing of the AP600 and the simplified boiling water reactor (SBWR). Unlike the current generation of LWRs or the evolutionary ALWRs, the passive ALWR designs make extensive use of safety systems that rely on the driving forces of buoyancy, gravity, and stored energy sources. These passive systems supply safety-injection water, perform core and containment cooling, and perform other functions. These passive safety systems contain no pumps and include valves that are operated by either air pressure or dc electric power from batteries, or use check valves actuated by the pressure differential across the valve. In addition to the active systems used during normal plant operations, the passive ALWR designs also include non-safety-grade active systems to provide defense-in-depth capabilities for reactor coolant makeup and decay heat removal. These systems are the first line of defense to reduce challenges to the passive systems in the event of transients or plant upsets.

The licensing design-basis analyses proposed by the industry for the passive designs rely solely on the passive safety systems to demonstrate compliance with the acceptance criteria of various design-basis transients and accidents. Since the passive ALWR design philosophy departs from current licensing practices, new regulatory and review guidance is necessary so that the staff can appropriately review the AP600 and SBWR submittals.

The enclosure discusses the staff's position, the current regulatory requirement or interpretations, and comments received from industry and vendors regarding eight technical and policy issues pertaining to the RTNSS for passive ALWR designs, including RAP. The RAP also applies to evolutionary ALWR designs. The staff has included a discussion of the basis for its position on each issue. The staff underscored the positions for which it is requesting the Commission's approval.

The staff development of the staff positions was based on the following:

(1) review of the available information on passive ALWR designs;

(2) consideration of insights from the available results of the probabilistic risk assessments (PRAs) of LWRs and ALWRs;

(3) completion of the safety evaluation report for the EPRI utility requirements document (URD) for passive ALWR designs;

(4) consideration of EPRI and industry comments on these issues which were raised during a meeting between NRC staff and the ALWR Steering Committee on January 22, 1993, in Palo Alto, California, and in meetings between NRC staff and EPRI representatives on April 15, and May 20, 1993, in Rockville, Maryland;

(5) review of EPRI's letters of February 23, and May 13 and 26, 1993, which detailed a proposed process for the RTNSS in passive plant designs; and

(6) consideration of EPRI, ACRS, and industry comments on a draft version of this paper which was forwarded to the Commission on September 7, 1993.

The staff concludes that the positions discussed in the enclosure are fundamental to the Agency's decisions on the acceptability of the passive LWR designs (and on the RAP for evolutionary plant designs). As discussed in SECY-91-262, "Resolution of Selected Technical and Severe Accident Issues for Evolutionary Light-Water Reactor (LWR) Designs," the staff proposes to implement final positions on these matters as approved by the Commission through individual design certifications and generic rulemaking, as appropriate.

The staff proposes to make this paper and its enclosure available to the public no sooner than 3 work days after this paper is forwarded to the Commission.

CONCLUSIONS:

The staff requests that the Commission approve the recommended positions for issues pertaining to the regulatory treatment of non-safety systems in passive advanced light water designs. This will enable the staff to proceed more effectively with its review of Westinghouse's AP600 and GE Nuclear Energy's simplified boiling water reactor ALWR designs and, in the case of RAP, resolve the evolutionary ALWR design reviews.

COORDINATION:

The Office of General Counsel (OGC) has reviewed this paper and has no legal objection. OGC notes that Commission approval would be tentative, subject to further review in design certification rulemakings, and that communications with vendors and EPRI regarding these Commission positions should state this fact.

The ACRS was briefed on August 5, and November 4, 1993. The ACRS provided its comments on the draft Commission paper issued September 7, 1993, in a letter to the Chairman dated November 10, 1993. In a letter dated February 2, 1994, the staff responded to the ACRS comments. Those responses are reflected in the positions contained in the enclosure to this paper.

Additional comments on RAP were provided by the ACRS in its letter dated February 17, 1994, and the staff will be responding separately. The staff's views on the ACRS concerns are reflected in the enclosure to this paper. We continue to believe that RAP provides a useful process to allow probabilistic and deterministic risk insights to be considered during the design and operation of ALWRs and is not inconsistent with provisions of the Maintenance Rule. The staff also agrees with the ACRS in the matter of infeasibility of demonstrating plant-specific structure, system, and component reliability.

RECOMMENDATIONS:

The staff recommends that the Commission

(1) Approve the positions underlined in the enclosure.

(2) Note that the staff will make the enclosure available to the public no sooner than 3 work days after this paper is forwarded to the Commission. The staff will indicate that the proposed resolutions are being considered by the Commission, and therefore, are not final positions.

James M. Taylor
Executive Director
for Operations

Enclosure:
Policy Issues Analysis
and Recommendations
for Passive Plants

POLICY ISSUES ANALYSIS AND RECOMMENDATIONS FOR PASSIVE PLANTS

A. Regulatory Treatment of Non-safety Systems

Unlike the current generation of light water reactors or the evolutionary advanced light water reactors (ALWRs), the passive ALWR designs use passive safety systems that rely exclusively on natural forces, such as density differences, gravity, and stored energy to supply safety injection water and provide core and containment cooling. These passive systems do not include pumps. All valves in these passive systems either require only dc electric power by means of batteries, are operated by air pressure, or are check valves operating by means of pressure differential across the valve. These passive systems do not receive safety-related ac electric power. The designers designate all the active systems as non-safety systems except for limited portions of the systems that provide safety-related isolation functions such as containment isolation.

As the passive ALWR designs rely on the passive safety systems to perform design-basis safety functions of reactor coolant makeup and decay heat removal, different portions of the passive systems also provide certain defense-in-depth backup to primary passive features. For example, while the passive decay heat removal heat exchanger is the primary safety-related heat removal feature in a transient, the automatic reactor depressurization system together with the passive safety injection features provide a safety-related defense-in-depth backup.

The passive ALWR designs also include active systems that provide defense-in-depth capabilities for reactor coolant makeup and decay heat removal. These active systems are the first line of defense to reduce challenges to the passive systems in the event of transients or plant upsets. As stated above, all active systems in passive plants are designated as non-safety systems. In addition, one of the principal design requirements of EPRI's ALWR utility requirements document (URD) is that passive systems should be able to perform their safety functions, independent of operator action or offsite support, for 72 hours after an initiating event. After 72 hours, non-safety, or active systems may be required to replenish the passive systems or perform core and containment heat removal duties directly. As specified in the URD, these active systems which may be needed to provide defense-in-depth capabilities include (1) the chemical and volume control system and control rod drive system, which provide reactor coolant makeup for the passive pressurized water reactor (PWR) and boiling water reactor (BWR), respectively; (2) the reactor shutdown cooling system and backup feedwater system for PWR decay heat removal, and the reactor water cleanup system for BWR decay heat removal; (3) the fuel pool cooling and cleanup system for spent fuel decay heat removal; and (4) the associated systems and structures to support these functions, including non-safety standby diesel generators. The ALWR URD also requires that the plant designer specifically define the active systems relied on for defense-in-depth for a standard design as necessary to meet passive ALWR plant safety and investment goals. These active systems may include additional systems beyond those discussed above. The passive ALWR designs also include other active systems, which are designated as non-safety, (such

as the heating, ventilation, and air conditioning (HVAC) system) that remove heat from the instrumentation and control (I&C) cabinet rooms and the main control room and prevent the excessive accumulation of radioactive materials in the control room to limit challenges to the passive safety capabilities for these functions.

In existing plants (and in evolutionary ALWR designs), the NRC has treated many of these active systems as safety-related systems. As stated earlier, active systems are not classified as safety-related in passive ALWR designs, and credit is not taken for these active systems in the Chapter 15 licensing design basis accident (DBA) analyses. In SECY-90-406, "Quarterly Report on Emerging Technical Concerns," December 17, 1990, the staff listed the role of these active systems in the passive design as an emerging technical issue. In SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs," April 2, 1993, the staff discussed the issue of regulatory treatment of active non-safety systems (the "RTNSS Issue") and stated that it would propose a resolution of this issue in a separate Commission paper.

