July 31, 1991

Docket No. STN 50-605

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

Dear Mr. Marriott:

SUBJECT: RESOLUTION OF ISSUES RELATED TO CHAPTER 7, "INSTRUMENTATION AND CONTROL SYSTEMS" OF THE GE ABWR SSAR

Enclosed is a summary of issues related to the staff's review of Chapter 7, "Instrumentation and Control Systems" of the Advanced Boiling Water Reactor (ABWR) Standard Safety Analysis Report. The issues describe a need for additional information to facilitate the staff's design certification review.

The staff considers the Instrumentation and Control System to be a very important aspect of the ABWR design and has consequently devoted significant and early attention to its review. The information contained within the enclosure should form the basis for timely discussions and meetings to resolve the issues. If you have any questions regarding the enclosed issues, please call me on (301) 492-1121.

Sincerely,

Original Signed By:

Victor M. McCree, Project Manager
Standardization Project Directorate
Division of Advanced Reactors
and Special Projects
Office of Nuclear Reactor Regulation

Enclosure:
As stated

cc w/enclosure:
See next page

DISTRIBUTION

Docket File
WTravers
DScaletti
TMurley, 12G18
LShao, NL007
WMorris, RES

NRC PDR
PShea
OGC, 15B18
FMiraglia, 12G18
RBosnak, NL007
BHardin, NLS169

PDST R/F
VMcCree
EJordan, MDBB 3701
JPartlow, 12G18
JO'Brien, NL217A
GSuh, 12E4 (2)

DCrutchfield
CPoslusny
ACRS (10), P-315
WRussell, 12G18
ZRosztoczy, NLS169
OGormley, RES

OFC	LA:PDST:DAR	PM:PDST:DAR	D:PDST:DAR				
NAME	PShea	VMcCree:tz	CMiller				
DATE	7/31/91	/ /91	7/31/91				

OFFICIAL RECORD COPY

Document Name: GE SSAR LTR

cc: Mr. Robert Mitchell
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

Enclosure

The followinc issues have becn developed from the staff's review of Chapter 7, of the ABWR SSAR and require resolution prior to design certification.

1. **The staff concluded that tne design, as presented in the Advanced Boiling Water Reactor (ABWR) Standard Safety Analysis Report (SSAR) to date, is not essentially complete.** GE should provide greater design detail for mout of the ABWR systems. References to past GE designs are irrelevant, including the GE NUMAC line of instrumentation and control equipment, unless specifically submitted as part of the design. The need for prototypes to demonstrate aspects of the design are included in this open issue. The following specific comments apply:

   a. The staff concluded that prototype testing of new technology is required to confirm expected safety performance, to confirm unforseen systems interactions, and allow the staff to reach its safety determination on systems which may not have extensive operating experience. Based on information currently available, the staff believes that prototypes will be needed to demonstrate acceptable performance of the interconnected RPS, ESFAS, EMS, and SSLC systems.

   b. The staff concluded that GE should specify which periodic reactor protection system tests will be used to satisfy technical specification (TS) requirements.

   c. The staff concluded from its review of the ABWR RPS and RC&IS conceptual design description and GE's responses to RAIs that more detailed information regarding this system is required for the staff to make its safety determination. The staff will conduct detailed discussions with GE to specify the scope of required information.

   d. The staff requests that GE formally submit (docket) its undocketed assessment of the loss of all four divisions of the ABWR Essential Multiplexing System (EMS), which concluded that the plant could be safely shutdown from the remote shutdown system.

   e. The staff concluded that the design of the EMS is not essentially complete and that GE should define the software architecture that runs in the EMS microprocessors. In addition, GE should demonstrate how the decision logic, which in an analog design is a parallel process, would be implemented by the software, which is usually a serial process. GE has provided high level block diagrams of the data signal paths; however, the software implied in the system block diagrams can mask much of the safety system's design complexity. Since the software is an essential line element in the execution of the safety system functions, a definition of the software architecture is required for the staff to make its safety determination. The architecture should include application specific software, operating system software and embedded software.

f. The staff concluded that GE should define the functional requirements of the EMS, the major parameters that define the data transmission attributes, and the criteria for selecting the data transmission hardware. The staff recognizes that the detail design of the EMS depends on the hardware that is selected, however, the functional requirements for the EMS as part of the ABWR safety systems are not hardware dependent.

