December 15, 1992

Docket No. 52-001

Mr. Patrick W. Marriott, Manager
Licensing & Consulting Services
GE Nuclear Energy
175 Curtner Avenue
San Jose, California 95125

Dear Mr. Marriott:

SUBJECT: ADVANCED BOILING WATER REACTOR (ABWR) DESIGN FOR INSTRUMENTATION AND CONTROL DIVERSITY

In the staff's Draft Final Safety Evaluation Report, an open item was identified dealing with the diversity in the instrumentation and control systems design for the ABWR. At the present time most of the technical aspects of this open item have been satisfactorily resolved between the staff and GE. The one exception deals with the need to add high pressure core flooder backup control and indication in the main control room.

I have enclosed a preliminary staff evaluation of the diversity issue for your information. I expect that the diversity issue will be discussed at the next senior management meeting scheduled for January 21, 1993, in San Jose, California.

Sincerely,
Original Signed By:
Chester Poslusny, Project Manager
Standardization Project Directorate
Associate Directorate for Advanced Reactors
and License Renewal
Office of Nuclear Reactor Regulation

Enclosure:
Preliminary Staff
Evaluation

cc w/enclosure:
See next page

DISTRIBUTION:

Docket File	PDST R/F	DCrutchfield	WTravers
PDR	WRussell, 12G18	RPierson	JNWilson
CPoslusny	TBoyce	PShea	GGrant, 17G21
JMoore, 15B18	ACRS (10)	JWermiel, 10D24	

w/o enclosure:
BBoger, 13A2 JStewart, 8H7 SNewberry, 8H7

OFC:	LA:PDST:ADAR	PM:PDST:ADAR	SC:PDST:ADAR
NAME:	PShea	CPoslusny:sg	JNWilson
DATE:	12/15/92	12/15/92	12/15/92

OFFICIAL RECORD COPY: DOCUMENT NAME: DIVERSIT.CP

170069

9212180127 921215
PDR ADOCK 05200001
A PDR

DF03 1/1

PDR FILE CENTER COPY

Mr. Robert Mitchell
General Electric Company
175 Curtner Avenue
San Jose, California 95114

Mr. Joseph Quirk
GE Nuclear Energy
Mail Code 782
General Electric Company
175 Curtner Avenue
San Jose, California 95114

Mr. L. Gifford, Program Manager
Regulatory Programs
GE Nuclear Energy
12300 Twinbrook Parkway
Suite 315
Rockville, Maryland 20852

Director, Criteria & Standards Division
Office of Radiation Programs
U. S. Environmental Protection Agency
401 M Street, S.W.
Washington, D.C. 20460

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

Mr. Steve Goldberg
Budget Examiner
725 17th Street, N.W.
Room 8002
Washington, D.C. 20503

Mr. Frank A. Ross
U.S. Department of Energy, NE-42
Office of LWR Safety and Technology
19901 Germantown Road
Germantown, Maryland 20874

Mr. Raymond Ng
1776 Eye Street, N.W.
Suite 300
Washington, D.C. 20006

Marcus A. Rowden, Esq.
Fried, Frank, Harris, Shriver & Jacobson
1001 Pennsylvania Avenue, N.W.
Suite 800
Washington, D.C. 20004

Jay M. Gutierrez, Esq.
Newman & Holtzinger, P.C.
1615 L Street, N.W.
Suite 1000
Washington, D.C. 20036

ENCLOSURE

PROPOSED RESOLUTION - ABWR DEFENSE IN DEPTH SER OPEN ISSUE

INTRODUCTION

The instrumentation and control (I&C) systems for the ABWR help ensure that the plant operates safely and reliability by monitoring, controlling, and protecting critical plant equipment and processes. The I&C system (both safety and non-safety) for the ABWR is primarily digital-based and differs significantly from the primarily analog systems used in previously licensed designs. The digital I&C system shares more data transmission functions and process equipment than was the practice with the analog systems. The ABWR I&C system use the same software and processing equipment (hardware) across the safety channels and, therefore, a hardware design error, a software design error, or a software programming error may result in a common mode or common cause failure of redundant equipment. The staff is concerned that the use of digital computer technology in I&C system could result in safety-significant common mode failures. The benefits of using digital equipment in I&C systems are many and the staff has concluded that the ABWR I&C can be implemented safely. However, the staff has also concluded that it is necessary for the ABWR to specifically address the potential common mode failures.