Because of limited operational experience and the low-driving force of the passive safety systems, the designers have not verified all aspects of the passive features and the overall capabilities of reactor coolant makeup and core and containment heat removal. The passive systems involve inherent phenomenological uncertainties such as those associated with the performance of check valves operating under natural circulation or gravity injection with low differential pressures that may not create sufficient force to fully open a stuck check valve, unlike the emergency core cooling systems in current operating plants in which pressure developed by pumps can overcome stuck valves. The staff expects these uncertainties to be reduced through carefully planned and implemented components performance tests, and separate effects and integral system tests, and/or prototype tests over a sufficient range of transient and accident conditions per 10 CFR 52.47(b)(2)(i)(B), combined with realistic analyses of the performance of passive systems and components for these ALWRs.

The residual uncertainties associated with passive safety system performance increase the importance of active systems in providing defense-in-depth functions to the passive systems. The NRC staff and EPRI have developed a process for maintaining appropriate regulatory oversight of these active systems in the passive ALWR designs. The staff will not require that these active systems meet all the safety-related criteria, but will expect a high level of confidence that active systems which have a significant safety role are available when challenged.

The ALWR URD specifies requirements concerning design and performance of active systems and equipment that perform non-safety, defense-in-depth functions. These requirements include radiation shielding to permit access after an accident, redundancy for the more probable single active failures, availability of non-safety-related electric power, and protection against more probable hazards. The requirements also address realistic safety margin basis analysis and testing to demonstrate the systems' capability to satisfy their

non-safety defense-in-depth functions. EPRI has proposed that the ALWR URD will not include specific requirements for the quantitative reliability of these systems.

The exclusive reliance on passive systems in meeting current licensing criteria is a departure from current design philosophy and licensing practice and must be evaluated. Therefore, the staff will need new guidance for reviewing the AP600 and SBWR submittals and in developing regulatory treatment of non-safety systems (RTNSS).

The staff met with representatives of the ALWR Program on several occasions to determine the steps needed to resolve the issue of RTNSS in passive plants, and define the scope of requirements and acceptance criteria to ensure that they have adequate capability and availability, when required. In a meeting between NRC and the ALWR Utility Steering Committee on January 22, 1993, the participants agreed to an overall process for determining the regulatory treatment of non-safety systems, and determining the importance of passive systems and components for meeting NRC safety objectives. This agreement included the following key elements:

1. EPRI has proposed that the passive ALWR URD will describe the process to be used by the designer for specifying the reliability/availability (R/A) missions of risk-significant structures, systems, and components (SSCs) needed to meet regulatory requirements and to allow comparison with NRC safety goals. An R/A mission is the set of requirements related to performance, reliability, and availability for an SSC function that adequately ensure its task, as defined by the focused PRA or deterministic analysis, is accomplished. The focused PRA is described in Section II.3, below.

2. The designer will apply the process to the design to establish R/A missions for the risk-significant SSC.

3. If active systems are determined to be risk significant, NRC will review these R/A missions to determine if they are adequate and if the operational reliability assurance program (O-RAP) or simple technical specifications and limiting conditions for operation are adequate to give reasonable assurance that the missions can be met during operation.

4. If active systems are relied on to meet the R/A missions, the designer will impose design requirements commensurate with risk significance on those elements involved.

5. NRC will not include any R/A missions in the design certification rule. Instead, NRC would include deterministic requirements on both safety and non-safety design features in the design certification rule.

To address these key elements, the staff and representatives of the ALWR Program later began preparing an appropriate process that the plant designers can use to address the RTNSS issue. In a letter of February 23, 1993, the ALWR Program submitted a proposed process for determining the appropriate regulatory treatment for active systems for passive ALWRs. In a meeting on

May 20, 1993, the staff and representatives of the ALWR Program agreed to a final process for resolving the RTNSS issue. In a letter of May 26, 1993, EPRI described the steps in this process for determining risk-significant non-safety features based on a Level 3 probabilistic risk assessment (PRA). The process involves constructing a "focused PRA" to determine the importance of various active systems in ensuring that the Commission's safety goal objectives are met. Risk-significant SSCs, their R/A missions, and regulatory oversight can then be determined. The steps of this RTNSS process described by EPRI in their May 26, 1993, submittal are as follows:

I. Scope and Criteria

The RTNSS basis applies broadly to those non-safety SSCs that perform risk-significant functions, and therefore, are candidates for regulatory oversight. The plant designer will apply the following criteria, proposed by EPRI in their May 26, 1993, submittal, to determine these SSC functions:

A. SSC functions relied upon to meet beyond design basis deterministic NRC performance requirements such as 10 CFR 50.62 for anticipated transient without scram (ATWS) mitigation and 10 CFR 50.63 for station blackout.

B. SSC functions relied upon to resolve long-term safety (beyond 72 hours) and to address seismic events.

C. SSC functions relied upon under power-operating and shutdown conditions to meet the Commission's safety goal guidelines of a core damage frequency of less than 1.0E-4 each reactor year and large release frequency of less than 1.0E-6 each reactor year.

D. SSC functions needed to meet the containment performance goal (SECY-93-087, Issue I.J), including containment bypass (SECY-93-087, Issue II.G), during severe accidents.

E. SSC functions relied upon to prevent significant adverse systems interactions.

The staff finds the proposed scope and criteria to be acceptable. It should be noted that the large release frequency of less than 1.0E-6 each reactor year specified in Item C, above, as one of the screening criteria was an agreement reached between the NRC and the ALWR Steering Committee and was proposed in the May 26, 1993, EPRI submittal. Subsequently, the Commission has decided to terminate the development of the definition of large release. Therefore, the staff will work with the ALWR vendors to assess the need for any alternative criterion. A conditional containment failure probability of 0.1 was previously approved by the Commission as a complement to the deterministic containment performance goal.

II. Specific Steps in the RTNSS Process for Each Design

1. Comprehensive Baseline PRA

The designer will construct comprehensive Level 3 PRAs (baseline PRAs) in accordance with the ALWR URD. These comprehensive baseline PRAs must include all appropriate internal and external events for both power and shutdown operations. Seismic events will be evaluated by a margins approach. Adequate treatment of uncertainties, long-term safety operation, and containment performance should be included. Containment performance should be addressed with considerations for sensitivities and uncertainties in accident progression and inclusion of severe accident phenomena, including explicit treatment of containment bypass. Mean values must be used to determine the availability of passive systems and the frequencies of core damage and large releases. Appropriate uncertainty and sensitivity analyses should be used to estimate the magnitude of potential variations in these parameters and to identify significant contributors to these variations. Results of an adverse systems interaction study will also be considered in the PRA.

2. Search for Adverse Systems Interactions

The designers must systematically evaluate adverse interactions between the active and passive systems. The results of this analysis should be used for design improvements to minimize adverse systems interaction, and be considered in making PRA models.

3. Focused PRA

The focused PRA includes the passive systems and only those active systems necessary to meet the safety goal guidelines proposed by EPRI in scope Criteria I.C. The designers should consider the following in constructing focused PRAs to determine the R/A missions of non-safety SSCs which are risk significant.

First, the scope of initiating events and their frequencies are maintained in the focused PRA as in the baseline PRA. As a result, non-safety SSCs used to prevent the occurrence of initiating events will be subject to regulatory oversight applied commensurate with their R/A missions for prevention, as discussed in Steps 4 and 5, below.

Second, following an initiating event, the comprehensive Level 3 focused PRA event tree logic will not include the effect of non-safety SSCs. As a minimum, these event trees will not include the defense-in-depth functions and their support such as ac power to determine if the passive safety systems, when challenged, can provide sufficient capability without non-safety backup to meet the NRC safety goal guidelines for a core damage frequency of 1.0E-4 each year and a large release frequency of 1.0E-6 each year. The designer should evaluate the containment performance, including bypass, during a severe accident. Non-safety SSCs which remain in the focused PRA model are subject to regulatory oversight based on their risk significance in Steps 4 and 5.

