



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 08-372

Docket No. 52-010

April 21, 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. 97 Related to ESBWR Design Certification Application - Technical Specifications RAI Numbers 16.2-135, 16.2-145, 16.2-152, 16.2-153, and 16.2-154**

Enclosures 1, 2, and 3 contain the GE Hitachi Nuclear Energy (GEH) responses to the subject NRC RAIs transmitted via the Reference 1 letter.

Verified DCD changes associated with this RAI response 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 this RAI response. 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 regarding the information provided here, please contact me.

Sincerely,

James C. Kinsey
Vice President, ESBWR Licensing

DOB8
NRD

Reference:

1. MFN 07-292, Letter from U.S. Nuclear Regulatory Commission to Robert E. Brown, *Request for Additional Information Letter No. 97 Related to ESBWR Design Certification Application*, May 10, 2007

Enclosures:

1. MFN 08-372 – Response to Portion of NRC Request for Additional Information Letter No. 97 Related to ESBWR Design Certification Application – Technical Specifications – RAI Numbers 16.2-135, 16.2-145, 16.2-152, 16.2-153, and 16.2 154
2. MFN 08-372 – DCD Markups for RAI Number 16.2-135
3. MFN 08-372 – DCD Markups for RAI Number 16.2-145

cc: AE Cabbage USNRC (with enclosures)
DH Hinds GEH (with enclosures)
RE Brown GEH (with enclosures)
eDRFs 79-2657, 79-2728, 79-2736, 79-2753, 79-2760

Enclosure 1

MFN 08-372

Response to Portion of NRC Request for

Additional Information Letter No. 97

Related to ESBWR Design Certification Application

- Technical Specifications -

RAI Numbers 16.2-135, 16.2-145, 16.2-152, 16.2-153, and 16.2-154

NRC RAI 16.2-135

Equipment within an RPS division of trip actuators includes load drivers and controllers for automatic scram and air header dump initiation. Load drivers are addressed in LCO 3.3.1.2. Operability requirements for the controllers are not addressed within the ESBWR DCD TS. Justify excluding controllers for automatic scram and air header dump initiation from TS.

GEH Response

DCD Revision 4, Section 7.2.1.2.4.1, describes the arrangement of the Reactor Protection System (RPS) division of trip actuators. Equipment within a division of trip actuators includes load drivers and controllers for automatic scram and air header dump initiation. The RPS includes two physically separate and electrically independent divisions of trip actuators receiving inputs from the four divisions of the Trip Logic Unit (TLU).

The DCD Revision 4 description of the RPS division of trip actuators refers to the primary automatic scram trip actuators as “load drivers” and the backup scram air header dump trip actuators as “controllers”. The intent was to distinguish that the backup trip actuators are physically and electrically independent from the primary trip actuators.

The primary automatic scram trip actuators (load drivers) are included in the Technical Specifications. The backup scram air header dump trip actuators (controllers) are not included in the Technical Specifications. Excluding the backup scram air header dump initiation trip actuators (or “controllers”) from Technical Specifications is justified in the response to RAI 16.0-1 (MFN 06-263). The Alternate Rod Insertion function of the control rod drive air header dump valves was included in the Availability Controls Manual (ACM 3.3.1, “Alternate Rod Insertion”) in DCD Revision 4.

GEH has reviewed the DCD Chapter 7 and Chapter 16B sections that describe the RPS division of trip actuators and the use of the term “controller” and determined that clarifying changes are warranted for consistency. The term “controller” is deleted since it implies a programmable logic controller. The description of the division of trip actuators is enhanced to clarify that the RPS has primary and backup scram trip actuators that are physically and electrically independent from each other. The trip actuators are described as load drivers for consistency with NEDO-33288, “Application of Nuclear Measurement Analysis and Control (NUMAC) for the ESBWR Reactor Trip System”. These editorial clarifications will be included in DCD Revision 5.

DCD Impact

DCD Chapter 7 and Chapter 16B will be revised in Revision 5 as shown in Enclosure 2.

NRC RAI 16.2-145

Channel operability based on allowable values (AVs), pre-defined as-found tolerance bands, and as-left tolerance bands as specified in the TS for the ESBWR are applicable only to analog protection systems using bistables. For the ESBWR digital protection systems, setpoints are controlled in the TS. The ESBWR TS require that the Nominal trip setpoint, embedded in the digital protection system, be equal to or conservative with respect to the LSSS.

Provide documentation to show that TS will require surveillances to verify operability of the critical functions (1) internal diagnostic methods that can monitor the "health" of different processors/memory boards and perform software checks to ensure that the proper software is executing, and (2) power-up tests (RAM, EPROM, etc.) and error checking on the data links as well as tests by a transmitting channel to ascertain that the transmitted signal has been properly received by the receiving channels during the channel functional test. This information is needed to understand how the proposed Setpoint Control Program will ensure that the requirements of 10 CFR 50.36.(c)(ii)(A) are met.

GEH Response

Channel operability (i.e., operability of instrumentation channels and actuation divisions) for the ESBWR continues to be based on providing automatic protective action consistent with meeting the Limiting Safety System Settings (LSSS) assumptions provided by the Setpoint Control Program (Technical Specification 5.5.11) that utilizes nominal trip setpoints, allowable values, as-found tolerances, and as-left tolerances. The basic operability requirements and objectives of the LSSS are not unique to digital protection systems compared to analog protection systems using bistables. The requirements for frequent monitoring for gross channel failure (Channel Checks), and periodic confirmation of actuation settings (Channel Calibrations), and the overall functioning of all the devices in the system (Channel Functional Test, Logic System Functional Test, Response Time Test) continue to apply to the ESBWR digital protection system.

