GE Nuclear Energy

General Electric Company
175 Curtner Avenue, San Jose, CA 95125

April 16, 1990
MFN No. 035-90
Docket No. STN 50-605
EEN-9016

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

Attention: Charles L. Miller, Director
Standardization and Non-Power Reactor Project Directorate

Subject: **Submittal of Responses to Additional Information as Requested In NRC Letter from Dino C. Scaletti, Dated March 14, 1990**

Reference:

Enclosed are thirty four (34) copies of further responses to subject Request for Additional Information (RAI) on the Standard Safety Analysis Report (SSAR) for the Advanced Boiling Water Reactor (ABWR). These responses pertain to Chapters 7 and 10.

It is intended that GE will amend the SSAR with these responses in a future amendment.

Sincerely,

P. W. Marriott, Manager
Regulatory and Analysis Services
M/C 382, (408) 925-6948

cc: F. A. Ross (DOE)
D. C. Scaletti (NRC)
D. R. Wilkins (GE)
J. F. Quirk (GE)

D028
1/34

bcc:

L. S. Gifford (GE-Rockville) w/o attach
R. C. Mitchell (GE) w/o attach

QUESTION

420.019 (7.1.2.1.6(4)) This section states that automatic self-test is performed sequencially on all four divisions, to minimize common mode effects, and that a complete self-test sequence through all four divisions takes no more than 30 minutes. The original response to question 19 revised this section. What hardware and software design features are provided to allow sequencing the testing of the four divisions without violating independence/isolation criteria? The revised section appears to allow a common centralized test driver. Illustrate with a block diagram.

RESPONSE

420.019 Please refer to the responses to questions 420.73 and 420.127, which are closely related. Figure 7.1-1 was revised in accordance with the design change which eliminated the on-line interconnecting concept for the self-test function. This provides the requested block diagram. The previous revision of subsection 7.1.2.1.6 was incomplete, but has now been completely revised consistent with this philosophy [see attached - 7.1.2.1.6(6)].

The updated ESLC self-test program includes an on-line test and an off-line test. Both are independently conducted on each division. There are no common centralized test drivers. Details are described in the updated 7.1.2.1.6(6), and in 7A.2 - responses (6) and (14).

.....

QUESTION

420.069 (7) Are there any limitations on the ABWR design concerning the use of expert systems? Any limitations on the use of technology not specifically described? The original response does not describe an approach for determining what hardware or software developments (which may occur between design certification and plant operation) can be implemented without changes to the design certification and NRC review.

RESPONSE

420.069 NOTE: THE FOLLOWING IS THE ORIGINAL RESPONSE TO QUESTION 420.69. A SUPPLEMENT HAS BEEN ADDED AT THE END IN RESPONSE TO THE AMMENDED PORTION OF THE QUESTION.

Advanced technology has been applied to RPS and overall safety system design for ABWR in order to produce a system that is more compact, more reliable, more accurate, and more responsive than analog/relay designs.

Previous experience with the Clinton Nuclear System Protection System (NSPS) proved that discrete, solid state, logic gates could provide a simple and testable replacement for RPS relay logic. However, this implementation required the use of several hundred printed circuit boards in the four protection divisions. The large quantity of equipment affected system reliability and required a complex, external, self-test system to ensure adequate availability (by fast detection and localization of circuit faults).

Investigations into the use of more advanced technology for ABWR RPS logic (part of Safety System Logic & Control) showed that significant cost savings and performance improvements were possible if locally digitized plant variables were multiplexed over fiber optic cables to the control room. The multiplexed data would be processed in microprocessor-based logic equipment controlled by software residing in

non-volatile memory ("firmware"). Control signals would also be multiplexed from the control room to the actuators of driven equipment for many systems. This type of configuration would greatly reduce the amount of processing equipment and cabling by replacing hardware logic with a software-based design requiring fewer integrated circuits.

RPS and other safety systems for ABWR based on the above configuration remain independent of plant control or computer systems; digital processing of sensor data for possible trip action is contained within the safety-grade boundaries of the protection divisions. Control systems or the process computer do not provide inputs to safety system logic.

In addition to multiplexing and microprocessor-based logic processing, application of advanced technology is limited to fault-locating self-diagnostics, auto-calibration, manual (semi-automatic) surveillance functions, graphical operator displays, and flat panel touch screens that replace most hardware switch functions. Plant automation features using expert systems or other computer-controlled processes are not applied, since they are unncessary for standby systems that ordinarily do not require any operator action (automatic trip and initiation conditions are well-defined and do not change over time). Emergency operator action is provided by direct, hardwired switches external to software logic (for example, manual scram).

At the equipment level, the basic constraint on new technology application for safety systems is the need to provide advanced performance features while preserving long term reliability and availability of the basic trip functions (at least equal to that of the original designs). While almost any existing microprocessor or other VLSI technology can implement safety system functions, the following constraints on state-of-the-art technology were considered necessary to achieve a practical design:

HARDWARE/SOFTWARE CONSTRAINTS:

a. Proven technology - must have failure rate history to support reliability goals. Advanced component designs, such as Reduced Instruction Set Computer (RISC) processors, Application Specific Integrated Circuits (ASICs), gate arrays or Programmable Logic Devices (PLDs) have a limited design history and unknown future support.

b. Not obsolescent - reasonably expected to be supported by vendors for several years with upgrading possible.

c. Second sources - affects availability of spare parts.

d. Components should be available in high reliability versions.

e. Maintainability - easily replaced modules, memory chips in sockets for expansion or upgrading.

f. Software support for hardware - appropriate development tools and compilers must be available for desired language and processor.

g. Programming language chosen should permit top down, structured, modular design and should result in easily readable source code.

h. Testability - automatic testability must be provided for logic inaccessible to manual surveillance and test methods.

i. Heat dissipation - equipment should require lowest power for required speed, preferably lower than previous designs. Sufficient panel space is available such that the highest density electronic packaging is not required.

