Docket No. 52-003

October 13, 1992

Docket File

Mr. Nicholas J. Liparulo, Manager
Nuclear Safety and Regulatory Activities
Westinghouse Electric Corporation
Box 355
Pittsburgh, Pennsylvania 15230-0355

Dear Mr. Liparulo:

SUBJECT: WESTINGHOUSE COMMENTS ON DRAFT POLICY PAPER, "DESIGN CERTIFICATION AND LICENSING POLICY ISSUES PERTAINING TO PASSIVE AND EVOLUTIONARY ADVANCED LIGHT WATER REACTOR DESIGNS," JUNE 25, 1992, REFERENCE (NSRA-APSL-92-0171)

Thank you for your letter of September 17, 1992, to the Chairman, in which you presented your comments on the staff's positions presented in the subject draft policy paper. The staff will consider your comments before issuing a final Commission paper.

A significant portion of your comments concerned the staff's proposed position on the regulatory treatment of non-safety systems. The staff is devoting a significant number of technical resources to determine an acceptable level of reliability for passive safety systems. The level of reliability will be only one means to determine if passive safety systems alone will meet licensing design basis requirements. The staff is also concerned about the interaction of non-safety systems with passive safety systems, the necessity for subcooled heat removal capabilities, and the role of the operator in using non-safety systems.

The staff expects to issue the results of its technical review to determine an acceptable level of reliability for passive safety systems by January 1993. When these results are available, the staff will schedule a meeting with the Electric Power Research Institute to discuss its findings. Thank you for your comments on these complex and difficult issues.

Sincerely,

(Original signed by)
Dennis M. Crutchfield, Associate Director
for Advanced Reactors and License Renewal
Office of Nuclear Reactor Regulation

cc: See next page

DISTRIBUTION:
See next page

OFC:	SC:PDST:ADAR	LA:PDST:ADAR	SC:PDST:ADAR	D:PDST:ADAR	
NAME:	RHasselberg:tz	PShea	RBorchardt	RPierson	WTR
DATE:	10/7/92	10/7/92	10/7/92	10/9/92	10/9/92

OFC:	ADAR:NRR	
NAME:	DCrutchfield	
DATE:	10/12/92	

OFFICIAL RECORD COPY: DOCUMENT NAME: GT08097.RH

DISTRIBUTION:

Docket File	EDO #08097	TMurley/FMiraglia, 12G18
NRC PDR (w/inc)	JTaylor, 17G21	MTaylor, 17G21
JSniezek, 17G21	HThompson, 17G21	JBlaha, 17G21
WRussell, 12G18	JPartlow, 12G18	FGillespie, 12G18
MCase, 12E4	DCrutchfield	WTravers
RPierson	RBorchardt	FHasselberg
JMoore, 15B18	TKenyon	AThadani, 8E2
OPA	PShea, 08097	BToms, 08097
PMagnanelli, 08097	EBeckjord, RES	ELJordan, MNBB3701
OCA	PDST GT/F	NRR Mail Room, #08097 (w/inc)

cc: Mr. B. A. McIntyre
Advanced Plant Safety & Licensing
Westinghouse Electric Corporation
Energy Systems Business Unit
Box 355
Pittsburgh, Pennsylvania 15230

Mr. M. D. Beaumont
Nuclear and Advanced Technology Division
Westinghouse Electric Corporation
One Montrose Metro
11921 Rockville Pike
Suite 350
Rockville, Maryland 20852

Mr. Daniel F. Giessing
U. S. Department of Energy
NE-42
Washington, D.C. 20585

Mr. S. M. Modro
EG&G Idaho, Inc.
Post Office Box 1625
Idaho Falls, Idaho 83415

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

EDO Principal Correspondence Control

ACTION

FROM:

DUE:

EDO CONTROL: 0008097
DOC DT: 09/17/92
FINAL REPLY:

N. J. Liparulo
Westinghouse Electric Corporation

TO:

Chairman Selin

FOR SIGNATURE OF: ** GRN **

CRC NO: 92-0776

DESC:

COMMENTS ON DRAFT POLICY "DESIGN CERTIFICATION AND LICENSING POLICY ISSUES PERTAINING TO PASSIVE AND EVOLUTIONARY ADVANCED LIGHT WATER REACTOR DESIGNS", JUNE 25, 1992

ROUTING:

Taylor
Sniezek
Thompson
Blaha
Beckjord, RES

DATE: 09/21/92

ASSIGNED TO: CONTACT:
NRR Murley

SPECIAL INSTRUCTIONS OR REMARKS:
FOR APPROPRIATE ACTION

OFFICE OF THE SECRETARY
CORRESPONDENCE CONTROL TICKET

PAPER NUMBER: CRC-92-0776 LOGGING DATE: Sep 18 92

ACTION OFFICE: EDO

AUTHOR: N.J. LIPARULO
AFFILIATION: WESTINGHOUSE ELECTRIC CORP.