The requirements of power-up tests, monitoring processor "health," code execution, and error checking on data links are met by the online self-diagnostic features of the ESBWR Distributed Control and Information System (DCIS) platforms in conjunction with the Technical Specification Monitor (TSM), which satisfy the Channel Check requirements by automatic cyclic comparison of channel outputs for unacceptable deviations. Trip setpoint parameters are continuously sent to the TSM for comparison of consistency between divisions and the required values.

The DCIS platforms are tested for errors, from the sensor input point to logic contact output during power-up and cyclically during subsequent operation. The self-diagnostic capabilities include features like microprocessor checks, system initialization, watchdog timers, monitoring memory integrity, checking I/O data integrity and communication bus interfaces, and checks on the application program (checksum). The TSM provides a log of the results, and sends out-of-limits alarms to the Alarm Management System (AMS). The online self-diagnostic features of the DCIS, in conjunction with the TSM, support the Channel Check requirements; which are enhanced over what is required in Standard Technical Specifications for BWR/6, providing overall instrumentation and actuation logic system verification of functionality.

These continuous automatic online diagnostics for both the safety-related DCIS (Q-DCIS) and nonsafety-related DCIS (N-DCIS) detect data transmission errors and hardware failures at the

replaceable card or module level. Q-DCIS online diagnostics meet the self-diagnostic characteristics for the safety-related digital computer based protection systems recommended by IEEE Std. 7-4.3.2.

DCD Revision 4, Section 7.1.3.4, "Q-DCIS Testing and Inspection Requirements," and Section 7.1.5.4, "N-DCIS Testing and Inspection Requirements," will be revised to provide basic design information for Technical Specification surveillance tests.

DCD Impact

DCD Subsections 7.1.3.4 and 7.1.5.4 will be revised in Revision 5 as shown in Enclosure 3.

NRC RAI 16.2-152

A Channel Functional Test (CFT) shall be the injection of a simulated or actual signal into the channel as close to the sensor as practicable to verify operability of all devices in the channel required for channel operability. Add Bases to ESBWR DCD Instrumentation TS to identify all devices in the channel required to be tested by a CFT for each instrument function.

GEH Response

The ESBWR CFT tests the entire channel from sensor input to logic contact output. The instrumentation channel and actuation divisions are adequately described in the DCD and outlined in the Technical Specification Bases. Revising the Chapter 16B Bases for CFT to include a specific list of devices tested would result in a level of detail not incorporated in NUREG-1434, "Standard Technical Specifications General Electric Plants, BWR/6," Bases. This level of detail more properly belongs in the design documents.

DCD Impact

No DCD changes will be made in response to this RAI.

NRC RAI 16.2-153

ESBWR instrumentation TS require a Logic System Functional Test (LSFT) to be a test of all components required for operability of a logic circuit. Add Bases to ESBWR DCD Instrumentation TS to define logic circuit and identify the logic circuit devices tested by LSFT.

GEH Response

The ESBWR LSFTs test the instrumentation channel's logic components from the sensor input to logic contact output up to, but not including, the actuating device. This is defined in Section 1.1, Definitions, of DCD Tier 2 Chapter 16, Technical Specifications.

Descriptions of the instrumentation channel and actuation divisions are provided in the DCD and outlined in the Technical Specification Bases.

Revising the Chapter 16B Bases for LSFT to include a specific list of devices tested would result in a level of detail not incorporated in NUREG-1434, "Standard Technical Specifications General Electric Plants, BWR/6," Bases. This level of detail is contained in the design documents.

DCD Impact

No DCD changes will be made in response to this RAI.

NRC RAI 16.2-154

Identify all ESBWR DCD TS LCO instrumentation devices required to be operable to ensure the LCO specified safety function can be met. Show that ESBWR DCD TS required testing and calibration will ensure the necessary quality of instrumentation devices is maintained.

GEH Response

The responses to NRC RAIs 16.2-145, 16.2-152, and 16.2-153 indicate that testing and calibration in accordance with the Technical Specifications maintain the necessary quality of instrumentation devices. Revising the Chapter 16 Bases to include a specific list of all instrumentation devices necessary for the LCO-specified safety function would result in a level of detail not required by NUREG-1434, "Standard Technical Specifications General Electric Plants, BWR/6," Bases. This level of detail is contained in the design documents.

DCD Impact

No DCD changes will be made in response to this RAI.

Enclosure 2

MFN 08-372

DCD Markups for

RAI Number 16.2-135

Verified DCD changes associated with this RAI response 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 this RAI response. Other changes shown in the markup(s) may not be fully developed and approved for inclusion in DCD Revision 5.

- ICS-PAM system (Subsection 7.45.41);
- CMS (Subsection 7.5.2);
- PRMS (Subsection 7.5.3); and
- Interlock Systems (Section 7.6).