4. Selection of Important Non-safety Systems

The designers will determine any combinations of non-safety SSCs that are necessary to meet NRC regulations, safety goal guidelines, and the containment performance goal objectives. The designers will determine these combinations for both scope Criteria A and E where NRC regulations are the bases for consideration and scope Criteria C and D where PRA methods are the bases for consideration. To address the long-term safety issue in scope Criterion B, the designer will use PRA insights, sensitivity studies, and deterministic methods to establish the ability of the design to maintain core cooling and containment integrity beyond 72 hours. Non-safety SSC functions required to meet beyond design basis requirements (Criterion A), to resolve the long-term safety and seismic issues (Criterion B), and to prevent significant adverse interactions (Criterion E) are subject to regulatory oversight as discussed in Step 6, below.

EPRI has proposed that the designers will take the following steps in using the focused PRA to determine the non-safety SSCs important to risk:

a. Determine those non-safety SSCs needed to maintain initiating event frequencies at the comprehensive baseline PRA levels.

b. Add the necessary success paths with non-safety systems and functions in the "focused PRA" to meet the safety goal guidelines, containment performance goal objectives, and NRC regulations. Choose the systems by considering the factors for optimizing the design effect and benefit of particular systems. Perform PRA importance studies to assist in determining the importance of these SSCs. Recognize that the staff could require regulatory oversight for all non-safety SSCs in the focused PRA model needed to meet NRC requirements, the safety goal guidelines, and containment performance goals.

5. Non-safety System Reliability/Availability Missions

The designers will determine and document from the focused PRA the functional R/A missions of active systems needed to meet the safety goal guidelines, containment performance goals, and other NRC performance requirements as described in Step 4. Repeat Steps 4, 5 and 6 to ensure that the best active systems and their R/A missions are selected.

As part of this step, the designer should establish graded safety classifications and graded requirements for I&C systems based on the importance to safety of their functional R/A missions. In SECY-91-292, the staff discussed the need for such classifications and requirements for I&C systems important to safety.

6. Regulatory Oversight Evaluation

Upon completing Steps 1-5, above, the designers will conduct activities such as:

a. Reviewing the standard safety analysis report (SSAR) and the PRA, and audit plant performance calculations to determine that the design of these risk-significant non-safety SSCs satisfies the performance capabilities and R/A missions.

b. Reviewing the SSAR to determine that it includes the proper design information for the reliability assurance program, including the design information for implementing the maintenance rule and operational reliability assurance program.

c. Reviewing the SSAR to determine that it includes proper short-term availability control mechanisms, if required for safety and determined by risk significance such as simple technical specifications.

After the designer has completed these or related activities, the staff will apply appropriate regulatory oversight.

7. NRC/Vendor Interaction

Early in the reviews, the staff and the designers will discuss the appropriateness of the focused PRA models and reliability values, R/A missions, and level of regulatory oversight for various active systems.

This process which EPRI has proposed for RTNSS was developed after several meetings with the NRC staff. The staff endorses the process described in this paper and finds it to be an acceptable method for handling the RTNSS issue.

As a part of NRC/EPRI agreement, EPRI will properly incorporate this RTNSS process in the ALWR URD for the passive plant designer to address the RTNSS issue. However, the risk significance of active systems cannot be determined until the design-specific baseline and focused PRA evaluation are completed because the design requirements of active systems depend on the R/A missions of the risk-significant active systems, which the plant designer will determine using the RTNSS process and the design-specific focused PRA. The staff cannot complete portions of its review for the performance goals of both passive and active systems, technical specification requirements, and the operational reliability assurance program before the designers submit the focused evaluation described above and before the PRA review is nearly completed to determine the R/A missions. These actions must be completed in a timely manner to ensure the designers and prospective owner/operators understand the results of these reviews and their implications on operational regulatory requirements in time to accommodate the requirements or explore alternative measures.

The designer must integrate into the design process the process for resolving the RTNSS issue. In particular, the designer should use the results from identifying the risk-significant important systems and their R/A missions and comparisons with the safety goal objectives, and report this information in the PRA. By including this information in the review of the PRA and related discussions with the designer, the staff will determine the regulatory oversight on the non-safety SSCs in the most efficient and timely way.

This RTNSS process is a comprehensive approach for resolving the RTNSS issue and other relevant issues evaluated in the process. In determining the R/A missions and the proper regulatory oversight of the risk-significant active systems during this evaluation, the staff will properly address these issues, which include the stable safe shutdown requirements and related passive system design basis of 72-hour capability, station blackout, electrical distribution, and control room habitability and inservice testing of pumps and valves.

The staff recommends that the Commission approve the proposed process as an acceptable method for resolving the regulatory treatment of non-safety systems in the passive ALWR designs.

B. Definition of Passive Failure

A single failure is defined in Appendix A to 10 CFR Part 50 as an occurrence which results in the loss of a component's capability to perform its intended safety functions. The deterministic single failure criterion is a simple, effective method to determine the redundancy of systems and components needed to ensure adequate reliability of safety functions. General experience indicates that even components and equipment that are made to high standards of quality may sometimes fail to function in a way and at a time that can be random and unpredictable.

The NRC regulations include the single failure criterion in the general design criteria (GDC) in Appendix A to 10 CFR Part 50, which require the design of certain systems important to safety to be capable of performing their defined safety functions or mission assuming the failure of any single component within the system or its supporting systems. For example, GDC 21, 34, and 35, respectively, require sufficient redundancy and independence to be designed into the protection, residual heat removal, and emergency core cooling systems such that no single failure results in the loss of these system safety functions.

In SECY-77-439, "Single Failure Criterion," the staff described how it is using the single failure criterion in reviewing reactor safety. Though the NRC established the single failure criterion without assessing the probabilities of component or system failure, it is not assumed that any conceivable failure could occur in applying the criterion. In general, only those systems or components judged to have a credible chance of failure are assumed to fail in applying the single failure criterion.

In SECY-77-439, the staff discussed the distinction between active and passive failures of a system or component. An active failure in a fluid system is (1) the failure of a component which relies on mechanical movement to complete its intended function on demand, or (2) an unintended movement of the component. Examples include the failure of a motor- or air-operated valve to move or to assume its correct position on demand, the spurious opening or closing of a motor- or air-operated valve, or the failure of a pump to start or stop on demand. Such failures can be induced by operator error. A passive failure in a fluid system is a breach in the fluid pressure boundary or a mechanical failure which adversely affects a flow path. Examples include the failure of a check valve to move to its correct position when required and the leakage of

fluid from failed components (such as pipes and valves), particularly through a failed seal at a valve or pump or line blockage. Motor-operated valves which have the source of power locked out are allowed to be treated as passive components.

In defining a single failure in Appendix A to 10 CFR Part 50, the NRC stated that fluid and electric systems are considered to be designed against an assumed single failure if the system maintains its ability to perform its safety functions in the event of either (1) a single failure of any active component (assuming passive components function properly) or (2) a single failure of a passive component (assuming active components function properly). The NRC further noted that single failures of passive components in electric systems should be assumed in designing against a single failure. Thus, no distinction is made between failures of active and passive components for electric systems, and all such failures must be considered in applying the single failure criterion. Appendix A also states that the conditions under which a single failure of a passive component in a fluid system should be considered in designing the system against a single failure are being developed.

In SECY-77-439, the staff stated the following:

> on the basis of the licensing review experience accumulated in the period since 1969, it has been judged in most instances that the probability of most types of passive failures in fluid systems is sufficiently small that they need not be assumed in addition to the initiating failure in the application of single failure criterion to assure safety of a nuclear power plant.

In keeping with the defense-in-depth approach, the staff does consider the effects of certain passive failures (e.g., check valve failure, medium- or high-energy pipe failure, and valve stem or bonnet failure) as potential accident initiators. In licensing reviews, however, only on a long-term basis does the staff consider passive failures in fluid systems as potential accident initiators in addition to initiating events. For example, Section 6.3 of the Standard Review Plan (SRP) requires consideration of passive failures in the emergency core cooling system during the recirculation cooling mode following emergency cooling injection, but does not define such a failure. The staff finds no reason to alter this regulatory practice for the passive ALWR designs, except for check valves as discussed below.