g. The staff concluded that GE should provide information describing in detail the fault tolerant design features of the SSLC system. In response to the staff request (Q420.49) to describe the fault tolerant features of the SSLC system, GE responded that the system will be capable of error correction of inputs and outputs, retry or rollback to last known correct state on fault detection, restart without lockup on fault such as EMI, data transmission error correction, continued operation through transient fault, and continued operation through permanent fault. GE's response should include additional information which describes the SSLC system design features that accomplish the described capabilities.

h. The staff concluded that GE should provide additional information which describes the bus protocol for the SSLC hardware design, bus data capacity, accommodations for hardware level interrupts, size of the memory, speed and size of the microprocessor, format of the status panel, hardware based interlocks, type of display media, and the method of providing the TLU trip status to the operator.

i. The staff concluded that GE should provide information which describes the design approach employed for the SSLC software. GE should also demonstrate how the decision logic, which in an analog design is a parallel process, will be implemented by the software, which is a serial process. GE should present design documentation of how the listed software elements will interact with each other and what considerations were given to ensure data integrity, error handling, task priority, timing, variable representations, module structures, interrupt handling, and fault tolerance.

j. The staff concluded that a top level design of the SSLC software is required for the staff to make its safety determination. The staff acknowledged GE's statements that the software design for the SSLC was not available for review because it is hardware dependent and the hardware had not been selected. The staff also reviewed the SSLC design description presented in the SSLC System Design Specification (SDS) (undocketed). The staff considered the documentation presented for the SSLC to be inadequate for design evaluation and not in conformance with the requirements for level of detail. Because software implements the functionality of computer-based SSLC, the top level design of the software is necessary for the staff review.

k. The staff concluded that GE should provide information, in accordance with IEEE Std 7-4.3.2, describing methods to be employed to verify and validate the development of the software which would implement the SSLC and EMS logic functions.

l. The staff concluded that GE should provide information which describes the EMS fiber optic local area network design requirements upon which the control standard, the software and hardware selection was based. Since the EMS is central to the functioning of all safety systems for the ABWR, the staff has concluded that more detailed specifications of the EMS are required prior to making its safety determination.

m. The staff concluded that a top level design of the EMS software is required for the staff to make its safety determination. The staff acknowledges GE's statements that the software design for the EMS was not available for review because it is hardware dependent and the hardware had not been selected. However, in the development of computer-based systems, the staff considers it to be good engineering practice to have a top level design of the software as a criteria to be considered in the hardware selection.

n. The staff requests that GE clarify the design description presented for the EMS regarding synchronous communication over the local area network. In SSAR Appendix 7A it stated that the "...systems are independent and will run asynchronously..." page 7A.A-2 in the EMS/SSLC Interface Requirements [MPL A32-4080] stated that the System timing will be asynchronous...", and page 5, "all communications shall be asynchronous...." However, the same document stated that "...communications processing circuitry... will append synchronizing and parity checking information" [page 14, Section 3.5.1 and Section 3.5.3.

o. The staff requests that GE clarify the contradictory design information provided on the Control Multiplexor Unit (CMU), an essential part of the EMS. From the information in Appendix 7A it was apparent that the EMS consisted of the Remote Multiplexor Unit (RMU), the CMU and the fiber optic cable connecting the RMU and CMU. However, in most of the drawings reviewed by the staff, the CMU was not shown as a separate component but as an implied part of the SSLC, although the RMU was shown explicitly connected to the multiplexor system (of which the RMU was a part).

p. The staff requests GE to clarify a discrepancy in the description of the major components of the EMS. The Multiplexing Control Units (MCU) is discussed in SSAR Section 15.B.4 although it was not discussed as a separate component in SSAR Chapter 7. It was unclear whether this was an abstraction to facilitate the FMEA or whether the EMS does indeed contain an element called MCU. The MCU was described as the bridge between the optical and digital signals, with the stated purpose of providing control of the data transmission. Other documentation stated that control of the fiber optic transmission medium was shared between RMUs and CMUs. It was also unclear whether the MCU was the communications module in the RMU and CMU.