7.1.6.6.1.2 Single Failure Criterion (IEEE Std. 603, 5.1)

The safety-related control systems include sufficient redundancy, diversity, and independence to meet system performance requirements if the system is degraded by any single credible failure. In the RPS, ~~NMS, logic controller (reactor and SSLC/ESF),~~ two-out-of-four redundancy and trip logic prevent a single failure from inhibiting a scram or reactor core cooling safety-related function. They also prevent a single failure from causing either an inadvertent reactor trip or an ~~emergency core cooling~~ ECCS action. Redundancy begins with the sensors monitoring the variables and continues through the signal processing, output devices, and actuators. More than one diverse sensor and control system initiates most protective actions. No single failure or two ~~division~~ failure within the safety-related system causes an AOO to degrade to an Infrequent Event or an Infrequent Event to degrade to an Accident.

Communication between redundant divisions or between safety-related control systems and nonsafety-related control systems is electrically isolated and one-way. (Refer to Subsection 7.1.3.3.) Communication is typically by optical couplers and fiber optic ~~cableing~~.

Each division is sufficiently independent from the other divisions so that no one division is dependent on information, timing data, or communication from any other division to initiate a safety-related trip signal. The failure of a single division does not prevent the initiation of a safety-related trip. Each safety-related logic ~~controller~~ evaluates the data from its own division's sensors and continuously broadcasts the result of its evaluation to the other divisions as either a "trip" or "no trip" signal.

A safety-related trip is initiated whenever any two working divisions sense conditions that require a safety-related trip. Each division receives input data from its own set of diverse and/or redundant sensors connected to the same process source and separately transmits trip signals to the other divisions. The trip actuators go to their trip state whenever they receive concurrent, like parameter trip signals from any two safety-related logic ~~controller~~ transmissions. The two-out-of-four voting logic treats the absence of an interdivisional trip signal as a signal. The signal isolators are qualified to withstand all credible faults, such as short circuits or high voltage, so that faults cannot propagate and degrade the performance of any safety-related control function.

Reference 7.1-4 describes the type of diversity that exists among the four echelons of defense-in-depth and identifies the dependency, redundancy, and independence among the echelons.

An analysis of the redundancy and independence of the safety-related protection systems and a block level ~~F~~failure ~~M~~mode and ~~E~~effects ~~A~~analysis (FMEA) is performed of the complete safety-related reactor protection, ESF, and DPS designs. In addition, the platform specific LTRs for the safety-related system architectures include analysis summaries of the architecture's conformance ~~with~~ to the requirements of IEEE Std. 603.

BPU and other control interfaces in the same division. Signals from one RPS division to another RPS division are isolated electronically using fiber optic cables.

The various manual switches provide the operator with the means to enforce interlocks within RPS trip logic for special operation, maintenance, testing, and system reset. The BPUs perform bypass and interlock logic for the division of channel sensors bypass and the division TLU bypass. Each BPU sends a separate bypass signal for the four channels to the TLU in the same division for channel sensors bypass. Each RPS BPU also sends the TLU bypass signal to the OLU in the same division.

The OLUs perform division trip, seal-in, reset, and trip test functions. Each OLU receives bypass inputs from the RPS BPU, trip inputs from the TLU of the same division, and manual inputs from switches within the same division. Each OLU provides trip outputs to the trip actuators.

Equipment within a division of trip logic is powered from the same division of safety-related power source. However, different pieces of equipment ~~may be~~ powered from separate low-voltage DC power supplies in the same division.

Divisions of Trip Actuators: Equipment within a division of trip actuators includes load drivers ~~and controllers~~ for automatic primary scram and air header dump initiation backup scram. The RPS includes two physically separate and electrically independent divisions of trip actuators receiving inputs from the four divisions of ~~the~~ OLU. The load drivers are isolated, solid-state, current-interrupting devices with fast response times and are used for the primary and backup scram actuators. They primary scram actuators are powered by 120 VAC and can tolerate the high current levels associated with Hydraulic Control Unit (HCU) scram solenoid operation.

The operation of the load drivers is such that a trip signal on the input side creates a high impedance current-interrupting condition on the output side. The output side of each load driver is isolated electrically from its input signal. The load driver outputs are arranged in the primary scram logic circuitry between the scram solenoids and scram solenoid 120 VAC power source. When in a tripped state, the load drivers cause the scram solenoids (scram initiation) to de-energize. The load drivers within a division interconnect with the OLU of all other divisions to form a special arrangement (connected in series and in parallel in two separate groups) that results in two-out-of-four scram logic. Reactor scram occurs if load drivers associated with any two or more divisions receive trip signals from the OLU (Refer to Figure 7.2--1).

~~The controllers~~ Load drivers are also used for back-up scram actuators, scram-follow initiation, and scram reset permissive actuators. When in a tripped state, the ~~controllers~~ load drivers for backup scram cause the air header dump valve solenoids (air header dump) to energize. The ~~controllers~~ load drivers of the backup scram are arranged in a two-out-of-four configuration similar to that described above for the primary scram load drivers. Backup scram is diverse in power source and function from primary scram.

Divisions of Manual Scram Controls: Equipment within a division of manual scram controls includes manual switches, contactors, and relays providing an alternate, diverse, manual means to initiate a scram and air header dump. Each division's manual scram function controls the

- Conformance: The RPS system design conforms to RG 1.209.

7.2.1.3.5 Branch Technical Positions

BTP HICB-3₂: Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service:

- Conformance: Because ~~There~~ is no reactor coolant pump, BTP HICB-3 ~~so this BTP~~ does not apply. -

BTP HICB-8₂: Guidance on Application of RG 1.22:

- Conformance: The RPS ~~design~~ conforms with BTP HICB-8 ~~this BTP~~.

