May 17, 1991

Project No. 669

Mr. E. E. Kintner, Chairman
Advanced Light Water Reactor
Steering Committee
GPU Nuclear Corporation
100 Interpace Parkway
Parsippany, New Jersey 07054

Dear Mr. Kintner:

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION ON EPRI ADVANCED LIGHT WATER REACTOR (ALWR) REQUIREMENTS DOCUMENT FOR PASSIVE PLANT DESIGNS - SAFEGUARDS BRANCH (TAC NOS. 77866, 77869, 77870 AND M77872)

As a result of its review of Volume III of the EPRI ALWR Requirements Document, submitted by letter dated September 7, 1990, the staff has determined that it needs additional information in order to complete its review of the design criteria. The additional information is needed in order to address other areas covered during the Safeguards Branch review of Chapter 5, "Engineering Safety Systems," Chapter 8, "Plant Cooling Water Systems," Chapter 9, "Site Support Systems," and Chapter 11, "Electric Power Systems," as discussed in the enclosure to this letter. The Chapter 9 questions are in addition to those which were transmitted by letter dated April 3, 1991.

The reporting and/or recording requirements contained in this letter affect fewer than ten respondents; therefore, OMB clearance is not required under P.L. 96-511.

Please respond to this request within 60 days of the date of receipt of this letter. If you have any questions regarding this matter please contact the project managers, T. Kenyon or J. Wilson, at (301) 492-1118.

Sincerely,

Original Signed By:
James H. Wilson, Project Manager
Standardization Project Directorate
Division of Advanced Reactors
and Special Projects
Office of Nuclear Reactor Regulation

Enclosure:
As stated

cc w/enclosure:
See next page

DISTRIBUTION:
Central File
NRC PDR
PDST R/F
PShea
JHWilson
TBoyce
TKenyon

DOCUMENT NAME: CH9
EJordan, MNBB3701
OGC, 15B18
ACRS (10), P-315
DCrutchfield
WTravers
WMorris, NLS007
WHardin, NLS169
PMcKee, 9D24
BMendelsohn, 9D24
RRanieri

LA:PDST	PM:PDST	PM:PDST	PM:PDST	D:PDST
PShea	JHWilson:cm	TKenyon	TBoyce	CMiller
5/17/91	5/17/91	/91	5/17/91	5/17/91

0665

Prof #669 DF03

Mr. E. E. Kintner, Chairman
ALWR Utility Steering Committee

Project No. 669
EPRI

cc:

Mr. John Trotter
Nuclear Power Division
Electric Power Research Institute
Post Office Box 10412
Palo Alto, California 94303

Mr. Brian A. McIntyre, Manager
Advanced Plant Safety & Licensing
Westinghouse Electric Corporation
Energy Systems Business Unit
Post Office Box 355
Pittsburgh, Pennsylvania 15230

Mr. Joseph Quirk
GE Nuclear Energy
Mail Code 782
General Electric Company
175 Curtner Avenue
San Jose, California 95125

Mr. Stan Ritterbusch
Combustion Engineering
1000 Prospect Hill Road
Windsor, Connecticut 06095-0500

ENCLOSURE

REQUEST FOR ADDITIONAL INFORMATION
EPRI ALWR REQUIREMENTS DOCUMENT FOR PASSIVE PLANT DESIGNS
SAFEGUARDS BRANCH

Chapter 5

910.21 Section 2.2.13.1 requires the safety systems to be so designed that their safety functions will be not only automatically initiated but ensured of "successful completion of their safety functions independent of any operator control actions." However, passive decay heat removal (PDHR) system isolation provisions are required to permit operator response to inadvertent system actuation or to heat exchanger tube leaks (e.g., Sections 4.3.3.9, 4.3.3.10, and 5.3.3.1.1.) Spurious PDHR system isolation could interfere with completion of passive decay heat removal. Clarify what design measures would prevent the operators from stopping the completion of automatically initiated safety functions.

910.22 Define what is meant in Sections 1.2.1.1 and 4.2.3.1.1 by "single action valves." Are these non-modulating valves that have only open and shut positions or are they similar to squib-operated valves that once actuated cannot be repositioned?