PERFORMANCE CONSTRAINTS

a. Robust design (power-on initialization without transients, power-down reset to safe state, immunity to noise and common-mode failures, operability in design basis thermal and seismic environments) is more important than the ability to support large memory arrays or perform complex calculations.

b. Speed should be minimum needed to support data throughput; faster speeds result in noise problems and require complex error detection and correction methods.

THE FOLLOWING RESPONSE SUPPLEMENTS THE ORIGINAL RESPONSE TO THIS QUESTION:

This response addresses the question of developing an approach for determining equipment changes that can be made after design certification without changes to the certification and without NRC review.

The basis for reliable design of safety system components will be conformance to Regulatory Guide 1.152, which endorses ANSI/IEEE-ANS-7-4.3.2-1982 (Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations). The methodology described in this standard establishes a program of independent verification and validation (V&V) for confirming correct implementation of integrated hardware and software. The V&V program will be used after design certification during the actual hardware and software implementation phases to verify and document all steps of the design and testing process. During final validation testing, acceptance criteria shall confirm correct operation of the completed system with regard to design specification requirements.

Design certification addresses system level design down to the hardware/software system specification level. A vendor may implement these functional requirements using different combinations of hardware and software. For example, because of hardware response time requirements, a certain function shown as originally being a software process in the system documents may be designed using discrete logic. Many other changes will be made because of cost, component availability and prototype test results. The structured design process, including design reviews, the V&V program and the overall Quality Assurance program, will ensure adherence to the intent of the design specifications. This development process will include provisions for meeting independence, separation and defense-in-depth requirements no matter what technology is used. In addition, all safety-related components will be qualified to the appropriate standards.

In general, only system level changes that alter the inputs and outputs or modify basic parameters, such as trip levels and response times,

should require changes to design certification or NRC review.

QUESTION
420.123 (15B4) SSAR 15B.4 describes the essential multiplexing system (EMS) in some detail. SSAR Figure 7A.2-1 states that the design is not limited to this configuration. It is our understanding that the EMS design is still in a preliminary design stage. Is SSAR 15B.4 still accurate and is the design limited to that configuration?

RESPONSE
420.123 SSAR 15B.4 is an accurate system-level description of EMS and reflects the components described in the EMS design specification and SSLC design specification, and is the chosen system configuration. The exact hardware implementation is not specified for design certification, since potential vendors could accomplish the multiplexing functions in several ways, given the restriction that qualification requirements must be met. However, certain design details to be imposed on such vendors are discussed in the various responses given in SSAR 7A.2. Hardware and software ("firmware") requirements down to the module level of the equipment are described.

The EMS design is presently defined to the level of the type of processing components needed to perform the data transmission task. The design requires remote multiplexing units, control room multiplexing units and fiber optic interconnecting links. The bi-directional, dual redundant token ring topology is the chosen configuration for these components, and is the configuration shown in SSAR Figure 7A.2-1. However, the multiplexing tasks shown in the figure could also be accomplished by the same components arranged in a star, bus, or point-to-point architecture (all still using a dual redundant configuration). This part of the design will be determined during the detailed design phase, depending upon the required system speed (data throughput), response time, the vendor's communications protocols, error detection/correction methods, and available hardware/software designs.

GE believes that specifying the exact EMS configuration at the design certification stage could skew competitive bidding for potential vendors of the equipment. The system requirements imposed on the multiplexed safety system design (e.g., single failure proof, signal isolation, 2-out-of-4 system logic, bypassing of failed components, self-test, easy repair, periodic surveillance, highly reliable materials, verification and validation of software, and integration testing) are sufficient to provide a qualified design.

QUESTION
420.124 (15B4) The FMEA submitted in SSAR 15B.4 is inadequate for a safety evaluation supporting the design certification. The FMEA appears to the staff to be oversimplified with one line item each for component failures and does not address potential software complications. The staff requests clarification of how this FMEA was developed given that the system design has not been finalized. The staff also believes that software failures need to be evaluated. The failure modes investigated should include, as a minimum, stall, runaway, lockup, interruption/restoration, clock and timing faults, counter overflow, missing/corrupt data, and effects of hardware faults on software.

RESPONSE

420.124 Definition of "level of detail" for design certification is presently undergoing review with the Staff. A full response to this question will be submitted following the results of that review. However, the specific failure modes of stall, interruption/restoration and timing faults were addressed in the responses to 420.53 and 420.54.

QUESTION

420.125 (7.4.1.4) This section provided additional clarification of the intended use of the remote shutdown system. The degree of independence and isolation from the Safety System Logic and Control (SSLC) and EMS are not clear. Is it intended in the SSAR to take credit for the RSS if there is a total loss of EMS?

RESPONSE

420.125 The remote shutdown system (RSS) is totally separate and independent from the SSLC and EMS in that it is "hard wired" and does not have any multiplexed signal interfaces.

The EMS consists of four independent and separate divisions. Therefore, a total loss of all four divisions of EMS is highly unlikely, and could only be attributed to common-mode failure (See response to 420.127). The extensive V&V steps which will be performed in the EMS development should make the possibility of a common-mode failure almost negligible. However, the RSS will provide an additional degree of protection from common-mode failures by providing an independent means of actuating core cooling functions diverse from both the EMS and the plant main control room.