BTP HICB-9₂: Guidance on Requirements for RPS Anticipatory Trips:

- Conformance: Hardware used to provide trip signals in the RPS is designed in accordance with IEEE Std. 603, Section 5.4 and is considered safety-related and meets the design requirements of BTP HICB-9 ~~this BTP~~.

BTP HICB-11₂: Guidance on Application and Qualification of Isolation Devices:

- Conformance: The RPS ~~design~~ conforms with to this position. The RPS logic controllers use optical CIM and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

Certain diverse and hardwired portions of RPS may use coil-to-contact isolation of relays or contactors. This is acceptable according to BTP HICB-11 ~~the BTP~~ when the application is analyzed or tested per the guidelines of RG 1.75 and RG 1.153.

BTP HICB-12₂: Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The RPS ~~design~~ conforms with to BTP HICB-12 ~~this position~~. The nominal setpoints are calculated based on the GEH instrument setpoint methodology (Reference 7.2-1). The setpoints are established based on instrument accuracy, calibration capability, and estimated design drift allowance data, and are within the instrument best accuracy range.

The digital RPS trip setpoints do not drift and any changes are reported to the N-DCIS as alarms ~~set for any change~~. The analog-to-digital converters are self-calibrating, and the RPS uses self-diagnostics, all of which are reported to the N-DCIS through isolated gateways. 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-13₂: 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, so~~ BTP HICB-13 ~~this BTP~~ 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 ~~with~~ to the guidance of BTP HICB-14 ~~this BTP~~. Discussion of software development is included in the LTRs “ESBWR I&C Software Management Plan,” NEDO-33226, NEDE-33226P, and “ESBWR I&C Software Quality Assurance Plan,” NEDO-33245, NEDE-33245P. (References 7.2-3 and 7.2-4.) Safety-related software (to be embedded in the memory of the RPS controllers logics) 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 ~~the BTP~~ HICB-14.

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

- Conformance: ~~This BTP~~ HICB-16 is applicable to all sections of the DCD. The RPS ~~Section~~ content conforms ~~with~~ to ~~this BTP~~ HICB-16.

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

- Conformance: The RPS controller logics conform ~~with~~ to BTP HICB-17 ~~this BTP~~. 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. Any portions of RPS design using commercial grade programmable logic controllers (PLCs) for safety-related functions conform with this BTP (and with BTPs 14, 17, and 21). Such PLCs are qualified to a level commensurate with safety-related system requirements.

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 ~~with~~ to BTP HICB-19 ~~this BTP~~ 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 Evaluation of Digital System Architecture and Real-Time Performance:

- Conformance: The real-time performance of RPS in meeting the requirements for safety-related system trip and initiation response conforms ~~with~~ to BTP HICB-21 ~~this BTP~~. 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 controller logic design. – Timing signals are neither exchanged between divisions of independent equipment nor between controllers within a division.

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) applies to the RPS and is addressed in Subsection 7.2.1.3.1. TMI action plan requirements are generally addressed in Table 1A-1 of ~~Tier 2, Chapter 1~~, 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~~ ing 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 ~~is~~ 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 Reactor Protection System:

- 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.

Safety-related RPS equipment is designed to allow inspection and testing during periodic shutdowns of the nuclear reactor and during refueling shutdowns.

7.2.1.4.2 Surveillance Testing and In-Service ~~Inspection~~ Testing

The RPS equipment testing includes ~~the following~~:

- Preoperational, startup and refueling/outage inspection testing; and

The trip setpoints are adjustable. The SRNM trip functions are shown in Table 7.2-2 (IEEE Std. 603, Section 6.8). A short period signal (the period withdrawal permissive) inhibits continuous control rod withdrawal to avoid a reactor scram (due to a shorter reactor period caused by excessive rod withdrawal).

7.2.2.2.4.6 Bypasses and Interlocks

The 12 SRNM channels are divided into four bypass groups. A controller logic processor allows only one SRNM at a time to be bypassed in each bypass group, allowing up to four SRNM channels to be bypassed at any one time. There is no additional SRNM bypass capability at the divisional level. However, it is possible to bypass all three SRNMs belonging to the same division. When this is required, a divisional bypass allows that division's NMS DTM to be bypassed. For SRNM calibration or repair, the bypass can be ~~done~~ performed for each individual channel separately through these SRNM bypasses without putting the whole division out of service. The SRNM subsystem satisfies the repair requirement of IEEE Std. 603, Section 5.10. Note that bypassing any of the SRNM sensors within a division does not affect the ability of the NMS to perform two-out-of-four trip determinations using the trip decisions from the SRNM divisions (with any three of the four divisions of safety-related power available). The SRNM subsystem satisfies the IEEE Std. 603, Section 5.1 single-failure criterion.

The SRNM bypass switches are mounted on the MCR panel. Bypass functions for the SRNM and the APRM in the NMS are separate. There is no single NMS divisional bypass affecting both the SRNM and the APRM. No APRM bypass forces a SRNM bypass. The individual SRNM power signals are combined and averaged to form a divisional SRNM power signal. Also, all NMS bypass logic control functions are located within the NMS, not in the RPS.

The SRNM has several major interlock logics. The SRNM trip functions are in effect when the Reactor Mode Switch is not in the Run position. The SRNM upscale trip setpoint is lowered (IEEE Std. 603, Section 6.8) in the NMS ~~Non-Coincident~~ mode (Table 7.2-2). The SRNM ATWS permissive signals are sent to the ATWS/SLC system to control initiation of SLC system boron injection and associated functions (such as feedwater runback).

