



POLICY ISSUE

(Notation Vote)

May 22, 1995

SECY-95-132

FOR: The Commissioners

FROM: James M. Taylor
Executive Director for Operations

SUBJECT: POLICY AND TECHNICAL ISSUES ASSOCIATED WITH THE REGULATORY TREATMENT
OF NON-SAFETY SYSTEMS (RTNSS) IN PASSIVE PLANT DESIGNS (SECY-94-084)

PURPOSE:

To provide the Commission with the staff's response to the staff requirements memorandum (SRM) of June 30, 1994, pertaining to SECY-94-084, and present the corresponding revision of SECY-94-084 for Commission review and approval.

BACKGROUND:

On March 28, 1994, the U.S. Nuclear Regulatory Commission (NRC) staff recommended, in SECY-94-084, positions for the following eight technical and policy issues pertaining to the RTNSS for passive advanced light-water reactors (ALWRs):

- A. RTNSS
- B. Definition of passive failure
- C. Safe shutdown requirements
- D. Control room habitability
- E. Reliability assurance program
- F. Station blackout
- G. Electric distribution
- H. Inservice testing of pumps and valves

In the SRM of June 30, 1994, the Commission (1) approved the staff recommendations for Items F and G, (2) approved the staff recommendations for Items A, B, and C but added comments, (3) disapproved the operational reliability assurance program (O-RAP) requirements but approved the design reliability assurance program (D-RAP) approach for Item E, and (4) deferred decisions on Items D and H by instructing the staff to clarify the recommendations.

CONTACT:
David T. Tang, NRR
415-1147

NOTE: TO BE MADE PUBLICLY AVAILABLE
WHEN THE FINAL SRM IS MADE
AVAILABLE

DISCUSSIONS:

Under Item A, the SRM of June 30, 1994, noted Chairman Selin's comment that "the licensees should use the complete plant probabilistic risk assessment (PRA) as opposed to the 'focused PRA' to provide an integrated assessment of the relative importance of various systems and components." Whether to use the complete plant PRA or the focused PRA has broadbase implications for the RTNSS. Because resolving the issue may help the staff clarify its RTNSS philosophy, the staff chose to respond to Chairman Selin's comment in a separate memorandum, "Staff Requirements Memorandum Dated June 30, 1994, on Regulatory Treatment of Non-Safety Systems," which was issued on October 21, 1994.

The staff's resolutions of the other questions raised in the SRM are contained in Attachments 1 and 2. Since the Commission, with all Commissioners agreeing, has approved the staff's recommendations on Items F and G, the staff's discussions and recommendations on these two items in SECY-94-084 remain intact and are not incorporated into the attachments to this paper. Attachment 1, therefore, provides the staff's detailed responses to the SRM for Items B, C, D, E, H, and the part of Item A regarding the graded-safety classification and requirements for instrumentation and control (I&C) systems. Attachment 2 contains the revised text for Items A, D, E, and H in SECY-94-084. The text reflects the revised or clarified staff positions of which the staff is seeking the Commission's approval.

On Item A (RTNSS), in Attachment 1, the staff addresses the Commission's instruction to accommodate the comments in Westinghouse letter NTD-NRC-94-4145 on the graded-safety classifications and requirements for I&C systems. The corresponding text clarification is included in Attachment 2. The staff also clarifies its position on Step 6, "Regulatory Oversight Evaluation," of the RTNSS process by stating that the sentence, "After the designer has completed these or related activities, the staff will apply appropriate regulatory oversight," was not intended to be an open-ended process. To avoid confusion, the staff modified, in Attachment 2, the applicable text by removing the words "or related" from the sentence.

On Item B (definition of passive failure), in Attachment 1, the staff addresses Commissioner de Planque's cautionary concern that a design that considers active failures may overall be less reliable.

On Item C (safe-shutdown requirements), the staff states in Attachment 1 that it will be receptive during design-specific review to technically justified arguments regarding the requirements to ensure passive residual heat removal (RHR) system capability for long-term safe shutdown.

On Item D (control room habitability), in Attachment 1, the staff describes the basis of and conduct of periodic pressurization surveillance tests for the control room and notes that the tests need not last 72 hours. In Attachment 2, the staff modified the original SECY-94-084 discussion to clarify this issue. The Commission instructed the staff to discuss this issue

with the applicant at greater length to resolve whether the leaktightness of the control room should be tested at every reload outage. The staff forwarded to and discussed with Westinghouse a draft of these clarifications. The staff believes that the discussion in Attachment 1 and revision in Attachment 2 have addressed the latest Westinghouse comments contained in its October 31, 1994, letter (Attachment 3) and have resolved the control room habitability issues.

On Item E (reliability assurance program), the SRM approved a design reliability assurance program (D-RAP) subject to resolution of the recommendation by the Office of the General Counsel (OGC) to implement the D-RAP using the inspections, tests, analyses, and acceptance criteria (ITAAC) process. The SRM disapproved the staff's proposal that an operational reliability assurance program (O-RAP) be continued for the life of the combined license (COL). In response to the instructions of the SRM, the staff modified SECY-94-084 to: 1) revise the statement of purpose of the reliability assurance program; 2) require the use of the maintenance rule methodology for performance monitoring so that industry design reliability assumptions are not translated into new regulatory requirements; 3) require the D-RAP to be verified using the ITAAC process; 4) remove the requirement that a separate O-RAP exist for the life of the plant; and 5) incorporate the objective of the O-RAP into existing programs. These clarifications are reflected in the revised text of SECY-94-084 in Attachment 2.