ADDRESSEE: CHAIRMAN SELIN

LETTER DATE: Sep 17 92 FILE CODE:

SUBJECT: COMMENTS ON DRAFT POLICY "DESIGN CERTIFICATION AND LICENSING POLICY ISSUES PERTAINING TO PASSIVE AND EVOLUTIONARY ADVANCED LIGHT WATER REACTOR DESIGNS" JUNE 25, 1992

ACTION: Appropriate

DISTRIBUTION: CHAIRMAN, COMRS, OGC, DSB, RF

SPECIAL HANDLING: NONE

CONSTITUENT:

NOTES:

DATE DUE:

SIGNATURE: DATE SIGNED:
AFFILIATION:

EDO —— 008097
92-0614A-A-00

THIS IS REVISION 1 TO LETTER ET-NRC-92-3748.

PLEASE DISREGARD THE PREVIOUS LETTER.

THANK YOU.

BRIAN A. McINYTRE, MANAGER
ADVANCED PLANT SAFETY & LICENSING

Westinghouse Electric Corporation
Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

ET-NRC-92-3748
NSRA-APSL-92-0171
Revision 1
Docket No. STN-52-003

September 17, 1992

Dr. Ivan Selin
Chairman
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

SUBJECT: COMMENTS ON DRAFT POLICY "DESIGN CERTIFICATION AND LICENSING POLICY ISSUES PERTAINING TO PASSIVE AND EVOLUTIONARY ADVANCED LIGHT WATER REACTOR DESIGNS", JUNE 25, 1992

Dear Dr. Selin:

The NRC staff has prepared a draft policy paper on eight issues related to the review of passive ALWRs. This draft policy paper was forwarded to the Commission on June 25, 1992. The ALWR Utility Steering Committee has developed a response to this draft position paper that was transmitted to you on August 21, 1992. The Westinghouse AP600 has been submitted to the NRC for review for a final design approval under Appendix O of 10 CFR 52 and a standard design certification under 10 CFR 52. Westinghouse would like to take this opportunity to provide comments on the positions presented in the draft policy paper with respect to the AP600 design.

The issue raised by the staff draft policy paper of most concern to Westinghouse is the proposed regulatory treatment of nonsafety systems. The staff proposal threatens to undermine the basic premise of the AP600 passive safety-related systems by requiring the nonsafety-related systems to meet safety grade criteria, including technical specification requirements.

The proposed staff position presumes a design approach which we firmly believe would result in significant design and operational complications without a corresponding increase in safety. This is explained in attachment H to this letter. The AP600 / URD design approach represents a significant improvement in both public safety and in commercial attractiveness. Accordingly we recommend that the NRC adopt a position which accommodates the AP600 / URD approach.

This design approach is an essential element behind the unique advantages of the AP600, providing significant improvements in public safety and at the same time providing significant improvements in plant operations and economics. The specific methods of treating the AP600 nonsafety-related active systems are identified in the AP600 SSAR. We recommend that the NRC review these methods in conjunction with the ALWR URD requirements, as an example of implementing the URD, to establish agreement on both the AP600 design and on the URD requirements.

6653A

The attachments to this letter contain a brief overall summary of our position on each issue, the basis for each position, and a discussion of the major points raised in the staff draft policy statement. In several cases, more detailed AP600 specific information is provided to further support our position.

We would be pleased to meet with you and other members of the Commission to discuss this matter further.

N. J. Liparulo, Manager
Nuclear Safety And Regulatory Activities

/nja

Attachment

cc:

Commissioner Kenneth Rogers	USNRC
Commissioner Forrest J. Remick	USNRC
Commissioner James R. Curtiss	USNRC
Commissioner E. Gail de Planque	USNRC
Mr. James M. Taylor	USNRC
Dr. Thomas Murley	USNRC
Dr. Ted Marston	EPRI
Mr. Dan F. Giessing	DOE
Dr. David Ward	ACRS

ATTACHMENT

A. DEFENSE AGAINST COMMON MODE FAILURES IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

We have assessed the defense in depth and diversity of the AP600 instrumentation and control systems and have determined that the probability of common mode failure is extremely low due to the extensive design verification, validation and qualification process.

Common mode failures are beyond design basis events and as such should be evaluated in a probabilistic rather than deterministic sense. Accordingly, we have evaluated and accounted for only high risk events as identified by the probabilistic risk assessment study. Relative to the assumed I&C failures, we have elected to take a worst-case approach and assume that the entire set of I&C cabinets in the protection system fail in the PRA. These two points, probabilistic scope definition and total I&C failure, form the basis for the design of the diverse actuation system.

We believe that the assumed failure is beyond the design basis. Our criterion is that the diverse system provide adequate (in terms of core melt frequency), as opposed to equivalent, protection. This means that generally the setpoints and time response of the diverse system will be adjusted to ensure that the diverse system will not actuate before the primary system.

Concerning the use of safety-related displays and controls, Westinghouse suggests that the wording be changed by replacing "...independent of the computer system(s)..."with"...independent of the normal display systems...".