7.2.2.2.4.7 Redundancy and Diversity

The signal outputs from the 12 SRNM channels are arranged so each of the four divisions includes a different set of designated SRNM channels covering different regions of the core. The SRNM monitoring and protection function is provided by an individual channel. Failure of an un-bypassed single SRNM channel causes an inoperative trip to only one of the four divisions, whereas a full scram requires divisional trips in two-out-of-four divisions within the NMS. Bypassing a single SRNM channel does not cause a trip output to the related SRNM division and does not prevent the remaining SRNM channels from performing their safety-related functions.

7.2.2.2.4.8 Environmental Considerations

The wiring, cables, and connectors located within the drywell are designed for continuous duty in the environmental conditions described in Appendix 3H.

protected from any rising neutron flux potentially exceeding these values. The nominal setpoints are calculated to be consistent with the GEH standard setpoint methodology (Reference 7.2-1), which conforms ~~with~~to RG 1.105. The setpoint margin calculated by this method also has considered additional uncertainties with the calibration interval. Therefore, the NMS meets BTP HICB-12~~this BTP~~.

Most of the uncertainty associated with safety-related NMS trip setpoints is associated with the various neutron sensors because the digital electronics in the NMS do not drift, and the setpoints are monitored and alarmed by the PCF of N-DCIS.

~~BTP HICB-14~~—2 Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Safety Systems:

- Conformance: Development of software for the safety-related system functions within NMS conforms ~~with~~to the guidance of BTP HICB-14~~this BTP~~ as discussed in the LTRs “ESBWR I&C Software Management Plan,” NEDO-33226, and “ESBWR I&C Software Quality Assurance Plan,” NEDO-33245. (References 7.2-3 and 7.2-4.) Safety-related software to be embedded in the memory of the NMS controllers-logics 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~~the BTP~~.

~~BTP HICB-16~~—2 Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: ~~This BTP is applicable to all sections of the DCD.~~—The NMS section content conforms ~~with~~to BTP HICB-16~~this BTP~~.

~~BTP HICB-17~~—2 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 ~~with~~to BTP HICB-17~~this BTP~~.

~~BTP HICB-18~~—2 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 conforms 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.~~Any portions of the NMS design using commercial grade programmable logic controllers (PLCs) for safety related functions conform with this BTP. The PLCs are qualified to a level commensurate with safety related system requirements.~~

~~BTP HICB-19~~—2 Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-based Instrumentation and Control Systems:

BASES

BACKGROUND (continued)

of the same division, and various manual inputs from switches within the same division. Each OLU provides trip outputs to the trip actuators.

Equipment within a division of trip logic is powered from the same division of safety-related power source. However, different pieces of equipment may be powered from separate low voltage dc power supplies in the same division. OPERABILITY requirements for the Divisions of Trip Logic are addressed in LCO 3.3.1.2, "Reactor Protections System (RPS) Actuation," with the exception of the digital trip function, which is addressed in LCO 3.3.1.1.

Divisions of Trip Actuators

Equipment within a division of trip actuators includes load drivers and ~~controllers~~ for automatic scram and air header dump initiation. The RPS includes two physically separate and electrically independent divisions of trip actuators that receive inputs from the four Divisions of Trip Logic. The load driver outputs are arranged in the scram logic circuitry, which is between the scram solenoids and scram solenoid 120 VAC power source. When in a tripped state, the load drivers within a division interconnect with the OLU of all other divisions to form an arrangement (connected in series and in parallel in two separate groups) that results in two-out-of-four scram logic. Reactor scram occurs if load drivers associated with any two or more divisions receive trip signals from the OLUs.

~~The controllers~~ Load drivers are also used for back-up scram actuators, scram-follow initiation, and scram reset permissive actuators. When in a tripped state, ~~the controllers~~ load drivers cause the air header dump valve solenoids to energize. ~~The controllers~~ load drivers of the backup scram are arranged in a two-out-of-four configuration similar to that described above for the primary scram load drivers. Backup scram is diverse in power source and function to primary scram.

A manual switch associated with each Division of Trip Actuators provides means to reset the seal-in at the input of all trip actuators in the same division. The reset does not have any effect if the conditions that caused the division trip have not cleared when a reset is attempted. All manual resets are inhibited for ten seconds to allow sufficient time for scram completion.

BASES

BACKGROUND (continued)

OPERABILITY requirements for the load drivers are addressed in LCO 3.3.1.2. OPERABILITY requirements for the ~~controllers-backup~~ scram load drivers are not addressed within the Technical Specifications.

Divisions of Manual Scram Controls

OPERABILITY requirements for the Divisions of Manual Scram Controls are addressed in LCO 3.3.1.3, "Reactor Protection System (RPS) Manual Trip Actuation."

Divisions of Scram Logic Circuitry

The two divisions of primary scram logic circuitry are powered from independent and separate power sources. One of the two divisions of scram logic circuitry distributes division 1 safety-related 120 VAC power to the A solenoids of the hydraulic control units (HCUs). The other division of scram logic circuitry distributes division 2 safety-related 120 VAC power to the B solenoids of the HCUs. The HCUs (which include the scram pilot valves and the scram valves, including their solenoids) are, components of the CRD system. A full scram of control rods associated with a particular HCU occurs when both A and B solenoid of the HCU are de-energized.