In accordance with the SRM, the staff has determined that most of the objectives of the O-RAP can be encompassed by programs established in order to implement existing requirements, such as the maintenance rule (10 CFR Part 50.65) or the Commission's quality assurance criteria (10 CFR Part 50, Appendix B). Failures caused by design errors or operational errors that degrade non-safety, risk-significant SSCs, however, are outside the scope of existing requirements. Design and operational reliability assurance activities for such SSCs is a relatively small part of the operations-phase reliability assurance activities, and does not warrant expanding the existing regulatory framework. While the staff does not propose to expand the scope of existing requirements, the staff proposes establishing a COL action item for these SSCs, as was included as a COL information item in the design control documents for the evolutionary designs (ABWR and System 80+). Such a COL action item would not establish a requirement, but would identify this matter as one that needs to be addressed by an applicant or licensee that references a design certification.

On Item H (inservice testing of pumps and valves), the SRM requested the staff to clarify two provisions pertaining to valve testing: (1) check valve testing in both forward- and reverse-flow directions and (2) periodic testing of safety-related valves such as blowdown valves at design-basis conditions. On check valve testing, the staff concluded that performance testing in both the forward- and reverse-flow directions is necessary to adequately assess the valve performance but noted that the non-safety direction test need not be as rigorous as the safety direction tests. On periodic testing of safety-related valves at design-basis conditions, the staff's position is that the frequency of this periodic verification of design capability should be based on the

safety importance of each valve, as well as on its maintenance and performance history. The test frequency and conditions should be sufficient to demonstrate continuing design-basis capability, but should not decrease the overall quality and safety of the plant. Further, the staff agrees with the Commission that design configuration changes to accommodate code-required quarterly testing should be done only if the benefits of the test outweigh the potential risk. The staff's detailed clarifications of these two provisions are included in Attachment 1. The text revisions for this item are in Attachment 2.

CONCLUSIONS:

The staff requests that the Commission approve the revised staff positions for the issues pertaining to Item D (control room habitability), Item E (reliability assurance program), and Item H (inservice testing of pumps and valves). These revisions, in conjunction with the resolution of the issue of focused PRA, which has been addressed in a separate memorandum, will enable the staff to review the passive ALWR designs more effectively.

COORDINATION:

OGC has reviewed this paper and has no legal objection. OGC notes that Commission approval would be tentative and subject to further review in design certification rulemakings and that communications with vendors and Electric Power Research Institute 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 on September 7, 1993, in a letter to the Chairman dated November 10, 1993. The staff responded to those comments in its letter to the ACRS dated February 2, 1994. Those responses were reflected in the positions contained in SECY-94-084.

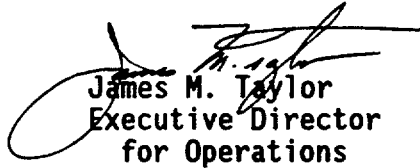
The ACRS provided additional comments on RAP in the letter dated February 17, 1994. In its letter to the ACRS, dated April 14, 1994, the staff discussed the integration of RAP into the implementation of existing programs. Those discussions have since been clarified further, and the revised staff positions on RAP are reflected in Attachment 2. An advance copy of the revised paper was forwarded to the ACRS on May 2, 1995. The staff has been asked by the ACRS to present the changes to the draft paper during the June meeting. The ACRS has indicated that the briefing is for their information only and they do not expect to write a letter following the briefing.

RECOMMENDATIONS:

The staff recommends that the Commission

- (1) Approve the positions underlined in Attachment 2.

- (2) Note that the staff will make the attachments available to the public no sooner than 3 working days after this paper is forwarded to the Commission.


James M. Taylor
Executive Director
for Operations

Attachments:

1. Response to SRM on
SECY-94-084
2. Policy Issues Analysis
and Recommendations
for Passive Plants
3. Westinghouse Comments, NTD-NRC-94-4333
on Control Room Habitability

Commissioners' comments or consent should be provided directly to the Office of the Secretary by COB Wednesday, June 7, 1995.

Commission Staff Office comments, if any, should be submitted to the Commissioners NLT Wednesday, May 31, 1995, 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
EDO
SECY

Responses to Staff Requirements Memorandum (SRM) on SECY-94-084

Item A Regulatory Treatment of Non-Safety Systems (RTNSS)

The staff has responded to Chairman Selin's comment on the use of "focused PRA" in a memorandum dated October 21, 1994. The staff's response to the first part of the SRM regarding the comments in Westinghouse letter NTD-NRC-94-4145 follows.

SRM Comment. The Commission (with all Commissioners agreeing) has approved the staff's recommendation on RTNSS. However, the Westinghouse comments on this item, as stated in the attachment to NTD-NRC-94-4145, should be accommodated.

Staff Response. In its review of the AP600 design, the staff will accommodate the following Westinghouse comments on RTNSS, stated in the attachment to NTD-NRC-94-4145:

On page 6 (SECY-94-084), Item 5 specifies that the designer should establish graded safety classifications and graded requirements for I&C systems based on the importance to safety of their functional reliability/availability (R/A) missions. The purpose of the RTNSS process is to develop regulatory oversight for non-safety-related systems, structures, and components (SSCs), including I&C systems. It is unnecessary and inconsistent to specify this type of requirement for I&C systems. The resulting regulatory oversight specified by the RTNSS results includes the establishment of appropriate safety classifications.