Reactor scram functions would most likely occur directly as a result of a postulated common-mode EMS failure, because of the "failsafe" design of the reactor protection system (i.e., loss of signals coming from EMS would cause scram). However, the standby liquid control (SLC) system is also available to shut down the reactor because it, too, is "hard wired" and does not interface with the EMS. The SLC is discussed in Subsections 7.4.1.2 and 7.4.2.2.

Both the RSS and SLC are identified as diverse mitigating systems for such scenarios in 7A.7 [Items 7A.5(4) and 7A.6(4)].

QUESTION

420.126 (7A-7) Compared with GESSAR II, the ABWR has significantly reduced the number of input sensors by use of sharing sensors. Provide a bases as to why this does not increase potential vulnerability to common mode failures by reducing sensor diversity.

RESPONSE

420.126 Sensor diversity is not compromised by the reduction of instruments, because each of the diverse RPV parameters monitored for the GESSAR II design is still represented in the ABWR. Only the quantity of similar instruments monitoring a given parameter is reduced.

Generally, the reduction in sensors does not necessarily degrade reliability or availability. In fact, simpler systems are usually more reliable. When additional components are used redundantly in a system

to improve reliability, a point is reached where the system reliability is dominated by common-cause failure, and additional redundancies add little, if any, improvement in system reliability. In the early stages of the ABWR design (before the instrument reduction program), the reliability of ECCS initiation was limited (in the analysis) by five common-cause interdivisional sensor miscalibration error probabilities. Following the instrument reduction program, there were only three groups of sensors subject to such probabilities. This reduction in common-cause miscalibration errors is because there are less sensors, and the sensors are shared.

Sharing of sensors does raise the possibility of common-cause sensor miscalibration error between safety functions. However, for the limiting-risk case, where low RPV water level is the sole sensed initiation condition, reactor trip and ECCS initiation have different sets and types of sensors. ECCS is initiated by two sets of wide-range water level sensors and RPS is initiated by a separate set of narrow-range sensors. With proper maintenance procedures and special precautions, the possibility of common-cause miscalibration resulting in loss of automatic initiation of both safety functions is very remote.

There is sharing of drywell pressure sensors between functions, but the primary purpose of these sensors is to sense increased drywell pressure resulting from a loss-of-coolant accident, and LOCAs are a very small contributor to core damage frequency or risk. The RPS and ECCS have separate trip units.

The same reactor pressure sensors are used for RPS and low-pressure ECCS permissive signals, but again, there are separate trip units that are calibrated separately. A common-cause failure of the RPV pressure sensing function would have very little effect on core damage frequency.

In the ABWR design, the 2-out-of-4 logic utilized in the GESSAR II RPS has been expanded to include all of the ESF systems as well. Thus, where ESF systems could tolerate any single instrument failure in the GESSAR II design, they can now tolerate any two instrument failures in the ABWR design. In other words, failure of 3 sensors is required to disable the signal in the ABWR, whereas failure of 2 sensors was sufficient in the GESSAR II design. Therefore, from a multiple-failure point of view, the ABWR has better protection compared to the GESSAR II design.

.....

QUESTION

420.127 (7) In general, the applicant should provide a clear presentation of how the ABWR with common software modules for any functions (including SSLC logic self-test programs) conforms with IEEE 279-1971 and is at least as single failure proof as GESSAR II. The discussion of shared sensors in 7A-7 does not address potential common mode software failures which may be capable of defeating the diverse parameters. Additionally, the applicant should address why diversity of software should not be a requirement to maintain system diversity.

RESPONSE

420.127 The complete independence of the SSLC self-test program is discussed in the revised subsection 7.1.2.1.6(6) [See response 420.19].

Each of the four electrical divisions has its own independent hardware and software. Software "modules" might be construed as "common" only to the extent that each of the independent and redundant hardware modules are similarly programmed in firmware before shipment.

With regard to single-failure, the SSLC trip logic has inter-divisional fiber-optic links to facilitate the 2/4 coincident voting capability. However, such links are unidirectional and their only failure mechanism is an erroneous logic signal to the voting processor. The remaining channels would revert to 1/3 (unbypassed) or 2/3 voting depending on the state of the logical failure. This is the same affect as any other failure within a given channel and is consistent with the single failure criteria defined in IEEE Standards 279, 603 and 379. With the full 4-divisional any-two-out-of-four logic configuration inherent for virtually all safety systems, the ABWR can actually withstand multiple failures in more postulated scenerios than could the GESSAR II design. Therefore, it is more "single failure proof" than GESSAR II.

Regarding postulated common-mode software failure, please review Appendix 7A.7, and the responses to questions 420.125 and 420.126, which are closely related to this question. These describe the increased reliability of the 2/4 logic over previous designs, the extensive V&V program to prevent common-mode failure, and the diverse SLC and RSS systems to mitigate consequences of such failures. The reasons why software diversity is not necessary, and could even be detrimental, are summarized as follows:

(1) The software is developed and documented in accordance with the NRC approved Nuclear Energy Group Boiling Water Reactor Quality Assurance Program. As described in Appendix 7A, the design methodology meets the requirements of Regulatory Guide 1.152, including all the necessary reviews, verification, testing, etc.

(2) The SSLC is actually governed by firmware that has been verified by the V&V program. This firmware can only be burned in at the factory prior to shipment. It is not possible to make program manipulations in the field which could result in a higher probability of common-cause failures.

(3) The SSLC is made up of four independent divisions, each having its own individual and independent microprocessors. The software (firmware) is thus distributed among separated processing hardware. The system is not dependent on a common central processor.

(4) Each division is independently controlled by its own timing system which is not synchronized with other divisions. Therefore, unlikely common-mode failures would be even less likely to occur at the same instant, thus initiating an inadvertent synchronized response.

