HITACHI

GE Hitachi Nuclear Energy

Richard E. Kingston
Vice President, ESBWR Licensing

PO Box 780 M/C A-65
Wilmington, NC 28402-0780
USA

T 910 819 6192
F 910 362 6192
rick.kingston@ge.com

MFN 09-381 Docket No. 52-010

June 15, 2009

U.S. Nuclear Regulatory Commission
Document Control Desk
Washington, D.C. 20555-0001

Subject: **Response to Portion of NRC Request for Additional Information Letter No. 337 Related to ESBWR Design Certification Application - Auxiliary Systems - RAI Number 9.5-71 S02**

The purpose of this letter is to submit the GE Hitachi Nuclear Energy (GEH) response to the U.S. Nuclear Regulatory Commission (NRC) Request for Additional Information (RAI) sent by NRC letter 337, dated May 14, 2009, Reference 1. The GEH response to RAI 9.5-71 S02 is addressed in Enclosure 1. Enclosure 2 contains the DCD markups associated with this response.

If you have any questions about the information provided here, please contact me.

Sincerely,

Richard E. Kingston

Richard E. Kingston
Vice President, ESBWR Licensing

Reference:

1. MFN 09-331, Letter from the U.S. Nuclear Regulatory Commission to Jerald G. Head, Request for Additional Information Letter No. 337, Related To ESBWR Design Certification Application, dated May 14, 2009

Enclosures:

1. Response to Portion of NRC Request for Additional Information Letter No. 337 Related to ESBWR Design Certification Application - Auxiliary Systems - RAI Number 9.5-71 S02
2. Response to Portion of NRC Request for Additional Information Letter No. 337 Related to ESBWR Design Certification Application - Auxiliary Systems - RAI Number 9.5-71 S02 - DCD Markups

cc:	AE Cubbage	USNRC (with enclosures)
	J G Head	GEH/Wilmington (with enclosures)
	DH Hinds	GEH/Wilmington (with enclosures)
	eDRF Section	0000-0096-5747, Revision 1

Enclosure 1

MFN 09-381

Response to Portion of NRC Request for

Additional Information Letter No. 337

Related to ESBWR Design Certification Application

Auxiliary Systems

RAI Number 9.5-71 S02

NRC RAI 9.5-71 S02

In consideration of the response to RAI 9.5-71 S01, address the following:

A. Within the DCD Tier 2 Section 9.5.1.10 markup there are numerous mentions of "fire zones." These should be changed to "fire areas."

B. Section 9.5.1.12 of the DCD states in part that:

"The ESBWR design satisfies the following guidance from the NUREG-0800 SRP 9.5.1and BTP SPLB 9.5-1:

Guidance - "Therefore, the designers of standard plants have been informed that they must demonstrate that safe shutdown of their designs can be achieved, assuming that all equipment in any one fire area has been rendered inoperable by fire and that reentry to the fire area for repairs and for operator actions is not possible. The control room should be excluded from this approach, subject to the need for an independent alternate shutdown capability that is physically and electrically independent of the control room."

Conformance - The design of the fire barrier system and safe shutdown systems for the ESBWR are such that complete burnout of any single fire area without recovery does not prevent safe shutdown of the plant."

Based on a phone conversation with GEH on March 31, 2009, regarding RAI 9.5-71 S01, this may not be the case in that a fire in any single fire area may cause a spurious actuation that could prevent safe shutdown. For example, MSIV and RPS circuit behavior was discussed during this phone conversation. These circuits have load drivers that open circuits to actuate and fail safe to the required safe shutdown position. However, hot shorts could bypass these load drivers and cause spurious actuations that could prevent safe shutdown even though the circuit fails safe and deviate from the above conformance criteria. Deviations to the above conformance criteria/commitment must be documented in the DCD.

GEH Response

A. Within the DCD Tier 2 Section 9.5.1.10 markup there are numerous mentions of "fire zones." These should be changed to "fire areas."

A. GEH Response:

GEH agrees that the term "fire area" is more appropriate for the discussion related to design features that prevent or mitigate spurious actuations than " fire zones." The DCD Tier 2 Section 9.5.1.10 markup provided in response to RAI 9.5-71S01 will be revised in response to this RAI supplement with these changes.

