

Enclosure 2

MFN-09-090

**Response to Portion of NRC Request for
Additional Information Letter No. 249
Related to ESBWR Design Certification Application
RAI Numbers 14.3-415 through 14.3-420
DCD Markup Pages**

comprising the control network cannot be disrupted, interrupted, or negatively affected by unauthorized users or external systems. Reference 7.1-8 documents the design commitments, which meet the applicable guidance of RG 1.152, Section C.2, and Positions 2.1 through 2.9.

Inspections, tests, analyses, and acceptance criteria (ITAAC) associated with the cyber-security program plan are provided in Tier 1 together with the SDP.

7.1.7 COL Information

None

7.1.8 References

7.1-1 (Deleted)

7.1-2 (Deleted)

7.1-3 (Deleted)

7.1-4 GE-Hitachi Nuclear Energy Licensing Topical Report (LTR) entitled, “ESBWR I&C Defense-In-Depth and Diversity Report.” NEDO-33251, Class I (Non-proprietary), Revision ~~12~~, August 2007.

7.1-5 (Deleted)

7.1-6 (Deleted)

7.1-7 (Deleted)

7.1-8 GE Energy, “ESBWR Cyber Security Program Plan,” NEDO-33295, Class I (Non-Proprietary); and “ESBWR Cyber Security Program Plan,” NEDE-33295-P, Class III (Proprietary).

7.1-9 GE-Hitachi Nuclear Energy, “GEH ABWR/ESBWR Setpoint Methodology,” NEDO-33304, Class I (Non-proprietary); and “GEH ABWR/ESBWR Setpoint Methodology,” NEDE-33304P, Class III (Proprietary), Revision 0, October 2007.

7.1-10 [GE [HitachiEnergy Nuclear Energy](#), “~~ESBWR I&C~~ Software Quality Assurance ~~Plan~~Program Manual (SQAPM),” NEDO-33245, Class I (Non-proprietary); and “~~ESBWR I&C~~ Software Quality Assurance ~~Plan~~Program Manual (SQAPM),” NEDE-33245P, Class III (Proprietary), Revision ~~23~~, July ~~2007~~2008.]*

7.1-11 GE Nuclear Energy, “General Electric Instrument Setpoint Methodology,” NEDO-31336, Class I (Non-proprietary); and “General Electric Instrument Setpoint Methodology,” NEDC-31336P-A, Class III (Proprietary), September 1996.

7.1-12 [GE [HitachiEnergy Nuclear Energy](#), “~~ESBWR I&C~~ Software Management ~~Plan~~Program Manual (SMPM),” NEDO-33226, Class I (Non-proprietary); and “~~ESBWR I&C~~ Software Management ~~Plan~~Program Manual (SMPM),” NEDE-33226P, Class III (Proprietary), Revision ~~32~~, July-June 2007.]*

7.1-13 ~~7.1-13 (Deleted)~~ *GE Energy Nuclear, "ESBWR Man Machine Interface System and Human Factors Engineering Implementation Plan," Revision 3, NEDO-33217.*

References that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

diagnostics, all of which are reported to the N-DCIS through the required safety-related isolation. It is expected that all of the variability in the parameter channel will be attributable to the field sensor. The established setpoints provide margin to fulfill both safety requirements and plant availability objectives.

BTP HICB-13, Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors:

- Conformance: Because the RPS uses sensor input for suppression pool temperature monitoring, which is based on thermocouple-type temperature sensors, BTP HICB-13 does not apply.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Safety Systems:

- Conformance: Development of software for the safety-related system functions within RPS conforms to the guidance of BTP HICB-14. Discussion of software development is included in the LTRs [\[“ESBWR I&C-Software Management ~~Plan~~Program Manual \(SMPM\),” NEDO-33226, NEDE-33226P, and “ESBWR I&C-Software Quality Assurance ~~Plan~~Program Manual \(SMPM\),” NEDO-33245, NEDE-33245P- \(References 7.2-3 and 7.2-4.\) Safety-related software \(to be embedded in the memory of the RPS logics_{\[RVS421\]}\) is developed according to a structured plan as described in References 7.2-3 and 7.2-4. These plans follow the software life cycle process described in BTP HICB-14.](#) [\[*\]](#)

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail in the RPS section content conforms to BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The RPS logics conform to BTP HICB-17. Discussions on self-test and surveillance tests of RPS are provided in Subsection 7.2.1.4.