The failure of a check valve to move to its desired position is not clearly defined as an active or passive failure. American National Standards Institute (ANSI)/American Nuclear Society (ANS)-58.9 cites the failure of a check valve to move to its correct position as an active failure. In SECY-77-439, the staff stated that the failure of a check valve to move to its correct position when required was a passive failure. The staff normally treats check valves, except for those in containment isolation systems, as passive devices. In an International Atomic Energy Agency (IAEA) paper, "Application of the Single Failure Criterion - A Safety Practice," (Safety Series 50-P-1) the authors stated that in some member States a failure of a simple swing type check valve to open need not be considered as a single failure, whereas in

other member States self-operating components such as check valves are considered to be active components if the state of the component is changed during the given event sequence after an initiating event. The authors of the IAEA paper determined that, with the test intervals of check valves of about one year, the probabilities of failure of check valves to open or close are closer to the failure probabilities of active components (3E-6 to 3E-5 per hour) than to those of passive components (1E-9 to 1E-8 per hour). The authors stated that a conservative approach is to assume a check valve failure in the single failure analysis.

For current plants, the NRC staff normally treats check valves, except for those in containment isolation systems, as passive devices during transients or design-basis accidents. Therefore, the staff would not consider the failure of a check valve to be a single active failure. Recognizing the unique features of the passive safety system designs having low-driving force, the staff examined current regulatory practice to determine how it will apply to check valve failures for the passive plant designs. These safety-related check valves in the passive designs will operate under different conditions (low flow and pressure without pump discharge pressure to open valves) than current generation reactors and evolutionary designs. Check valves have high safety significance in the operation of the passive safety systems, and operating experience of check valves suggests that they may have a lower reliability than originally anticipated.

EPRI stated that the ALWR program endorses ANSI/ANS 58.9-1981 considering check valves to be active components when they are required to change state to perform their safety function. Failures of these components are considered to be active failures that occur coincident with event initiators. The ANS standard allows exemptions where the proper function of a component can be demonstrated despite any credible condition, and it requires documentation of the exemptions in the single failure analysis. EPRI further stated that the ALWR reliability program will include a thorough review of check valve applications in the passive safety systems. This will include determining the particular check valves which play a key role in ensuring core damage frequency requirements are met, reviewing whether available check valve reliability data is applicable and sufficient for passive plant safety systems, and determining appropriate measures for assuring that check valves will operate reliably throughout the plant operating life. EPRI stated that its intent is to rigorously evaluate these valves to establish the best technical solution rather than simply relying on single failure to ensure safety. In a position paper, "NRC Policy Issue Analysis and Recommendation," submitted with a May 5, 1992, letter, EPRI contended that check valves when appropriately designed for the application will be extremely reliable. EPRI also contended that the URD requirements, ALWR safety goals, and the iterative use of PRA in the design process ensure that the unavailability of check valves will be sufficiently low and independent of the initiating failure that check valves need not be assumed to fail. EPRI recommended that check valve failures not be redefined as active failures for the passive safety systems. In its letter of December 10, 1992, EPRI also stated that this industry position is consistent with ANS 58.9, which appears to be inconsistent with

EPRI's earlier endorsement of ANSI/ANS 58.9-1981 that considers check valves as active components if they must change state to perform their safety function.

The staff proposes that, except for those check valves whose proper functions can be demonstrated and documented, check valves in the passive safety system designs be subject to single active failure consideration. In determining an exemption to single failure consideration for a particular check valve application, the plant designer shall perform a comprehensive evaluation of check valve test data or operational data for the similar check valve designs in similar applications and operating environments to demonstrate that the reliability of the particular check valve application is such that the probability of failure is comparable to those of passive components. A failure probability on the order of 1E-4 per year or less would be low enough to be considered as a passive failure. An example of possible exemption is the accumulator check valves installed in applications identical to those for currently licensed plants where the accumulator pressure will eventually create a large pressure differential to force open the valves as the reactor coolant system (RCS) pressure falls.

Redefining check valves as active components, subject to consideration for single active failures would cause these valves to be evaluated in a more stringent manner than that used in previous licensing reviews.

The staff recommends that the Commission approve the staff's proposal to maintain the current licensing practice for passive component failures on the passive ALWR designs, and to redefine check valves, except for those whose proper function can be demonstrated and documented, in the passive safety systems as active components subject to single failure consideration.

C. Safe Shutdown Requirements

In GDC 34 of Appendix A to 10 CFR Part 50, the NRC regulations require that the design include a residual heat removal (RHR) system to remove residual heat from the reactor core so that specified acceptable fuel design limits (SAFDLs) and the design conditions of the reactor coolant pressure boundary are not exceeded. GDC 34 further requires suitable redundancy of the components and features of the RHR system to ensure that the system safety functions can be accomplished, assuming a loss-of-offsite power or onsite power, coincident with a single failure. The NRC promulgated these requirements to ensure that the RHR system is available for long-term cooling to ensure a safe shutdown state.

The NRC regulations have several definitions for safe shutdown. For example, in 10 CFR 50.2, the NRC regulations define "safe shutdown (non-design basis accident)" for station blackout as bringing the plant to those shutdown conditions specified in plant technical specifications as hot standby or hot shutdown, as appropriate (plants have the option of maintaining the RCS at normal operating temperatures or at reduced temperatures). Appendix R to 10 CFR Part 50 states that the phrase "safe shutdown" is used throughout the appendix as applying to both hot and cold shutdown. The regulation does not define safe shutdown of the plant after normal operation or a design basis

accident, nor does it define what constitutes a safe shutdown state. In implementing the GDC 34 requirements, the staff specified in Regulatory Guide (RG) 1.139 "Guidance for Residual Heat Removal," and Branch Technical Position (BTP) RSB 5-1 the conditions for cold shutdown (93.3 °C (200 °F) for a PWR and 100 °C (212 °F) for a BWR) using only safety-grade systems within 36 hours. In the regulatory guide, the staff presents the basis for this requirement as follows:

> even though it may generally be considered safe to maintain a reactor in a hot standby condition for a long time, experience shows that there have been events that required eventual cooldown and long-term cooling until the reactor coolant system was cold enough to perform inspection and repairs. It is therefore obvious that the ability to transfer heat from the reactor to the environment after a shutdown is an important safety function for both PWRs and BWRs. Consequently, it is essential that a power plant have the capability to go from hot-standby to cold shutdown conditions. . .under any accident conditions.

Passive ALWR designs are limited by the inherent ability of the passive heat removal processes because they use passive heat removal systems for decay heat removal. These designs cannot reduce the temperature of the reactor coolant system below the boiling point of water for the heat to be transferred to the water pool where heat exchangers are submerged, that is, the in-containment refueling water storage tank of the AP600 or the isolation condenser of the simplified boiling water reactor (SBWR). Even though active shutdown cooling systems are available to bring the reactor to cold shutdown or refueling conditions, these active RHR systems are not safety-grade and do not comply with the guidance of RG 1.139 or BTP RSB 5-1.

EPRI defined a safe stable shutdown condition as 215.6 °C (420 °F) and stated that passive safety systems need not be capable of achieving cold shutdown. EPRI based this contention on the belief that the passive decay heat removal systems have an inherently high long-term reliability. EPRI contended that the passive ALWR designs meet the GDC 34 requirements because they use a redundant safety-grade passive system that can operate at full RCS pressure and place the reactor in the long-term cooling modes immediately after shutdown, and because conditions maintained by the systems are safe and fully consistent with the GDC 34 requirement to maintain fuel and reactor coolant pressure boundary within acceptable limits.

In evaluating the EPRI position on safe shutdown, the staff considered the conditions that constitute a safe shutdown state and assessed the acceptability of EPRI's proposed approach for meeting GDC 34. In RG 1.139 and BTP 5-1, the staff position that an RHR system be able to bring the plant to cold shutdown conditions was to enable the licensee to perform inspection and repair at the plant. The staff believes that other plant conditions may constitute a safe shutdown state as long as reactor subcriticality, decay heat removal, and radioactive materials containment are properly maintained for the long term.

The URD for passive designs specifies performance requirements for the passive decay heat removal systems to have sufficient capacity to reduce reactor

coolant temperature to 215.6 °C (420 °F) within 36 hours of reactor shutdown. To ensure the means are available to remove decay heat in accordance with GDC 34, the URD also specifies that, upon a single failure, safety-grade decay heat removal from the reactor coolant system shall be possible from full RCS operating pressures and temperatures to a safe stable condition for all plant conditions. EPRI also required that the operation of the plant in the long-term cooling mode be automatic, eliminating the need for operator actions to cool down the plant. The operation of the passive RHR system does not require ac power, pump, or valve operation (except for initial operation for alignment of the system), or support systems (such as component cooling water or service water), and is stable and self-contained, requiring no makeup water for a period of at least 3 days following reactor shutdown. Therefore, the licensee could maintain a safe stable condition with the safety-grade passive RHR system.

