



HITACHI

GE Hitachi Nuclear Energy

James C. Kinsey
Vice President, ESBWR Licensing

PO Box 780 M/C A-55
Wilmington, NC 28402-0780
USA

T 910 675 5057
F 910 362 5057
jim.kinsey@ge.com

MFN 08-250

Docket No. 52-010

March 20, 2008

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. 135 Related to ESBWR Design Certification Application – RAI Numbers 7.1-69 and 7.1-72**

The purpose of this letter is to submit the GE Hitachi Nuclear Energy (GEH) responses to the U.S. Nuclear Regulatory Commission (NRC) Requests for Additional Information (RAI) sent by NRC letter dated January 14, 2008.

Verified DCD changes associated with these RAI responses are identified in the enclosed DCD markups by enclosing the text within a black box. The marked-up pages may contain unverified changes in addition to the verified changes resulting from these RAI responses. Other changes shown in the markup(s) may not be fully developed and approved for inclusion in DCD Revision 5.

If you have any questions or require additional information, please contact me.

Sincerely,

James C. Kinsey
Vice President, ESBWR Licensing

DOB
NRO

Reference:

1. MFN 08-038, Letter from U.S. Nuclear Regulatory Commission to Robert E. Brown, GE, *Request For Additional Information Letter No. 135 Related To ESBWR Design Certification Application*, dated January 14, 2008

Enclosures:

1. Response to Portion of NRC Request for Additional Information Letter No. 135 Related to ESBWR Design Certification Application - RAI Numbers 7.1-69 and 7.1-72
2. DCD Markups

cc: AE Cabbage USNRC (with enclosure)
GB Stramback GEH/San Jose (with enclosure)
RE Brown GEH/Wilmington (with enclosure)
DH Hinds GEH/Wilmington (with enclosure)
eDRF 0000- 0080-0550 (RAI 7.1-69)
0000-0080-00611 (RAI 7.1-72)

MFN 08-250

Enclosure 1

**Response to Portion of NRC Request for Additional
Information Letter No. 135 Related to ESBWR Design**

Certification Application –

RAI Numbers 7.1-69 and 7.1-72

NRC RAI 7.1-69

Explain why the N-DCIS Design Bases removed reference to data communication through the firewall to the TSC, EOF, ERDS and "generally" provides information to other external users.

GEH Response

Secure Data Communication refers to communication pathways that are designed in accordance with the philosophy and commitments specified in the GEH Licensing Topical Report (LTR) NEDE-33295P, "Cyber Security Program Plan" (Cyber Security LTR). Secure Data Communication is inclusive of firewall technology and other security measures for data communication.

The Cyber Security LTR (NEDE-33295P) defines a "Firewall" as "*An inter-network connection device that restricts data communication traffic between two connected networks.*" It is also noted that, "*A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance) that forwards or rejects/drops packets on a network. Typically, firewalls are used to define zone borders. Firewalls generally have rules restricting what ports are open.*"

Other sections in the Cyber Security LTR (NEDE-33295P) that discuss appropriate areas of Secure Data Communication are

- Section 3.3 describes the ESBWR Cyber Security Defensive Model, which configures N-DCIS to Security Level 3.
- Subsection 4.1.2 lays out the design basis of the Communication Pathways, which explains the communication interfaces between different security levels.
- Section 4.4 discusses the required separation associated with the ESBWR Cyber Security Defensive Model. It also describes GEH's commitment to utilize "best in class" technologies, including firewalls, in meeting the cyber security requirements.

Based on the above, replacing "firewall" with "secure data communication" does not remove the intent of using a firewall, but instead points to the Cyber Security LTR (NEDE-33295P) for detailed information regarding the security design of the N-DCIS to external user communication pathway.

The phrase "*and generally provide information to other external users*" was added to indicate that secure communication is used for any authorized external plant communications. For example, N-DCIS also provides information to the utility offsite engineering computer systems other than the TSC, EOF and ERDS. However, since there is no other pathway in which information is communicated with other authorized external users, the phrase "*generally provide information to*" will be deleted from the DCD Tier 2, Subsection 7.1.4.2 bullet list item (as shown in the Enclosure 2 markup). This deletion emphasizes that secure data communication pathway is the only communication interface between the internal workstations and authorized external workstations, eliminating any misinterpretation with use of the word "generally".