(5) Each individual microprocessor module is sufficiently simple that it can be verified and validated with great confidence prior to shipment from the factory. Diverse programs would complicate verification and validation activities making them much more costly and difficult to manage. For example, software diversity would require working the bugs out of up to four different system programs. Such cost increases could

defeat the potential savings from applying software-based systems.

(6) System self-test runs as a background task in each SSLC logic processor. The operating system or executive program for each processor schedules self-test differently depending upon what other tasks are being processed. Thus, self-test is independent and unsychronized in the four divisions. In addition, both hardware and software watch-dog timers alert the operator to inoperative failures so mitigative action can be taken. Multi-divisional failiures in SSLC or EMUX would cause scram directly because of the fail-safe (loss of signal = scram) design of the RPS.

(7) Manual diverse backup systems (SLC and RSS) are provided for critical functions of reactor shut-down and core cooling. Manual "hard-wired" scram is provided for reactor trip. This provides additional defense-in-depth despite high reliability of qualified safety-related hardware/software equipment.

(8) Although the probability of common-cause failures of multiple divisions is reduced by utilizing diverse firmware, the probability of individual failures is increased due to the increased numbers of diverse paths over which postulated failures could occur. In addition, diverse firmware curtails the benefits of standardization in control and instrumentation equipment.

(9) As summarized in Appendix 7A, hardware diversity principles are incorporated at both the signal and system levels similar to operating BWRs and GESSAR II. The ABWR fully meets the intent of NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the Resar-414 Integrated Protection System", May 1985.

QUESTION
420.128 (7A.7) Will software be used to isolate data? If so, what are the design and qualification criteria that are to be applied? Are there any systems which have non-Class 1E software such as keyboard or display control software that interface with the Class-1E systems? Are there any interface with the Class-1E systems which receive inputs from non-Class 1E systems or other channels of 1E systems?

RESPONSE
420.128 The following cases are presented to illustrate situations where software may be used to isolate data between Class 1E and non-class 1E system interfaces:

1. SYSTEM LEVEL

   a. NON-CLASS 1E TO CLASS 1E: In general, transfer of data from non-Class 1E systems to Class 1E systems is not permitted. All plant sensors and other inputs to safety systems, such as contact closures from relays and manual control switches, that are connected to the Essential Multiplexing System (EMS) or directly to safety system logic must be Class 1E.

      A few situations require data from a non-safety-related system. In these cases, only qualified, Class 1E devices shall be used to acquire and transmit the data, using electrical and physical isolation as required (typical applications are Main Turbine and Control Rod Drive). An analysis must be performed to confirm

that failure of the device or supporting structures will not affect the safety systems or EMS.

Electronic devices such as touch panels used for software-based safety system controls must also be Class 1E.

b. CLASS 1E TO NON-CLASS 1E: Transfer of data from Class 1E systems to Non-Class 1E systems is permitted with appropriate hardware and software isolation. Typical applications are safety system outputs to the Performance Monitoring and Control System (PMCS); i.e., output signals used for status displays, annunciator alarms, and computer logging. Other applications are the scram-following outputs from the Reactor Protection System (RPS) to the Rod Control & Information System (RC&IS) and recirculation pump trip outputs from RPS to the Recirculation Flow Control System. These outputs will be transmitted over an isolating medium (in general, fiber optic data links) to PMCS or the other non-safety systems.

The safety system equipment shall broadcast its data to the non-safety systems with little or no control signal handshaking. No interrupts shall be used by the non-safety systems to request data from the safety systems. No hardware or software failure on the non-safety side shall affect the safety system side; i.e., safety-critical functions shall not be inhibited. Non-safety-related software shall not affect safety-related software, causing it to fail into a non-safe state or causing an unwanted transient response.

Software for data transfer that resides in the safety system equipment shall be written and tested as safety-related code. The code shall be verified and validated under the same V&V program as the other portions of software written for safety functions, thus conforming to Regulatory Guide 1.152.

c. CLASS 1E TO CLASS 1E: Data transfer between multiple channels of Class 1E systems or between different Class 1E systems is permitted, except that the essential multiplexing systems in multiple channels shall not directly communicate with each other. All permitted communications shall be over fiber optic data links for signal isolation. A hardware or software failure in either channel shall not affect the other channel's normal software performance. All data transfer shall be under the control of error detection/correction software at both the transmitting and receiving ends. Communication protocols shall employ parity checking, checksum, CRC or some combination of these methods in addition to reasonableness, limits, and bounds checking of transferred data. An appropriate trip or warning alarm shall be generated on communication failure if automatic recovery within time limits is not possible. All safety-related software shall be developed under the guidelines of Regulatory Guide 1.152.

2. EQUIPMENT LEVEL

a. KEYBOARD OR KEYPAD INPUTS: Individual logic processing instruments that implement microprocessor-based, software-controlled safety functions will allow technician access (by administrative control, using key access or passwords) to

certain calibration and test functions. However, since safety equipment control programs are in read-only memory (ROM), the basic safety-critical functions cannot be changed even when calibration is performed.

Keypad input shall not affect any safety-related signal path. However, some setpoints may be changeable in the field (under administrative control) because of varying plant conditions. Gaining access to setpoint, calibration or test functions shall automatically cause the equipment to go off-line and cause the affected system to be placed in a bypass condition or to go off-line in the appropriate tripped or untripped state, so that the system remains in a safe state.

b. FRONT PANEL DISPLAYS: Safety-related data for local display shall be sent via isolated paths to separate display processors. There shall be no interaction between display software and safety-critical software. For example, failure of a handshaking control signal during data transfer shall not affect normal data flow in safety-critical software. No data shall be transferred from the display processor to the safety-related portions of the hardware or software. The entire instrument, including both the safety function processor and the display processor and associated software, shall be qualified as Class 1E, nuclear safety-related.