After the passive RHR system or main steam system effected the initial shutdown, a non-safety-grade reactor shutdown cooling system will be available to bring the plant to cold shutdown conditions for inspection and repair. EPRI stated that

> these non-safety systems are required to be highly reliable. . .and there is no single failure of these systems or their support systems which would result in inability to terminate use of the passive safety grade system and achieve cold shutdown if desired.

The staff believes that the passive RHR systems offer potential advantages over current active systems, and can maintain the plant in conditions that are fully consistent with the requirement of GDC 34 to maintain the fuel and reactor coolant pressure boundary within acceptable limits, and therefore, contain radioactive materials which may be present. The passive safety injection system and the associated depressurization system can also protect against the loss of reactor coolant inventory during long-term passive RHR operation. These passive system capabilities can be demonstrated by appropriate evaluations during detailed design analyses, including

1. A safety analysis to demonstrate that the passive systems can bring the plant to a safe stable condition and maintain this condition, that no transients will result in the SAFDLs and pressure boundary design limit being violated, and that no high-energy piping failure being initiated from this condition will result in violation of 10 CFR 50.46 criteria.

2. A probabilistic reliability analysis, including events initiated from the safe shutdown conditions, to ensure conformance with the safety goal guidelines. The PRA would also determine the R/A missions of risk-significant systems and components as a part of the effort for regulatory treatment of non-safety systems.

The staff is concerned that, with the passive system design basis of 72-hour capability, the passive RHR system water pool, without refill, will have water capacity to permit only 72 hours of operation after a scram. A long-term safe stable condition, however, can be maintained if a reliable non-safety support

system or equipment is available to replenish the water pool to sustain long-term operation of the passive RHR system after 72 hours. The passive URD requires that non-safety equipment necessary for plant recovery after the assumed 72-hours accident duration be designed for the expected environment, and that only simple, unambiguous operator actions and easily accomplished offsite assistance be necessary after 72 hours to prevent fuel damage. The staff recommended in Section A of this paper that the Commission approve an acceptable process for resolving the RTNSS issue. With an acceptable resolution of the RTNSS issue, the staff expects that non-safety support systems and equipment and active decay heat removal systems will be evaluated for their risk significance and will meet appropriate design and reliability criteria to provide backup capability to passive systems beyond 72 hours. This will ensure proper operation of the passive RHR system to maintain a safe stable condition over the long term, as well as reliable non-safety systems that will be necessary to bring the plant to cold shutdown conditions.

The staff concludes that cold shutdown is not the only safe stable shutdown condition which can maintain the fuel and reactor coolant boundary within acceptable limits, and that the EPRI proposed 215.6 °C (420 °F) as a safe stable shutdown condition is acceptable on the basis of acceptable passive safety system performance and acceptable resolution of the regulatory treatment of non-safety systems.

The staff recommends that the Commission approve the EPRI's proposed 215.6 °C (420 °F) or below, rather than the cold shutdown condition required by RG 1.139, as a safe stable condition, which the passive decay heat removal systems must be capable of achieving and maintaining following non-LOCA events. This recommendation is predicated on an acceptable passive safety system performance and an acceptable resolution of the issue of regulatory treatment of non-safety systems.

D. Control Room Habitability

GDC 19 of Appendix A to 10 CFR Part 50 states that (1) a control room should be provided from which actions can be taken to operate the nuclear power plant safely under normal conditions and to maintain it in a safe condition under accident conditions including a loss-of-coolant accident and (2) adequate radiation protection should be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident. In current plants, safety-grade, filtered control room HVAC systems with charcoal adsorbers are used to ensure that radiation doses to operators will be maintained within the GDC 19 criteria in the event of an accident.

In SRP Section 6.4, "Control Room Habitability Systems," the staff defined the acceptable operator dose criteria in terms of specific whole-body and critical organ doses (5 rem to the whole body and 30 rem each to the thyroid and skin).

Originally, EPRI proposed the exposure limit for control room operators of 5 rem whole body, 75 rem beta skin dose, and 300 rem thyroid dose. EPRI

stated that each operator would be provided with individual breathing apparatus and protective clothing, if required, to meet regulatory limits. The staff determined that EPRI did not adequately justify its requirements for the thyroid and beta skin doses. The staff informed EPRI that the long-term use of breathing apparatus during design-basis accidents has never been allowed. More importantly, the long-term use of breathing apparatus is likely to degrade control room operator performance during and after an accident.

EPRI stated that the control room would be designed to be maintained during a 72-hour period as the primary location from which personnel can safely operate in the event of an accident. The staff's position is that the required duration for certain accident sequences may be much longer than 72 hours in design basis accidents. GDC 19 states that "adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions. . .for the duration of the accident," which has typically been assumed to be 30 days. Consequently, the staff concluded that analyses of control room habitability should consider the duration of the accident which may extend beyond the EPRI-proposed 72-hour period as the design basis.

In its letter of May 5, 1992, EPRI proposed an alternative in which a safety-grade pressurization system could be recharged remotely after 72 hours. The URD for passive plants requires (1) a passive, safety-grade control room pressurization system which would use bottled air to keep operator doses within the limits of GDC 19 and SRP 6.4, Revision 2 of the SRP for the first 72 hours of the event, and (2) safety-grade connections for the pressurization system to allow the use of offsite, portable air supplies if needed after 72 hours to minimize operator doses. The staff agrees with the concept of a safety-grade pressurization system and EPRI's commitment to limit the operator doses to those specified in GDC 19 and SRP 6.4, Revision 2. The staff will evaluate the feasibility and the capability of the proposed pressurization systems on a vendor-specific basis.

In its letter of August 17, 1992, the Advisory Committee on Reactor Safeguards (ACRS) stated that the members had discussed control room habitability with EPRI and the staff during a June 4 and 5, 1992, meeting. At that meeting, the staff told the ACRS that it was evaluating the EPRI proposal for the safety-grade pressurization system. ACRS stated that it had several comments about the design features of the passive control room pressurization system proposed by EPRI. The ACRS stated that the staff should consider these comments when performing its evaluation and that the ACRS may make additional recommendations after the staff has completed its evaluation. In an October 29, 1992, reply to the ACRS, the staff stated that it had not completed its review of the control room habitability issue and would consider the ACRS comments during its review of the EPRI Requirements Document.

The staff reviewed the EPRI proposal for a safety-grade pressurization system and determined the following:

- The present licensing of nuclear power plants does not require the licensee to have engineered safety feature (ESF) ventilation systems unless the licensee cannot meet the dose criteria associated with the design basis accidents (DBAs) or other safety criteria. If the licensee

cannot meet these criteria, it must ensure that an ESF system or some other safety-grade system is available to mitigate the consequences of a DBA.

- The use of a pressurization system, such as a bottled air system, may not preclude the need for other safety-grade ventilation equipment within the control room. For example, such safety-grade equipment could be required to maintain cooling to the electrical instruments in the control room.

- At least once each refueling cycle, the licensee must demonstrate the adequacy of such a system to pressurize the control room for a 72-hour period and maintain all the other conditions, including temperature, within the acceptable range for the control room envelope. This requirement is consistent with the present requirements for bottled air systems.

- The regulatory treatment of the portable air supply and the non-safety-grade ventilation system will be in accordance with the staff's position described in Section A of this paper.

The staff agrees with EPRI's concept of the safety-grade pressurization system and the use of safety-grade connections for the pressurization system to allow the use of backup, portable air supplies after 72 hours to minimize operator doses for the duration of the accident. However, the staff has some reservations about limiting the occupancy inside the control room envelope to 5 people for 72 hours. Each of the passive ALWR designs includes design operational conditions similar to the interim operational conditions allowed at existing plants while they implemented permanent modifications to upgrade the systems to meet the requirements of GDC 19. These interim operational conditions were allowed for only a limited period of time because they may not have ensured sufficient control room habitability for the life of the plant. Therefore, a designer must demonstrate (1) the feasibility and capability of the safety-grade pressurization systems to satisfy GDC 19 criteria regarding control room habitability and (2) the availability and capability of the backup air supplies.