BTP HICB-18, Guidance on Use of Programmable Logic Controllers in Digital Computer-based Instrumentation and Control Systems:

- Conformance: Q-DCIS hardware, embedded and operating system software, and peripheral components conform to the guidance of BTP HICB-18. The Q-DCIS is built and qualified specifically for ESBWR applications as safety-related and not as commercial grade programmable logic controllers (PLCs). The embedded and operating system software meet the acceptance criteria contained in BTP HICB-14, for safety-related applications.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems (Item II.Q of SECY-93-087):

- Conformance: The Reactor Trip (Protection) System designs conform to BTP HICB-19 by implementation of an additional diverse instrumentation and control (I&C) system described in Section 7.8 as the DPS.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The real-time performance of RPS in meeting the requirements for safety-related system trip and initiation response conforms to BTP HICB-21. The real-time performance of the safety-related control system is deterministic based on the Q-DCIS internal and external communication system design and the RPS logic design. Timing signals are neither exchanged between divisions of independent equipment nor between logics within a division.

Text sections that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

7.2.1.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for Chapter 7 and with Table 7.1-1, 10CFR50.34(f)(2)(v)[I.D.3] and 10 CFR 50.34(f)(2)(xxiii)[II.K.2.10] apply to the RPS and are addressed in Subsection 7.2.1.3.1. TMI action plan requirements are generically addressed in Table 1A-1 of Appendix 1A.

7.2.1.4 Testing and Inspection Requirements

7.2.1.4.1 System Testing: Operational Verifiability

The RPS is designed so its individual operating elements are tested periodically and independently to demonstrate that RPS reliability is maintained ~~(IEEE Std. 603, Section 5.7 and 6.5).~~

The RPS design and the design of other systems providing the RPS with instrument channel inputs permit verification of the operational availability of each input sensor used by the RPS with a high degree of confidence even during reactor operation. Channel checks are continuously performed by the PCF.

The instrument channels are calibrated periodically and adjusted to verify that the necessary precision and accuracy are being maintained. Such periodic checking and testing during plant operation is possible without loss of scram capability and without causing an inadvertent scram.

Safety-related sensors are designed with the capability for test and calibration during reactor operation, with the following two exceptions in the RPS:

- MSIV limit switches, and
- TSV limit switches.

These limit switches are not accessible during reactor operation. While they are tested/checked for operability during reactor operation, they cannot be calibrated until the reactor is shutdown.

- Conformance: [Development of software for the safety-related system functions within NMS conforms to the guidance of BTP HICB-14 as discussed in the LTRs “ESBWR I&C Software Management ~~Plan~~Program Manual (SMPM),” NEDO-33226, NEDE-33226P, and “ESBWR I&C-Software Quality Assurance ~~Plan~~Program Manual (SQAPM),” NEDO-33245, NEDE-33245P; (References 7.2-3 and 7.2-4.) Safety-related software to be embedded in the memory of the NMS logics ^[RVS498]is developed according to a structured plan described in References 7.2-3 and 7.2-4. These plans follow the software life cycle process described in BTP HICB-14.]*

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The NMS section content conforms to BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The safety-related subsystems of the NMS are designed to support the required periodic testing. (Refer to Subsection 7.2.2.4.) The NMS system equipment features a self-test design operating in all modes of plant operations. This self-test function does not interfere with the safety-related functions of the system. The NMS design conforms to BTP HICB-17.

BTP HICB-18, Guidance of Use of Programmable Logic Controllers in Digital Computer-based Instrumentation and Control Systems:

- Conformance: Q-DCIS hardware, embedded and operating system software, and peripheral components conform to the guidance of Branch Technical Position HICB-18. Q-DCIS is built and qualified specifically for ESBWR applications as safety-related and not as commercial grade PLCs. The embedded and operating system software meet the acceptance criteria contained in BTP HICB-14, for safety-related applications.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-based Instrumentation and Control Systems:

- Conformance: The NMS design conforms to BTP HICB-19 by implementation of an additional diverse instrumentation and control system described in Section 7.8.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The SRNM/APRM digital subsystems (and the OPRM digital subsystem) are designed to respond in real time to ensure that specified fuel limits are not exceeded, and core power oscillations are detected and suppressed. The NMS conforms to BTP HICB-21.

Text sections that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

7.2.3.4 Testing and Inspection Requirements

Proper functioning of analog temperature sensors is verified by channel cross-comparison during the plant normal operation mode. The bulk pool temperatures are continuously compared between divisions and alarmed (for inconsistency) by the PCF.

Each of four SPTM safety-related divisions is testable during plant normal operation to determine the operational availability of the system. Each safety-related SPTM division has the capability for testing, adjustment, and inspection during a plant outage.