QUESTION
420.129 (7) List those systems or major components in the I&C design area for which the design is not complete to the "purchase specification" level.

RESPONSE
420.129 Definition of "purchase specification level" for design certification is presently undergoing review with the Staff. A response to this question will be submitted following the results of that review.

QUESTION
420.130 (Response 420.63) In this response a MTBF goal of 100,000 hours (11.4 years) is given for the essential multiplexing system. Is this goal for one channel or the complete system? If this goal is for the complete system it appears to the staff that the ABWR can expect to loose control at the control room of many of the safety systems (RPS, RHR, ADS) five or six times over the lifetime of the plant. How does this compare with the reliability/availability of multiple ESF systems in the BWR/5 & 6 design (or GESSAR II)?

RESPONSE
420.130 The MTBF goal for the essential multiplexing system (EMS) is 100,000 hours per channel.

QUESTION
420.131 (19.2.3.4) Are multiplexer and software failures included in these systems interactions and common cause failures?

RESPONSE
420.131 Multiplexer failures are explicitly modeled in the ECCS instrumentation fault trees, as is the multiplexer common cause failure between electrical divisions. Software is an integral part of the ESF logic, and such failures are included in the ESF logic failure rates.

QUESTION
420.132 (19.3.1.3.1(b)) (Response 420.47) Section 19.3.1.3.1(b) states that "if core cooling is accomplished without the use of an RHR system and the suppression pool cooling begins overheating, the suppression pool cooling mode of the RHR will be initiated by the operator." Is any manual action required prior to 30 minutes?

RESPONSE
420.132 No. Suppression pool cooling is not required prior to 30 minutes for any Design Basis Event.

QUESTION
420.133 (19.3.1.3.1(c)(i)) This section describes the MSIV closure sequence with the most desirable outcome requiring operator action at 30 seconds to insert rods. If that fails the operator must inhibit ADS valves from opening and initiate SLCS within 10 minutes. These activities do not appear to be consistent with a stated design goal of no operator action for 30 minutes following a transient. Provide a description of how the MSIV closure sequence meets the 30 minute rule (6.3.1.1.1) same question for Loss of Offsite Power (LOOP).

RESPONSE
420.133 The reference design goal specified in 6.3.1.1.1 is applicable to Design Basis Accidents. The events considered in 19.3.1.3.1(2)(c)(i) and 19.3.1.3.1(2)(c)(iv) [MSIV Closure and LOOP, respectively] are multiple failure ATWS events which are beyond the design basis. Therefore, the 30-minute design goal is not applicable.

QUESTION
420.134 (19D.3.4) Equipment maintenance or test unavailabilities are taken from GESSAR PRA and are based upon BWR experience. In the past, I&C has been a large contributer to system downtime. How do these systems (RHR, RCIC) unavailability numbers take into account the new multiplexing and microprocessors?

RESPONSE

420.134 The system maintenance unavailabilities presented in Table 19D.3-2 do not address the new multiplexing and microprocessors.

Multiplexing and microprocessor logic are explicitly modeled in the ECCS actuation instrumentation system fault trees presented in Figure 19D.6-15. To assess the unavailabilities of systems such as RHR and RCIC, support system fault trees (electric power, instrumentation, service water, etc.) are first linked directly to the front line system trees, and then the composite trees evaluated to determine overall system unavilability. In this manner, unavailabilities attributable to the new multiplexing and microprocessors are directly taken into account.

QUESTION

420.135 (Table 19D.6-10) Provide the justification for a Mean Time to Repair (MTTR) of 4 hours for multiplexers and 30 minutes for ESF logic. Invertors and battery chargers have restoration time given (Table 19A.8) as 48-56 hours. Are the multiplexers designed with all test and maintenance equipment installed?

RESPONSE

420.135 The multiplexing network has been designed with an integral test feature which tests system performance on a thirty minute cycle and annunciates component failures. Therefore, on the average, the mean time to detect annunciated failures is 15 minutes. Failed components at the module or logic card level are automatically indicated to the operator or technician.

The mean time to repair of 30 minutes for ESF logic is based upon the assumption that ESF logic cards are located in the control room and that replacement cards are readily available. On this basis, 30 minutes is judged to be adequate for ESF logic card replacement.

A mean time to repair for multiplexers of four hours is based upon divisional multiplexer components being located external to the control room and requiring greater time to reach and replace. As in the case of ESF logic cards, replacement components are assumed to be readily available. On this basis, four hours is judged to be adequate for multiplexer repair. Time required to perform any related plant administrative procedures is not considered to be part of mean time to repair.

QUESTION

420.136 (7A) The staff has reviewed the commitments in the SSAR and has reviewed the available documentation describing the verification and validation plans. To date, the information has been vague, general in nature and lacking in essential detail to demonstrate conformance with ANSI/IEEE 7-4.3.2. Does the applicant intend to enclose the V&V Plan as Appendix B of SSAR Chapter 7 or will the V&V details be left as an interface requirement? The staff required a formal, structured V&V plan to be in place and implemented early in the software design process.

RESPONSE

420.136 Definition of "level of detail" for design certification is presently undergoing review with the Staff. A response to this question will be submitted following the results of that review.

.....

7.1.2.1.6(6)

The sixth test is an integrated self-test provision built into the microprocessors within the safety system logic and control (SSLC). It consists of an on-line, continuously operating, self-diagnostic monitoring network; and an off-line semi-automatic (operator initiated, but automatic to completion), end-to-end surveillance program. Both on-line and off-line functions operate independently within each of the four divisions. There are no multi-divisional interconnections associated with self-testing.