q. The staff requests GE to clarify its design information on the Self Test System (STS). GE indicated that the STS must cycle from circuit-to-circuit very rapidly. It is not clear to the staff what circuits are referred to since the SSLC is implem nted using digital microprocessors. GE did not state if the STS would place the SSLC software in a special testing mode to allow very rapid cycling of the system test.

r. The staff requests GE to clarify design information which describes how the transfer of sensor transmitter outputs would occur without the loss of the calibration data updates. The staff notes that the calibration data updates would be stored in the SSLC system microprocessors which would presumably be disconnected from the readouts.

s. The staff concluded that GE should provide design information to demonstrate the manner in which safety related data will be processed and displayed, and describe dependencies on supporting hardware and software. The staff acknowledges that GE has provided a comprehensive list of variables that were considered essential for providing safety related information to the operators. Explicit tables of conformance and specific exceptions to RG 1.97 were provided in the SSAR, and functional requirements for display of data were provided in the process system descriptions in the SSAR.

t. The staff concluded that GE should provide design documentation to demonstrate that conformance to appropriate standards will be achieved. The staff acknowledges GE's commitment in the SSAR which states that interlock systems important to safety (i.e., Neutron Monitoring System, Process Radiation Monitoring System, High Pressure/Low Pressure Interlocks, Fuel Pool Cooling and Cleanup System, Drywell Vacuum Relief System, Containment Atmosphere Monitoring System and Suppression Pool Temperature Monitoring System) are in conformance with the applicable GDCs, Regulatory Guides and Branch Technical Positions, however, GE has not provided design information to confirm that these commitments will be manifest in the design.

u. The staff concluded that GE should provide additional information on the I&C design of the Recirculation Flow Control System to facilitate an assessment of possible single failure points of the design such as manual control, automatic speed control input, the interprocessor communication links and load demand signal from main turbine pressure regulator.

v. The staff concluded that GE should provide additional information to facilitate an evaluation of the EMS/NEMS connection and how it addresses the isolation requirements of IEEE 279.

w. The staff concluded that GE should provide additional information which demonstrates that equipment design and installation standards are incorporated to prevent electrostatic discharge (ESD) at keyboards, keyed switches and other exposed equipment components.

2. **Isolation of corrupted data transmitted via the multiplexors must be addressed in addition to electrical and physical isolation criteria.** (7.2.1., 7.8,

a. The staff concluded that GE should provide additional information on the Reactor Protection System (RPS) to address the electrical and physical separation between the four channels. Because of the extensive use of multiplexors and software, the staff considers that isolation of information (error handling) to be an essential factor in its safety determination.

b. The staff concluded that GE should clarify design information provided on the issues of electrical, data and control isolation and separation. The manner of sending data to the plant computer was stated in general terms and key design issues remained unclear. GE stated that the sensor data is taken from the CMU and sent to the plant computer through a data buffer. It was stated that the buffer provided isolation between the plant computer and the safety system EMS, but no data was provided about the location of the data buffer, how the read/write access was controlled, and which device cleared the buffer.

c. The staff concluded that GE should provide design information to address the issue of safety system connectivity to non-safety systems. It appears to the staff that the Non-Essential Multiplexing System (NMES) is directly connected to the EMS through the CMU of the EMS. Since the EMS is uced to carry safety system sensor data and to activate and control ESF systems, a failure in the EMS would disable a division. A failure of the NEMS or plant computer could challenge or adversely affect the operation of the EMS, unless the broadcast software had design features that would make such failure propagation improbable. In particular, the staff was concerned with software failures in the NEMS that could lead to undetected software failures in the EMS.

d. The staff concluded that GE should provide information in Section 7.8 of the SSAR to specifically address non-safety information interfaces; that is, information transfer between safety and non-safety systems. The staff acknowledged that GE performed a study of each of the I&C systems included in Chapter 7 of the SSAR and determined that there are no safety-related electrical signal interfaces and therefore no interface requirements for the utility applicant. However, the SSAR did not address information transfer to equipment outside of the scope of the SSAR.

e. The staff concluded that GE should provide additional information on the STS and SSLC to address the issue of data and control separation. The staff noted that fiber optical data links will be used to ensure electrical separation, however, the issue of information separation has not been addressed. GE should demonstrate that the STS and SSLC designs preclude adverse effects within the extensive data and control software considering the interconnection of STS modules in each division within the control room. GE should also examine the safeguards incorporated to provide isolation and separation according to IEEE-279.