At the conclusion of Item 6 on page 7 (SECY-94-084), the SECY states that "after the designer has completed these or related activities, the staff will apply appropriate regulatory oversight." The process outlined in the paper represents the complete process as agreed to by the industry and the staff. Without the identification of specific "related activities," this statement allows the process to remain open-ended.

The staff intends to consider the functional R/A missions in its review of non-safety-related systems identified as important by the RTNSS process, including I&C systems, for passive plant designs. Accordingly, in Attachment 2, the staff replaces the words "I&C systems" with "SSCs" and made corresponding editorial changes in Paragraph II.5 of Item A in SECY-94-084. As a matter of clarification, in reviewing non-safety-related systems identified as important by the RTNSS process, the staff will consider graded requirements for assurance of functionality, performance, reliability, environmental durability, and quality assurance (QA) and quality control consistent with the importance to safety of the system identified by the RTNSS process. The staff will work with Westinghouse to determine proper classification of systems during its AP600 review.

With regard to the statement in the conclusion of Item 6 on page 7 that "after the designer has completed these or related activities, the staff will apply appropriate regulatory oversight," the phrase "related activities" is not intended to allow the process to be open-ended. The related activities are not specified, but are meant to include any activities, other than those identified in Item 6, that the designer may perform related to the regulatory oversight. To avoid confusion, however, the staff will remove the words "or related" from the sentence.

Item B Definition of Passive Failure

SRM Comment. The Commission (with all Commissioners agreeing) has approved the staff's recommendation on this item. Commissioner de Planque cautioned that in some situations, a design that considers such failures may overall be less reliable (due to added complexity, new failure modes) than one where the valve is treated as passive.

Staff Response. The staff believes that treating the check valves as active components subject to single active failure considerations will in general enhance overall system reliability. However, the staff recognizes that a change in the treatment of check valve single failure may make the system more complex and possibly even introduce new failure modes. For this reason, the staff will carefully review the specifics of the system design (including check valve arrangement) to ensure that overall system functional reliability is not degraded by treating valves as active components subject to single failure consideration. As discussed in SECY-94-084, check valves whose proper function can be demonstrated and documented may still be categorized as passive components. No change to staff position is required.

Item C Safe Shutdown Requirements

SRM Comment. The Commission (with all Commissioners agreeing) has approved the staff's recommendation on this item. With respect to the 72-hour capacity of the passive residual heat removal (RHR) system water pool, the requirements for replenishing the water in the pool should be based on design-specific attributes and that the applicant's justification of these requirements should not be based solely on the 72-hour criterion of the utility requirement document (URD). The staff should be receptive to arguments for longer periods, if technically justified.

Staff Response. The objective of replenishing the passive RHR system water pool, whether by supporting systems or other means, is to ensure capability of the passive RHR system to maintain a long-term safe shutdown. Specific requirements regarding the water pool replenishment will be based on design-specific attributes. No requirement with respect to the supporting systems to replenish the water pool will be imposed if the plant is designed so that sufficient

pool water can be maintained for long-term operation of the passive RHR system without being replenished by support systems. For example, a plant may be designed to maintain the pool water through a closed-loop operation in which the steam from boiloff of the pool water is condensed and the condensate is returned to the water pool. During design-specific reviews, the staff will be receptive to technically justified arguments with regard to the requirements to ensure passive RHR system capability for long-term safe shutdown. No change to staff position is required.

Item D Control Room Habitability

SRM Comment. The Commission (with all Commissioners agreeing) has decided to defer decision on this issue until the staff and the applicant can discuss at greater length to resolve whether to require testing of the leaktightness of the control room at every reload outage. When the staff returns with a recommendation, it should also address whether, and if so, how the control room should be manned during the 72-hour testing proposed for each refueling outage.

Staff Response. Control room habitability has been a longstanding issue for operating reactors and is the subject of Generic Issue 83. Generic Issue 83, in part, concerns control room integrity and the ability of the safety-related ventilation systems to maintain a positive pressure in the control room. The staff's position for passive advanced light-water reactors (ALWRs) is that the leaktightness of the control room should be tested at every refueling outage. This is consistent with the Standard Review Plan (SRP) guidance and current Westinghouse Standard Technical Specifications. Testing is necessary at every refueling outage because small breaches in the control room envelope due to maintenance can easily result in leakages in excess of the makeup capability. Operating reactors typically have leakage rates of hundreds of standard cubic feet per minute (scfm). The small leakage rates proposed for the passive ALWRs (<20 scfm) will require diligent maintenance practices.

The SRP guidance for ventilation systems that will pressurize the control room during a radiation emergency distinguishes between three categories of systems: systems having pressurization rates of (1) greater than or equal to 0.5 volume changes per hour, (2) less than 0.5 and greater than or equal to 0.25 volume changes per hour, and (3) less than 0.25 volume changes per hour. The guidance states that, for systems in the second and third categories, the planned leaktight design features should be analyzed to ensure that the design makeup air flow can maintain 1/8-inch water gauge differential. For systems in the third category, tests should be performed every 18 months to verify that the makeup rate is within ± 10 percent of the design rate and that the control room can be pressurized to at least 1/8-inch water gauge relative to all surrounding air spaces while makeup air is applied at the design rate.