To meet the applicable provisions of GDC 4 and 19, both the passive AP600 and SBWR designs provide a safety-related pressurization system to maintain at least 31.1 Pascal (1/8-inch water gauge (WG)) positive differential pressure. The AP600 and SBWR designs also claim that unfiltered leakage into the control room envelope will be restricted to 1.4E-4 to 2.4E-4 cubic meters per second (0.3 to 0.5 cubic feet per minute), respectively. The vendor-specific reviews will be based on the guidelines of SRP Section 6.4, including experience obtained from the operating plants concerning (1) the provisions for maintaining and periodically testing for leaktightness to maintain at least 31.1 Pascal positive pressure relative to all surrounding areas, (2) the adequacy of the ESF filtration system, if needed, (3) the ability of the postaccident safety-related cooling to maintain a habitable environment for control room operators and to provide equipment operability, and (4) protection against the effects of accidental release of toxic gases and smoke inside the control room pressure boundary.

Each of the passive ALWR designs includes non-safety ventilation systems for the control room envelope. The system would be switched to a recirculation mode with filtered makeup on high radiation signal and would be available for control room habitability as long as the ac power is available and the system is operational. The non-safety system is isolated from the control room on a high-high radiation signal measured in the HVAC duct supplied from the non-safety system. There is some probability that the non-safety HVAC systems would be available for control room habitability during a postulated design-basis accident in a period when ac power is available. However, this system and the power supplies are non-safety-related, as designed, and cannot be relied upon for control room habitability during a postulated design-basis accident. Therefore, no credit for the non-safety system can be taken in the safety analysis for design-basis accidents.

The staff will separately consider the control room habitability of each vendor's design for acceptance. The staff will review the designs for control room habitability to ensure that the requirements specified in GDC 19 are met and that personnel and equipment in the control room have a suitable environment for the duration of the accident.

The staff recommends that the Commission approve the following positions on control room habitability for passive plants:

1. The concept of using a passive, safety-grade control room pressurization system which would use bottled air to keep operator doses within the limits of GDC 19 and SRP 6.4, Revision 2 of the SRP for the first 72 hours of the event, and safety-grade connections for the pressurization system to allow the use of offsite, portable air supplies is acceptable if needed after 72 hours to minimize operator doses for the duration of the accident.

2. COL holders must demonstrate through performance of the applicable ITAAC, the feasibility and capability of a pressurization system and the capability and availability of backup air supplies to maintain control room habitability for the duration of the accident.

3. The regulatory treatment of the portable air supply and the non-safety-grade ventilation system should be in accordance with the staff's position described in Section A of this paper.

E. Reliability Assurance Program

In SECY-89-013, "Design Requirements Related to the Evolutionary ALWR," the staff stated that the reliability assurance program (RAP) would be required for design certification to ensure that the design reliability of safety-significant SSCs is maintained over the life of a plant. The staff had informed the ALWR vendors and EPRI that it was considering this matter in November 1988.

The ALWR RAP would apply to those plant SSCs that are risk-significant (or significant contributors to plant safety) as determined by using probabilistic, deterministic, or other methods of analysis used to identify and quantify

risk such as the design certification PRA. The purposes of the RAP are to provide reasonable assurance that (1) an ALWR is designed, constructed, and operated in a manner that is consistent with the reliability assumptions and risk insights for these risk-significant SSCs, (2) the reliability of these risk-significant SSCs does not degrade during plant operations, (3) the frequency of transients that challenge ALWR SSCs are minimized, and (4) these SSCs function reliably when challenged.

The staff views the RAP for ALWRs as a two-stage program. The first stage applies to the design phase of the plant life cycle, and would be referred to as the design reliability assurance program (D-RAP). The second stage applies to the construction and operations phases of the plant life cycle, and would be referred to as the operational reliability assurance program (O-RAP). An applicant for design certification would be required to establish the scope, purpose, objective, and essential elements of an effective RAP and would implement those portions of the D-RAP that apply to design certification. A combined license (COL) applicant will be responsible for augmenting and completing the remainder of the D-RAP to include any site-specific design information. Once the D-RAP has been established and the risk-significant SSCs identified and prioritized, the procurement, fabrication, construction, operation, and maintenance of these SSCs would be accomplished under the licensee's O-RAP.

The O-RAP can be thought of as an inclusive program that integrates aspects of existing programs (e.g., maintenance, surveillance testing, inservice inspection, inservice testing, and quality assurance) to achieve its objective. The O-RAP would apply to the construction and operation phases of plant life. Reliability performance goals for risk-significant SSCs would be established under the O-RAP, based on information from the D-RAP. The COL applicant would establish performance and condition monitoring requirements to provide reasonable assurance that the reliability of risk-significant SSCs is maintained or not unacceptably degraded. However, the RAP does not attempt to statistically verify the numerical values used in the PRA through performance monitoring. In addition, O-RAP would provide a feedback mechanism for periodically re-evaluating risk significance based on actual equipment, train, or system performance. Most of the O-RAP would be based on the requirements of the Maintenance Rule, 10 CFR 50.65, whose scope includes systems, structures, and components that are: (1) safety-related and (2) non-safety-related (a) relied upon to mitigate accidents or transients or used in plant emergency operating procedures; or (b) whose failure could prevent safety-related structures, systems, and components from fulfilling their safety-related function or (c) whose failure could cause a reactor scram or actuation of a safety-related system.

The staff and the ACRS have discussed the form and content of the ALWR RAP. In letters and during meetings with the staff, the ACRS noted the similarity between the Maintenance Rule, the license renewal rule, and the RAP. The ACRS has stated that the staff should issue consistent guidance on the elements of an acceptable program that will satisfy these three sets of requirements. In separate correspondence, the staff has provided the following discussion responding to the ACRS comments.

Implementation of the Maintenance Rule following the guidance contained in RG 1.160, "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," will meet the requirements of the O-RAP for degradation in SSC reliability or availability associated with maintenance. SSCs which are risk-significant (i.e., those within the scope of O-RAP) are given special treatment during implementation of the maintenance rule. They may be either monitored against specific goals or subject to preventive maintenance which assures acceptable performance and requires root cause analysis and corrective action for failure to meet performance criteria. Based upon industry guidance in NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," which is endorsed by RG 1.160, performance criteria for risk significant SSCs will include consideration of overall SSC availability. If an SSC failure occurs, the licensee will be required to determine whether or not it was maintenance preventable. Where failures are determined to be maintenance preventable, corrective actions and an evaluation of the effectiveness of that action on subsequent performance must be taken. Where failures of safety-related SSCs are caused by design deficiencies or operational errors, the quality assurance (QA) requirements of 10 CFR Part 50 Appendix B require corrective actions.

Therefore, implementation of the Maintenance Rule consistent with RG 1.160 plus corrective action for design or operational error-related failures under Appendix B QA programs, would meet the requirements for O-RAP for risk-significant, safety-related SSCs. Corrective action for design errors or operational errors which degrade non-safety, risk significant SSCs would require corrective action pursuant to O-RAP. Maintenance preventable failures for the SSCs would be evaluated and corrected pursuant to the Maintenance Rule. Thus, the difference between Maintenance Rule implementation and O-RAP relates to treatment of risk-significant non-safety SSCs whose failure is due to design or operational error.

The objective of an O-RAP is to provide reasonable assurance that the reliability and availability of SSCs are maintained commensurate with their risk-significance. The staff believes that this objective could be achieved through implementation of reliability performance monitoring, problem and failure identification, and a comprehensive corrective action program. The O-RAP corrective action program would include performance of a detailed root cause analysis of failures of risk-significant SSCs, implementation of effective corrective actions taken in response to all failures, and verification that the corrective action implemented was effective.