One scram pilot valve is located in the Hydraulic Control Unit (HCU) for each control rod drive pair. Each scram pilot valve is operated by two solenoids, with both solenoids normally energized. The scram pilot valve controls the air supply to the scram inlet valve for the associated control rod drive pair. When either of two scram pilot valve solenoids is energized, air pressure holds the scram valve closed and therefore, both scram pilot valve solenoids must be de-energized to cause a control rod pair to scram. The scram valve controls the supply for the control rod drive (CRD) water during a scram.

OPERABILITY requirements for components of the Divisions of Scram Logic Circuitry are addressed in LCO 3.1.3, "Control Rod OPERABILITY."

The RPS is designed to provide reliable single-failure proof capability to automatically or manually initiate a reactor scram while maintaining protection against unnecessary scrams resulting from single failures. The RPS satisfies the single-failure criterion even when one entire division of channel sensors is bypassed and/or when one of the four automatic RPS trip logic divisions is out-of-service.

B 3.3 INSTRUMENTATION

B 3.3.1.2 Reactor Protection System (RPS) Actuation

BASES

BACKGROUND

The RPS is designed to initiate a reactor scram when one or more monitored parameters exceed their specified limit, to preserve the integrity of the fuel cladding, preserve the integrity of the reactor coolant pressure boundary, and preserve the integrity of the containment by minimizing the energy that must be absorbed following a LOCA. This can be accomplished either automatically or manually.

A detailed description of the RPS instrumentation and RPS actuation logic is provided in the Bases for LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation."

This Specification provides requirements for the RPS actuation circuitry that consists of the Divisions of Trip Logic (with the exception of OPERABILITY of the digital trip function, which is addressed in LCO 3.3.1.1), and the Divisions of Trip Actuators (except for OPERABILITY of the controllers-backup scram load drivers which are not addressed within the Technical Specifications).

APPLICABLE SAFETY ANALYSES

The actions of the RPS are assumed in the safety analyses of Reference 1. The RPS initiates a reactor scram when monitored parameter values exceed the trip setpoints to preserve the integrity of the fuel cladding, preserve the integrity of the reactor coolant pressure boundary, and preserve the integrity of the containment by minimizing the energy that must be absorbed following a LOCA. RPS actuation channels support the OPERABILITY of the RPS Instrumentation, "LCO 3.3.1.1, Reactor Protection System (RPS) Instrumentation" and therefore is required to be OPERABLE.

RPS Actuation satisfies the requirements of Selection Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Although there are four RPS automatic actuation divisions, only three RPS automatic actuation divisions are required to be OPERABLE to ensure no single automatic actuation division failure will preclude a scram to occur on a valid signal. The three required divisions are those divisions associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems -

Enclosure 3

MFN 08-372

DCD Markups for

RAI Number 16.2-145

Verified DCD changes associated with this RAI response 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 this RAI response. Other changes shown in the markup(s) may not be fully developed and approved for inclusion in DCD Revision 5.

any clarification or justification for exceptions, is presented in the safety evaluation sections for each specific system.

7.1.3.4 Q-DCIS Testing and Inspection Requirements

~~The testing and inspection requirements for each system within the Q-DCIS are presented in specific subsections in Chapter 7.~~

~~The components of the Q-DCIS are readily accessible for testing purposes. The continuous automatic online diagnostics of the Q-DCIS detect most data transmission errors and hardware failures at the replaceable card or module level. Continuous self-diagnostics in each RMU monitor the status of each module or card.~~

~~The DCIS functions are closely interfaced with the following:~~

- ~~Safety-related logic functions,~~
- ~~Integrated hardware and software functions of the Q-DCIS, and~~
- ~~Safety-related logic including network parameters.~~

~~Data status of these functions are checked and tested together. Some of the key diagnostics include the following:~~

- ~~CPU status check,~~
- ~~Parity checks,~~
- ~~Watchdog timer status,~~
- ~~Voltage level in controllers,~~
- ~~Data path integrity and data validation checks, and~~
- ~~Data cycling time.~~

~~The DCIS functions are closely interfaced with the safety-related logic functions, the integrated hardware and software functions of the Q-DCIS and safety-related logic including network parameters and data status are checked and tested together. Some of the key diagnostics include the CPU status check, parity checks, watchdog timer status, voltage level in controllers, data path integrity and data validation checks, and data cycling time. The A/D converters (and the D/A converters if used) in the RMUs are the only components requiring periodic calibration checks, which can be performed automatically. In the Q-DCIS, online diagnostics are qualified as safety-related in conjunction with functional software qualification (IEEE Std. 603, Section 5.7).~~

~~Any detected hardware failure results in an alarm in the MCR. Corrupted data are detected through error detection functions in the network.~~

The Q-DCIS uses two diverse platforms, NUMAC for RTIF functions (RPS/NMS and the MSIV isolation function) and TRICON for SSLC/ESF functions (ADS, GDCS, ICS, SLC, LD&IS functions (except MSIV isolation), and CRHS).

Both platforms are readily accessible for testing purposes. Their continuous automatic online diagnostics detect data transmission errors and hardware failures at the replaceable card or module level. Online diagnostics for NUMAC and TRICON are qualified as safety-related in conjunction with functional software qualification (IEEE Std. 603, Section 5.7), and also meet the self-diagnostic characteristics for digital computer based protection systems recommended by IEEE Std. 7-4.3.2.

Both NUMAC and TRICON have self-diagnostic features that check the validity of input signals. An analog input outside expected limits creates an alarm.