Westinghouse has addressed these issues through the diverse actuation system, which is an enhancement of the ATWS mitigation system that has been supplied for operating plants.

The diverse actuation system (DAS) is a nonsafety-related system that provides a diverse backup for selected functions of the protection system. This backup is included to support the aggressive AP600 risk goals by reducing the probability of a severe accident which potentially results from the unlikely coincidence of postulated transients and postulated common mode failure in the protection and control systems.

The protection system is designed to prevent common mode failures. However, in the low probability case where a common mode failure does occur, the DAS provides diverse protection. The specific functions performed by the DAS are selected based on the PRA evaluation. The DAS functional requirements are based on an assessment of the protection system instrumentation common mode failure probabilities combined with the event probability. A detailed description of the DAS is provided in the AP600 Standard Safety Analysis Report.

0553A

B. ANALYSIS OF EXTERNAL EVENTS BEYOND THE DESIGN BASIS

SEISMIC MARGINS

Westinghouse generally concurs with the staff position on seismic margin assessment beyond the design basis. A seismic margin assessment for critical components is included in Appendix H of the PRA Report. It will be supplemented to discuss the vulnerabilities of the plant (from a systems success viewpoint) in the event of an earthquake.

The staff position states that "if the value of the plant HCLPF is less than about twice the design ground motion zero period acceleration, the designer should perform a more detailed evaluation against which to strengthen protection". Both EPRI and Westinghouse disagree with this threshold. Westinghouse has proposed in the PRA report a Review Level Earthquake of 0.45g (i.e. 1.50 times the SSE). This is the threshold below which strengthening the protection would be considered. This 1.5 factor is consistent with past NRC practice in the IPEEE program on existing plants.

FIRE AND FLOOD

Westinghouse generally agrees with the staff position stated in SECY-90-016 regarding internal flooding and fire analyses. PRAs have been performed for both internal fire and flooding events which may cause problems. These PRAs were done in accordance with the requirements of GL 88-20 and its supplements, and reflect the AP600 design.

Westinghouse acknowledges that the fire PRA contains uncertainties that are conservatisms. These uncertainties are mainly present in determination of the fire initiation frequencies. Westinghouse used the fire frequencies listed in NUREG/CR-4840, and subdivided these according to AP600 combustible loadings. This was considered conservative in that these frequencies were derived from active plants, which have many more ignition sources (active components) than the passive AP600.

Other traditional sources of uncertainty were not a factor in the analysis due to the compartmentalized AP600 design, or the analysis method. For example, human error calculations are traditionally a source of uncertainty. In the AP600 fire PRA, manual responses were not credited. The COMPBRN heat transfer computer code is another source of uncertainty, but it was not run because exact fiber optic and copper cable routing is not yet determined. Rather, complete damage within a fire area was postulated, given a fire. Fire propagation was not considered credible between areas separated by three hour fire barriers. This is consistent with industry experience.

OTHER EXTERNAL EVENTS

Westinghouse generally concurs with the staff position regarding site-specific "other" external events. Such site-specific other events include severe winds, tornadoes, external flood transportation and nearby facility accidents, etc. The staff recommendation that a bounding analysis be performed to demonstrate that such events are insignificant is in agreement with the guidelines set forth in NUREG-1407 titled "Procedure and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities," issued in May 1992 by the Nuclear Regulatory Commission. In fact, if it can be demonstrated that the hazard frequency for an external event is acceptably low, the bounding analysis may not be required as per aforementioned NUREG-1407.

C. ELIMINATION OF OPERATING BASIS EARTHQUAKE

Westinghouse generally concurs with the staff position. The OBE has already been eliminated in the AP600 SSAR. Supplemental criteria have been incorporated in the SSAR, and by EPRI in the URD, to address criteria gaps that occur once OBE is eliminated. The NRC staff is still evaluating similar supplemental requirements. Meanwhile, its interim positions are overly conservative.

The NRC staff is proposing an interim position for piping fatigue evaluation in which 75 cycles of one half SSE stresses should be included. An interim position is also established for equipment qualified by test in which 50 cycles of one half SSE input are applied. The URD and AP600 position is to use 20 cycles.

The NRC states they will develop new guidelines after conducting regulatory research. These guidelines should define the number of earthquake cycles that might be expected during the life of the plant. We encourage the development of these guidelines as soon as possible. This issue is primarily an investment protection issue and should not be a safety issue.

D. MULTIPLE STEAM GENERATOR TUBE RUPTURE

The ALWR program developed in response to this issue includes Westinghouse input. The ALWR response includes the following elements:

- both the evolutionary and passive PWR plants address SGTR containment bypass by features which significantly reduce the potential for core damage and for releases directly to the atmosphere in SGTR accident sequences
- ALWR utilities are seeking design features in ALWR plants which could simplify operator response to SGTR
- evolutionary plants are designed to terminate SGTR by operator actions with a 30 minute grace period; passive plants have the same operator assisted capability but also include capability to mitigate SGTR without operator action
- the likelihood of multiple SGTR is reduced by the numerous SG design enhancements to address corrosion issues and loose parts
- the passive PWR response to multiple SGTR is not expected to experience unique (relative to evolutionary plants) thermal-hydraulic response to multiple SGTR
- multiple SGTR should not be included as a passive PWR design basis.