The primary purpose of the self-test is to improve the availability of the SSLC by optimizing the time to detect and determine the location of a failure in the functional system. It is not intended that self-test eliminate the need for the other five manual tests. However, most faults are detected more quickly than with manual testing alone.

The self-test function is classified as safety associated. However, its hardware and software are an integral part of the SSLC and, as such, are qualified to Class 1E standards.

The hierarchy of test capability is provided to ensure maximum coverage of all EMS/SSLC functions, including logic functions and data communications links. Testing shall include:

(1) On-line Continuous Testing.

A self-diagnostic program monitors each signal processing module from input to output. Testing is automatic and is performed periodically during normal operation. Tests will verify the basic integrity of each card or module on the microprocessor bus. All operations are part of normal data processing intervals and will not affect system response to incoming trip or initiation signals. Automatic initiation signals from plant sensors will override an automatic test sequence and perform the required safety function. Process or logic signals are not be changed as a result of self-test functions.

Self-diagnosis includes monitoring of overall program flow, reasonableness of process variables, RAM and PROM condition, and verification of 2/4 coincidence logic and device interlock logic. Testing includes continuous error checking of all transmitted and received data on the serial data links of each SSLC controller; for example, error checking by parity check, checksum, or cyclic redundancy checking (CRC) techniques.

A fault is considered the discrepancy between an expected output of a permissive circuit and the existing present state.

Actuation of the trip function is not performed during this test. The self-test function is capable of detecting and logging intermittent failures without stopping system operation. Normal surveillance by plant personnel will identify these failures, via a diagnostic display, for preventive maintenance.

Self-test failures (except intermittent failures) are annunciated to the operator at the main control room console and logged by the process computer. Faults are identified to the replacement board or module level and positively indicated at the failed unit.

The continuous surveillance monitoring also includes power supply voltage levels, card-out-of-file interlocks, and battery voltage levels on battery-backed memory cards (if used). Out-of-tolerance conditions will result in an inoperative (out-of-service) condition for that particular system function.

Automatic system self-testing occurs during a portion of every periodic transmission period of the data communication network. Since exhaustive tests cannot be performed during any one transmission interval, the test software is written so that sufficient overlap coverage is provided to prove system performance during tests of portions of the circuitry, as allowed in IEEE 338.

The Essential Multiplexing System (EMS) is included in the continuous, automatic self-test function. Faults at the Remote Multiplexing Units (RMUs) are alarmed in the main control room. Since EMS is dual in each division, self-test supports automatic reconfiguration or bypass of portions of EMS after a detected fault, such that the least effect on system availability occurs.

(2) Off-line Semi-automatic End-to-End Testing

The more complete, manually-initiated, internal self-test is available when a unit is off-line for surveillance or maintenance testing. This test exercises the trip outputs of the SSLC logic processors. The channel containing the processors will be bypassed during testing.

A fault is considered the inability to open or close any control circuit.

Self-test failures are displayed on a front panel readout device or other diagnostic unit.

To reduce operator burden and decrease outage time, a Surveillance Test Controller (STC) is provided as a dedicated test instrument in each division of SSLC. The STC performs semi-automatic (operator-initiated) testing of SSLC functional logic, including trip, initiation, and interlock logic. Test coverage includes verification of correct operation of the following capabilities, as defined in each system IBD:

a. Each 2/4 coincident logic function.

b. Serial and parallel I/O, including manual control switches, limit switches, and other contact closures.

c. The 1/N trip selection function.

d. Interlock logic for each valve or pump.

A separate test sequence for each safety system is operator-selectable; testing will proceed automatically to conclusion after initiation by the operator. Surveillance testing is performed in one division at a time.

The STC injects test patterns through the essential multiplexing system (EMS) communications links to the RMUs. It then tests the RMUs ability to format and transmit sensor data through and across the EMS/SSLC interface, in the prescribed time, to the load drivers. Under the proper bypass conditions, or with the reactor shut down, the load drivers themselves may be actuated.

All testing features adhere to the single failure criterion, as follows: 1) No single failure in che test circuitry shall incapacitate an SSLC safety function. 2) No single failure in the test circuitry shall cause an inadvertent scram, MSIV isolation, or actuation of any safety systems served by the SSLC.

CHAPTER 10 QUESTIONS/RESPONSES

QUESTION 281.15

In a letter from Thomas E. Murley, NRR, to Ricardo Artigas, G.E. dated August 7, 1987, the staff provided the ABWR licensing review bases as well as the scope and content of the and content of the ABWR Standard Safety Analysis Report (SSAR). In Section 8.7, Water Chemistry Guidelines, of the referenced letter, it states that GE has committed to using BWR Owners Group water chemistry guidelines. These guidelines are necessary to maintain proper water chemistry in BWR cooling systems to prevent intergranular stress corrosion cracking of austenitic stainless steel piping and components and to minimize corrosion and erosion/corrosion-induced piping wall thinning in single-phase and two-phase high energy carbon steel piping. Water chemistry is also important for the minimization of plant radiation levels due to activated corrosion products. Section 10.4.6.3 of the ABWR indicates that the condensate cleanup system complies with Regulatory Guide 1.56. Section 10.4 should indicate that the system meets the guidelines published in:

EPRI NP-4947-SR, BWR Hydrogen Water Chemistry Guidelines 1987 Revision, dated October 1988.

EPRI NP-5283-SR-A, Guidelines for Permanent BWR Hydrogen Water Chemistry-1987 Revision, dated September 1987.

The use of zinc injection as a means of controlling BWR radiation-field build-up should be discussed.

