File

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

February 2, 1994

Dr. J. Ernest Wilkins, Jr., Chairman
Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

Dear Dr. Wilkins:

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

This letter is in response to your letter to the Chairman of November 10, 1993, in which you commented on the staff's draft Commission paper concerning the regulatory treatment of non-safety systems (RTNSS) for advanced light-water reactors in which passive features will be used for the ultimate safety protection of the plant.

Of the eight policy issues in the draft Commission paper, your letter commented on three: (1) RTNSS itself; (2) the definition of passive failure; and (3) the reliability assurance program. In the enclosure, the staff responds in detail to your comments on each of the three policy issues.

As described in the enclosure, the staff shares many of the concerns raised in your November 10, 1993, letter. The staff recognizes that the RTNSS process proposed by the industry is just one step in the staff's review process. The specific details of implementation will have to be developed when the staff reviews an individual application for final design approval/ design certification.

The staff believes that its recommendations regarding the policy issues associated with RTNSS will ensure that appropriate regulatory oversight is

003001

150053

applied to important defense-in-depth systems in passive plant designs. Therefore, the staff will recommend that the Commission approve the staff's positions on these issues, modified as described in the enclosure.

Sincerely,

Original signed by
James M. Taylor

James M. Taylor
Executive Director
for Operations

Enclosure:
Response to ACRS Comments
on the Draft SECY Papers
on RTNSS

cc w/enclosure:
Chairman Selin
Commissioner Rogers
Commissioner Remick
Commissioner de Planque
SECY

DISTRIBUTION:

Central File (w/inc)	PDST R/F (w/inc)	EDO #0009516	JTaylor, EDO
PDR (w/inc)	EDO R/F	JSniezek, EDO	HThompson
JBlaha, EDO	TMurley/FMiraglia	LCallan, 12G18	DCrutchfield
WTravers	RBorchardt	RArchitzel	JHWilson
JNWilson	MTaylor, EDO	EBeckjord, RES	WDean, EDO
RBernero, NMSS	EJordan, AEOD	JMoore, 15B18	PShea
AThadani, 8E2	BSweeney	PMagnanelli	OCA OPA OGC

* SEE PREVIOUS CONCURRENCE

OFC	PM:PDST	LA:PDST	TECH ED*	SC:PDST*
NAME	JHWilson:tz	PShea	RSanders	RArchitzel
DATE	01/27/94	01/28/94	01/12/94	01/13/94

OFC	D:PDST*	ADAR:NRR*	ADT:NRR	D:NRR	EDO
NAME	RBorchardt	DCrutchfield	WRussell	TMurley	JTaylor
DATE	01/13/94	01/14/94	01/28/94	01/30/94	02/ 2/94

OFFICIAL RECORD COPY: GT009516.JHW

RESPONSE TO ACRS COMMENTS ON THE DRAFT SECY PAPER ON

THE REGULATORY TREATMENT OF NON-SAFETY SYSTEMS (RTNSS)

A. Regulatory Treatment of Non-safety Systems:

1. ACRS Comment: The staff is still proposing the use of a "large release" frequency of $1x10^{-6}$/yr as a "safety goal guideline." Since a different segment of the staff previously recommended abandoning this concept (we think for good reason), it is disturbing to see it being resurrected here. We believe the RTNSS process would be better served by use of a conditional containment failure guideline.

   Staff Response: Before the Commission's approval to terminate the development of a large release definition, NRC and the ALWR Steering Committee agreed that the "large release frequency of $1x10^{-6}$ each reactor year" safety goal guideline would be one of the screening criteria in the RTNSS process for determination of risk-significant systems, structures, and components (SSCs). Since the Commission has decided to forgo the large release frequency as a safety goal implementation guideline, the staff will work with the ALWR vendors to assess the need for any alternative criterion. A conditional containment failure probability (CCFP), such as recommended by the ACRS, will be considered. The staff notes that the Commission has approved the use of a CCFP of 0.1 as a complement to the deterministic containment performance goal, currently included as one of the screening criteria for the RTNSS process.

   The staff will add a paragraph after Item I.E as follows:

   > It should be noted that the large release frequency of less than 1.0E-6 each reactor-year specified in Item I.C 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 CCFP of 0.1 was previously approved by the Commission as a complement to the deterministic containment performance goal.