The AP600 SSAR includes a design basis analysis of a single SGTR which shows that the passive safety-related systems automatically terminate primary to secondary leakage without ADS actuation. The passive RHR system is initiated by a high SG water level signal and functions to remove sufficient heat from the primary system to cause pressure equalization between primary and secondary. The AP600 PRA results show that SGTR scenarios contribute less than 1% of the total core damage frequency and thus are a small contributor to release frequency and overall risk.

The multiple SGTR scenario should not be considered a design basis event. This event should be explicitly treated only in the risk assessment domain where best estimate analyses are used to assess plant response to scenarios beyond the design basis events.

E. PRA BEYOND DESIGN CERTIFICATION

In the staff's detailed discussion of this issue, it is stated that in the design certification process, PRA insights be used to select among design options, to strengthen the design against previously known vulnerabilities, to characterize the design, and to evaluate the balance between event prevention and mitigation in the design. Westinghouse accomplished this for the AP600 by adhering to a policy of continual interaction between PRA analysts and design engineers. This process has resulted in many modifications to the AP600 design. The AP600 PRA was revised to include these modifications and reflect the AP600 design described in the Standard Safety Analysis Report.

The staff recommends that, throughout the duration of the combined or operating license, the PRA should be revised to address significant plant modifications, operating experience, and other developments that may affect previous PRA insights. Westinghouse agrees with the ALWR response to this recommendation that notes that PRA is considered to be a valuable tool supporting plant operation, aiding in the evaluation of plant modifications, RAP implementation, etc., but that common understandings regarding PRA's legal status under Part 52 must be established, followed by thorough industry-NRC dialogue on PRA's regulatory significance. Consideration of new NRC requirements and associated industry commitments regarding the maintenance of the PRA must proceed from common understanding of the legal and regulatory implications.

F. ROLE OF THE OPERATOR IN A PASSIVE PLANT CONTROL ROOM

The AP600 M-MIS testing program, described in Chapter 18 of the SSAR, will demonstrate the adequacy of the M-MIS to support the functions and tasks required of the operations crew to properly and safely operate the AP600. This ITAAC describes how evaluation issues are identified, tests are designed, the fidelity and scope requirements imposed on the testbed are defined to be consistent with the specific issue being evaluated and success criteria are established.

The AP600 design of the plant systems, the instrumentation and control systems and the M-MIS offers significant improvements over current plants. These include:

1. The AP600 provides for completely automatic actuation and control of the passive safety-related systems.

2. The simplified design of the AP600 includes fewer components to monitor and control and fewer manual actions, thereby reducing operator work load and increasing the time available for decision making.

3. The AP600 provides greater redundancy for some specific plant systems, thereby increasing the set of resources available to the operations crew in dealing with anticipated plant events.

4. A rigorous M-MIS design process that specifically identifies and considers the tasks and functions required for plant operations is integrated into the AP600 program.

5. The AP600 M-MIS design process directly provides for the verification and validation of the M-MIS.

These improvements provide significant operational benefits in terms of increased plant availability and safety. In the AP600, the number of operator actions taken to respond to a design basis event will be less than those required for a similar event for a conventional plant. The plant simplification and automatic nature of the passive safety-related systems reduces the number of operator actions required to maintain plant safety during an event. This reduction can be expected to improve human reliability in that fewer actions are executed and more time is provided during the evolution of an event to monitor the performance of the plant systems, evaluate their performance, and make operating decisions based on this evaluation as compared to a conventional plant. The plant design also provides additional resources in the form of multiple redundancies for certain plant systems. These resources are available for use by the operator to deal with specific anticipated plant events and provide a greater defense-in-depth. This makes additional success paths for mitigating these specific events available to the operating crew.

With regard to the M-MIS, the integrated design and verification and validation approach described in Chapter 18 of the SSAR will explicitly identify those functions and tasks required of the operations crew, provide resources to support these functions and tasks and evaluate the adequacy of the operators and the M-MIS to perform these functions and tasks through a "sufficient man-in-the-loop

testing" program. The testing program utilizes testbeds of the required fidelity and scope, as necessary, to support the M-MIS design process. A high fidelity, near full scope control room prototype (equivalent to a training simulator) is included near the end of the program to perform certain verification and validation tests. Part-task, limited scope prototypes and simulators are included earlier in the program plan, where they satisfy the needs of design verification and provide a cost or programmatic benefit. This is because some test results are needed early in the design to be factored back into the process.