B. Based on a phone conversation with GEH on March 31, 2009, regarding RAI 9.5-71 S01, this may not be the case in that a fire in any single fire area may cause a spurious actuation that could prevent safe shutdown. For example, MSIV and RPS circuit behavior was discussed during this phone conversation. These circuits have load drivers that open circuits to actuate and fail safe to the required safe shutdown position. However, hot shorts could bypass these load drivers and cause spurious actuations that could prevent safe shutdown even though the circuit fails safe and deviate from the above conformance criteria. Deviations to the above conformance criteria/commitment must be documented in the DCD.

B. GEH Response

GEH disagrees with the statement that the ESBWR design will allow a fire in any single fire area to cause a spurious actuation that could prevent safe shutdown.

Response to this original RAI describes how redundant circuit paths for MSIV and RPS load drivers ensure safe shutdown function.

The ESBWR plant is designed to prevent spurious actuations induced by a fire in a single fire area that could adversely affect the capability to achieve and maintain safe shutdown. The ESBWR design features as described in DCD Tier 2, Subsection 7.1.3 minimize the adverse affect on safe shutdown from fire-induced spurious actuations. First, the ESBWR instrumentation and control system is digital. A spurious signal cannot be induced by fire damage in a fiber optic cable. The hard wires are minimized to limit the consequences of a postulated fire. The communication links between the main control room (MCR) and the DCIS rooms do not include any copper or other wire conductors that could potentially cause fire-induced spurious actuations that could adversely affect safe shutdown. From the DCIS rooms to the components, fiber optics will also be used up to the Remote Multiplexing Units (RMUs) in the plant. Hard wires then are used to control the subject components. Typically, two or three load drivers in series are actuated simultaneously in order to actuate the component. To eliminate spurious actuations, these multiple load drivers are located in different fire areas. Therefore, a fire in a single fire area cannot cause spurious actuations of all load drivers. The exposure of the distributed control and information system (DCIS) equipment to heat and smoke caused by a fire in a single fire area does not cause spurious actuations that could adversely affect safe shutdown. Also fire barriers of 3-hour fire resistance rating are provided in the ESBWR plant design that separate:

- Safety-related systems from any potential fires in nonsafety-related areas that could affect the ability of safety-related systems to perform their safety function.
- Redundant divisions or trains of safety-related systems from each other to prevent damage that could adversely affect a safe shutdown function from a single fire.
- Components within a single safety-related electrical division that present a fire hazard to components in another safety-related division.
- Electrical circuits (safety-related and nonsafety-related) whose fire-induced failure could cause a spurious actuation that could adversely affect a safe shutdown function.

GEH agrees that multiple hot shorts need to be considered for equipment that has hard wires for its power or control circuits to ensure that this equipment can be placed in its safe-shutdown position. DCD Subsection 8.3.1.4.1 describes that safety-related electric equipment and wiring are segregated into separate divisions so that no single credible event is capable of disabling enough equipment to hinder reactor shutdown, removal of decay heat from the core, or isolation of the containment in the event of an accident. Separation requirements are applied to control power and motive power for all systems involved. Each division of safety-related AC and DC system cables is provided with its own independent and separate raceway system.

The ESBWR PROBABILISTIC FIRE ANALYSIS (NEDO-33201) provides a deterministic analysis which credits the ESBWR digital instrument and control system design will prevent spurious actuations caused by a fire in a single fire area that could adversely affect safe shutdown. The existence of fire detection and suppression systems, fire barriers, and adequate monitoring and supervision means that it can be assumed that fire propagation to the neighboring zones separated by those barriers is a relatively negligible contribution. Nevertheless, potential inter-division propagation cases are considered in this analysis. The ESBWR, due to its basic layout and safety design features, is inherently capable of mitigating potential internal fires. Safety system redundancy and physical separation by fire barriers ensure that in all cases a single fire limits damage to a single safety system division or only one system of defense-in-depth (DID) system redundancy. Fire propagation to neighboring areas presents a relatively minor risk contribution.