The NUMAC hardware has a watchdog timer that monitors the execution of the software. If the software stops executing (suspending the self-diagnostics), the watchdog timer resets the affected instrument. This results in a channel trip and alarm while the instrument is resetting.

The TRICON, a Triple Modular Redundant (TMR) system, has three Main Processors (MPs). The MPs are monitored by individual watchdog timers that reset or fail an MP depending on the severity of the problem. A single or double MP failure causes alarms, but the division continues to function to provide the required automatic protective actions.

Both NUMAC and TRICON are cyclically tested from the sensor input point to logic contact output. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, I/O data integrity checks, communication bus interfaces checks, and checks on the application program (checksum). Cyclically monitored items include:

- Sensor inputs to the I/O for unacceptably high/low levels,
- Proper execution of application code/checksum verification of code integrity,
- Internal clocks,
- Functionality of input cards/modules, and their MP communication,
- MP communication with the output contact (TRICON),
- Inter-divisional communication between RPS/NMS instruments (NUMAC), and
- Functionality of the output contact by momentarily reversing its state and confirming readiness to change state on demand (TRICON).

Subsequent to verification and validation (V&V) of software during factory and preoperational testing in accordance with approved test procedures, there is no mechanism for the NUMAC/TRICON code, response time, or coded trip setpoints to inadvertently change. For user adjustable parameters a new checksum is calculated at the time acceptable changes are implemented. The new checksum is used from that point forward to validate the application software. The trip setpoint parameters are continuously sent to the N-DCIS technical specifications monitor (TSM) for comparison of the setpoints to confirm consistency between divisions and the required values.

The following describes the periodic testing performed to support surveillance requirements of the Technical Specifications. Additional information on testing and inspection requirements for each system within the Q-DCIS is presented in specific subsections in Chapter 7.

Channel Check

The channel check is a qualitative assessment of channel behavior during operation. The online self-diagnostic features of NUMAC/TRICON, in conjunction with the TSM, accomplish the channel check requirements for detecting unacceptable deviations by automatic cyclic comparison of channel outputs. Technical specifications monitor provides a log of the results and sends out-of-limits alarms to the Alarm Management System (AMS). The TSM uses a hardware/software platform different from NUMAC and TRICON. The TSM functions are listed in Subsection 7.1.5.2.4.5.

If there are any self-diagnostic test results and indicating alarms, a summary report is available to the operator on demand.

Sensor and actuation logic channel monitoring capability are provided at the VDUs to enable manual validation of TSM report results.

Channel Functional Test

The channel functional test ensures that the entire sensor and actuation logic channel performs its intended function. The online self-diagnostic features of NUMAC and TRICON, in conjunction with the TSM, support the channel functional test requirements. The channel functional test can be conducted by manual injection of a simulated signal, one division at a time. The channel functional test confirms the channel through its logic output contact is functioning correctly. The coincidence logic, involving more than one channel, and the final control elements are not activated in the channel functional test.

Logic System Functional Test

The logic system functional test is performed from sensor inputs to the actuated devices for all logic components required for operability of a logic circuit. To confirm that the trip logic is functioning, testing requires manual injection of simulated signals in two sensor channels of NUMAC/TRICON.

Response Time Test

The response time test is performed by a series of sequential, overlapping, or total steps to measure the entire response time. The instrument self-diagnostics and the TSM support the performance of the response time test for the NUMAC/TRICON. Watchdog timers monitor instrument internal clocks and alarms for out-of-limit conditions and the completion of application code per instrument cycle. Since the clocks set the response time, there is no mechanism for the response time to change without alarm or trip. All time delays incorporated into system logics are performed by software and the values are set during factory and preoperational testing in accordance with approved test procedures. Subsequent to final V&V of the code, there is no mechanism for the time delay values to inadvertently change.

The response time tests for the remaining portions (i.e. sensors (except neutron radiation detectors) and final control elements/actuators) are performed separately from self-diagnostics and the TSM.

7.1.3.5 Q-DCIS Instrumentation and Control Requirements

The data transmission function delivers system data to all nodes in the network, such as distributed logics of the Q-DCIS RMUs and specific safety-related logic system components, and in certain safety-related systems through dedicated data paths. The Q-DCIS thus provides the necessary integrated support for the distributed control logic functions of the RMUs and safety-related logic equipment. The data I/O and transmission functions do not require any manual operator intervention and have no operator controls.

The Q-DCIS operates continuously in all modes of plant operation to support the data transmission requirements of the interfacing systems. When one network of the dual network system fails, operation continues automatically without operator intervention. In the event that a channel failure occurs, the network alarms in the MCR indicate the failed component. The failed segment of the channel can be isolated from the operating segments and repaired on-line (IEEE Std. 603, Section 5.7, 5.10, and 6.5).

The following Q-DCIS displays and alarms, as a minimum, are provided in the MCR (IEEE Std. 603, Section 5.8).

- MCR Alarms:
 - Division 1 Q-DCIS trouble,
 - Division 2 Q-DCIS trouble,
 - Division 3 Q-DCIS trouble, and
 - Division 4 Q-DCIS trouble.
- MCR Indications:
 - Division 1 Q-DCIS diagnostic displays,
 - Division 2 Q-DCIS diagnostic displays,
 - Division 3 Q-DCIS diagnostic displays, and
 - Division 4 Q-DCIS diagnostic displays.