The Westinghouse AP600 main control room envelope is smaller than current LWRs (40,000 ft³ versus 100,000 ft³). The AP600 emergency habitability system consists of pressurized air bottles and has a pressurization rate of less than 0.03 volume changes per hour. Westinghouse has stated that by isolating the non-safety-related ventilation system from the main control room envelop, a significant source of leakage, the ventilation ductwork, is eliminated.

The staff's position is that the pressurization tests for passive ALWR control rooms should be performed using the safety-related pressurized air bottles, although the staff would consider other testing methods proposed by a COL applicant. The tests would not need to last 72 hours, only long enough to demonstrate that the main control room envelope can be maintained at a positive 1/8-inch water gauge relative to all surrounding air spaces while makeup air is applied at $\pm$ 10 percent of the design rate. The control room leakage rate must be within the design capacity of the safety-related air bottles to pressurize the control room for 72 hours. As with current plants, the test only pressurizes the main control room envelope to 1/8-inch water gauge, so the main control room would be manned as usual and access to the control room need not be restricted during the test.

In addition to the pressurization tests performed at every refueling outage, the staff expects that an initial test using the safety-related air bottles will be conducted as part of the ITAAC as proposed by industry. This test would establish that the air bottles are capable of maintaining the required positive pressure in the control room for 72 hours. As with the refueling outage surveillance, the test only pressurizes the main control room envelope to 1/8-inch water gauge, so the main control room would be manned as usual and access to the control room need not be restricted during the test.

The staff has discussed this clarification with Westinghouse as part of the review of the AP600 and believes that this clarification resolves the concerns of the Commission and the industry on control room habitability. The staff requests that the Commission approve the proposed staff positions as underlined in Attachment 2.

Item E Reliability Assurance Program

SRM Comment. The SRM approved a design reliability assurance program (D-RAP) subject to resolution of the OGC recommendation to implement the D-RAP using the ITAAC process. It disapproved the staff's proposal that an operational reliability assurance program (O-RAP) be continued for the life of the COL license. The SRM further stated that (1) the staff should modify the statement of purpose of the reliability assurance program, (2) the staff should consider how it will monitor licensees' reliability assurance efforts without effectively translating industry design reliability assumptions into new regulatory requirements that result in core damage frequency and

conditional containment failure probability values that are lower than the subsidiary objectives approved by the Commission, (3) the D-RAP should be implemented using the ITAAC process, and (4) the staff should ensure that the objective of the O-RAP is incorporated into existing programs for maintenance or quality assurance.

SRM Response. As presented in Attachment 2 to this paper, the text of the SECY-94-084 has been modified to incorporate the Commission's changes to the statement of purpose of the reliability assurance program and to require the use of the maintenance rule methodology for performance monitoring so that industry design reliability assumptions are not translated into new regulatory requirements. The staff resolved the D-RAP applicable regulation and implementation recommendations with OGC by requiring, as part of design certification rulemaking, the D-RAP to be verified using the ITAAC process.

The staff removed the requirement that a separate O-RAP exist for the life of the plant. Operations-phase reliability assurance activities will be incorporated into existing programs. For structures, systems, and components (SSCs) that are within the scope of the maintenance rule, the maintenance program is sufficient to address reliability assurance concerns for risk-significant SSCs that have maintenance-preventable functional failures. For safety-related SSCs that have reliability concerns caused by design or operations problems, the 10 CFR Part 50, Appendix B quality assurance program adequately addresses reliability assurance program objectives. Non-safety-related, risk-significant SSCs that have reliability concerns caused by design or operations-related problems are outside the scope of the existing maintenance and quality assurance regulatory framework. The staff established a COL action item for the evolutionary designs to address this "gap," and will evaluate this approach for the passive designs. Although the staff recognizes that this approach does not have the legal enforceability of an additional rule-making, the staff considers the gap to be a relatively small part of the operations-phase reliability assurance activities, and does not warrant expanding the existing regulatory framework to encompass this gap. In addition, as discussed in an NEI letter dated April 22, 1994, revisions to the industry guidance document for the maintenance rule or an industry guidance document regarding the maintenance and use of PRA for advanced reactors would ensure that the appropriate objectives of the reliability assurance program were met for the operations-phase of the plant life cycle. The modified text of SECY-94-084 on the RAP is given in Attachment 2.

Item F Station Blackout

The Commission has approved the staff's recommendation in SECY-94-084 on this item.

Item G Electric Distribution

The Commission has approved the staff's recommendation in SECY-94-084 on this item.

Item H Inservice Testing of Pumps and Valves

SRM Comment. The Commission (with all Commissioners agreeing) has deferred a decision on this issue, requesting the staff to clarify two provisions pertaining to valve testing: (1) check valve testing in both forward- and reverse-flow directions and (2) periodic testing of safety-related valves such as blowdown valves at design-basis conditions.