Additional description of design features to prevent or mitigate spurious actuations and prevent multiple hot shorts for equipment that has hard wires for its power or control circuits and could result in the equipment not being able to be placed in its safe-shutdown position will be added to the DCD. This does not include the Staffs request to revise the COL applicant item for updating the FHA to ensure the detailed design does not introduce the potential for new spurious actuations, including the consideration of hot shorts. This COL applicant item was revised based on discussion with the NRC Staff at the April 22 DCWG. The NRC agreed at the May 14 DCWG that this item adequately addresses the safety issues associated with hot shorts. No additional COL item revisions are necessary.

DCD Impact

DCD Tier 2, Subsection 9.5.1.10 has been revised to include the design consideration of multiple hot shorts for equipment that has hard wires for its power of control circuits to ensure that this equipment can be placed in the required safe-shutdown position. See attached markup.

DCD Tier 2, Subsection 7.1.3.2 and Subsection 7.1.5.3 have been revised to include the design consideration to minimize the potential of for hot shorts and inadvertent and spurious actuation associated with the Q-DCIS, N-DCIS and DPS. See attached markup.

Enclosure 2

MFN 09-381

Response to Portion of NRC Request for

Additional Information Letter No. 337

Related to ESBWR Design Certification Application

Auxiliary Systems

RAI Number 9.5-71 S02

DCD Markup

active cooling is available, such as when the system is operating on only battery power during DBEs, the cooling is passive. The Q-DCIS components, including the fiber optic cable network, are not located in containment or in high radiation areas. Signals from within these areas are hardwired by copper cable to the RMUs. Electromagnetic compatibility (EMC) of the RMUs and Q-DCIS equipment is ensured by conformance to the following program.

- The Q-DCIS components are designed to minimize susceptibility to and generation of electromagnetic interference (EMI) and radio frequency interference (RFI).
- The Q-DCIS components are subjected to tests for EMI, RFI, and surge conditions that conform to guidelines in RG 1.180.
- Grounding of RMU and Q-DCIS equipment follows the guidance given in IEEE Std. 518 and IEEE Std. 1050.

To minimize EMI effects, the Q-DCIS electrical equipment incorporates shielding and filtering. The equipment is mounted in grounded panels provided with isolated instrument grounds.

The four divisions of Q-DCIS are physically located in four separate quadrants of the reactor building and four separate equipment rooms in the control building. These locations represent separate fire areas. Within the reactor building, there are separate fire areas within a division. The intra division fire areas are used to separate the RMUs that contain the series-connected load drivers used to operate safety-related solenoids and squib valves. The same reactor building fire areas are used to separate the DPS RMUs that contain the series-connected multiple load drivers used to operate nonsafety-related solenoids and squib valves. The fire area separation for both the safety-related and nonsafety-related RMUs will prevent inadvertent actuations affecting safe shutdown whether from hot shorts or fires in a single fire area. Finally, the control building Q-DCIS, N-DCIS, and DPS rooms are all separated into different fire areas.

7.1.3.2.1 Reactor Trip Systems

The Reactor Trip Systems include the RPS, the NMS, and SPTM functions.

7.1.3.2.1.1 Reactor Protection System

The safety-related RPS initiates an automatic reactor shutdown by rapid insertion of control rods (scram) if monitored system variables exceed pre-established limits. This action prevents fuel damage, limits system pressure, and, thus, minimizes the release of radioactive material. Refer to Subsection 7.2.1 for additional information.

7.1.3.2.1.2 Neutron Monitoring System

The safety-related NMS monitors the core thermal neutron flux from the startup source range to beyond rated power. The NMS provides logic signals to the RPS to automatically shut down the reactor when a condition necessitating a reactor scram is detected. Refer to Subsection 7.2.2 for additional information.

7.1.3.2.1.3 Suppression Pool Temperature Monitoring Subsystem

The safety-related SPTM ~~Subsystem~~ function of the CMS monitors suppression pool temperatures under all operating and accident conditions. This subsystem operates continuously during reactor operation. If the suppression pool temperature exceeds established limits, SPTM

N-DCIS failures are alarmed in the MCR. Periodic surveillance, using off-line tests with simulated input signals, verifies the overall system integrity.