DCD Impact

DCD Tier #2, Subsection 7.1.4.2 (6th bullet) will be revised in DCD Revision 5 as noted in the Enclosure 2 markup.

NRC RAI 7.1-72

The EMI environmental limit envelope has been removed. Please update the DCD to identify a new reference or process (by ITAAC) that that will identify that envelope.

GEH Response

A selection from the response to RAI 7.1-37 submitted via MFN 07-285 states:

DCD, Tier 2, Revision 1, Reference 7.1-8 "EPRI TR-102323, Guidelines for Electromagnetic Interference Testing in Power Plants, Final Report, June 1994," is listed in Revision 3 as Reference 7.1-3. This reference will be deleted in a later DCD revision because existing references to, RG 1.180 Revision 1, Mil Std 416E and IEC 61000-4 are sufficient.

Additional information will be added to DCD Tier 2, Section 7.1.6.4, to make it clear that the EQ program includes EMI environmental limit envelopes.

DCD Impact

DCD Tier 2, Section 7.1.6.4 will be revised in DCD Revision 5 to add the text shown in the Enclosure 2 markup.

MFN 08-250

Enclosure 2

DCD Markups

Verified DCD changes associated with these RAI responses are identified in the enclosed DCD markups by enclosing the text within a black box. The marked-up pages may contain unverified changes in addition to the verified changes resulting from these RAI responses. Other changes shown in the markup(s) may not be fully developed and approved for inclusion in DCD Revision 5.

DCD Markup for RAI 7.1-69

where several system logic functions are combined. The N-DCIS logic is implemented in triple redundant control systems for core nonsafety-related key systems, such as the Feedwater Control System (FWCS), SB&PC, and Plant Automation System (PAS). The N-DCIS logic is always at least redundant for systems required for power generation, so that no single failure of an active DCIS component can cause or prevent a BOP trip or reactor scram.

The N-DCIS provides the control and monitoring operator interface on the N-DCIS nonsafety-related VDUs in the MCR and RSS panels. The VDUs operate independently of one another yet each can normally access any component in the N-DCIS. This gives the RSS panels the same control and monitoring capability as the displays in the MCR. The N-DCIS provides gateways/datalinks as necessary to allow vendor supplied or prepackaged ("foreign") control systems to be integrated into the DCIS. Examples may include the Condensate Purification System (CPS) and the Area Radiation Monitoring System (ARMS).

The N-DCIS components that support power generation are provided with two or three sources of uninterruptible power with battery backup for at least two hours. For loss of offsite power events or after DCIS battery backup power is lost, the N-DCIS operates continuously from either of the two diesel generators.

The N-DCIS provides extensive self-diagnostics that monitor communication, power, and other failures to the replaceable card, module or chassis level. Process diagnostics include system alarms and the ability to identify sensor failures. All of the process and self-diagnostic system alarms are provided in the MCR.

7.1.4.1 N-DCIS Safety-Related Design Bases Summary

The N-DCIS does not perform or support the performance of any safety-related function. It is classified as a nonsafety-related system, and has no safety-related design basis.

7.1.4.2 N-DCIS Nonsafety-Related Design Bases Summary

The nonsafety-related design bases for the N-DCIS include the following requirements to:

- Provide functional/operational independence of nonsafety-related divisions important to power generation;
- Perform closed loop control and system logic;
- Tolerate a single failure of an N-DCIS component without loss of power generation capability or challenge to a safety-related system;
- Receive selected signals from the Q-DCIS and send them to nonsafety-related devices;
- Collect and archive data for transient analysis, data trending, sequence of events recording, display of Safety Parameter Display System (SPDS) and accident monitoring information, and managing the annunciation of alarm conditions in the MCR;
- Provide secure data communication to all authorized external systems, including the Technical Support Center (TSC), the Emergency Operating Facility (EOF), and the

~~Emergency Response Data System (ERDS) and generally provide information to other external users.~~

- Provide gateway interfaces to control and logic processing equipment supplied by parties other than the primary N-DCIS equipment supplier;
- Perform various PCF that includes calculations, displays, and alarms;
- Provide for report generation; and
- Provide for a Plant Configuration Database (PCD).