7.2.3.5 Instrumentation and Controls Requirements

The I&C requirements related to SPTM are addressed in Subsections 7.2.3.1 and 7.2.3.2.

7.2.4 COL Information

None.

7.2.5 References

- 7.2-1 GE-Hitachi Nuclear Energy, "GEH ABWR/ESBWR Setpoint Methodology," NEDO-33304, Class I (Non-proprietary); and "GEH ABWR/ESBWR Setpoint Methodology," NEDE-33304P, Class III (Proprietary), Revision 0, October 2007.
- 7.2-2 ~~Deleted~~ ~~GE Nuclear Energy, NUMAC LTR, NEDO-33288, "Application of Nuclear Measurement Analysis and Control (NUMAC) for the ESBWR Reactor Trip System, Revision 0, March 2007".~~
- 7.2-3 ~~[GE Hitachi Nuclear Energy, "ESBWR I&C Software Management PlanProgram Manual," NEDO-33226, Class I (Non-proprietary); and "ESBWR I&C Software Management PlanProgram Manual," NEDE-33226P, Class III (Proprietary), Revision 23, July June 20072008.]*~~
- 7.2-4 ~~[GE Hitachi Nuclear Energy, "ESBWR I&C Software Quality Assurance PlanProgram Manual," NEDO-33245, Class I (Non-proprietary); and "ESBWR I&C Software Quality Assurance PlanProgram Manual," NEDE-33245P, Class III (Proprietary), Revision 23, July 20072008.]*~~

References that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The SSLC/ESF design conforms to BTP HICB-12. Setpoint implementation is in accordance with Reference 7.3-2.

BTP HICB-13, Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors:

- Conformance: BTP HICB-13 does not apply to the SSLC/ESF because this system does not use resistance temperature detector-type sensors.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-based Instrumentation and Control:

- Conformance: [D] *Development of software for the safety-related system functions within SSLC/ESF conforms to the guidance of BTP HICB-14 as discussed in the LTRs “ESBWR ~~I&C~~ Software Management ~~Plan~~Program Manual,” NEDO-33226, NEDE-33226P and “ESBWR ~~I&C~~ Software Quality Assurance ~~Plan~~Program Manual,” NEDO-33245, NEDE-33245P. (References 7.3-3 and 7.3-4.) Safety-related software to be embedded in the memory of the SSLC/ESF controllers is developed according to a structured plan outlined in References 7.3-3 and 7.3-4. [I*]*

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail in the SSLC/ESF subsection conforms to BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions in Digital Computer-based Instrumentation and Control Systems:

- Conformance: The RPS and SSLC/ESF controller designs conform to BTP HICB-17. Discussions on self-test and surveillance tests of RPS and ESF are provided in Subsections 7.2.1.3.5 and 7.3.5.4, respectively.

BTP HICB-18, Guidance on Use of Digital Computer-based Instrumentation and Control Systems:

- Conformance: Q-DCIS hardware, embedded and operating system software, and peripheral components conform to the guidance of Branch Technical Position HICB-18. The Q-DCIS is built and qualified specifically for ESBWR applications as safety-related and not as commercial grade programmable logic controllers (PLCs). The embedded and operating system software meet the acceptance criteria contained in BTP HICB-14, for safety-related applications.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems:

- Conformance: SSLC/ESF has a four-division, independent and separated equipment arrangement. Isolation of signal transmission between safety-related divisions and

between safety-related and nonsafety-related equipment, is provided by non-conductive fiber optic cable. System functions are segmented among multiple controllers. Automatic functions are backed up by diverse automatic and manual functions. Control system functions are separate, independent, and diverse from the protection system functions. The RPS logic is implemented using a diverse microprocessor-based platform. Additional diverse features are discussed in Section 7.8, which specifically addresses compliance with the guidance of BTP HICB-19.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- **Conformance:** The real-time performance of SSLC/ESF in meeting the requirements for safety-related system trip and initiation response conforms to BTP HICB-21. Each SSLC/ESF controller operates independently and asynchronously with respect to other controllers. The real-time performance of the safety-related control system is deterministic based on the Q-DCIS internal and external communication system design and the SSLC/ESF controller design. Timing signals are not exchanged – neither between divisions of independent equipment, nor between controllers within a division.

Text sections that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

7.3.5.4 Testing and Inspection Requirements

A periodic, automatic self-test feature is included to verify proper operation of each SSLC/ESF logic processor. The self-test is an on-line, continuously operating self-diagnostics function (~~IEEE Std. 603, Sections 5.7 and 6.5~~). The on-line self-test operates independently within each of the four SSLC/ESF divisions.