2. ACRS Comment: We believe that the risk significance of the active systems (as developed from the baseline and focused probabilistic risk assessment (PRA)) will be sensitive to the reliability values assumed in the PRAs for the passive systems. We are concerned that there does not exist a sufficient data base to establish appropriate reliability values for use in the proposed process.

Enclosure

Staff Response: We agree that the risk significance of the active systems will be sensitive to the reliability values assumed in the PRAs for the passive systems. The passive plant designers are required to provide the justifications or bases for the reliability values used in the PRA. The appropriateness of these reliability values and passive system modeling will be carefully evaluated by the staff.

The staff is also concerned about the lack of a sufficient data base and methods to establish appropriate values for passive system reliability. Therefore, we have initiated research projects to address this concern. For example, in response to an NRR request, RES has initiated a passive safety system reliability program to identify the issues of most importance in assessing passive safety system reliability. As part of the RES program, a workshop of experts will be convened to support the identification of the issues of most importance in evaluating the reliability of passive safety systems, and assess the extent to which the planned experimental programs will define the reliability of passive safety systems.

3. ACRS Comment: We were told that the reliability/availability (R/A) "missions" for the risk-significant active non-safety systems will, in fact, be reliability values. The proposed process is vague about how the review and regulatory audit processes can determine whether or not such reliability "missions" will have been met in the design and maintained during operation. We believe that the proposed review and audit process, reliability assurance program, and implementation of the maintenance rule will not provide assurance that such "missions" have been met.

Staff Response: The R/A mission of a SSC function is a set of requirements related to performance, reliability, and availability for the SSC function as defined by the focused PRA or deterministic analysis. However, the staff review and regulatory audit processes are not intended to determine whether or not the numerical value of the mission is met, but to ensure that the supporting assumptions are realistic and achievable, and to have reasonable assurance that the actual design, operation, and maintenance are consistent with those assumptions.

During the design certification review, the staff will evaluate the system and component designs to assess their capability and reliability. This will include evaluation of test data and other available data bases; assessment of thermal-hydraulic uncertainties; review of system design with respect to redundancy, diversity, testability, environmental qualification, and inspection, test, analysis, and acceptance criteria (ITAAC); evaluation of the proposed technical specifications (TS); and evaluation of the reliability assurance program (RAP).

During the COL application review, the staff will evaluate the system and component designs added as a result of site-specific design or interface requirements. This will include an evaluation similar to that performed for the design certification and a review of the updated (site-specific) PRA and PRA insights to assess any changes to risk-significant SSCs and site-specific vulnerabilities that may require a change in the R/A missions.

In the operational phase of a plant, compliance with the Maintenance Rule, operational RAP (O-RAP) and plant TS will be used to monitor and control the performance and condition (including reliability and availability) of risk-significant SSCs. The O-RAP is intended to monitor and evaluate the performance and condition of risk-significant SSCs against goals to gain reasonable assurance that they are performing commensurate with PRA assumptions. In cases where SSC performance does not meet goals, performance is evaluated in the context of its impact upon risk by updating the PRA with operational data to show that overall goals are met or by correcting and monitoring the SSC performance such that it is consistent with the goal.

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

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

Thus, the Maintenance Rule, O-RAP and plant TS implementation will be based on R/A missions or goals considering design information from the certified design and COL application reviews.

4. ACRS Comment: The document calls for generating uncertainty distributions for the PRA results. Since the only numerical goals mentioned were based on mean values, it is not clear to us how the uncertainties are to be used by the staff.

Staff Response. The mean estimates are used for the purpose of implementing the safety goal guidelines. However, use of the mean estimates does not eliminate the need to quantify and understand the important uncertainties involved in the accident risk predictions. Such uncertainties as thermal-hydraulic assumptions and the phenomenology of core-melt progression, and fission product release and transport, arise because we lack severe accident experience or knowledge of accident phenomenology as well as data related to probability distributions. Therefore, it is necessary to estimate the range of uncertainty surrounding probabilistic estimates, and to identify by sensitivity studies those uncertainties most important to the probabilistic estimates. This will help in judgment about the degree of confidence to be given to the mean estimates and assumptions.

For clarification, the sentence in the first paragraph on Page 5 of the SECY paper that reads "Appropriate uncertainty distributions and mean values must be used to determine the availability of passive systems and the frequencies of core damage and large releases" will be modified as follows:

> 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.

