GE Energy

**David H. Hinds**
Manager, ESBWR

PO Box 780 M/C L60
Wilmington, NC 28402-0780
USA

T 910 675 6363
F 910 362 6363
david.hinds@ge.com

MFN 06-146

Docket No. 52-010

May 25, 2006

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

Subject: **Partial Response to NRC Request for Additional Information Letter No. 6 Related to ESBWR Design Certification Application – Instrumentation and Control Systems – RAI Numbers 7.0-1, 7.2-1, 7.2-4, 7.9-1, and 9.5-2**

Enclosure 1 contains GE's response to the subject NRC RAIs transmitted via the Reference 1 letter.

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

Sincerely,

Kathy Sedney for

David H. Hinds
Manager, ESBWR

D068

Reference:

1. MFN 06-045, Letter from U.S. Nuclear Regulatory Commission to David Hinds, *Request for Additional Information Letter No. 6 Related to ESBWR Design Certification Application,* January 31, 2006

Enclosure:

1. MFN 06-146 – Partial Response to NRC Request for Additional Information Letter No. 6 for the ESBWR Design Certification Application – Instrumentation and Control Systems – RAI Numbers 7.0-1, 7.2-1, 7.2-4, 7.9-1, and 9.5-2

cc: WD Beckner USNRC (w/o enclosures)
AE Cubbage USNRC (with enclosures)
LA Dudes USNRC (w/o enclosures)
GB Stramback GE/San Jose (with enclosures)
eDRF 0000-0053-1891, 0000-0053-7136

# ENCLOSURE 1

# MFN 06-146

## Partial Response to NRC Request for Additional Information

## Letter No. 6 for the ESBWR Design Certification Application

## Instrumentation and Control Systems

## RAI Numbers 7.0-1, 7.2-1, 7.2-4, 7.9-1, and 9.5-2

NRC RAI 7.0-1

*The DCD states that development of software for the safety system functions within RPS and SSLC conforms to the guidance of BTP HICB-14. DCD Section 7B listed the following software development documents:*
*- Software Quality Assurance*
*- Software Management Plan*
*- Software Development Project Plan*
*- Software Configuration Management Plan*
*- Verification and Validation Plan*
*- Software Safety Plan (SSP)*
*- Software Test Plan (SVTP)*
*- Operations and Maintenance Manual*
*Three of these documents have been submitted for review: the Software Management Plan, Software Development Plan and Software Configuration Management Plan. The staff's acceptance of software for safety system functions is based on (1) confirmation that the software was developed in accordance with acceptable software development plans, (2) evidence that the plans were followed in an acceptable software life cycle, and (3) evidence that the process produced acceptable design outputs. The staff will follow the BTP HICB-14 step by step to perform the ESBWR design review. Please submit the Software Test Plan for staff review.*

GE Response

The Software Verification and Validation Plan, submitted to the NRC on January 18, 2006 (GE Letter MFN 06-016) outlines the formal set of standards and procedures necessary to comprehensively verify and validate Quality Class Q and Class N DCIS software-based products during all phases of the software development life cycle.

The Software Integration Plan (SIntP) submitted to the NRC on January 31, 2006 (GE Letter MFN 06-038) establishes procedures and guidelines necessary to prepare, execute, and document software testing for Quality Class Q software based products. Quality Class N software based products may be tested in accordance with this plan or in accordance with standard procedures. Table 3.2-1 of DCD Tier 1, Rev 01 provides a definition of the inspections, tests and/or analyses, together with associated acceptance criteria, which will be applied to the safety-related software life cycle.

Software testing carried out in accordance with the SIntP satisfies all software test requirements invoked by the Software Management Plan (SMP). The SIntP also addresses software test requirements pertaining to Reg. Guide 1.170, "Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants", and Reg. Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

NRC RAI 7.2-1

*In order for staff to confirm the ESBWR is in full compliance with IEEE Std. 7-4.3.2 requirements, please provide the ESBWR safety system design basis as outlined in IEEE Std. 7-4.3.2. (Note: The Reg. Guide 1.152, Rev. 2 which endorses IEEE Std. 7-4.3.2-2003 and includes requirements for cyber security is in the process of being issued. This latest version of RG 1.152 will be used in the review of ESBWR.) Demonstrate each requirement per the standard and beyond IEEE Std. 603 is met per the following items identified in IEEE Std. 7-4.3.2:*

*5.3 Quality - The following requirements are necessary in order to meet the quality criterion:*
*a. Software development including Software quality metrics*
*b. Software tools*
*c. Verification and validation*
*d. Independent V&V (IV&V) requirements*
*e. Software configuration management*
*f. Software project risk management*