The major purpose of automatic self-testing is improving system availability by checking and confirming transmission path continuity for safety-related signals, verifying operation of each two-out-of-four coincidence trip logic function, and detecting, alarming, and recording the location of hardware or software faults. Tests verify the basic integrity of each card and the microprocessors. Discrete logic cards contain diagnostic circuitry monitoring critical points within the logic configuration and determine whether a discrepancy exists between an expected output and the existing present state. The self-test operations are part of normal data processing and do not affect system response to incoming trip or initiation signals. Automatic initiation signals from plant sensors override automatic test sequences and perform the required safety-related function. Process or logic signals are not changed as a result of self-test.

The self-testing includes continuous error checking of transmitted and received data on the serial data links of each SSLC/ESF controller; for example, error checking by parity check, checksum, or Cyclic Redundancy Checking (CRC) techniques. Self-test failures are alarmed to the operator at the MCR console and recorded in a log maintained by the PCF of the N-DCIS.

In-service testing of the SSLC/ESF is performed periodically to verify operability during normal plant operation and to assure that each tested channel can perform its intended design function. The surveillance tests include, as required, instrument channel checks, functional tests,

- Drywell and wetwell temperature indications;
- VB isolation valve bypass status; and
- Status indication of bypass leakage.

The VB isolation function instrumentation located in the drywell is designed to operate in the harsh drywell environment that results from a LOCA. Safety-related instruments, located outside the drywell, are qualified for the environment in which they must perform their safety-related function.

7.3.7 COL Information

None

7.3.8 References

- 7.3-1 ~~Deleted~~ ~~Triconex Topical Report 7286-545-1-a, "Qualification Summary Report", March 08, 2002.~~
- 7.3-2 GE-Hitachi Nuclear Energy, "GEH ABWR/ESBWR Setpoint Methodology," NEDO-33304, Class I (Non-proprietary); and "GEH ABWR/ESBWR Setpoint Methodology," NEDE-33304P, Class III (Proprietary), Revision 0, October 2007.
- 7.3-3 [GE] ~~Hitachi~~*Energy Nuclear Energy*, "ESBWR ~~I&C~~ Software Management ~~Plan~~*Program Manual*," NEDO-33226, Class I (Non-proprietary); and "ESBWR ~~I&C~~ Software Management ~~Plan~~*Program Manual*," NEDE-33226P, Class III (Proprietary), Revision ~~23~~, ~~July~~*June 2007*2008^{*}
- 7.3-4 [GE] ~~Hitachi~~*Energy Nuclear Energy*, "ESBWR ~~I&C~~ Software Quality Assurance ~~Plan~~*Program Manual*," NEDO-33245, Class I (Non-proprietary); and "ESBWR ~~I&C~~ Software Quality Assurance ~~Plan~~*Program Manual*," NEDE-33245P, Class III (Proprietary), Revision ~~23~~, ~~July~~*2007*2008^{*}
- 7.3-5 ~~Deleted~~ ~~GE-Hitachi Nuclear Energy, "ESBWR I&C TRICON (SSLC/ESF) Platform Application," NEDO-33388, Class I (Non-proprietary), and "ESBWR I&C TRICON (SSLC/ESF) Platform Application," NEDE-33388P, Class III (Proprietary), Revision 0, September 2007.~~

References that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

- The man-machine interface (MMI) is implemented so that the equipment is structured into small units with sufficient diagnostics that a user can repair equipment by replacing modules and can operate the equipment by following straightforward instructions;
- The software design process specifies modular code;
- Software modules have one entry and one exit point and are written using a limited number of program constructs;
- Code is segmented by system and function:
 - Program code for each safety-related system resides in independent modules that perform setpoint comparison, voting, and interlock logic;
 - Code for calibration, signal input/output, online diagnostics, and graphical displays are common to all systems;
 - Fixed message formats are used for plant sensor data, equipment activation data, and diagnostic data. Thus, corrupted messages are readily detected by error-detecting software in each digital instrument;
- Software design uses recognized defensive programming techniques, backed up by self-diagnostic software and hardware watchdog timers;
- Software for control programs is permanently embedded as firmware in controller Read Only Memory (ROM);
- Commercial development tools and languages with a known history of successful applications in similar designs are used for software development;
- Automated software tools aid in verification and validation (V&V), and
- Reliable software is implemented by ensuring that the quality of the design and requirements specification is controlled under the formal V&V program which is discussed in the LTR “ESBWR -I&C Software Quality Assurance Plan-Program Manual (SQAPM),” NEDO-33245, NEDE-33245P. (Reference 7.8-3.)*