BACKGROUND

The first design reviewed by the staff specifically to address the defense-in-depth against potential common mode failures was the Westinghouse RESAR-414 design. The results of this study were published in NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System" (March, 1979). This NUREG discussed common mode failures and different types of diversity and presented a method for assessing the defense in depth of design.

The staff described concerns with common mode failures and other digital design issues in SECY-91-292, "Digital Computer Systems for Advanced Light Water Reactors."

This paper describes how common mode failures could defeat not only the redundancy achieved by the hardware architectural structure but also could result in the loss of more than one echelon of defense in depth provided by the monitoring, control, reactor protection, and engineered safety functions performed by the digital I&C systems. The two principle factors for defense against common mode/common cause failures are quality and diversity. Maintaining high quality will increase the reliability of both individual components and complete systems. Diversity in assigned functions, for both equipment and human activities, and diversity in equipment, hardware and software, can reduce the probability that a common mode failure will propagate.

The modules in the ABWR Safety System Logic and Control (SSLC) are to be

implemented by microprocessor based designs with identical or similar hardware and software to be used in all four divisions. Because of this similarity the concerns expressed in NUREG-0493 and SECY 91-292 apply directly to the SSLC.

In particular, the staff review of the ABWR concludes that these concerns remain valid for several reasons.

1. The commonality of the timing between channels is such that an error in one channel is expected to occur in all identical channels and equipment within a few milliseconds of each other.

2. The possibility that the initiating transient or accident itself creates the set of circumstances that reveal the software error. The staff considers that the models of the systems used to develop the test sets may not contain sufficient inputs for all situations and, therefore, certain situations may not be adequately tested. In most software applications it is not possible to include a 100% test of all software inputs.

3. The inability to demonstrate a specific reliability or proof of correctness. There is not a general consensus as to a method to assess a quantitative measurement of software reliability. Some assumptions, such as the GE ABWR PRA assumption of 4.25×10^{-8} failures/demand for the Essential Multiplexing System (EMS or EMUX), can not be demonstrated with the current software metrics and are unrealistically low.

4. Redundancy in software does not increase reliability/availability of the overall systems to an acceptably high level as it can in analog systems. Some of the failure modes of a software based system are fundamentally different from that of a analog system.

5. Self diagnostics and periodic testing provide a significant safety improvement by reducing the possibility of undetected failures during plant operation but they do not prevent the failures from occurring. The improved self-diagnostics of digital systems do not resolve the common-mode failure issue. The analysis described latter in this SER describes the analysis of the failure and the ABWR design attributes which mitigate that failure.

Digitally-based instrumentation systems provide many safety improvements if implemented properly, however, the staff continues to believe that a level of diversity is necessary to defend against potential common-mode software errors so that necessary safety functions can be performed reliably. The staff considers common-mode software errors to be special case of single failure and that must be protected against.

There are several different types of diversity, each of which offers certain protection against the common-mode error. Forms of diversity include signal diversity, equipment diversity, aspect diversity, and people diversity. Signal diversity includes the use of different signals to initiate action, such as neutron flux and reactor temperature rise. The ABWR design includes

the alternate rod insertion (ARI) which provides diverse equipment from the RPS. Equipment diversity includes using different kinds of equipment to perform a function. The ABWR includes this diversity in that the remote shutdown station (RSS) is hardwired analog and is diverse from the microprocessor based SSLC. The ABWR also includes functional algorithm diversity between the Digital Trip Module (DTM) functions within a channel. People diversity refers to using different groups of people to design or maintain different equipment. People diversity in the ABWR design includes the QA function and the requirement for the software verifier to be independent from the software designer.