Staff Response. On check valve testing in both forward- and reversed-flow directions, the staff notes that Section XI of the American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code (ASME Code) requires that check valves be exercised in the positions in which they perform their safety function. This requirement assumes that the valve will be capable of moving to the position required to perform the safety function. The ASME/American National Standards Institute (ANSI) Part 22 of Operations and Maintenance (O&M-22) Committee indicated that utilities generally only perform bidirectional testing (forward- and reverse-flow direction) for valves that have safety functions in both the open and closed directions. The Oak Ridge National Laboratory recently studied check valve performance. The findings, presented in NUREG/CP-0123, Supplement 1, indicated that testing of check valves, as it has been done by the industry, may not always detect check valve failures. For example, a test of a check valve with a safety function in the open direction only may verify that the check valve will pass the required system flow, but may not detect a severely worn hinge pin or a missing obturator. Although the safety function may be in the open direction only, assuring disk integrity prevents a dislodged disk from damaging other safety equipment downstream of the check valve. Performance testing in the reverse-flow direction ensures that the check valve disk is intact, regardless of whether the check valve has a safety function in the reverse-flow direction (e.g., leaktightness or ability to prevent reverse flow). Similarly, a test of a valve with a safety function in the closed direction only may not detect a condition in which the hinge pin is severely worn and the disk is simply stuck to its seat. A test in the open direction would increase the likelihood of detecting degradation or failure of valve internals. The O&M-22 Committee has been working on changes in ASME guidance for valve exercising to improve check valve performance, and is expected to establish the requirements as follows. Valves should be performance tested in both the forward- and reverse-flow directions. However, the non-safety direction test need not be as rigorous as the safety direction test. Further, valve obturator movement may be verified by observing a direct indicator (e.g., a position-indicating device) or by other positive means including nonintrusive test methods.

Therefore, the staff recommends that, to the extent practicable, the passive system design should incorporate provisions to permit all critical check valves to be tested for performance in both forward- and reverse-flow directions but that the demonstration of the non-safety direction test need not be as rigorous as the corresponding safety direction test.

On periodic verification of safety-related valves design-basis capability, the staff notes that the NRC regulations require that valves important to safety be designed, fabricated, erected, tested, and maintained to quality standards commensurate with the importance of the safety functions they must perform. Design qualification testing before installation will ensure that the valve will operate as intended under its design-basis conditions. Testing before start up will verify the performance of the valve in the as-installed configuration. Periodic inservice testing is necessary to detect age-related degradation and to verify that the valve's capability to function under design-basis conditions is maintained.

For safety-related power-operated valves including motor-operated valves (MOV's), periodic inservice testing is expected to include the ASME Code, Section XI quarterly testing and periodic design-basis capability verification testing similar to that recommended for MOV's in Generic Letter (GL) 89-10, "Safety-Related Motor-Operated Valve Testing and Surveillance." As discussed in Item 2 of Item H of SECY-94-084, the 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. 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 the Code-required quarterly testing. The staff agrees with the Commission that design configurations to accommodate Code-required quarterly testing should be done only if the benefits of the test outweigh the potential risk (e.g., the effect of a more complex design configuration on system reliability). Therefore, in SECY-94-084 the staff recommended that, to the extent practicable, the passive ALWR piping systems should be designed to accommodate the applicable Code-required quarterly testing of valves.

Periodic valve testing at design-basis conditions is necessary to verify that the valve's capability to function under design-basis conditions is maintained. Re-verifying the design-basis capability may also be needed after repairs, maintenance, and modifications. The staff recognizes that in situ testing at design-basis conditions might not be practicable in all cases. The staff will consider static or reduced-flow periodic testing with diagnostic systems combined with analysis where design-basis testing is not practicable. Further, the frequency of this periodic verification of design-basis capability

should be based on the safety importance of each valve, as well as on its maintenance and performance history. The frequency and test conditions should be sufficient to demonstrate continuing design-basis and required operating capability, but should not decrease the overall quality and safety of the plant. This staff position applies to all safety-related power-operated valves, including MOVs. In the SRM of June 26, 1990, on SECY-90-016, "Evolutionary Light Water Reactor (LWR) Certification Issues and Their Relationship to Current Regulatory Requirements," the Commission approved the staff's position on MOV testing at design-basis condition.

For the blowdown valves discussed in the SRM of June 30, 1994, the staff will require that a qualification test be performed under a range of differential pressure and flow conditions up to design-basis conditions before installation. Testing after installation, including periodic verification testing, may be performed under various differential pressures and flows up to maximum achievable conditions.

In some cases, a system's configuration might make design-basis tests impracticable. By using the results of the qualification test as baseline data, the results of testing under in situ or installed conditions can be extrapolated to demonstrate the capability of the blowdown valve to operate under design-basis conditions.

In addition to testing before and upon installation, the staff recommends that the Commission approve the staff's proposal to require periodic testing of safety-related valves during the life of the plant to verify that their capability to function under design-basis conditions is maintained.

Policy Issues Analysis and Recommendations for Passive Plants

On the basis of the staff's responses to the staff requirements memorandum (SRM), in Attachment 1 to this paper, only the text for three items in SECY-94-084, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs," need be revised for Commission's review and approval: Item D (control room habitability), Item E (reliability assurance program), and Item H (inservice testing of pumps and valves). As discussed in Attachment 1, the staff made minor revisions to clarify the Item A (RTNSS) text of SECY-94-084, including editorial changes to remove reference to the operational reliability assurance program.

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 (ALWR) 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 operations-phase reliability assurance activities 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 requirements for SSCs based on the importance to safety of their functional R/A missions.

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), results of systems interaction studies, 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.
- 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 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 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.

D. Control Room Habitability

General Design Criterion (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. SRP Section 6.4, "Control Room Habitability Systems," defines 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). In current plants, safety-grade, filtered control room heating, ventilation, and air conditioning (HVAC) systems with charcoal absorbers are used to ensure that radiation doses to operators will be maintained within the GDC 19 limits in the event of an accident.

Originally, Electric Power Research Institute (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 (DBAs). 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 a safety-grade pressurization system for the control room envelope which 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 Section 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 Section 6.4, Revision 2.