We agree with the Staff that the operators will need to understand the operation of the nonsafety-related systems and their interfaces with the safety-related systems. This is consistent with existing practice in current operating plants and is not a new requirement attributable to the passive nature of the AP600 safety-related systems. The concept of interaction and utilization of safety-related and nonsafety-related systems is no different than that of a conventional plant. The operational philosophy of the AP600 is to utilize all available means (processes, systems and equipment) for preventing or mitigating an event, this same philosophy is embodied in the Westinghouse Owners Group (WOG) Emergency Response Guidelines that were developed for conventional plants. The functions and tasks that the passive plant operators will be required to perform are very similar to those performed in current plants. An example which clearly illustrates this point follows:

> In the case of a reactor coolant system leak in a conventional plant, the operators are instructed by procedures, and reinforced by training, to attempt to locate and isolate the leak and to make use of the nonsafety-related charging pumps in the Chemical and Volume Control System to maintain reactor coolant inventory while stabilizing the plant. If the charging pump capacity is adequate to maintain acceptable reactor coolant system inventory, an orderly shutdown is initiated without safety-related system actuation. In the event that the leakage from the reactor coolant system exceeds the capacity of the charging pump, safety-related systems are actuated either automatically or manually to ensure plant safety is maintained. This example scenario is valid for both a current plant and the AP600. The functions and tasks performed by the operators in both plants are very similar and include: monitoring the performance of the nonsafety-related system, implementing corrective actions if equipment malfunctions occur, determining whether actuation of safety-related systems is required, verifying the initiation of automatic actions, initiating protective functions manually if required, performing any necessary manual actions, and monitoring the performance of the safety-related systems. However, in the AP600, most of the nonsafety-related systems that provide defense-in-depth functions automatically actuate without any operator action to prevent the unnecessary actuation of the passive safety-related systems.

In summary, the AP600 M-MIS design approach satisfies the Staff's recommendation. This results from consideration of the need to define an operational philosophy consistent with: the plant process characteristics, the technology chosen for implementation of the M-MIS and the capacity of humans to reason and react in a process control environment. We believe that the program we have put in place for the design of the AP600 M-MIS correctly considers and integrates these factors.

0553A

G. CONTROL ROOM ANNUNCIATOR (ALARM) RELIABILITY

Recent events at operating U.S. nuclear plants involving the loss of the plant annunciator system have revealed the vulnerability of the power supply of these systems to single failures. In a few special cases, specific alarms are required to comply with regulatory requirements because they are essential for the manual initiation of protective actions.

The alarm system being used for AP600, the AWARE alarm system, has been designed from the beginning to be fault tolerant. One of its features is internal redundancy and its ability to accept redundant power feeds. For AP600, these power feeds are provided by two sources of non-Class 1E power which are derived from redundant uninterruptable power supplies. The AWARE alarm system meets the ALWR requirements for fault tolerance.

The AWARE alarm system is a non-safety related system and is not designed to meet the requirements of Class 1E equipment. While, generally the passive design of the plant requires no operator actions to remain safe, there are a few transients that require operator action on the AP600. These are a limited number of transients which develop very slowly and provide ample opportunity for the operators to intervene. An example is boron dilution during refueling. There is no need for an alarm to alert the operators to these types of events since they will be discovered by the normal, routine, surveillance of the displays.

H. REGULATORY TREATMENT OF NON-SAFETY SYSTEMS

AP600 POSITION

The basic design approach that Westinghouse and the Utilities (through the URD) have selected for the passive safety features of the AP600 is to meet the existing NRC Regulations and Safety Policy without relying on active systems. The AP600 nonsafety-related active systems are designed to provide reliable support for normal plant operations and to provide defense-in-depth to minimize unnecessary challenges to the safety-related passive systems. These active systems are designed for more probable component and system failures. The systems include reliable, proven equipment and component designs. These active systems are capable of being powered by the nonsafety-related diesel-generators. The active nonsafety-related systems have automatic actuation and controls that are separate from those of the safety-related systems. The active nonsafety-related systems are not required to mitigate accidents.

The capability of the AP600 passive safety-related systems will be demonstrated through extensive safety analysis and testing to satisfy the NRC and the utilities/investors. The design of these systems is carried out in a systematic manner including the use of system specification documents which contain the system design criteria, system and equipment design requirements, and operation and in-service testing requirements. The reliability and availability of the passive safety-related systems is assured through a systematic design process, a conservative design (including redundancy, diversity, and separation), quality assurance, the ITAAC program, pre-operational and in-service testing, Technical Specifications, and the AP600 and Owner Reliability Assurance Programs (DRAP & ORAP).

The reliability and availability of the nonsafety-related systems will be controlled in a manner consistent with their safety importance. The design process for these systems is similar to that used for the passive safety-related systems although there are no safety-related requirements. The equipment used to perform these defense in depth functions are assigned to a quality level that is equivalent to the Reg Guide 1.26 Group D. The reliability and availability of these nonsafety-related systems is controlled through a systematic design process, quality assurance, the ITAAC program, redundancy, pre-operational and in-service testing, the DRAP and the ORAP.