DSER ASSESSMENT

Because of the concern about potential common cause failures or common mode errors, which were expressed early in the preliminary reviews of the ABWR, the staff requested and GE accepted a licensing review basis agreement (1987) for GE to prepare an analysis based upon NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System (1979)". GE responded to the NRC request in Appendix 7A of the SSAR. In the SSAR, GE stated that the use of shared sensors in the design theoretically escalates the effects of potential common mode failures. Therefore, the SSLC system architecture is designed to provide maximum segregation of system functions by using separate Digital Trip Modules (DTMs) and Trip Logic Units (TLUs) within each of the four I&C divisions. The response also noted that for the reactor shutdown function there are five different methods for controlling reactivity including the RPS hydraulic scram, the air header dump valves of the Alternate Rod Injection (ARI), the fine motion control rod drive insert function of the ARI, the Standby Liquid Control System (SLCS), and the Control Rod Drive System (CRD). The reactor core cooling systems also have four functions described in the SSAR including the motor driven Feedwater control system, the motor driven High Pressure Core Flooder, the turbine driven Reactor Core Isolation cooling System (RCIC), and the low pressure mode of the Residual Heat Removal system. Appendix 7A also described the Remote Shutdown Station (RSS) which provides diverse (hardwired) core cooling functions. GE concluded that the ABWR fully meets the intent of NUREG-0493.

The staff concluded in SECY-91-294, "Draft Safety Evaluation Report on the General Electric Boiling Water Reactor Design Covering Chapter 7 of the Standard Safety Analysis Report" (9/18/1991) that GE had not adequately addressed the potential common mode failures and that this issue was an open item.

DFSER ASSESSMENT

As stated above, the two principle factors for defense against common mode failures are quality and diversity. The quality of the ABWR I&C systems has been addressed in the DFSER. This includes the use of quality design standards for the hardware and software and substantial testing.

The DFSER concluded that the quality issues have been substantially resolved (with a few open issues). The DFSER also concluded that GE had not adequately demonstrated that the ABWR I&C systems have sufficient defense-in-depth against potential common mode failures.

Though there were some studies performed by GE in the design process, no analyses were presented to the staff which adequately demonstrated how the SSLC design complied with NUREG-0493 provided adequate defense against potential common mode failures. The staff concluded in the DFSER that this concern had not yet been addressed adequately by GE. GE did not present hardware design control which conformed to current criteria and standards, in particular for hardware diversity. GDC 22 requires that design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

The design details that would allow the staff to assess the actual diversity and defense in depth of the design independently of GE to determine if the design was in conformance with the Licensing Review Bases commitment to a NUREG-0493 analysis, are not included in the SSAR. Instead, because of the rapid evolution of this technology, GE has committed to a design process for the I&C systems which is described in and will be verified by the ITAAC process.

Because the staff determined that the ABWR SSAR and related documentation had not adequately addressed this concern, the staff performed a common-mode failure assessment of the ABWR based upon the guidance of NUREG-0493. Some additional considerations were added to the original NUREG-0493 approach, such as evaluation of information available to the operator, common mode failures during accidents as well as transients, the time available for systems actuation, and allowing the use of non Class-1E systems to provide a diverse means of accomplishing the safety function if the safety system has failed. An assessment was performed by the Lawrence Livermore National Laboratory (LLNL) (under contract to the staff) of the diversity and defense-in-depth capabilities of the ABWR design (referred to as the LLNL diversity study). The results were made available to GE to review for proprietary information. GE was also requested to review the study and inform the staff of any factual errors in the design assessment. GE has informed the staff of some errors in the study which have been corrected.

The LLNL diversity study evaluated all of the SSAR Chapter 15 events. This set of events was judged by the staff to be a sufficiently complete set of initiators to assess this issue. The study evaluated each event in conjunction with a set of postulated common-mode failures. Two specific events were selected for detailed study in the preliminary stages of the review. Those events were generator load rejection with normal bypass and steam system piping break outside containment. Assumptions made by the staff and LLNL during the review were documented in the study. One aspect that was not specifically evaluated in the study was anticipated operator actions. As described latter in this SER, operator actions have now been considered.