To meet the applicable provisions of GDC 4 and 19, both the AP600 and Simplified Boiling Water Reactor (SBWR) passive designs provide a safety-related pressurization system to maintain at least 1/8-inch water gauge positive differential pressure relative to all surrounding areas. The AP600 and SBWR designs also claim that unfiltered leakage into the control room envelope will be restricted to 0.3 and 0.5 cubic feet per minute, respectively. The vendor specific reviews will be based on the guidelines of SRP Section 6.4 and experience obtained from the operating plants concerning (1) the provisions for maintaining and periodically testing for leaktightness to maintain at least 1/8-inch water gauge positive pressure relative to all surrounding areas, (2) the adequacy of the engineered safety feature (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 keep equipment operable, and (4) protection against the effects of accidental release of toxic gases and smoke that could be drawn into the control room pressure boundary.

Each of the passive ALWR designs has a non-safety ventilation system for the control room envelope. The system would be switched to a recirculation mode with filtered makeup on a 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 may not be

available for maintaining control room habitability during a postulated DBA. Therefore, the amount of credit that can be taken for the non-safety system in the safety analysis for design-basis accidents will be determined as part of the regulatory treatment of non-safety systems process as discussed in Section A of this paper.

The SRP guidance for ventilation systems that will pressurize the control room during a radiation emergency distinguishes between three categories of systems: systems having pressurization rates of (1) greater than or equal to 0.5 volume changes per hour, (2) less than 0.5 and greater than or equal to 0.25 volume changes per hour, and (3) less than 0.25 volume changes per hour. The guidance states that, for systems in the second and third categories, the planned leaktight design features should be analyzed to ensure that the design makeup air flow can maintain 1/8-inch water gauge differential. For systems in the third category, tests should be performed every 18 months to verify that the makeup rate is within ± 10 percent of the design rate and that the control room can be pressurized to at least 1/8-inch water gauge relative to all surrounding air spaces while makeup air is applied at the design rate.

The staff's position is that the pressurization tests for passive ALWR control rooms should be performed every refueling outage using the safety-related pressurized air bottles, although the staff would consider other testing methods proposed by a COL applicant. The tests would not need to last 72 hours, only long enough to demonstrate that the main control room envelope can be maintained at a positive 1/8-inch water gauge relative to all surrounding air spaces while makeup air is applied at ± 10 percent of the design rate. The control room leakage rate must be within the design capacity of the safety-related systems to pressurize the control room for 72 hours. As with current plants, the test only pressurizes the main control room envelope to 1/8-inch water gauge, so the main control room would be manned as usual and access to the control room need not be restricted during the test.

In addition to the pressurization tests performed at every refueling outage, an initial test using the safety-related air bottles will be conducted as part of the ITAAC as proposed by industry. This test would establish that the air bottles are capable of maintaining the required positive pressure in the control room envelope for 72 hours. As with the refueling outage surveillance, the test only pressurizes the main control room to 1/8-inch water gauge, so the main control room would be manned as usual and access to the control room need not be restricted during the test.

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 ESF ventilation systems unless the licensee cannot meet the dose criteria associated with the 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 passive safety-grade pressurization system, such as a bottled air system, may not preclude the need for other safety-grade 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.
- An initial test using the safety-related air bottles will be conducted as part of the ITAAC, as proposed by industry. This would establish that the air bottles are capable of maintaining the required positive pressure in the control room for 72 hours.
- At least once each refueling cycle, the licensee must perform pressurization tests to demonstrate that the control room can be pressurized for a 72-hour period. The pressurization tests for passive ALWR control rooms should be performed using the safety-related pressurized air bottles or other approved testing methods. The tests would not need to last 72 hours, only long enough to establish that the safety-related air system can pressurize the main control room envelope to 1/8-inch water gauge with respect to the surrounding spaces. The control room leakage rate must be within the design capacity of the safety-related air bottles to pressurize the control room for 72 hours.
- The regulatory treatment of the portable air supply and the non-safety-grade ventilation system will be in accordance with the staff's position on the regulatory treatment of non-safety systems process as described in Section A of this paper.
- The staff is continuing to discuss with industry the number of people in control room that can be supported for 72 hours by the safety-related air bottles.

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 said 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 in evaluating this issue and that the ACRS may make additional recommendations after the staff has completed its evaluation. As committed to in the October 29, 1992, response to the ACRS, the staff has considered the ACRS comments in finalizing its position on this issue. Further discussions with the ACRS regarding the passive control room habitability systems will be conducted during the vendor-specific reviews.

The staff will evaluate the feasibility and the capability of the proposed pressurization systems on a vendor-specific basis. The staff will review the designs for control room habitability, including the refueling outage pressurization surveillance tests as discussed above, to ensure that the requirements in GDC 19 and guidelines in SRP Section 6.4 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 is acceptable. The proposed design would use bottled air to keep operator doses within the limits of GDC 19 and Section 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 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 and periodic surveillance tests, the capability of the 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 on the regulatory treatment of non-safety systems process 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 informed the advanced light water reactor (ALWR) vendors and EPRI that it was considering this matter in November 1988.

The advanced reactor (including ALWR) RAP would apply to those plant SSCs that are risk-significant (or significant contributors to plant safety) as determined by using a combination of 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 advanced reactor is designed, constructed, and operated in a manner that is consistent with the assumptions and risk insights for these risk-significant SSCs, (2) the risk-significant SSCs do not degrade to an unacceptable level during plant operations, (3) the frequency of transients that challenge advanced reactor SSCs are minimized, and (4) these SSCs function reliably when challenged.