Staff Position on RAP

The staff's position is, for design certification of all ALWRs, a RAP applicable to design certification (D-RAP) should be required, and for a COL application that references a certified design, a RAP plan (augmented D-RAP and O-RAP) and inspections, tests, analyses, and acceptance criteria (ITAAC) should be required. The SSAR should include the details of the D-RAP, including the conceptual framework, program structure, and essential elements. The SSAR for the D-RAP should also (1) identify, prioritize, and list the risk-significant SSCs based on the design certification PRA, deterministic methods, such as, but not limited to, nuclear plant operating experience and relevant

component failure data bases; (2) ensure that the design certification applicant's design organization determines that significant design assumptions, such as equipment reliability and unavailability, are realistic and achievable; (3) include design assumption information for the equipment procurement process; and (4) provide these design assumptions to the COL for consideration in the O-RAP. A COL applicant would augment the design certification D-RAP with site-specific design information and would implement the balance of the D-RAP, including information for the procurement process. The COL applicant would also establish and implement the O-RAP. A COL applicant would be required to submit a RAP plan that integrates the design certification D-RAP, site-specific design information and augmented D-RAP, including information for the procurement process, and the O-RAP.

The O-RAP should consist of reliability performance monitoring, problem and failure identification, root cause analyses, and a corrective action program. However, the RAP does not attempt to statistically verify the numerical values used in the PRA through performance monitoring. The O-RAP corrective action program should include performance of a detailed root cause analysis of all failures of risk-significant SSCs, implementation of effective corrective actions taken in response to all failures, and verification that the corrective actions were effective.

Any SSCs identified as risk-significant in the D-RAP, by actual performance during operation or other methods, would require performance monitoring under the O-RAP. The reliability performance monitoring of risk-significant SSCs under O-RAP would be similar to that required by the Maintenance Rule (10 CFR 50.65). The performance targets or goals established and used with the reliability performance monitoring should provide a means to identify problems and equipment degradation prior to failure. Root cause analyses in the O-RAP would be required for each failure of a risk-significant SSC. Also, corrective actions taken in response to failures or problems and the results of those corrective actions would be monitored as part of the O-RAP.

The O-RAP should also make use of SSC data generated as part of the implementation of existing requirements and programs. For example, results from surveillance testing, inservice inspection and testing, and quality assurance activities, could provide a means of obtaining information on performance and reliability of risk-significant SSCs during procurement, construction, fabrication, testing, operation, and maintenance.

The COL applicant's RAP plan that covers the augmented D-RAP and O-RAP would be reviewed and approved by the NRC staff at the time the COL is issued, with all subsequent changes subject to NRC staff approval prior to implementation, similar to current QA Programs. The staff would verify implementation of the RAP plan with inspections and audits during detailed design, procurement, fabrication, construction, and testing prior to fuel load and would continue to inspect and audit implementation of the reliability assurance program for the duration of the license.

In accordance with SECY-92-287, the staff is proposing a regulation that requires an application for design certification to include: a description of the reliability assurance program used during the initial design that

includes, scope, purpose, and objectives; the methodology used to evaluate and prioritize the structures, systems, and components in the certified design based on their degree of risk-significance; and a list of the structures, systems, and components designated as risk-significant. For those structures, systems, and components designated as risk-significant, an application for design certification must also include: the methodology used to determine dominant failure modes that considered industry experience, analytical models, and existing requirements; and key reliability assumptions and risk insights from the PRA including any operation, maintenance, and monitoring activities that should be considered by a licensee that references the standard design.

The staff is also proposing a regulation that would require each application for a combined license that references a certified design would be required to include: a proposed reliability assurance program plan, applicable for the entire life of the plant, that incorporates the RAP from that certified design; and proposed tests, inspections, and analyses, and acceptance criteria, as required by 10 CFR 52.79(c), for the reliability assurance program plan. Additionally, each licensee under 10 CFR Part 52 would implement the reliability assurance program plan approved by the NRC.

The staff recommends that the Commission approve the staff's position that requirements concerning reliability assurance be incorporated into the design-specific rulemaking for an applicant for design certification and for an applicant for a combined license, that references a certified design.

F. Station Blackout

The station blackout rule (10 CFR 50.63) allows design alternatives to ensure that an operating plant can be safely shut down if all ac power (offsite and onsite) is unavailable. In SECY-90-016, "Evolutionary LWR Certification Issues and Their Relationship to Current Regulatory Requirements," the staff concluded that the preferred method of demonstrating compliance with 10 CFR 50.63 for evolutionary designs is by installing a spare (full-capacity) alternate ac power source of a diverse design.

The passive ALWR designs do not require ac power for 72 hours following an event and will include provisions for offsite assistance (including additional ac power) beyond 72 hours. Thus, EPRI and the passive plant designers have not made the same provisions for certain ac power system features found in existing plants or in the evolutionary plant designs. The passive designs lack an alternate ac power source and a normally available second offsite power circuit. They also use non-safety-grade emergency generators (typically diesel generators on existing plants) and non-safety-grade ac electrical distribution systems. Each of these is addressed below.

An alternate ac power source or the ability to cope with a station blackout for a specified duration are the options available to comply with the requirements of the station blackout rule. The staff prefers the use of an alternate ac power source to meet the requirements of the rule in evolutionary plant designs because it offers several advantages. An alternative ac power source could power a larger complement of shutdown equipment and bring the plant to cold shutdown, it could be used for other purposes in addition to station

blackout, it is not limited by time while providing power during a station blackout, and it provided for a uniform hardware approach requiring less analysis and fewer specialized operating procedures. However, EPRI and the passive plant designers stated that the passive plants will be designed to remain in a safe and stable condition for 72 hours without ac power, and without operator actions. This period can be extended well beyond 72 hours with preplanned offsite assistance and simple operator actions. This strong coping capability, reduced reliance on ac power, and minimal required operator actions would seem to obviate the need for an alternate ac source. However, EPRI also reduced the requirements on certain other ac power system features on which the station blackout requirements were premised.

GDC 17 requires that two offsite power circuits be available during plant operating modes. In the URD for the passive plant designs, however, EPRI required that the design include only a single offsite power circuit to supply the plant loads during operating modes. A second circuit is required in the passive plant designs for use only "in the event of an extended unavailability of the normal power supply, e.g., during plant outages." In the passive URD, EPRI stated as rationale for this requirement that it

> will ensure that adequate power supply will be maintained (either from another offsite source at the same site or from offsite) at all times during plant shutdown modes when major maintenance is required on one of the onsite power sources or on the normal offsite circuit.

The staff believes that if two offsite circuits are not available during plant operating modes, the frequency of loss-of-offsite power events and the time needed to recover offsite power will likely be greater than they are for existing plants. The designer should evaluate these difficulties against the stronger coping capability of the passive plant designs. The passive URD also requires that installed spare main and auxiliary transformers be available to replace their counterparts in no more than 12 hours, which should help to reduce the likelihood of an extended loss of the single normally available offsite power circuit.

In addition, EPRI and the passive plant designers are providing non-safety-grade onsite emergency generators (diesel generators or combustion turbine generators) and non-safety-grade ac electrical distribution systems. The staff believes that at least two aspects of this approach could directly affect station blackout. EPRI specified an overall reliability of 0.9 for the emergency generators. The maintenance unavailability and the start/run reliability that EPRI indicates would be consistent with this overall reliability are worse than typically seen on safety-grade diesel generators in existing plants. Secondly, EPRI stated that the emergency generators could be used as peaking units to supply power to the grid. EPRI and the passive plant designers, however, have not provided for a distribution system design that would facilitate the use of the emergency generator in this manner, since it would require that the power be delivered to the grid through the plant buses and distribution circuits. Both of the foregoing provisions could increase the likelihood of a station blackout.

Each of the ac power system features discussed in this section shares two aspects. They are viewed as non-safety systems or components for the passive plant designs, and their potential negative effects on station blackout must be judged against the strong coping capability of the passive plants. The staff, therefore, concludes that this issue is a good candidate to be addressed by the process for the regulatory treatment of non-safety systems described in Section A of this paper.

The staff recommends that the Commission approve the staff's proposal to resolve the station blackout issue and related GDC 17 issues on passive ALWR designs by evaluating the ac power system features discussed above under the process defined herein for resolving the regulatory treatment of non-safety systems issue. The staff will pursue regulatory treatment of these features if they are found to be risk significant or are relied on to meet the R/A missions.