The LLNL study identified several areas of concern. The use of the essential

multiplexor system (EMS) for the RPS, ESF and information to the operator was a particular vulnerability, along with the common elements shared with the DTMs and TLUs. The study concluded that, in general, there was information and system controls to mitigate each of the transients investigated, however, there may not be time and information to complete all necessary activities manually, especially if the actions included use of the remote shutdown station.

The DTM and TLU/SLU components of the SSLC share common software design features which would result in a failure of all four channels if there is a software error. The study was intended to reveal any other potential common-mode failure points.

The study found several features in the design, several of which GE had previously presented as solutions to the potential common-mode software error concern and indicate that the ABWR design has several attributes which provide defense against the potential software error.

1. The turbine inputs to the RPS are hardwired (do not use the EMS), therefore, an EMS common-mode failure would not disable these inputs. The Neutron Monitor System (NMS) and the Process Radiation Monitor (PRM) inputs use microprocessors but are directly wired to the SSLC and do not use the EMS.

2. Manual scram functions and manual MSIV actuation are hardwired from the control room, do not use the EMS, and are not dependent upon microprocessors for the function.

3. The Alternate Rod Insertion (ARI) function that is part of the anticipated transient without scram (ATWS) system is independent of the EMS. The ARI system is a non-Class-1E system that is diverse from the RPS.

4. The Non-Essential Multiplexor System (NEMS) is diverse in both hardware and software from the EMS. As the name implies, the NEMS is a non-Class-1E system.

5. The Remote Shutdown Station (RSS) is conventionally hardwired from the station to the actuation devices (does not use the EMS) and does not use microprocessors. The RSS is outside of the main control room as is required for the primary design function of shutting down the reactor upon abandoning the main control room. The RSS is a two channel station which contains most of the ESF capabilities.

6. Final display to the operator has diversity between the Class-1E fixed mimic display and the Class-1E divisional Visual Display Units (VDUs). The alarms and parameter information are also available on the non-Class-1E VDUs and plant computer.

7. The NMS bypasses the DTM and is input directly to the TLU. A common DTM failure will not fail the NMS scram function. The ARI also

DTM failure will not fail the NMS scram function. The ARI also bypasses the DTM because the ARI is not part of the SSLC.

8. The DTMs and TLU/SLUs have a significant level of functional diversity between the RPS and ESF functions and between portions of the ESF. As shown on figures 7.2-1 and 7.2-2 of this FSER, there are three DTMs, one TLU and two SLUs per channel of the SSLC. The algorithms are functionally diverse between the functions as a result of the equipment to be tripped/actuated.

9. GE has stated that the SSLC software will be relatively simple which will result in a high degree of assurance that the required testing will reveal virtually all of the errors. The EMS software is even simpler. No supporting analysis has been provided to support these conclusions. All the safety-related software will be verified and validated. The staff concludes that software, even that which has been verified and validated with a high quality program, may still have undetected errors.

The study concluded, for the two examples reviewed in detail by LLNL, the staff, and GE that some postulated failures in the SSLC (and EMS) result in disabling the indication and control of the ESF systems from the main control room. Some postulated failures also resulted in the loss of significant amounts of information available to the operator. The study concluded that it was necessary to access the RSS to initiate the ESF equipment to mitigate the event. For the events reviewed, there was display and mitigation available for any postulated failure. The mitigation was occasionally at the RSS or was a non-1E system. This study gave credit to non-1E systems to mitigate an event if it was reasonably expected to be available. Normal control systems such as feedwater were included, while systems not normally used such as manually valving in a fire water system for water injection, were not.

At the same time as this study was being evaluated, the staff prepared a generic position paper on defense in depth for consideration by the Commission. The staff recommended in a draft Commission paper, "Design Certification and Licensing Policy Issues Pertaining to Passive and Evolutionary Advanced Light Water Reactor Designs," (June 25, 1992) that the Commission approve an approach for assessing defense in depth and a requirement for a backup system which is not based on software and which is used for systems-level actuation and displays.