The N-DCIS networks and components are distributed throughout the plant and are powered by redundant internal power supplies fed from two 120 VAC UPS. Some systems, such as the DPS, TGCS, FWCS, SB&PC System, and PAS, are triple redundant and are powered by three nonsafety-related UPS load groups.

7.1.5.3 N-DCIS Safety Evaluation

The N-DCIS is classified as nonsafety-related and is not required for safety-related purposes. Its operability is not required during or after any DBE. The N-DCIS is required to operate in the normal plant environment and is significant for power production applications. The N-DCIS does not perform any safety-related functions as a part of its design; however the N-DCIS does provide an isolated alternate path for safety-related data from Q-DCIS to N-DCIS that is presented in the MCR. The N-DCIS network that supports the dual/triple, fault-tolerant controllers of the process control systems uses a proven technique for high speed transfer of data different from Q-DCIS and thus provides diversity in design.

The N-DCIS equipment is located throughout the plant and is subject to the environment of each area. Specifically:

- RMUs are located throughout the plant and auxiliary buildings; and
- Computer equipment and peripherals are located mainly in the CB in the MCR and Back Panel areas. They are also located in other areas such as the EOF, Radwaste Building, TSC, Auxiliary Fuel Building, Auxiliary Fuel Building roof area, or alternate building designations specific to the plant design.

Most of the N-DCIS controller cabinets are located in two different rooms of the control building that are in separate fire areas. These rooms include the DPS equipment rooms and any of the Q-DCIS control building equipment rooms. The RMUs that support the N-DCIS controllers are located in most buildings of the power plant. Where the controllers support PIP A and PIP B systems, the controllers and RMUs are located in different fire areas. The DPS controllers are located in fire areas separate from the N-DCIS and Q-DCIS equipment rooms and the four DPS RMUs are located in the reactor building. Two of the four RMUs are located in fire areas (quadrants) of the reactor building separate from the other two RMUs. The two RMUs of each pair are located in separate fire areas to separate the DPS RMUs that contain the series connected multiple load drivers used to operate solenoids and squib valves and will prevent inadvertent actuations affecting safe shutdown whether from hot shorts or fires in a single fire area. Finally, the input signals/sensors that provide DPS backup scram, isolation and ECCS functions, and the DPS squib/solenoid valve outputs are arranged such that half of the inputs/outputs are on each pair of RMUs such that a single event cannot lose more than two of the signals needed for the two-out-of-four logic or all DPS (output) actuation.

The N-DCIS panels and components are designed to retain their structural integrity during and after DBEs so that proximate safety-related equipment is not prevented from performing its safety-related function.

Table 7.1-1 identifies the N-DCIS elements and the associated regulatory requirements, guidelines, and codes and standards applied. The N-DCIS major subsystems are summarized in

Manual fire alarm stations (pull box stations) are provided at the normal exit paths or every 61 meters (200 feet), whichever is less, throughout normally occupied buildings. Manual fire alarm stations (pull box stations) are provided at normal exit paths only for normally unoccupied buildings. Visible fire notification is provided in manned office areas such as in the Control Building and the Service Building.

9.5.1.10 Fire Barriers

Fire barriers of 3-hour fire resistance rating are provided separating:

- Safety-related systems from any potential fires in nonsafety-related areas that could affect the ability of safety-related systems to perform their safety function;
- Redundant divisions or trains of safety-related systems from each other to prevent damage that could adversely affect a safe shutdown function from a single fire;
- Components within a single safety-related electrical division that present a fire hazard to components in another safety-related division; and
- Electrical circuits (safety-related and nonsafety-related) whose fire-induced failure could cause a spurious actuation that could adversely affect a safe shutdown function.

Penetrations through fire barriers are sealed or closed to provide fire resistance ratings at least equal to that of the barrier. Only noncombustible materials qualified per ASTM E-119 are used for construction of fire barriers. Fire dampers protect ventilation duct openings in fire barriers as required by NFPA 90A.