We strongly disagree with the proposed NRC position because it presumes a design with reliance on nonsafety-related systems to meet NRC Regulations and Safety Policy. The AP600 / URD design approach represents an significant improvement in both public safety and in commercial attractiveness. Accordingly we recommend that the proposed NRC position be revised to accommodate the AP600 / URD approach.

RESPONSE TO SPECIFIC NRC STAFF CONCERNS

In its draft position paper, the NRC staff has identified several specific issues regarding the use of passive systems. Each of these should be resolvable during the detailed review of the AP600 design described in the SSAR and the PRA.

1) Reliability of Passive Safety Systems

The NRC staff has expressed concerns about the reliability of the passive safety-related systems including effects of low driving heads on the operability of the CMTs / IRWSTs / PRHR HXs. They also have concerns about the basic thermal-hydraulic performance of the gravity injection systems and the ADS.

Westinghouse is committed to demonstrating the passive systems are both capable and reliable. We have developed an extensive test program such that, along with the SSAR and PRA, we will demonstrate to both the NRC and the utilities that these passive systems meet the NRC Regulations and Safety Policy. Some of the original tests have been expanded and others have been added to better address NRC concerns, including the addition of a full height/full pressure integral systems test. The remaining tests and analyses provide the basis for confirming the capability and reliability of the passive safety-related systems.

2) Safe Shutdown Condition

The NRC staff expresses their belief that, by their nature, the passive systems cannot achieve cold shutdown conditions by themselves and therefore, the nonsafety-related systems may be required to achieve safe shutdown.

The AP600 design can achieve a safe shutdown condition using only passive systems that are automatically initiated and can be maintained indefinitely without operator actions. This provides a capability which improves upon current LWR long-term residual heat removal capabilities. These improvements include the automatic actuation of a closed loop, full pressure RHR system that only requires the opening of one of two fail-open air operated valves. As the passive RHR HX removes heat the RCS temperature will be automatically reduced, reaching 420 F in 36 hours and 400 F in 72 hours. The RCS pressure will correspondingly decrease to about 310 psia at 36 hours and 250 psia in 72 hours. These reduced pressures significantly reduce the RCS pipe stresses and therefore the chance of a leak or LOCA developing during such a shutdown condition. This shutdown condition can be maintained for an indefinite time by the passive safety-related systems without the operation of the nonsafety-related systems.

Because of the AP600 safe shutdown capability, there should be no concern over achieving and maintaining a safe shutdown condition even though it is not a "cold" shutdown. This capability does not rely on the nonsafety-related systems. See SSAR section 7.4 for additional discussion of the AP600 safe shutdown condition.

3) Long Term Shutdown Operation

The NRC Staff has expressed concern that after 72 hours the licensee may need to rely on active systems to mitigate an accident, thereby increasing the need to rely on nonsafety-related systems.

The AP600 is designed so that the passive safety-related systems are capable of protecting the public without operator action for 72 hours. (Note that existing plants often require operator action within 1/2 hour or less). By providing this capability the AP600 has achieved a major improvement in safety. It is essential to note that beyond 72 hours, the AP600 passive safety-related systems continue to maintain safe shutdown conditions, providing core cooling and containment cooling without any additional actions. The AP600 passive safety-related systems are also designed to maintain reduced containment pressures and to provide control room habitability and plant monitoring capability beyond 72 hours with some limited operator actions. These operator actions can be performed using readily available, pre-identified, offsite equipment and designed in, safety-related connections in the plant. Hence it is not necessary to rely on the nonsafety-related systems to maintain a safe shutdown. The specific operator actions required after 72 hours are outlined in SSAR section 1.9.5.4.

4) Passive Safety System Capabilities During Shutdown

The NRC Staff notes that the passive safety-related systems will likely be isolated during shutdown and, therefore, active systems may be the only available means of removing heat and making up core coolant. They consider, therefore, that the nonsafety-related systems are particularly important in plant shutdown.

With regard to shutdown cooling capability, the AP600 SSAR contains Technical Specifications (SSAR section 16.1) that require passive safety-related core cooling availability during all shutdown conditions. The safety-related systems are required by Technical Specifications to be available down to mid-loop conditions. Containment integrity is required by Technical Specification down to and including mid-loop operation. During mid-loop conditions the IRWST and ADS are required to be available. As an example, attachment 1 is the Technical Specification for the PRHR HX from the AP600 SSAR.

During flooded refueling conditions, the inventory of water in the refueling cavity provides the passive core cooling capability. This water inventory is sufficient to prevent core uncovery and damage for at least 72 hours without operator action even with the containment open. Beyond 72 hours, the AP600 has provisions for readily connecting portable equipment to continue operation of the passive safety-related features for an indefinite time. When containment integrity can be reestablished in several hours, then the passive systems would be able to cool the core indefinitely without water makeup. See SSAR section 6.3.3.4 for additional discussion of passive system capability during plant shutdown conditions.