910.23 Section 2.3.2 requires redundant components and features of safety features to be independent and separate except where physically impractical or less safe.

a) The fifth bullet states that barriers shall be designed to enhance resistance to sabotage. This could result in a door between two redundant safety components being a locked security door instead of a closed but unlocked fire door or unlocked but alarmed security door. Because of the potential for locked doors to delay access to safety equipment in an emergency, the NRC has not been encouraging locked doors that connect one vital area to another. Clarify that "less safe" includes unacceptable access delay in an emergency.

b) The sixth bullet specifies spatial separation for redundant components in the same raceways. Explain why spatial separation rather than a barrier is acceptable for these raceways.

910.24 Chapter 5, Section 2.2.6 of Volume III (passive) corresponds to Chapter 5, Section 2.2.5 of Volume II (evolutionary), except that "divisional separation" has been replaced with "separation of redundant components."

a) Is there any safeguards significance to this difference in wording?

b) The minimum number of individual actions (i.e., safety and non-safety component failures) that saboteurs would have to accomplish in order to create a beyond-design-basis plant condition can be taken as a rough measure of how good is the inherent sabotage protection of the design (assuming that containment is inaccessible to sabotage actions.) What is this measure of effectiveness expected to be for the passive designs? Is it expected to be the same or greater than for the evolutionary designs?

910.25 Section 5.3.3.1.2 requires the PWR PDHR air operated return line valves to fail in the open position on loss of air. The importance of protection of the DC power supply would be lessened if the PDHR system initiated on loss of DC power. Section 4.3.3.8 requires BWR PDHR actuation valves to fail open in the event of loss of control or motive power.

a) Discuss if there should be also a requirement for the PWR PDHR return line valves to fail open on loss of all DC power.

b) Discuss if there should be a similar requirement for the PWR passive containment cooling system to be actuated on loss of air or loss of DC power.

910.26 Section 4.3.3.4 specifies that the BWR PDHR pool and condensing heat exchanger "shall be located outside the primary containment but inside a structure adequate to provide the physical protection required for a safety-related system." Since the pool is vented to the atmosphere, a breach of a condenser tube (at full reactor pressure when the PDHR is not isolated from the RCS) could result in a LOCA outside containment. Discuss whether or not a BWR PDHR pool would be a credible sabotage target, and whether any additional requirements on its structure or vent are warranted to enhance its inherent resistance to sabotage or to improve the robustness of the design relative to threat assumptions.

910.27 Passive decay heat removal systems for the passive PWR include PDHR heat exchangers submerged in an in-containment refueling water storage tank (IRWST) which is open to containment atmosphere, and a passive containment cooling system (PCCS). The PCCS includes a steel containment shell within a concrete shield building and an airflow intake and chimney that provides for air cooling of the steel shell. Section 8.3.3.12 requires access ladders for inspection of air baffling and flow passages. Discuss whether access to the cooling air intakes and discharges and exterior of the steel containment shell would need to be protected against sabotage actions.

910.28 Section 3.4.9 requires the identification of critical valves which will require locking and/or control room position indication. NUREG-1267, "Technical Resolution of Generic Safety Issue A-29," states that the USI A-45 study report discussed means of disabling

redundant safety systems "without any obvious indication of system failure through casual observation. This fact is especially true for systems in standby mode that lack a status indicator in the control room. This type of system failure will not be detected until the system is called upon to perform a function or upon close examination." Locked valves can be defeated both accidentally by operators who carry out a procedure on the wrong valve, or by deliberate tampering. Discuss whether the plant designer should need to justify a decision to use a locked valve to assure correct alignment instead of control room indication of a misaligned valve.

Chapter 8

910.29 In its August 8, 1989 letter, EPRI agreed to add a requirement to Section 3.3.5 of Chapter 8 (for evolutionary ALWR) to ensure that maintenance access provisions for manually clearing debris from trash racks will be so coordinated with design of security barriers and intrusion detection systems that the maintenance access provisions do not provide a potential path for covert penetration from the water into the protected area. (This would only be applicable for sites at which the intake formed part of the protected area perimeter, which is required to be avoided if possible by Section 5.2.7 of Chapter 9.) We understand that this change will be included in a future revision of Volume II. Will the change also be made to Volume III?

Chapter 9

910.30 Although it may not be important that the policy statement reflects the performance requirements in Section 5, the staff suggests that EPRI modify the policy statement on protection against sabotage (Section 1.4.1) to include reference to the sabotage vulnerability analyses required by Section 5.2.2.1 of Chapter 9. This would improve consistency between the ALWR policy statement and the Commission's Severe Accident Policy Statement provision that:

> "The issues of both insider and outsider sabotage threats will be carefully analyzed and, to the extent practicable, will be emphasized in the design and in the operating procedures developed for new plants."