B. Definition of Passive Failure:

ACRS Comment: The draft Commission paper identifies certain passive failures that could initiate accidents. Included are check valve failures, medium- or high-energy pipe failures, and valve stem or bonnet failures. We note that valve stem or bonnet failures are included as initiating failures for the passive plants. To the best of our knowledge, the staff does not postulate such failures as current licensing practice for evolutionary plants. If such a failure were postulated to occur in the outboard containment isolation valve for the reactor water cleanup system of the advanced boiling-water reactor, and the postulated single active component failure results in a failure to close the inboard containment isolation valve, the final result would be an unisolated loss-of-coolant accident outside the primary containment.

Concerning check valves, we support the staff position to redefine check valves (except for those whose proper function can be demonstrated and documented) in the passive safety systems as active components subject to single-failure consideration.

Staff Response: The consideration of the passive failures of valve stem and bonnet as potential accident-initiating events was described in the Commission paper SECY-77-439. The comment that the staff does not postulate such failures as current licensing practice for evolutionary plants is correct. For example, failures of certain outboard containment isolation valves are not considered as initiating events because of

special design requirements for those portions of piping systems in the containment penetration areas. Branch Technical Position (BTP) MEB 3-1 states that, for high-energy fluid system piping in containment penetration areas, breaks and cracks need not be postulated in those portions of piping from containment wall to and including the inboard and outboard isolation valves provided they meet the requirements of the ASME Code, Section III, Subarticle NE-1120, and design requirements described in BTP MEB 3-1. Also, failures of other valves are not explicitly analyzed because their consequences are bounded by other initiating events, e.g., failures of the valves inside containment are bounded by LOCA analysis. The same review requirements are applied to the passive advanced reactor designs.

C. Reliability Assurance Program (Issue E in the draft Commission paper)

ACRS Comment: We are in substantial agreement with the staff proposal on the RAP. It is noted that this program represents a significant commitment of resources by the ALWR vendor and, even more, the COL applicant. The use of modern risk assessment methods in identifying the systems, structures, and components to be covered within this program, and hence the use of these resources, is an important feature of the staff approach. We continue to recommend that the RAP be integrated with implementation of the maintenance rule.

Staff Response: The staff agrees with the ACRS recommendation that the RAP be integrated with implementation of the maintenance rule.

Development of a plant-specific RAP and a program for maintenance rule implementation is a COL action item which will be reviewed by the staff at the time of a license application. Consistency and integration of these programs will be a consideration in the staff review.

24 - Borchardt

ACTION

EDO Principal Correspondence Control

FROM: J. Ernest Wilkins, Jr.
ACRS

DUE: 12/16/93

EDO CONTROL: 0009516
DOC DT: 11/10/93
FINAL REPLY:

Received 11/15/93

TO:

Chairman Selin

FOR SIGNATURE OF : ** GRN **

Executive Director

CRC NO:

DESC:

DRAFT COMMISSION PAPER, "POLICY AND TECHNICAL ISSUES ASSOCIATED WSITH THE REGULATOR' TREATMENT OF NON-SAFETY SYSTEMS IN PASSIVE DES ;NS"

ROUTING:

Taylor
Sniezek
Thompson
Blaha
Mat Taylor
Beckjord, RES
Bernero, NMSS
Jordan, AEOD
OGC

DATE: 11/12/93

ASSIGNED TO: NRR

CONTACT: Murley

SPECIAL INSTRUCTIONS OR REMARKS:

PREPARE RESPONSE TO ACRS FOR EDO SIGNATURE.
PUT COMMISSIONERS AND SECY ON CC (SHOWN ON ORIGINAL) FOR REPLY.
USE SUBJECT LINE IN RESPONSE.

ACTION

DUE TO NRR DIRECTOR'S OFFICE

BY Dec. 13, 1993

NRR RECEIVED: NOVEMBER 12, 1993
NRR ACTION: DAR:CRUTCHFIELD

NRR ROUTING: TEM/FJM
JC
WR
FG
KB
Paolo

Jim - action (copies given to section & JW) Ralph 11/15

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

November 10, 1993

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

Dear Chairman Selin:

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

During the 403rd meeting of the Advisory Committee on Reactor Safeguards, November 4-6, 1993, we reviewed the NRC staff's positions and recommendations in the subject draft Commission paper, which reflects changes resulting from public comments on an earlier draft. We reviewed this earlier draft during our 400th meeting, August 5-6, 1993. Also, our Subcommittee on Improved Light Water Reactors reviewed this matter during a meeting on August 4, 1993. During this review, we had the benefit of discussions with representatives of the NRC staff and EPRI. We also had the benefit of the documents referenced.