The AP600 PRA also provides insights to the importance of shutdown events to risk. The calculated core damage frequency for shutdown events is 8.9 E-8/yr which is lower than the frequency for at-power events, (3.3 E-7/yr).

The leading causes of core damage during shutdown are for events occurring at mid-loop. The frequency of mid-loop initiating events is on the order of 1 E-4/yr including the frequency of being in mid-loop and the probability of failure of the normal RHR pumps, CCW pumps, or the SW pumps. The protection for these events is provided solely by the passive safety-related systems, in particular the IRWST injection to the RCS. The only impact that the nonsafety-related systems have on these events is the probability of their failure which could initiate such an event. As such, this is similar to being at power with the nonsafety-related main feedwater providing heat removal, except that mid-loop only occurs for a very limited period of time. Also refer to item 5 for additional discussion on the measures that have been incorporated into the AP600 to control the reliability of the nonsafety-related systems.

5) Use of Nonsafety-Related Systems as the First Level of Defense

The NRC staff notes that some systems which have been traditionally safety grade, e.g., emergency ac power and auxiliary feedwater, are nonsafety-related systems in the passive plants. The NRC staff expresses concern that certain transients, such as total loss of feedwater or loss of ac which are very demanding events for operators in existing plants may, therefore, be more likely and there will be a greater burden on the plant operators.

Several traditional safety-related systems are nonsafety-related in the AP600 design; however, this does not result in greater operator burden or a less safe design. On the contrary, the AP600 design should significantly reduce the operator burden and stress during these events.

The AP600 passive systems automatically accommodate these events without requiring operator action. Further, the AP600 has a reliable startup feedwater system (SFWS) and ac emergency power system to minimize the probability of such events occurring. The AP600 specifies the SFWS pumps to be AP600 quality level D, which is equivalent to NRC Regulatory Guide 1.26 quality group D. The availability of these pumps is controlled by the ORAP. The AP600 SSAR spells out the DRAP requirements which include the functions required, the modes of plant operation where the system should be available and when planned maintenance should be performed, the test frequency (via reference to the AP600 PRA), and the remedial actions in case of equipment unavailability. As an example, Attachment 2 (Table 16.2-2 from the AP600 SSAR) shows the DRAP requirements for the AP600 SFWS. Attachment 3, from the AP600 PRA section C8, shows the PRA test frequency for the SFWS.

The AP600 also includes multiple levels of defense provided by the passive safety related systems themselves. The PRA was used to determine whether there were sufficient levels of defense because it accounts for initiating event frequency and the reliability of the protection features. For more probable events, the PRA indicates the need for more reliable protection. The PRA also quantifies the passive systems reliabilities including their vulnerability to common mode failures. The AP600 PRA shows that the multiple levels of defense provided by the passive safety-related systems support the NRC safety goal without the use of the nonsafety-related active systems. The nonsafety-related systems provide additional margin to core damage.

An example of the multiple levels of defense within the passive systems is the PRHR HX and passive feed and bleed cooling. The passive residual heat removal heat exchanger is the safety-related feature that removes decay heat during a transient. In case of multiple failures in the PRHR HX, defense in depth is provided by passive safety injection and automatic depressurization (passive feed and bleed). Therefore, since the passive systems provide automatic safety-related protection for such events and since they also provide defense in depth themselves, there is no need to apply additional regulatory requirements or oversight to the nonsafety-related systems.

6) Reliance on Nonsafety-Related Systems in PRA

The NRC staff notes that nonsafety-related equipment may contribute significantly to preventing and mitigating severe accident core damage and to recover the plant after a severe accident. We agree that the AP600 nonsafety-related systems reduce the potential for events leading to core damage. The AP600 PRA sensitivity studies show the contribution of the nonsafety-related systems.

	Core Damage Frequency (per year)	
	AP600	Typical Current Plant
- Base case, all systems	3.3 E -7	~ 1 E -5 to 1 E-4
- Safety systems and DAS	2.6 E -6	~ 1 E -4 to 1 E-3
- Only safety systems	9.0 E -6	~ 1 E -4 to 1 E-3

The AP600 core damage frequencies are taken from the AP600 PRA for internal events at power found in PRA section 8.0. The core damage frequencies for shutdown events and external events are even smaller. In current plants, there are several risk significant nonsafety-related features, including normal pressurizer spray, CVCS auxiliary spray, pressurizer PORV and diverse I&C actuation for ATWT. The RCS depressurization equipment is most important for the CDF since this function must be performed to be able to mitigate a SGTR. Also note that in current plants such nonsafety-related features credited in the PRA do not typically have availability controls such as those proposed for the AP600.