910.31 The first paragraph of Section 1.4.1 of Chapter 9 states that sabotage resistance is enhanced by "physically separated, redundant safety systems...." For the passive designs, should this say instead "physically separated, redundant non-safety auxiliary systems as well as safety systems...?"

910.32 The staff concludes that the introduction and organization of Section 5.1.3 of Chapter 9, titled "Design Bases," is confusing. Rather than stating that the "design basis assumptions and criteria shall meet the requirements of 10 CFR 73.55(a)(1)," make clear that the site security system must meet the requirements of 10 CFR 73.55(a)(1). The items in Section 5.1.3 that should be security system performance criteria (e.g., "security detection systems cannot be disabled without detection and timely response by the security force"), need to be distinguished from what should be assumptions used in the systems design and/or analysis (e.g., "insider threat is based on one knowledgeable individual without armament or explosives.")

910.33 Item 6 of Section 5.1.3 of Chapter 9 should be modified. It now states: "The continuous presence of several employees precludes acts of sabotage in the control room. However, the control room is a vital area and will be protected in accordance with 10 CFR Part 73.55." The staff accepts that protecting the control room in accordance with 10 CFR Part 73.55 would meet regulatory requirements, but disagrees with the assumption as stated. Certainly the presence of several employees would discourage insider sabotage, but it might not preclude insider sabotage and cannot be counted on to preclude outsider sabotage. Although the staff believes that adequate protection against insider sabotage results from security requirements that assure the trustworthiness of individuals granted unescorted access, additional protection against insider sabotage might result if plant designers give consideration, in the sabotage vulnerability analysis required by Section 5.2.2.1 of Chapter 9, to assuring that control room operators are aware of any maintenance activities or tampering with back panels in the control room that are out of their view.

910.34 Section 5.2.1.1 of Chapter 9 is identical in Volumes II and III. It includes in its definition of vital equipment reference to Section 2.1.3 of Chapter 5, for equipment necessary for core damage prevention. But in Volume II that reference includes only safety systems, while in Volume III it includes both safety and redundant non-safety systems. Discuss EPRI's rationale for these differences.

910.35 The rationale of the sixth "bullet" in Section 5.2.7 of Chapter 9 could be improved by revising it to read:

> "Unobstructed observation of an area interior to the intrusion detection system is required for adequate alarm assessment. Adequate coverage of the interior and exterior isolation zones is also necessary to meet the requirements of 10 CFR Part 73.55(c)(3)."

910.36 The third "bullet" in Section 5.2.4.1 of Chapter 9, which is unchanged from the same paragraph in Volume II, refers to location of and security for service water pumps. In Volume III, although the service water system is needed for both plant operation and safe shutdown using the non-safety auxiliary systems, it is not relied upon for safe shutdown by the passive safety related systems. Discuss why this requirement is appropriate for the passive plants, considering the importance but changed safety classification claimed for this system. (Section 5.2.7 of Chapter 9 would still discourage the service water cooling pond from intersecting the Protected area boundary.)

Chapter 11

910.37 10 CFR 73.55(e)(1) and (f)(4) and Generic Letter 87-08 specify that on-site secondary power supply systems for certain security equipment must be located in a vital area. Vital areas are in turn required to be located within a plant's protected area. Section 2.3.2 of Volume III, Chapter 11 identifies the security system as a permanent non-safety load. Section 2.3.4 requires the permanent non-safety loads to be supplied by either two redundant on-site non-safety standby power sources or one on-site standby source and one alternate standby source located in the vicinity of the plant.

a) Is a separate dedicated security diesel generator and uninterruptible power supply (UPS) to be provided in a vital area or will one or both of the standby sources (and batteries, inverters, switchgear, fuel, cooling, starting, control systems, etc.) be located in a vital area?

b) If only one standby source is on-site, discuss security power vulnerability to off-site actions during scheduled maintenance on the on-site supply. How would this compare to a site with a single dedicated security diesel generator on-site?

910.38 Generic Letter 87-08 states that the security secondary power supply "is to provide auxiliary power during power interruptions or outages. The duration of such interruptions or outages should be determined on a site-specific basis under station blackout conditions." What duration of battery power to security alarm annunciator and non-portable communications equipment would be required for the passive reactors?