G. Electrical Distribution

In SECY-91-078, "Chapter 11 of the Electric Power Research Institute's (EPRI's) Requirements Document and Additional Evolutionary Light-Water Reactor (LWR) Certification Issues," March 25, 1992, the staff recommended that the Commission approve its position that an evolutionary plant design should include the following elements:

- an alternate source of power to the non-safety loads unless the designer can demonstrate that the design margins will result in transients for a loss of non-safety power event that are no more severe than those associated with the turbine-trip-only event in current plants

- at least one offsite circuit to each redundant safety division supplied directly from one of the offsite power sources with no intervening non-safety buses in such a manner that the offsite source can power the safety buses upon a failure of any non-safety bus.

In the staff requirements memorandum (SRM) of August 15, 1991, the Commission approved the staff's positions. In a letter of May 5, 1992, EPRI stated that this issue does not apply to passive designs.

The first position identified above involved the lack of a second source of power on evolutionary plant designs (typically an offsite circuit on existing plants) to the traditional non-safety electrical buses that power plant loads required for unit operation. These loads include the reactor coolant pumps (recirculation pumps for BWRs), feedwater pumps, condensate pumps, and circulating water pumps. In SECY-91-078, the staff took this position to ensure that a second power source be provided to a sufficient string of these traditional non-safety loads so that forced circulation could be maintained, and the operator would have the normal complement of non-safety equipment available to bring the plant to a stable shutdown condition after a loss of the normal power supply and plant trip.

In the passive plant designs, the same complement of loads identified above (with the exception of the recirculation pumps in the BWRs that are no longer

used) are fed from traditional non-safety load buses with only a single source of offsite power available to them. However, recognizing the strong coping capability without ac power of the passive plant designs, EPRI has not required that a second offsite power source normally be available to any of the plant loads, non-safety or safety.

The staff took the second position in SECY-91-078 to address the connection of at least one offsite circuit directly to the safety buses with no intervening non-safety buses. In the evolutionary designs, this was accomplished with a direct connection of the second offsite circuit to the safety-grade diesel generator buses. The configuration shown in the passive URD is similar to that for the evolutionary plant, except that the second circuit is only intended to be available during extended plant outages as a maintenance type feed. Furthermore, the diesel generator buses to which the second circuit is connected and most of the ac distribution system are non-safety-grade. Thus, intervening non-safety buses and one transformer are located between the second circuit and the safety-grade ac bus that is now located at the 480-volt motor control center level. The one normally available offsite power circuit connection to the safety buses also has a number of intervening non-safety buses and transformers.

Both of the positions on this issue are closely tied to the lack of a second normally available offsite circuit identified in Section F of this paper. The staff, therefore, concludes that this issue is a good candidate to be addressed by the process for the regulatory treatment of non-safety systems described in Section A of this paper.

The staff recommends that the Commission approve the staff's proposal to resolve the electrical distribution issue on passive ALWR designs by evaluating the ac power system features using the process defined herein for resolving the regulatory treatment of non-safety systems. The staff will pursue regulatory treatment of these features if they are found to be risk significant or are relied on to meet the R/A missions.

H. Inservice Testing of Pumps and Valves

In SECY-90-016, the staff recommended that the Commission approve the following four issues for the inservice testing of safety-related pumps and valves beyond the current regulatory requirements in 10 CFR 50.55(a) for ASME Code Class 1, 2, and 3 components:

- Piping design should incorporate provisions for full-flow testing (maximum design flow) of pumps and check valves.
- Designs should incorporate provisions to test motor-operated valves under design basis differential pressure.
- Check valve testing should incorporate the use of advanced, non-intrusive techniques, to address degradation and performance characteristics.

- A program should be established to determine the frequency necessary to disassemble and inspect pumps and valves to detect unacceptable degradation that cannot be detected through the use of advanced, nonintrusive techniques.

The staff concluded that these requirements are necessary to give adequate assurance of operability of the components.

In its SRM of June 26, 1990, the Commission approved the staff's position as supplemented in the April 27, 1990, staff response to ACRS comments. In that response, the staff agreed with the ACRS recommendations to emphasize the requirements of Generic Letter (GL) 89-10 for evolutionary plants, to resolve check valve testing and surveillance issues, and to indicate how these requirements are to be applied to evolutionary plants. The staff also agreed that the requirements should permit consideration of proposed alternatives for meeting inservice and surveillance requirements. The Commission further noted that due consideration should be given to the practicality of designing testing capability, particularly for large pumps and valves.

The staff will conduct its plant-specific reviews with consideration that SECY-90-016 guidelines on design for testing at design basis conditions may not be practical in all cases, particularly for large pumps and valves. The staff is requesting that a qualification test (under design basis differential pressure) be conducted before installation and inservice valve testing be conducted under the maximum practicable differential pressure and flow when it is not practicable to achieve design basis differential pressure during an inservice test.

In its letter of May 5, 1992, EPRI stated that the ALWR program agrees with the above staff positions for the passive and evolutionary plants. In its letter of August 17, 1992, the ACRS supported the staff's recommendation that the above design, testing, and inspection provisions should be imposed on all safety-related pumps and valves for passive ALWRs.

The staff recommended that the Commission approve the position that these requirements should be imposed on passive ALWRs. The staff also concluded that additional inservice testing requirements may be necessary for certain pumps and valves in passive plant designs. The unique passive plant design places significant reliance on passive safety systems, but also depends on non-safety systems (which are traditional safety-related systems in current LWRs) to prevent challenges to passive systems. Therefore, the reliable performance of individual components is a very significant factor in enhancing the safety of passive plant design. The staff recommends that the following provisions be applied to passive ALWR plants to ensure reliable component performance:

1. The staff may not require important non-safety-related components to meet criteria similar to safety-grade criteria. However, the important non-safety-related pumps and valves as identified by the RTNSS process should be designed to accommodate testing in accordance with ASME Code, Section XI, requirements. Specific positions on the inservice testing

requirements for those components will be finalized when the staff completes its review of the regulatory treatment of non-safety systems.

2. ASME/ANSI OM Part 10 referenced in Section XI, ASME Code, 1989 Edition, provides for the relaxation in the valve testing frequency from quarterly intervals to cold shutdowns or refueling outages if testing during normal plant operations or cold shutdown conditions is not practical. These rules do not accommodate quarterly testing because they address the testing of valves in currently operating reactors where the detailed piping system designs were completed before the NRC promulgated the inservice testing requirements. The vendors for advanced passive reactors, for which the final designs are not complete, have sufficient time to include provisions in their piping system designs to allow testing at power. Quarterly testing is the base testing frequency in the Code and the original intent of the Code. Also, the COL holder may need to test more frequently than during cold shutdowns or at every refueling outage to ensure that the reliable performance of components is commensurate with the importance of the safety functions to be performed and with system reliability goals. Therefore, to the extent practical, the passive ALWR piping systems should be designed to accommodate the applicable Code requirements for the quarterly testing of valves, rather than to allow designs that only accommodate testing during cold shutdowns or refueling outages.

3. The passive system designs should incorporate provisions (1) to permit all critical check valves to be tested for performance in both forward and reverse flow directions and (2) to verify the movement of each check valve's obturator during inservice testing by observing the direct instrumentation indication of the valve position such as a position indicator or by performing nonintrusive test methods.

4. The passive system designs should incorporate provisions to test safety-related power-operated valves under design basis differential pressure and flow. The design basis capability of these types of valves should be verified before the valves are installed, before startup, and periodically through a program similar to that recommended for motor-operated valves in GL 89-10. The staff will determine if and the extent to which this concept should be applied to power-operated valves in important non-safety-related systems when the staff completes its review of the regulatory treatment of non-safety systems.

5. To the extent practical, provisions should be incorporated to verify that motor-operated valves (MOVs) in a safety-related system are capable of recovering from mispositioning. Mispositioning may occur through actions taken locally (manual or electrical), at a motor control center, or in the control room, and includes deliberate changes of valve position to perform surveillance testing. The staff will determine if and the extent to which this concept should be applied to MOVs in important non-safety-related systems when the staff completes its review of the regulatory treatment of non-safety systems.