Text sections that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

7.8.2.2 Defense Against Common Mode Failure

In addition to the DPS and the ATWS mitigation features, safety-related logic processing systems used in the RPS and SSLC/ESF perform the following simple and repetitive tasks. These tasks are performed continuously and simultaneously in four independent and redundant divisions of logic. They are:

- Setpoint comparison;
- Two-out-of-four voting logic processing;

- 7.8-2 NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, December 1994
- 7.8-3 [GE Hitachi Nuclear Energy, "ESBWR ~~I&C~~ Software Quality Assurance ~~Plan-Program Manual~~ (SQAPM)," NEDO-33245, Class I (Non-proprietary); and "ESBWR ~~I&C~~ Software Quality Assurance ~~Plan-Program Manual~~ (SQAPM)," NEDE-33245P, Class III (Proprietary), Revision ~~23~~, July ~~2007~~2008~~1~~]*
- 7.8-4 GE-Hitachi Nuclear Energy, "GEH ABWR/ESBWR Setpoint Methodology," NEDO-33304, Class I (Non-proprietary); and "GEH ABWR/ESBWR Setpoint Methodology," NEDE-33304P, Class III (Proprietary), Revision 0, October 2007.

References that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

17.1 QUALITY ASSURANCE DURING DESIGN

The QA Program described in Section 17.1 is applicable to the ESBWR design activities supporting the standard design certification. Quality assurance is the responsibility of the DCD applicant for these design activities. The QA Program for design activities related to a specific plant is defined in Section 17.2.

17.1.1 Organization

“GENE QA Program Description”, NEDO-11209-04A (Reference 17.1-1) Section 1, establishes requirements for the Organization structure used during design of the ESBWR.

17.1.2 Quality Assurance Program

“GENE QA Program Description”, NEDO-11209-04A (Reference 17.1-1) Section 2, establishes requirements for the Quality Assurance Program used during design of the ESBWR.

The identification of safety-related structures, systems and components (Q list) to be controlled by the GEH QA Program is shown in Table 3.2-1.

“GENE QA Program Description”, NEDO-11209-04A (Reference 17.1-1) Section 2, establishes a 10 CFR Part 21 notification and posting system which is procedurally controlled. The requirement of 10 CFR Part 21 is imposed on all safety-related purchase documents.

17.1.3 Design Control and Verification

“GENE QA Program Description”, NEDO-11209-04A (Reference 17.1-1) Section 3, establishes requirements for Design Control used during design of ESBWR. Minimum design requirements are identified in Table 3.2-2.

[ESBWR -~~Instrumentation & Control (I&C)~~ Software Quality Assurance ~~Plan~~Program Manual, NEDO-33245, NEDE-33254P (Reference 17.1-2), establishes the requirements for Software Verification and Validation Quality Controls. Software Design Verification and Validation is discussed in Subsection 7.8.2.1 and Appendix 7B.]*

Text sections that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

17.1.4 Procurement Document Control

“GENE QA Program Description”, NEDO-11209-04A (Reference 17.1-1) Section 4, establishes requirements for Procurement Document Control used during design of the ESBWR.

17.1.5 Instructions, Procedures, and Drawings

“GENE QA Program Description”, NEDO-11209-04A (Reference 17.1-1) Section 5, establishes requirements for Instructions, Procedures, and Drawings used during design of the ESBWR.

17.1.6 Document Control

“GENE QA Program Description”, NEDO-11209-04A (Reference 17.1-1) Section 6, establishes requirements for Document Control used during design of the ESBWR.

17.1.25 References

- 17.1-1 GE Nuclear Energy, "GE Nuclear Energy Quality Assurance Program Description," NEDO-11209-04A (NRC accepted), Revision 8, March 1989.
- 17.1-2 [GE] ~~Hitachi~~*Energy Nuclear Energy*, "ESBWR ~~I&C~~ Software Quality Assurance ~~Plan~~*Program Manual (SOAPM)*," NEDO-33245, *Class I (Non-proprietary); and "ESBWR - Software Quality Assurance Program Manual (SOAPM)," NEDE-33245P, Class III (Proprietary), Revision 23, July 20072008*[*]
- 17.1-3 GE Hitachi Nuclear Energy, "NP-2010 COL Demonstration Project Quality Assurance Program," NEDO-33181, Revision 5, February 2008.

References that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.