3. **The Failure Modes and Effects Analysis provided in SSAR 15.B.4 is inadequate. The staff requires a significantly more detailed analysis including a software hazards analysis.** (7.2.3)

a. The staff concluded that GE should provide Failure Modes and Effects Analysis information in accordance with GDC 23, "Protection System Failure Modes." This information should demonstrate that all postulated RPS and ESF failures result in a known safe state if conditions such as disconnection of the system, loss of energy or a postulated adverse environment are experienced.

4 **GE did not demonstrate conformance with the Electric Power Research Institute (EPRI) Requirements Document (RD), Chapter 10, "Man-Machine Interface Systems."** (7.1)

a. The staff concluded that GE should provide additional information for the following items required or discussed by the EPRI RD:

RG 1.106, RG 1.33, GL 83-08, 10CFR50.62, GDC 3, GDC 17, GDC 26, IEEE 730, IEEE 829, IEEE 472, BTPCMEB9.5-1, 10CFR APP B, ISA 67-15, ANSI C96.1, NEMA, DOD 263, IPCEA 561402, NUREG CR4640, NUREG 0993, NUREG CR3958, NUREG CR4385, NUREG CR4386, NUREG CR4387, NUREG 0572, NUREG 0977, NUREG 1000, NUREG 0696, NUREG 1154, NUREG 0985, NSAC-39, EPRI 2184-7, MILSPEC 338, MILSPEC 217E, MILSPEC 781, MILSPEC 472, EPRI NP3659, EPRI NP6209, EPRI 5693, EPRI NP3448, EPRI NP3701, EPRI NP3659 and EPRI RP27057

5. **The SSAR did not provide adequate commitment to the industry standards and criteria as required with GDC 1.** (7.1)

a. The staff concluded that GE should provide additional information to demonstrate its commitment to GDC 1 for the SSLC and EMS design. The staff noted that there was no evidence in the SSAR that current IEEE and other computer/electronics industry standards related to advanced technology had been considered in the design; for example, no standards were identified regarding electromagnetic compatibility, local area networks, communications protocols, and software design.

6. **The method of determining Master and Standby status of the dual loop network in the Essential Multiplexing System (EMS) is not adequately described.** (7.2.2)

a. The staff requests that GE provide information to clarify how the two Digital Trip Modules (DTM) in the EMS network arbitrate to determine which will be the MASTER loop. The staff noted that the two EMS network loops are designated MASTER and STANDBY by the receiving fiber optic interface. The designation of which loop is MASTER is on the basis of transmission errors and checksum errors, as well as the results of self test. The hardware diagrams that the staff has reviewed showed that each Digital Trip Module (DTM) in the SSLC has two fiber optic interfaces. The design parameters of how the MASTER loop is designated is important to the evaluation because it could address possible software failure modes like deadly embrace, lockup, and other contention issues that can disrupt communications EMS. This designation is also applicable at the RMU level where ESF equipment actuation commands are received.

7. **The SSLC Self Testing System (STS) is required to be qualified to the same level as the system it serves.** (7.2.2)

a. The staff concluded, based on the information presented, that the STS should be considered a safety grade system because it is embedded in the SSLC and interfaces directly with the safety system software. The staff noted that when the STS has possession of the EMS token, a non-safety system (the STS) is in control of a safety system (the EMS), albeit only a short time. A failure of the STS to pass on the token would result in the EMS being disabled until the timeout for lost token expired, and a new one would be generated. Since the STS software was considered a non-safety system, it must be assumed that the STS software will fail in any conceivable mode, including the mode whereby it keeps running tests. The staff also requests that GE provide information which describes how the STS would acquire the token to send an EMS message and specify the duration of the token timeout.