The results of the LLNL defense-in-depth study and the recommended staff position have been presented to GE. The staff had four primary concerns arising out of the review which are also reflected in the position recommended to the commission. The staff concluded that the response to the initiating event needed to be confined to the main control room, there was an incomplete analysis on the time available for manual operator actions, there was a lack of necessary system level actuation from the control room for the ESF functions, and there is a lack of necessary Class-1E variables displayed in the main control room. The staff requested GE to complete their review of the LLNL study and respond to the above concerns.

GE completed their review using events that GE believes envelope the Chapter 15 events. GE has stated that they disagree with the position that the staff has taken on this issue and proposed that the staff reconsider their position on this issue. GE has stated that they have adequate defense in depth and diversity and the staff position should consider the likelihood of the events in conjunction with the postulated common-mode failures and allow credit for the RSS to mitigate the event.

In response to the GE position the staff prepared a list of the set of equipment which it believes could bring the ABWR design into accordance with the proposed positions. The list was prepared by using a functional, symptom-based approach to assure that adequate reactivity control, core cooling, reactor coolant system integrity, and primary containment integrity are maintained for all events. This list was also based upon a review of the emergency procedure guidelines and the safety functions of RG 1.97.

GE has completed three studies related to this issue. The first was an analysis of the common-cause failure of ABWR multiplex equipment (SSAR Appendix 19N, amendment 22). This study identified the following potential common cause failure mechanisms:

Earthquake
Loss of DC Power
Loss of Cooling
Sensor Miscalibration
Remote Multiplexor Unit (RMU) Miscalibration
Set Point Drift
Maintenance/Test Error
Manufacturing Error
Electromagnetic Interference
Fire
Software Fault

GE addressed each of issues listed above. Most of these issues were evaluated by GE as not being credible causes due to the qualification of the equipment, physical separation or administrative controls. The study concluded that common-cause software fault is a credible, although unlikely, possibility. GE committed to administrative controls to minimize errors, technical specification requirements to assure failure detection, and symptom based procedures to assure that adequate core cooling is maintained in the event of a common mode EMS failure.

GE prepared an inventory of controls, displays, and alarms which provide a listing (SSAR Appendix 18F) of these items and describes their location. This listing provides additional information that demonstrates that the displays will have separation and some diversity. The diversity for the safety displays is primarily between the fixed mimic panel and the safety channel VDUs.

The third study prepared by GE is an event-based common mode failure evaluation (Meeting minutes 8/26/92 San Jose). This study followed the emergency operating procedure entry conditions assuming a common mode failure.

The study evaluated 14 events from the SSAR Chapter 15 transients and accidents. The study discussed the automatic actions that would occur following each event coincident with the postulated common mode failure. The common mode failure postulated for each of the events was an undiscovered common mode failure of the Essential Multiplex System (EMUX or EMS) in such a manner that all valid and correct EMUX control and monitoring data transmissions are lost. The study then discussed the Emergency Operating Procedure (EOP) entry conditions. In several events more than one monitored parameter is expected to indicate the need to enter the EOPs. Reactor Pressure Vessel Water (RPV) Level Low was the entry condition for many of the events with Drywell Pressure High for several others. The study next evaluated the operator actions per the EOPs with the equipment which was not disabled by the common mode failure. The containment response was evaluated for each event and a comparison to the SSAR Chapter 15 analysis (which does not assume common mode failures of I&C equipment) was performed. A summary of each event was provided which concluded that, for one hour or more, sufficient water is available for decay heat removal. Scram, isolation, and pressure control is also achieved.

A significant factor in this analysis is the function of the feedwater system during the transient or accident. For each of the events (except for the feedwater line breaks or failures) the feedwater system is assumed to remain operational. The feedwater system is also assumed to react properly to the specific event scenario. For example, a LOCA inside of containment, a loss of condenser vacuum or a loss of auxiliary power transformer will require the feedwater to reduce flow. GE has stated that this is a normal function of the feedwater system and should be expected to occur. If the feedwater system continues to run at 100% flow the available water inventory will be exhausted in approximately 4 minutes. If the feedwater responds as assumed in this study the water inventory will be available for over an hour.