The AP600 is less sensitive to the availability of the nonsafety-related systems than for current plants. The AP600 fully complies with the NRC requirement that equipment which is important to prevent and mitigate severe accidents need not be safety grade but should be designed for the service and environment under which it is desired to function. As a result there is not a need to impose additional design requirements or to extend formal regulatory oversight to such systems and equipment. Additionally, the AP600 has an extremely robust containment which along with the associated passive containment cooling systems, provides a markedly increased level of public safety even in the event of severe accident.

The AP600 is designed to achieve low risk of severe accidents, well within the NRC Safety Policy goals, without relying on nonsafety-related systems. Therefore, it is appropriate to treat these systems as nonsafety-related and to not require additional licensing requirements.

7) Verification of Nonsafety-Related System Performance

The staff suggests that the SSAR should contain safety analysis that verifies that the nonsafety-related active systems can not prevent the operation of the passive safety-related systems.

The previous items have pointed out the nonsafety-related active systems are not required; to mitigate accidents, to maintain safe shutdown in the short or long term, or to meet the NRC safety goals. Therefore their ability to prevent the passive safety-related systems from actuating should be performed in design calculations, not in safety analysis contained in the SSAR. We disagree with the approach set forth by the staff in their draft policy paper.

RECOMMENDATIONS

We recommend that the draft NRC position on the treatment of nonsafety-related systems in passive plants be modified to accommodate the AP600 / ALWR design approach. This design approach is to design and verify the passive safety-related systems to meet the NRC Regulation and Safety Policy without reliance on the nonsafety-related active systems.

This design approach is an essential element behind the advantages of the AP600, providing significant improvements in public safety and at the same time providing significant improvements in plant operations and economics. The specific methods of treating the AP600 nonsafety-related systems are identified in the AP600 SSAR. We recommend that the NRC staff review these methods in conjunction with the ALWR URD requirements, as an example of implementing the URD, to establish agreement on both the AP600 design and on the URD requirements.

0553A

3.5 PASSIVE CORE COOLING SYSTEMS

3.5.3 Passive Residual Heat Removal System (PRHRS)

LCO 3.5.3 The Passive Residual Heat Removal System must be OPERABLE.

---NOTE---
If any RCPs are operating, at least one RCP must be operating in loop one.

APPLICABILITY: MODES 1, 2, 3, 4, and 5 (loops filled)

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Motor operated inlet valve not fully open.	A.1 Restore motor operated inlet valve to fully open condition.	[TBD]
B. One air operated outlet valve inoperable.	B.1 Restore both air operated outlet valves to OPERABLE status.	[TBD]
C. Presence of non-condensible gases in the high point vent.	C.1 Vent non-condensible gases.	[TBD]

(continued)

ATTACHMENT 1

Table 16.2-2 (Sheet 2 of 10)

Designer Recommendations for
Defense-in-Depth Nonsafety-Related Systems

Startup Feedwater System

1.0 Recommendations

1.1 The Startup Feedwater System (FWS) is available in Modes 1, 2, 3, and 4.

1.2 Availability of the FWS includes the various system components necessary to provide the following defense-in-depth function:

- Steam generator makeup from the deaerator storage tank.

1.3 System maintenance and testing requirements to support the specified functions are defined by the Combined License applicant's surveillance testing and maintenance procedures and are consistent with assumptions in the PRA evaluation.

1.4 Planned maintenance that requires system functions to be inoperable for an extended time period is expected to be performed during Mode 6. Reduced system operability during maintenance and testing, such as the unavailability of equipment due to preventive or corrective maintenance, is allowable and is consistent with the PRA assumptions for component unavailabilities.

1.5 If the availability testing criteria are not satisfied, the specific system component which does not meet the identified criteria is considered unavailable at the time it is discovered that these criteria are not met.

2.0 Remedial Actions

2.1 If any of the specified FWS components are determined to be unavailable, they are restored within [TBD] to maintain the validity of the PRA evaluation results.

2.2 If any of the specified FWS components are not restored within [TBD], actions are taken as specified by the Combined License applicant. These actions do not include plant shutdown requirements.

ATTACHMENT 2

16

AP600

Table C8-5

COMPONENT TEST ASSUMPTIONS

Components	Identification Type/Name	Expected Frequency of Test
Startup feedwater system		
Pumps	FWS-MP 03A/B	3 months
Manual valves	FWS-V053	3 months
	FWS-V054	3 months
	FWS-V069	3 months
	FWS-V070	3 months
Motor-operated valves	FWS-V065	3 months
	FWS-V066	3 months
	FWS-V038	3 months
	FWS-V039	3 months
	FWS-V042	3 months
Check valves	FWS-V061	3 months
	FWS-V062	3 months
Steam generator system		
Stop-check valves	SGS-V067A/B	3 months
Flow control valves	SGS-V250A/B	3 months
	SGS-V255A/B	3 months
Condenser/steam dump		
Steam dump valves	MSS-V012A/B	24 months
	MSS-V013A/B	24 months
	MSS-V014A/B	24 months
	MSS-V015A/B	24 months

Notes:

FWS: Main and startup feedwater system
MSS: Main steam system
SGS: Steam generator system