*5.4 Equipment qualification - Equipment qualification testing shall be performed with the computer functioning with software and diagnostics that are representative of those used in the actual operation. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostic, associated components, communication paths, and interfaces. Testing shall demonstrate that the design basis performance requirements have been met.*

*5.5 System Integrity - In addition to the requirements of IEEE Std. 603, the design for computer integrity, test and calibration and fault detection and self-diagnostics shall be addressed.*

*5.6 Independence - Data communication between safety channels or between safety and nonsafety systems shall not inhibit the performance of the safety function. Identify barrier requirements to provide adequate confidence that the nonsafety portions cannot interfere with performance of the safety portion of the software or firmware.*

*5.11 Identification - The following identification requirements specific to software systems shall be met; a) Firmware and software identification shall be used to assure the correct software is installed in the correct hardware component. b) Means included in the software such that the identification may be retrieved from the firmware using software maintenance tools. c) Physical identification requirements per IEEE 603-1998.*

*5.15 Reliability - In addition to requirements of IEEE 603- 1998, when reliability goals are identified, the proof of meeting the goals shall include software. (Note: As stated in RG 1.152 and SRP Chapter 7, the NRC staff does not endorse the concept of quantitative reliability goals as a sole means of meeting the requirements for reliability of safety systems. Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of safety I&C systems.)*

GE Response

The ESBWR design basis addresses the requirements of IEEE Std. 7-4.2.3 as documented in section 7.1.2.2 of DCD Tier 2, Rev. 01. Specific criteria and guidelines stated in ANSI/IEEE-ANS-7-4.3.2, as endorsed by Regulatory Guide 1.152, are used as a basis for design procedures established for programmable digital equipment.

Software quality is addressed in Appendix 7B and in NEDO-33245, "Software Quality Assurance Plan".

Equipment qualification requirements that address computer equipment and software are discussed in Design Definition (Requirements) Phase of the Software Management Plan (NEDO-33226P). These design activities address the development of equipment design and configuration requirements in accordance with Reg. Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

The remaining items are addressed in Subsection 7.1.2.3.3, "Safety System Criteria Per IEEE Std. 603", (IEEE Std. 603, "IEEE Standard Criteria for Safety Systems - Nuclear PWR"). Specific criteria related to software system (BTP HCIB-14) are also discussed in this section.

NRC RAI 7.2-4

*With respect to level of detail for design certification application under 10 CFR Part 52, Section B.3.3 of BTP HICB-16 describes material that should be provided in addition to the material identified by Reg. Guide 1.70. Please provide the following: (1) system features provided to meet the requirements of 10 CFR 50.34(f), "TMI related requirements," (2) a description of the overall system architecture and the functional block diagrams for each system, (3) the computer-based I&C system characteristics that the self-diagnostics and on-line testing will detect to indicate computer system failures, (4) the interconnections of test and diagnostics with the system functional hardware and software, and (5) the mechanisms available to modify software in the installed systems. The material identified above should be discussed in sufficient detail to allow staff determination that the design meets requirements related to postulated single failures, common-mode failures, and appropriate signal isolation. Additional detail for the items requested above is provided by BTP HICB16, Section B.3.3.*

GE Response

I&C System features that are provided to meet the requirements of 10CFR 50.34(f) " Conformance to TMI Action Plan Requirements TMI Related requirements" are discussed in Subsection 7.1.2.2 of DCD Tier 2, Rev 01. The specific regulatory acceptance criteria and guidelines requirements applicable to each of these systems (safety-related or nonsafety-related but important for plant operation) identified in the Standard Review Plan are identified and tabulated in Table 7.1-1. The regulatory requirements applicability matrix of Table 7.1-1 is followed in Section 7.2 through Section 7.9 for the regulatory conformance discussions of each specific system. The degree of applicability and conformance, along with any clarifications or justification for exceptions, are presented in the evaluation sections for each specific system.

The ESBWR instrumentation and control (I&C) systems consist of both safety-related and nonsafety-related control systems. The primary safety-related systems, such as the Reactor Protection System (RPS), Leak Detection and Isolation System (LD&IS), and the ESF initiation logics, are encompassed by the Safety System Logic and Control (SSLC) framework. The safety-related data communication network, the Essential Distributed Control and Information System (E-DCIS), supports the SSLC and safety-related systems. The nonsafety-related (control) systems include all other plant I&C systems, which are supported by the nonsafety-related data communication network, the Non-Essential Distributed Control and Information System (NE-DCIS). A simplified block diagram of the ESBWR I&C architecture is shown in Figure 7.1-1. Specific block diagrams for each system are located in the appropriate system subsections.

On-line self-diagnostic tests that check the critical performance of the digital control instrument are performed continuously within SSLC/ESF. An illustration of SSLC and its relationship to the RPS and other interfacing systems is shown in Figure 7.3-5 of DCD Tier 2.