The study concluded that there was sufficient capability to mitigate each event for enough time until the remote shutdown station capabilities could be used. Reactor systems branch and HICB reviewed the study and agreed with the conclusions with the exception that the staff believes that there is an overly extensive reliance upon the feedwater system and, therefore, additional backup capability in the main control room should be provided. This is discussed further in the conclusions section of this DSER.

GE has not submitted a point-by-point comparison of the ABWR with the Electric Power Research Institute (EPRI) Utility Requirements Document (URD) as requested by the Commission. The EPRI document discussed requirements for engineering activities and design implementation for digital I&C systems in Chapter 10 of the EPRI URD. The EPRI document includes discussion of common mode failures to ensure that they are addressed in man-machine interface system designs. EPRI stated that the ALWR program has recognized that there is no accepted standard to accurately quantify software reliability at the present time. To offset this concern, the ALWR program has emphasized the need for software quality and for a defense-in-depth approach to ensure the integrity of I&C functions including requirements for a backup hardwired (to the lowest level practical) manual actuation capability for system level actuation of safety functions.

The staff position presented to the Commission on defense in depth has changed as a result of the comments received from the ACRS, EPRI, and industry on the draft position. Analyses that demonstrate adequate, rather than equivalent, defense against the postulated common mode failures would be allowed in the diversity assessment required of the applicant. For the events postulated in the SSAR, an acceptable plant response should not result in a non-coolable geometry of the core or violation of the integrity of the primary coolant pressure boundary or violation of the integrity of the containment. The critical safety functions that require backup manual controls and displays should be specified. The staff will consider allowing more flexibility in implementing the independent set of displays and controls. The flexibility necessary depends on the specific equipment and design features of the I&C system and will be evaluated individually with each vendor. The intent is to permit the use of diverse digital equipment that is not affected by the identified common-mode failures and to reduce complexity in the design. The staff will not be so inflexible as to require only analog equipment and will consider allowing simple digital equipment.

As a result of these changes, the staff revised the initial position proposed in the draft Commission paper. The staff now recommends that the Commission approve the following revised staff position:

1. The applicant shall assess the defense in depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common mode failures have been adequately addressed. The staff considers software design errors to be credible common mode failures that must be specifically included in the evaluation. An acceptable method of performing analyses is described in NUREG-0493, "A Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979. Other methods proposed by an applicant will be reviewed individually.

2. In performing the assessment, the vendor or applicant shall analyze each postulated common mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR). The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

3. If a postulated common mode failure could disable a safety function, then a diverse means, with a documented bases that the diverse means is unlikely to be subject to the same common mode failure, shall be required to perform either the same function or a different function that provides adequate protection. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions. Diverse digital or non-digital systems are considered to be acceptable means. Manual actions from the control room are acceptable if time and information are available to the operators. The amount and types of diversity may vary among designs and will be evaluated individually.

4. A set of safety grade displays and controls located in the main control

room shall be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above. The specific set of equipment shall be evaluated individually, but shall be sufficient to monitor the plant states and actuate systems required by the control room operators to place the nuclear plant in a hot shutdown condition and intended to control the following critical safety functions: reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity.

The displays and controls shall be hardwired in the safety computer system architecture to the lowest level practical. To achieve system-level actuation at the lowest level in the safety computer system architecture, the controls may be hardwired either to analog components or to simple, dedicated, and diverse software-based digital equipment that performs the system-level actuation logic. The safety parameter displays may include digital components exclusively dedicated to displays. This requirement would provide for an independent and diverse control logic for manual system-level actuation of the safety function that would be connected downstream of the lowest level safety software-based component without affecting the hardware (interconnecting cables and interfaces) between the lowest level electronic cabinets and the plant's electro-mechanical equipment.