The staff considers the RAP for advanced reactors to have two stages. The first stage applies prior to initial fuel load, and is referred to as the design reliability assurance program (D-RAP). The D-RAP can be divided into the design certification phase, the COL application phase, and the COL holder phase. An applicant for design certification would be required, by the D-RAP

applicable regulation, 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 and identify and prioritize the risk-significant SSCs as required by the D-RAP applicable regulation. Once the site-specific D-RAP has been established and the risk-significant SSCs identified and prioritized, the procurement, fabrication, construction, and preoperational testing would be implemented in accordance with the COL holder's D-RAP or other programs and would be verified using the ITAAC process.

The second stage applies to reliability assurance activities for the operations phase of the plant life cycle. These activities can be integrated into existing programs (e.g., maintenance, surveillance testing, inservice inspection, inservice testing, and quality assurance). Reliability performance goals for risk-significant SSCs would be established consistent with the existing maintenance and quality assurance processes on the basis of information from the D-RAP. The COL applicant would establish performance and condition monitoring requirements to provide reasonable assurance that risk-significant SSCs do not degrade to an unacceptable level during plant operations. The reliability performance monitoring does not need to statistically verify the numerical values used in the PRA. It would provide a feedback mechanism for periodically reevaluating risk significance on the basis of actual equipment, train, or system performance. Most of the reliability assurance activities could be incorporated into 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. The non-safety-related SSCs included in the maintenance rule are those that are: (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 remaining activities could be incorporated into the quality assurance program developed to implement 10 CFR Part 50, Appendix B.

The staff and the ACRS discussed the form and content of the advanced reactor reliability assurance program. 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 stated that the staff should issue consistent guidance on the elements of an acceptable program that will satisfy these three sets of requirements. In the April 14, 1994, letter addressing the ACRS comments, the staff stated that the objective of the RAP during the operations phase of plant life cycle is to provide reasonable assurance that the reliability and availability of SSCs are maintained commensurate with their risk significance. With the exception of reliability assurance related to design or operation of risk-significant, non-safety-related SSCs, this objective can be accomplished within the existing maintenance rule and Appendix B quality assurance regulatory requirements.

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 objective of reliability assurance for monitoring and correcting degradation in SSC reliability or availability associated with maintenance. SSCs that are risk-significant are given special treatment during implementation of the maintenance rule. They may either be monitored against specific goals or be subject to preventive maintenance that assures acceptable performance and requires root cause analysis and corrective action for failure to meet performance criteria. On the basis of 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 SSCs will include consideration of overall SSC availability. If failure of an SSC 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, risk-significant SSCs are caused by design deficiencies or operational errors other than maintenance, the 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 quality assurance programs, would meet the objective of the RAP during plant operation for risk-significant, safety-related SSCs. Maintenance preventable failures for non-safety-related SSCs would also be evaluated and corrected pursuant to the maintenance rule. Failures determined to be caused by design errors or operational errors that degrade non-safety-related, risk-significant SSCs are outside the scope of the existing maintenance and quality assurance regulatory framework. The COL applicant will propose a method by which it will incorporate the objectives of the reliability assurance program into other programs for design or operational errors that degrade non-safety-related, risk-significant SSCs.

Applicable Regulation for D-RAP

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 that certified design.

Specifically, in the final safety evaluation reports, NUREG-1462 for the System 80+ and NUREG-1503 for the advanced boiling water reactor, the Commission approved the following applicable regulation for D-RAP:

An application for advanced reactor design certification or a combined license must contain: (1) the description of the reliability assurance program used during the design that includes, scope, purpose, and objectives; (2) the process used to evaluate and prioritize the structures, systems, and components in the design, based on their degree of risk significance; (3) a list of the structures, systems, and components designated as risk significant; and

(4) for those structures, systems, and components designated as risk significant: (i) a process to determine dominant failure modes that considered industry experience, analytical models, and applicable requirements; and (ii) key assumptions and risk insights from probabilistic, deterministic, or other methods that considered operations, maintenance, and monitoring activities.

Each licensee that references the advanced reactor design must implement the design reliability assurance program approved by the NRC.

The applicable regulation for D-RAP must be satisfied for the design certification, the COL application, and by the COL holder. The design certification D-RAP will be verified using the staff's safety evaluation review process. The COL applicant's D-RAP will be approved by the staff prior to granting a COL. The COL applicant's D-RAP should incorporate all aspects of reliability assurance that will be accomplished prior to fuel load (i.e., procurement, fabrication, construction, and preoperational testing phases). The D-RAP shall be verified using the inspections, tests, analyses, and acceptance criteria (ITAAC) process. 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) describe the methods used to 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 for the COL applicant's consideration in planning operations-phase reliability assurance activities. 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, fabrication, construction, and preoperational testing phases that will be completed prior to fuel load. The COL applicant would incorporate into the existing maintenance and QA programs operations-phase reliability assurance activities.

The COL applicant's D-RAP will 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 D-RAP with the ITAAC process as well as inspections and audits during detailed design, procurement, fabrication, construction, and preoperational testing prior to fuel load and would continue to inspect and audit implementation of the operations-phase reliability assurance activities for the duration of the license using the maintenance and quality assurance regulations (i.e., 10 CFR 50.65 and 10 CFR Part 50, Appendix B).

H. Inservice Testing of Pumps and Valves

In SECY-90-016, the staff recommended that the Commission approve the following four positions 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 MOVs 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.