RESPONSE 281.15

A new Subsection 9.3.9 will be added to describe the hydrogen addition system. Revised Subsection 5.2.3 indicates that the guidelines in EPRI NP-4947-SR, BWR Hydrogen Water Chemistry Guidelines 1987 Revision, October 1988 and EPRI NP-5283-SR-A, Guidelines for Permanent BWR Hydrogen Water Chemistry-1987 Revision, September 1987 will be met. This will also be indicated in new Subsection 9.3.9.

Subsection 9.3.11 has been added to describe the zinc addition system.

QUESTION 281.16

In Section 10.4.6.3, the ABWR SSAR indicates that the condensate cleanup system removes some radioactive material, activated corrosion products and fission products that are carried over from the reactor. More important functions involve removal of condensate system corrosion products, and possible impurities from condenser leakage to assure meeting BWR Hydrogen Water Chemistry Guidelines. This should be discussed.

RESPONSE 281.16

Subsection 5.2.3.2.2.3 has been modified to discuss the removal of condensate system corrosion products and possible impurities from condenser leakage.

QUESTION 281.17

The condensate (Figure 10.4-4) and feedwater (Figure 10.4-7) system diagrams do not indicate the location of the oxygen injection into the condensate system and hydrogen and zinc oxide into the feedwater system. This information should be provided.

RESPONSE 281.17

The location of oxygen addition for the condensate system is in Subsection 9.3.10. The location of hydrogen addition to the feedwater system will be shown in Subsection 9.3.9. The location of zinc addition to the feedwater system is in Subsection 9.3.11.

QUESTION 281.18

Section 10.4 does not discuss design improvements involving material selection, water chemistry, system temperatures, piping design and hydrodynamic conditions that are necessary to control erosion/corrosion. The EPRI CHECMATE or other erosion/corrosion computer codes may be useful design tools to minimize wall thinning due to erosion/corrosion. The ABWR SSAR should discuss design considerations to minimize erosion/corrosion and procedures and administrative controls to assure that the structural integrity of single-phase and two phase high-energy carbon steel piping system is maintained.

RESPONSE 281.18

A discussion on the control of erosion-corrosion of carbon steel has been added to Subsection 5.2.3.2.2.3.

9.3.10 Oxygen Injection System

9.3.10.1 Design Bases

The oxygen injection system is designed to add sufficient oxygen to the Condensate System to suppress corrosion and corrosion product release in the condensate and feedwater systems. Experience has shown that the preferred feedwater oxygen concentration is 20 to 50 ppb. During shutdown and startup operation the feedwater oxygen concentration is usually much above the 20 to 50 ppb range. However, during power operation, deaeration in the main condenser may reduce the condensate oxygen concentration below 20 ppb, thus, requiring that some oxygen be added. The amount required is up to approximately 5 cubic feet per hour.

9.3.10.2 System Description

The oxygen supply consists of high pressure gas cylinders or a liquid tank. A condensate oxygen injection module is provided with pressure regulators and associated piping, valves, and controls to depressurize the gaseous oxygen and route it to the condensate oxygen injection modules. There are check valves and isolation valves between the condensate injection modules and the condensate lines upstream of the condensate filters.

The flow regulating valves in this system are operated from the main control room. The oxygen concentration in the condensate/feedwater system is monitored by analyzers in the sampling system (subsection 9.3.2). An operator will make changes in the oxygen injection rate in response to changes in the condensate/feedwater oxygen concentration. An automatic control system is not required because instantaneous changes in oxygen injection rate are not required.

9.3.10.3 Safety Evaluation

The oxygen injection system is not required to assure any of the following conditions.

(1) integrity of the reactor coolant pressure boundary;

(2) capability to shut down the reactor and maintain it in a safe shutdown condition; or

(3) ability to prevent or mitigate the consequences of events which could result in potential offsite exposures.

Consequently, the injection system itself is not safety-related. The high pressure oxygen storage bottles are located in an area in which large amounts of burnable materials are not present. Usual safe practices for handling high pressure gases are followed.

9.3.10.4 Tests and Inspections

The oxygen injection system is proved operable by its use during normal operation. The system valves may be tested to ensure operability from the main control room.

9.3.10.4 Instrumentation Application

The oxygen gas storage bottles have pressure gages which will indicate to the operators when a new bottle is required. A flow element will indicate the oxygen gas flow rate at all times. The gas flow regulating valves will have position indication in the main control room.

The oxygen monitors are discussed in Subsection 9.3.2.

281.17

9.3.11 Zinc Injection System

9.3.11.1 Design Bases

The continuous presence of small amounts of dissolved zinc in the reactor water has been shown to reduce radiation levels on primary system surfaces. Zinc injection shall be initiated during the reactor startup tests when high temperature operation commences. The amount of dissolved zinc required in the reactor water is 10 to 15 ppb zinc during an initial conditioning period and 5 to 10 ppb over the fuel cycle.

A dilute zinc solution is prepared and injected into a bypass loop around the feedwater pumps.

9.3.11.3 Safety Evaluation

The injection system is not necessary to assure:

1) the integrity of the reactor coolant pressure boundary;

2) the capability to shut down the reactor; or

3) the capability to prevent or mitigate the consequences of events which could result in potential offsite exposures.

The zinc injection system will help keep radiation levels as low as possible, thus, reducing personal exposure especially during outages.

281.15

9.3.11.4 Tests and Inspections

The zinc injection system is proved operable during initial operation of the plant. Zinc injection will not be performed when the plant is in cold shutdown. During these periods, the system can have maintenance or testing performed.

9.3.11.5 Instrumentation

The injection of zinc solution will be stopped automatically if feedwater flow stops. The zinc injection rate is manually adjusted based on zinc concentration data in the reactor water.