Human engineering principles and criteria shall be applied to the selection and design of the particular displays and controls. The design of the displays and controls shall ensure that the human system interface shall be adequate to support the human performance requirements.

The hardwired system-level controls and displays provide the plant operators unambiguous information and control capabilities. These controls and displays are required to be in the main control room to enable the operators to expeditiously mitigate the effects of the postulated software common mode failure of the digital safety I&C system. The control room would be the center of activities to safely cope with the event which could also involve the initiation and implementation of the plant emergency plan. The design of the plant should not require operators to leave the control room for such an event. For the longer term recovery operations, credit may be taken for actions from outside the main control room, when the emergency response organization is fully briefed and in place to take such actions.

CONCLUSION

The staff has concluded that the following items need to be added for the ABWR design to provide acceptable defense in depth against potential common mode failures of the I&C systems. [The integration into the control room of the additional required items will also be reviewed.]

1. The following control capability shall be added in the control room:

   a. Clean Up Water (CUW) line isolation valve (inboard) manual initiation. This item is required by both position 3 and 4 of the staff position listed above. This line does not have a control grade isolation capability as backup and, therefore, this is required to meet position 3. This isolation capability is also one of the critical safety functions identified in position 4. This item shall be provided with safety grade equipment.

   b. Reactor Core Isolation Cooling (RCIC) steamline isolation valve (inboard) manual initiation. This item is required by both position 3 and 4 of the staff position listed above. This line does not have a control grade isolation capability as backup and, therefore, this is required to meet position 3. This isolation capability is also one of the critical safety functions identified in position 4. This item shall be provided with safety grade equipment.

   c. High Pressure Core Flooder (HPCF) system manual initiation. In the analyses that have been completed (by LLNL, GE, and the staff) many of the events rely upon the feedwater system to mitigate the event in combination with the common mode failure. Experience with feedwater systems at operating plants raises a concern that they may not be reliable enough to satisfy the position 3 requirement that the backup system be of sufficient quality to perform the necessary function under the associated event conditions. The ABWR feedwater system uses a triplicated I&C system and electric motor driven pumps which should provide a higher degree of reliability than the previous operating plants, however, the specific reliability of the I&C system, especially responding to transients and accidents for which it was not particularly designed, can not be determined. The staff has concluded that it is prudent to require this backup capability to provide water to the reactor vessel. The staff has concluded that an HPCF backup control in the main control room capability provides additional assurance that the core cooling will continue for a long enough period of time for implementation of the emergency action plan, manning of the remote shutdown station or other actions. The staff has concluded that this backup capability need be provided for only one channel and that it be system-level actuation at the lowest level in the safety computer system architecture. The controls may be hardwired either to analog components or to simple, dedicated, and diverse software-based digital equipment that performs the system-level actuation logic. The components used shall be safety grade.

3. The following display capability shall be added:

a. RPV water level
b. RPV water level (level 3) alarm
c. Drywell pressure
d. Drywell pressure (high) alarm
e. CUW isolation valve status
f. RCIC steamline isolation valve status
g. HPCF flow.

These displays shall be safety grade. The displays may be analog components or simple, dedicated, and diverse software-based digital displays.

4. The remote shutdown station displays shall be operable during normal operations. This will permit an operator to assess the status of the displayed parameters without transferring control from the main control room.

5. The feedwater control system shall be designed and tested to verify the event analyses described above. This testing is required to provide a level of assurance that the Feedwater system can respond as assumed to these conditions which are beyond the normal design basis. The inclusion of only a single instrumentation and control channel of water injection capability (HPCF) in the main control room is predicated upon operation of the feedwater system during the events as demonstrated by testing. For each event analyses of the SSAR Chapter 15 events (the GE and LLNL analyses referenced above) which shows that feedwater provides the mitigation following the common mode failure of the safety I&C systems function the feedwater I&C system shall be tested using simulated inputs to demonstrate that the feedwater system will perform as assumed in the analyses. This requirement shall be added to the ITAAC.