7.1.4.3 N-DCIS Safety Evaluation Summary

~~The N-DCIS is classified as a nonsafety-related system. It is used as the primary control, monitoring, and data communication system with power production applications. The N-DCIS is not required for safety-related purposes, nor is its operability required during or after any DBE. The system is required to operate in the normal plant environment and is relied on for data communications and power production applications. The N-DCIS provides an isolated alternate path for safety-related data to be presented to the plant operators. The N-DCIS network that supports the dual/triplicate, fault-tolerant digital controllers and communication scheme is diverse from the Q-DCIS network design in both hardware and software.~~

The N-DCIS equipment is located throughout the plant and is subject to the environment of each area. RMUs are typically located throughout the plant and auxiliary buildings. Computer equipment and peripherals are typically located mainly in the CB (MCR and Back Panel areas), Radwaste Building, TSC, EOF, and other auxiliary buildings.

The N-DCIS panels and components are designed to maintain structural integrity, during and after a DBE, and do not prevent any safety-related equipment in their area from performing its safety-related function.

Table 7.1-1 identifies the DCIS systems and the associated codes and standards applied, in accordance with the SRP. ~~The following subsection addresses summarizes N-DCIS conformance with regulatory requirements, guidelines, and industry standards.~~

7.1.4.4 N-DCIS Regulatory Requirements Conformance Summary

~~As shown in Table 7.1-1 and/or described in Subsection 7.1.6 the N-DCIS meets applicable sections portions of: the following regulations, guidelines, and industry standards as shown in Table 7.1-1 and/or described in subsection 7.1.6.~~

- 10 CFR 52.47;
- NUREG 0694, 0718, and 0737;
- IEEE Std. 7-4.3.2, 323, 344, 338, 383, 384, 497, 518, 603, 828, 829, 830, 1008, 1012, 1028, 1042, 1074;
- ANSI/ISA S67.04.01;

DCD Markup for RAI 7.1-72

among activities by defining the source activities that produce the inputs and the destination activities that receive the outputs. The standard specifies activities that must be performed and their inter-relationships; it does not specify complete acceptance criteria for determining whether the activities themselves are properly designed. Therefore, the standard should be used in conjunction with guidance from other appropriate RGs, standards, and software engineering literature. Safety-related systems use the guidance in this standard, as described in References 7.1-10 and 7.1-12, to develop portions of the overall SDP and thus comply with ~~this~~ RG 1.173.

RG 1.180—Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems: Electrical and electronic components in the I&C safety-related systems are qualified for anticipated levels of EMI at their as-installed locations. EMC of I&C equipment is verified through factory testing and site-specific testing for both individual equipment and interconnected systems to meet EMC requirements for protection against the following:

- EMI,
- RFI,
- Electrostatic Discharge, and
- Electrical Surge.

EMI qualifications, including methods of evaluating EMI operating envelopes, follow the requirements defined in Mil Std. 461E and IEC 61000-4. Q-DCIS equipment is qualified to perform continuously within specified ranges even when exposed to EMI environmental limits at the hardware mounting location. To that end, EMI qualifications for safety-related systems meet the proposed requirements of RG 1.180, Rev 1 "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems."

RG 1.204—Guidelines for Lightning Protection of Nuclear Power Plants: The surge withstanding capability of the safety-related I&C design conforms with IEEE Std. 1050. See Subsection 8A.1.2 for detailed information about the lightning protection system and conformance with to RG 1.204, and the lightning protection system.

RG 1.209, Guidelines For Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants. The safety-related system design conforms to RG 1.209.

7.1.6.5 Branch Technical Positions

BTPs that are applicable to the I&C systems are identified relative to the I&C systems in Table 7.1-1. BTPs are guidance documents; the I&C systems are generally designed to conform ~~with~~ to the BTPs. The degree of conformance, along with any clarifications or exceptions, is discussed in the safety evaluation subsections of Sections 7.1 through 7.8.

BTP HICB-1—Guidance on Isolation of the Low Pressure Systems from the High Pressure Reactor Coolant System. For details of compliance with BTP HICB-1 see Subsection 7.3.1.2.3.5.