51-182

cessive oxidation, hydriding, or crud deposition may lead to a breach of the cladding wall.

Metallic impurities can result in neutron losses and associated economic penalties which increase in proportion to the amount being introduced into the reactor and deposited on the fuel. With respect to iron oxide-type crud deposits, it can be concluded that operation within the BWR water chemistry guidelines (specifically the limits on feedwater iron levels) effectively precludes the buildup of significant deposits on fuel elements.

5.2.3.2.2.2 Radiation Field Buildup

The primary long-term source of radiation fields in most BWRs is cobalt-60, which is formed by neutron activation of cobalt-59. Corrosion products are released from corroding and wearing surfaces as soluble, colloidal, and particulate species. The formation of cobalt-60 takes place after the corrosion products precipitate, adsorb, or deposit on the fuel rods. Subsequent reentrainment in the coolant and deposition on out-of-core stainless steel surfaces leads to buildup of the activated corrosion products (such as cobalt-60) on the out-of-core surfaces. The deposition may occur either in a loosely adherent layer created by particle deposition, or in a tightly adherent corrosion layer incorporating radioisotopes during corrosion and subsequent ion exchange. Water chemistry influences all of these transport processes. The key variables are the concentration of soluble cobalt-60 in the reactor water and the characteristics of surface oxides. Thus, any reduction in the soluble cobalt-60 concentration will have positive benefits.

281.10, Item 1

As a means to reduce cobalt, GE has reduced cobalt content in alloys to be used in high fluence areas such as fuel assemblies and control rods. In addition, cobalt base alloys used for pins and rollers in control rods have been replaced with noncobalt alloys.

281.10, Item 8

The reactor water cleanup system, which processes reactor water at a rate of 2% of rated feedwater flow, will remove both dissolved and undissolved impurities which can become radioactive deposits. Reduction of these radioactive deposits will reduce occupational radiation exposure during operation and maintenance of the plant components.

Water quality parameters can have an influence on radiation buildup rates. In laboratory tests, the water conductivity and pH were varied systematically from a high purity base case. In each case, impurities increased the rate of cobalt-60 uptake over that of the base case. The evidence suggests that these impurities change both the corrosion rate and the oxide film characteristics to adversely increase the cobalt-60 uptake. Thus, controlling water purity should be beneficial in reducing radiation buildup.

Prefilming of stainless steel in cobalt-60 free water, steam, or water/steam mixtures also appears to be a promising method to reduce initial radiation buildup rates. As an example, the radiation buildup rates are reduced significantly when samples are prefilmed in high temperature (288°C), oxygenated (200 ppb oxygen) water prior to exposure to cobalt-60 containing water. Mechanical polishing and electropolishing of piping internal faces should also be effective in reducing radiation buildup.

5.2.3.2.2.3 Sources of Impurities

Various pathways exist for impurity ingress to the primary system. The most common sources of impurities that result in increases in reactor water conductivity are condenser cooling water inleakage, improper operation of ion exchange units, air inleakage, and radwaste recycle. In addition to situations of relatively continuous ingress, such as from low level condenser cooling water inleakage, transient events can also be significant. The major sources of impurities during such events are resin intrusions, organic chemical intrusions, inorganic chemical intrusions, and improper rinse of resins. Chemistry transients resulting from introduction of organic substances into the radwaste system comprised a significant fraction of the transients which have occurred.

INSERT NEXT PAGE

The following factors are measured for control or diagnostic purposes to maintain proper water chemistry in the ABWR.

281.16

The condensate cleanup system has two stages of water treatment. The first stage, the hollow fiber filters, is effective in removing insoluble solids, such as condensate system insoluble corrosion products. The second stage, the deep bed demineralizers, is effective in removing soluble solids, such as soluble corrosion products and impurities from possible condenser leakage.

sion following HWC implementation.

(b) Quantitative assessment of water chemistry transients.

(c) Long-term quantification of the success of the HWC program.

The major impurities in various parts of a BWR under certain operating conditions are listed in Table 5.2-5. The plant systems have been designed to achieve these limits at least 90% of the time. The plant operators are encouraged to achieve better water quality by using good operating practice.

281.10 Items 6 & 9

Water quality specifications require that erosion-corrosion resistant low alloy steels are to be used in susceptible steam extraction and drain lines. Stainless steels are considered for baffles, shields, or other areas of severe duty. Provisions are made to add nitrogen gas to extraction steamlines, feedwater heater shells, heater drain tanks, and drain piping to minimize corrosion during layup. Alternatively, the system may be designed to drain while hot so that dry layup can be achieved.

281.10 Item 7

Condenser tubes and tubesheet are required to be made of titanium alloys.

← INSERT NEXT PAGE

Erosion-corrosion (E/C) of carbon steel components will be controlled as follows. The mechanism of E/C or, preferably, flow assisted corrosion is complex and involves the electrochemical aspects of general corrosion plus the effects of mass transfer. Under single phase flow conditions, E/C is affected by water chemistry, temperature, flow path, material composition and geometry. For wet steam (two phase), the percent moisture has an additional effect on E/C.

The potential deterioration of ABWR carbon steel piping from flow assisted corrosion due to high velocity single phase water flow and two phase steam water flow will be addressed by using the EPRI developed CHECMATE (Chexal Horowitz Erosion Corrosion Methodology for Analyzing Two-phase Environments) computer code. CHECMATE will be used to predict corrosion rates and calculate the time remaining before reaching a defined acceptable wall thickness. Thus, this code will be used to identify areas where design improvements (piping design, materials selection, hydrodynamic conditions, oxygen content, temperature) are required to ensure adequate margin for extended piping performance in the ABWR design.

281.18