Modification of installed software used in I&C Systems will be in accordance with the plans, procedures, processes, and activities for software corrections and for software enhancements as documented in NEDO-33248, "ESBWR I&C Software Operation and Maintenance Plan".

NRC RAI 7.9-1

*In DCD section 7.9, provide sufficient detail of the design of the Essential Distributed Control and Information System (E-DCIS). Major design considerations include:*
- *Quality of components and modules*
- *Software quality*
- *Performance requirement*
- *Reliability*
- *Control of access*
- *Single failure criterion*
- *Independence*
- *Failure modes*
- *System testing and inoperable surveillance*
- *EMI/RFI susceptibility*
- *Defense-in-depth and diversity analysis*
- *Exposure to seismic hazard*

GE Response

The major design considerations listed above are addressed in Revision 1 of DCD Tier 2, Section 7.1.2.2 "Conformance to Regulatory Requirements and Industry Standards" and Section 7.1.2.3.3 "Safety System Criteria per IEEE Std. 603." DCD Table 7.1.1 identifies the associated codes and standards applied in accordance with the Standard Review Plan with a conformance summary provided in Section 7.8.3. In addition, the specific design bases are discussed in the Tier 2 section(s) listed below.

| Design Consideration | DCD Tier 2 Sections | Requirements |
|---|---|---|
| Quality of components and modules | 7.1.2.3.3 | RG 1.152;<br>10CFR50.55a(a)(1);<br>IEEE Std. 603, 5.3 |
| Software quality | 7.1.2.2; 7.B | RG 1.152;<br>BTP HICB-14; RG 1.168;<br>RG 1.169 thru RG 1.173<br>GE Ltr MFN 06-016 submitted via licensing of the SQAP, NEDO-33245, January 2006 |
| Performance requirement | 7.1.2.3.3; 7.3.4.1 | IEEE 603 |
| Reliability | 7.1.2.2; 7.1.2.3.3; 7.8.2.1 | IEEE 603, 5.15 |
| Control of access | 7.1.2.2; 7.1.2.3.3 | IEEE-603 |
| Single failure criterion | 7.1.2.2; 7.1.2.3.3 | RG 1.53, IEEE 603, 5.1 |
| Independence | 7.1.2.3.3 | IEEE 603, 5.6 |
| Failure modes | 7.1.2.2; 7.1.2.3.3; 7.8.2.2; 7.8.3 | BTP-HICB-19 |
| System testing and inoperable surveillance | 7.1.2.2; 7.1.2.3.3; 7.7.3.4; 7.7.5.4 | RG 1.22; RG 1.118<br>IEEE Std 603, 5.7 |
| EMI/RFI susceptibility | 7.1.2.3.3 | IEEE Std 603, 5.4 |
| Defense-in-depth and diversity analysis | 7.1.1.9; 7.1.2.2; 7.8.1.2 | BTP-HICB-19<br>NEDO-33251 |
| Exposure to seismic hazard | 7.1.2.2; 7.1.2.3.3 | IEEE 323; IEEE 344 |

NRC RAI 9.5-2

*9.5-2 According to the SRP 9.5-2 demonstration of effective communication is required for:*

- *Communication among personnel using protective equipment e.g. respirators.*
- *Communication among personnel in vital areas under maximum plant noise levels and worst-case EMI/RFI conditions.*

*Regarding the communication systems described in DCD 9.5.2, demonstrate their capability of providing effective communications under conditions described in SRP 9.5.2.*

GE Response

Normal and emergency off-site communications are provided by public telephone lines and the COL holder network connected to the Private Automatic Branch (Telephone) Exchange. Communication among personnel using protective equipment is described in Subsection 9.5.2.2 System Description, of DCD Tier 2, Rev 01 and is designed and tested in accordance with the referenced criteria:

- Security radio system in accordance with 10 CFR 73.55(f)
- Crisis management radio system in accordance with the intent of NUREG-0654
- Fire brigade radio system in accordance with BTP SPLB 9.5-1, position C.5.g(4)

The security and crisis management radio systems are powered from the security system power supply that is backed up by batteries and a standby generator. The remaining communication systems are operable during a loss of off-site power.

Communication among personnel in vital areas under maximum plant noise levels and worst-case EMI/RFI conditions is also addressed in DCD Subsection 9.5.2.2.

The performance of preoperational testing of these systems is discussed in DCD Subsection 9.5.2.4 Inspection and Testing Requirements. The description for the system testing invokes the testing as a COL Holder responsibility and is described within the "Initial Plant Testing Program", which is found in DCD Subsection 14.2.8.1.38 "Plant Communications System Preoperational Test". Also, DCD Subsection 14.2.8.1.12 "Remote Shutdown System Preoperational Test" further discusses, "The ability to establish and maintain communication among personnel performing the remote shutdown operation".