The basic issue under review is that passive plant designs rely on passive safety systems to meet the regulatory requirements, but also include active non-safety systems as a first line of defense to reduce challenges to the passive safety systems in the event of transients or plant upsets. As this represents a departure from the current licensing approach, the draft Commission paper is intended to develop regulatory and review guidance for the AP600 and SBWR certification submittals.

In the draft Commission paper, the staff identified eight issues that pertain to the regulatory treatment of non-safety systems (RTNSS) for passive LWRs. We are in general agreement with the staff's positions and recommendations for resolving these issues, but have the following specific comments on three particular issues.

A. Regulatory Treatment of Non-Safety Systems

This specific issue has the same name as the general subject because it addresses an overall process for resolving the various issues. The overall process proposed by the staff would make innovative use of PRA to determine the risk significance of active non-safety systems with respect to meeting the ancillary safety goal on core-melt frequency, and a large release goal not fully defined. Reliability/availability "missions" for the active non-safety systems would be developed and regulatory oversight procedures applied that would depend on the assessed risk significance.

In general, we think the proposed RTNSS process is a bold and positive step in the direction of risk-based regulation. We recommend that the Commission approve this general process, and we encourage the staff to proceed with further development, to address some of our specific concerns, and to begin the implementation of the process. Our specific concerns are as follows:

1. The staff is still proposing the use of a "large release" frequency of 1×10^{-6}/yr as a "safety goal guideline." Since a different segment of the staff previously recommended abandoning this concept (we think for good reason), it is disturbing to see it being resurrected here. We believe the RTNSS process would be better served by use of a conditional containment failure guideline.

2. We believe that the risk significance of the active systems (as developed from the baseline and focused PRA) will be sensitive to the reliability values assumed in the PRAs for the passive systems. We are concerned that there does not exist a sufficient data base to establish appropriate reliability values for use in the proposed process.

3. We were told that the reliability/availability "missions" for the risk-significant active non-safety systems will, in fact, be reliability values. The proposed process is vague about how the review and regulatory audit processes can determine whether or not such reliability "missions" will have been met in the design and maintained during operation. We believe that the proposed review and audit processes, reliability assurance program, and implementation of the Maintenance Rule will not provide assurance that such "missions" have been met.

4. The document calls for generating uncertainty distributions for the PRA results. Since the only numerical goals mentioned were based on mean values, it is not clear to us how the uncertainties are to be used by the staff.

B. Definition of Passive Failure

The draft Commission paper identifies certain passive failures that could initiate accidents. Included are check valve failures, medium- or high-energy pipe failures, and valve stem or bonnet failures. We note that valve stem or bonnet failures are included as initiating failures for the passive plants. To the best of our knowledge, the staff does not postulate such failures as current licensing practice for evolutionary plants. If such a failure were postulated to occur in the outboard containment isolation valve for the reactor water cleanup system of the Advanced Boiling Water Reactor, and the postulated single active component failure results in a failure to close the inboard containment isolation valve, the final result would be an unisolated loss-of-coolant accident outside of the primary containment.

Concerning check valves, we support the staff position to redefine check valves (except for those whose proper function can be demonstrated and documented) in the passive safety systems as active components subject to the single failure consideration.

C. Reliability Assurance Program
(Issue E in the draft Commission Paper)

We are in substantial agreement with the staff proposal on the reliability assurance program (RAP). It is noted that this program represents a significant commitment of resources by the ALWR vendor and, even more, the COL applicant. The use of modern risk assessment methods in identifying the systems, structures, and components to be covered within this program, and hence the use of these resources, is an important feature of the staff approach. We continue to recommend that the RAP be integrated with implementation of the Maintenance Rule.

Sincerely,

J. Ernest Wilkins Jr.

J. Ernest Wilkins, Jr.
Chairman

References:

1. Draft Commission Paper (Undated), from James M. Taylor, NRC Executive Director for Operations, for The Commissioners, Subject: Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs, received July 21, 1993
2. Revised Draft Commission Paper (Undated), Subject: Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs, received November 4, 1993