In conducting its plant-specific reviews, the staff will consider 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 that 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 design, testing, and inspection provisions noted above 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 relies significantly on passive safety systems, but also depends on non-safety systems (which are traditionally safety-related systems in current light-water reactors) 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. Important non-safety-related components are not required to meet criteria similar to safety-grade criteria. However, the non-safety-related piping systems with functions that have been identified as being important by the RTNSS process should be designed to accommodate testing of pumps and valves to assure that the components meet their intended functions. Specific positions on the inservice testing requirements for those components will be determined as a part of the staff's review of plant-specific implementation of the regulatory treatment of non-safety systems for passive reactor designs.
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. The rules of OM 10 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. Furthermore, 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 practicable, the passive ALWR piping systems should be designed to accommodate the applicable Code requirements for the quarterly testing of valves. However, design configuration changes to accommodate Code-required quarterly testing should be done only if the benefits of the test outweigh the potential risk.
3. The passive system designs should incorporate provisions (1) to permit all critical check valves to be tested for performance, to the extent practicable, in both forward- and reverse-flow directions, although the demonstration of a non-safety direction test need not be as rigorous as the corresponding safety direction test, and (2) to verify the movement of

each check valve's obturator during inservice testing by observing a direct instrumentation indication of the valve position such as a position indicator or by using 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 initial startup, and periodically through a program being developed as a follow-on to GL 89-10. Similarly, to the extent practicable, the design of non-safety-related piping systems with functions under design-basis condition that have been identified as being important by the RTNSS process should incorporate provisions to test power-operated valves in the system to assure that the valves meet their intended functions under design-basis condition.
5. To the extent practicable, provisions should be incorporated in the design to assure that MOVs in safety-related systems 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 reviews the implementation of the regulatory treatment of non-safety systems.



Westinghouse
Electric Corporation

Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

NTD-NRC-94-4333
DCP/NRC0239
Docket No.: STN-52-003

October 31, 1994

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

ATTENTION: R. W. Borchardt

Subject: Westinghouse comments on the proposed revision to Control Room Habitability section of SECY-94-084, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-safety Systems in Passive Designs"

Reference: Letter from R. W. Borchardt to N. J. Liparulo dated October 4, 1994

Dear Mr. Borchardt:

This letter documents the October 27, 1994 telecon between NRC (Jim Lyons, Tom Kenyon, David Tang, and Janak Raval) and Westinghouse (Dan McDermott, Mark Wills, and Andrea Sterdis). The purpose of the telecon was to provide Westinghouse comments on the contents of the referenced letter.

The comments are as follows:

- The revised control room habitability discussion specifies a limitation of the required maximum leakage to less than 4 standard cubic feet per minute (SCFM) for the AP600 design. Although design calculations show that the control room envelope design should result in a leakage rate of less than 4 SCFM, a leakage rate of up to 20 SCFM is acceptable, provided the passive control room habitability system flow rate of 20 SCFM maintain a 1/8-inch water gauge differential pressure. Less specific references to determining leakage rates should also be revised to allow maintenance of pressure as an acceptable criteria. For example, the last bullet on page 3 of the revised SECY should be reworded as follows: "...The tests would not need to last 72-hours, only long enough to maintain pressurization or to measure leakage rate..."
- The first full paragraph on page 2 of the revised SECY compares the volume change per hour for the AP600 control room envelope to that of the Standard Review Plan (SRP) and current plant designs. This comparison is not totally appropriate since the AP600 design isolates the control room envelope with far less volume exchanges because the normal HVAC is isolated. This paragraph should be revised as we discussed.
- It is unnecessary to perform a 72-hour control room envelope pressurization test every ten years. By assuring the functionality of the control room pressurization function and the adequacy of the bottled air supply every refueling outage, the function of the passive control room habitability system is verified.

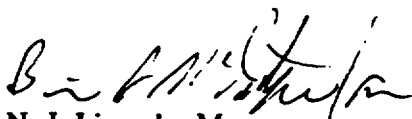
100016

ECOY 10
#

October 31, 1994

- The background discussion along with the revised SECY section state that a "COL licensee must demonstrate (1) the feasibility and capability of the safety-grade pressurization systems to satisfy GDC 19 criteria regarding control room habitability..." This statement should be revised since design certification of the passive control room habitability system will demonstrate the feasibility of the system to satisfy GDC 19.
- The background information and the revised SECY should be revised from "...the control room would be manned as usual and access to the control room would not be restricted during the test," to indicate that access to the control room need not be restricted. To perform the test, the COL holder may wish to limit control room ingress and egress.
- On page 2 of the SECY revision, the statement pertaining to staff reservations relative to control room staffing limitations is inappropriate. The adequacy of control room staffing levels will be confirmed during design certification.
- The first sentence on page 3 of the SECY revision (item 4) should be re-worded to state "protection against the effects of accidental release of toxic gases and smoke outside or drawn inside the control room pressure boundary."
- References to specific AP600 design valves, such as leakage rates and volume changes should be deleted from both the background discussion and the SECY revision.
- The background discussion and SECY revision should be re-worded to allow for 24-month refueling outages. This can be accomplished by indicating that the tests would be performed at each refueling outage rather than specifying an interval.

If you have any questions or require additional clarification, please contact Andrea Sterdis on (412) 374-5292.



N. J. Liparulo, Manager
Nuclear Safety Regulatory and Licensing Activities

/nja