Fire barrier separation of electrical circuits (safety-related and nonsafety-related) whose fire–induced failure could cause a spurious actuation that could prevent safe shutdown per NRC Regulatory Guides 1.75 and 1.189, GDC 17 and 18, and IEEE Standard 384 is described in detail in DCD Tier 2 Subsection 8.3.1.4.1.

Design features that prevent or mitigate spurious actuations include:

- The ESBWR Distributed Control and Information System (DCIS) is located in four general areas of the plant; 1) The main control room where all four divisions may be found in a common fire area, 2) four safety-related DCIS (QDCIS) rooms - one per division, 3) two nonsafety-related DCIS (N-DCIS) rooms that correspond to plant investment protection (PIP) A and (PIP) B DCIS trains and 4) remote multiplexing unit (RMU) equipment locations throughout the plant (such as the Reactor Building, Control Building, Fuel Building, etc).
- The main control room consoles are connected to the equipment in the safety-related or nonsafety-related DCIS rooms via optical fiber; the DCIS equipment rooms are in separate fire areas from each other and from the main control room. The VDUs require that at least two distinct operator actions be performed for any actuation to satisfy GEH human factors requirements. Additionally each of the messages associated with those two operator actions are authenticated by sending/receiving addresses, and (for safety related and DPS communications) sequence numbering, cyclic redundancy checks and, hash functions. At least two distinct actions are required to be performed for any actuation. It is essentially impossible for a smoke or fire impaired VDU or its controller

to inadvertently emit the required commands/authentication once and then again representing the operator actions.

- There are also hard wires between the MCR/RSS and actuation equipment that represent "fail safe" functions like reactor scram and turbine trip. Inadvertent actuation of these functions will not prevent a safe shutdown. In addition, there is no loss of automatic actuation of these functions upon the unlikely loss of manual actuation from the MCR or RSS.
- The two nonsafety-related DCIS equipment rooms and four safety-related DCIS rooms are in separate fire areas and single fires can only affect one division or PIP train at a time. The communication between the controllers in these rooms and their RMUs is protected such that neither fires nor smoke will cause inadvertent triggering of 2/4 logic or cause competent inadvertent commands to be sent (nor would it affect the "intelligence" in the remote equipment). A single fire in these areas is not expected to cause inadvertent actuations affecting a safe shutdown.
- The RMUs in the field contain the logic/"intelligence" that responds to the controllers and operates the switches. The MSIV and RPS load drivers open circuits to actuate; these are fail-safe in that inadvertent actuation causes safe shutdown. The switches that operate the various ECCS solenoids or squib igniters are either a series circuit of two (solenoid) or three (squib) switches; the switches (even within the same division) are located in separate cabinets that are in separate fire areas. A single fire could only affect one of the cabinets and therefore could not "hot short" and cause an inadvertent actuation. The logic/"intelligence" in the switches will not close the output contacts on either the loss of communication or incompetent communication from the DCIS equipment room controllers.
- The fire protection program considers multiple hot shorts for any equipment that has hard wires for its power or control circuits that could cause equipment to either actuate or not actuate which could result in the equipment not being able to be placed in its safe-shutdown position. Hard wires that are in conduit do not have to consider hot shorts from conductors/cables that are outside of the conduit. Hard wires in cabinets/panels that are in wire bundles are considered for hot shorts. RG 1.189 Regulatory Position 5.3 separation criteria such as 3-hour fire barriers separation between redundant success paths is considered in the safe-shutdown circuit analysis. The fire protection program uses a deterministic analysis approach for the safe-shutdown circuit analysis and, therefore, does not use any performance based approach like fire modeling that take into account the location of cables and equipment. This deterministic approach would assume that if a hot short could adversely affect safe-shutdown, then the cable that could cause that hot short would be present or nearby. The fire protection program could take an exception to the above, but this cable routing/arrangement including cabinet bundles would then be controlled by procedure to prevent the safe-shutdown analysis from being invalidated. Exceptions are discussed in Subsection 9.5.1.12.1.1 or 9.A.6 as appropriate.

The COL applicant shall provide specific design and certification testing details for fire barriers and electrical raceway fire barrier systems in accordance with applicable sections of NFPA 251, ASTM E-119 and guidance in Regulatory Guide 1.189 (COL 9.5.1-5-A).