8. **The design bases and criteria for electromagnetic compatibility and environmental qualification should be provided.** (7.2.3)

a. The staff concluded that GE should provide information which identifies the design bases and criteria for EMC and environmental qualification. The quality levels of the SSLC hardware, thermal design implementation limits and design practices or standards to limit possible electromagnetic interference (EMI) effects should also be provided. The lack of design control for these parameters could result in common mode failures for multiple divisions, from such failures as loss of HVAC, and electromagnetic interference pulses from unanticipated field effects common to all divisions. The potential for disabling multiple RPS and ESF logic divisions is a critical safety concern that requires additional review.

b. The staff concluded that ESD should not be considered a site specific concern and recommends that it be removed as an interface requirement from Section 7.8 and Table 1.9-1.

c. The staff concluded that GE should provide additional information to address design limit(s) for HVAC equipment designs. The staff noted the HVAC cooling design provided in the SSAR represents traditional BWR cooling designs, but does not reflect consideration of any additional cooling required to limit the presence of hot spots due to higher current densities within the digital chip designs employed in the ABWR. The staff also requests GE to comment on any additional HVAC controls and direct cooling requirements.

d. The staff has concluded that GE should define the sensitivity of safety computer systems to electromagnetic fields and provide information to identify acceptable radiation levels and frequency ranges for plant communication transmitters and receivers. Controls, test programs, field measurements and operational descriptions should be employed to implement EMC and avoid effects such as spurious actuation of safety related equipment.

9. **Clarification is required as to which signals are multiplexed and which are not.** (7.2.3)

a. The staff requests that GE clarify which RPS signals are multiplexed and which are not. Figure 7A-1 in GE Document No. 23A1317 of undocketed MPL Document A32-4080, showed that many of the RPS related sensors are connected directly to the Digital Trip Modules (DTM) and do not go through the EMS. This was contradicted by Figure 7.A.2-1 in SSAR Chapter 7A which showed all the sensor signals sent via the EMS.

10. **The common mode failure of software has not been adequately addressed.** (7.2)

a. The staff concluded that GE should provide additional information which describes design features to preclude the common mode failure of software, including an analyses which demonstrates how the SSLC, EMS, ESF, and STS designs comply with NUREG-0493.

Since the ARI function and the SLCS instrumentation are subject to the common mode failure of the EMS and SSLC systems for effects such as EMI or software operational problems, the analysis should consider the detailed effects of such failures and how operation of the systems could continue. The staff also noted the possibility that the EMS and NEMS would use the same software modules and, therefore, upon a software error, could fail simultaneously. This would represent a challenge to defense-in-depth and should be evaluated. Since a detailed failure modes and effects analysis will not be performed for the STS system, it was also unclear to the staff how the SSLC design would mitigate the results of a postulated common mode failure of the STS software (related open item - no. 7).

11. **Failure analysis must include possible outages for maintenance in the evaluations.** (7.2.3)

a. The staff concluded that GE should provide an I&C failure analysis which includes outages due to I&C maintenance and a discussion of acceptable maintenance practices. The staff noted that additional information provided in response to questions has not provided enough detail for the staff to evaluate the GE findings. The staff also requests that GE clarify its maintenance requirements for Reactor Internal Pump (RIP) maintenance and the associated reliance, in part, on leak detection instrumentation to detect failures. The clarification should also describe the availability of the leak detection system during shutdown maintenance on the RIPs.

12. **There is an apparent contradiction in the power supply sources for the Automatic Depressurization System (ADS) and the Reactor Core Isolation Cooling System (RCIC).** (7.3.1)

a. The staff requests that GE clarify an apparent contradiction in the power supply sources for the ADS and RCIC systems. SSAR Section 7.3.1.1.1.2 (2) indicates that the ADS is powered from Divisions I & II. However, SSAR Figure 7.2-1 (Amendment 5) indicates that the ADS power supplies are from divisions I and IV. Similarly, the SSAR section 7.3.1.1.1.3 (3) indicates that the RCIC is powered from Division I, however, Figure 7.2-1 indicates that RCIC is powered from Divisions II and IV.

13. **The method of operation of the remote shutdown station is not described.** (7.4)

a. The staff requests that GE provide information which describes how the two Remote Shutdown Panels, which are to be located in separate areas, can be operated simultaneously or in a master/slave arrangement. In addition, the staff requests GE to clearly describe in the SSAR how data is transferred to the two remote shutdown panels in the event that the control room becomes unusable.