7.1.3.6 Q-DCIS Boundaries

The Q-DCIS does not include any N-DCIS components. In addition, the Q-DCIS ~~does not~~ includes neither the sensors, or the sensor wiring to the RMUs, nor the RMU output wiring to the actuators.

7.1.5.3.5 Branch Technical Positions

BTP HICB-14: Guidance on Software Reviews for Digital Computer-based I&C Safety-related systems:

- Conformance: The N-DCIS conforms ~~with~~to the intent of BTP HICB-14~~this guideline~~ as outlined in References 7.1--8, 7.1--10, and 7.1--12 ~~ISO-17799~~ for Security Management of the N-DCIS Control Network.

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

- Conformance: The level of detail ~~is~~in this subsection (7.1.5) conforms to BTP HICB-16~~commensurate with this BTP.~~

From the foregoing analyses, it is concluded that the N-DCIS meets its regulatory and industry design bases.

7.1.5.4 N-DCIS Testing and Inspection Requirements

~~The~~ Testing and inspection requirements for N-DCIS systems~~for each system within the N-DCIS~~ are presented as specific subsections in Chapter 7.

Channel check, channel functional test, logic system functional test, channel calibration, and response time test are required for some N-DCIS systems in support of technical specification surveillance requirements. Similar to the tests described for Q-DCIS in Section 7.1.3.4, the N-DCIS online diagnostic features described below support the technical specification surveillance requirements.

The N-DCIS controllers, displays, monitoring and I/O communication interfaces continuously function during normal power operation. Abnormal operation of these components ~~can be~~is detected and alarmed. In addition, similar to the functionality of the Q-DCIS platforms described in Section 7.1.3.4, the N-DCIS controllers are equipped with on-line diagnostic capabilities for cyclically monitoring the operability~~identifying and isolating failure~~ of I/O signals, buses, power supplies, processors, and inter-processor communications. On-line diagnostics are performed without interrupting the normal ~~control~~operation of the N-DCIS.

The N-DCIS components and critical components of interfacing systems are tested to ensure that the specified performance requirements are satisfied. Factory, construction, and preoperational testing of the N-DCIS ~~are~~is performed before fuel loading and startup testing to ensure that the system functions as designed and that tested system performance is within specified criteria.

As in the case of Q-DCIS, N-DCIS interfaces with the TSM for automatic cyclic comparison of channel outputs and monitoring of unacceptable deviations. The TSM provides a log of the results, and sends out-of-limits alarms to the AMS.

The N-DCIS uses diverse platforms for implementing nonsafety-related nuclear functions for 3D Monicore, RC&IS, automatic fixed in-core probe (AFIP), multi-channel rod block monitor

(MRBM), automated thermal limit monitor (ATLM), and rod worth minimizer (RWM). Self-diagnostic routines with alarms ensure operability.

- 3D Monicore monitors the reactor core, by accepting signals from the AFIP and the LPRMs. The LPRMs are calibrated with respect to the AFIP signals. Failed sensor inputs are rejected so that they do not contribute to calculations. Subsection 7.1.5.2.4.8 provides a functional description of 3D Monicore. There are two active redundant trains, but only one is manually selected by the operator at any time to periodically send fuel thermal limits information to the two redundant ATLMs. The same information is also sent to the TSM to support channel check and channel functional test surveillances.
- The MRBM and the AFIP are subsystems of the NMS. AFIP signals are routed to the 3D Monicore for calibrating the LPRM. Subsection 7.7.6.2.1 provides a functional description of the AFIP. The MRBM sends rod block signals to RC&IS to ensure that fuel thermal safety limits are not violated. Subsections 7.7.6.2.2 and 7.7.2.2.7.4 respectively provide a functional description of the MRBM and the rod block function.
- The ATLM and the RWM have two redundant channels that are subsystems of RC&IS, which ensures consistency between specific control rod pattern restrictions and the actual pattern of the rods in the reactor. Subsection 7.7.2 provides a functional description, and Figure 7.7-2 shows a block diagram of RC&IS.
- The ATLMs receive data from 3D Monicore through message-authenticated data links. They interchange data and generate alarms on disagreements. They send rod block signals to RC&IS to prevent violation of fuel operating thermal limits. Subsection 7.7.2.2.7.7 provides a functional description of the ATLM. ATLM failure automatically generates a rod block and an alarm. Only one ATLM can be bypassed at any time, and so there is always an active ATLM in service; additionally automated plant operation is not possible without both ATLMs being in service.
- Fuel thermal limits and rod block signals from the ATLMs and the MRBM are periodically sent to the TSM to support Channel Check and Channel Functional Test surveillances.

As described above, the 3D Monicore and ATLMs send fuel thermal limit information to the TSM to support channel check and channel functional test surveillances. The data downloads from the two systems are synchronized. The TSM conducts a check to compare the values, and generates alarms if the values are not comparable within acceptable limits.

Once per shift, in steady state operation, an automatic check of rod block capability is generated by the ATLM to close rod block contacts to RC&IS (this signal can also be sent by operator VDU command). The TSM detects the rod block command and generates an alarm. This routine tests the functionality of the output contacts for rod block, and will execute only after checking and confirming that the nuclear parameters as seen by 3D Monicore are in steady-state.

Additional surveillance tests associated with RC&IS ensure control rod operability and control rod pattern control. The control rod separation switches are also checked for functionality during a refuel outage, along with individual scram time testing on all the rods. A physical coupling

and decoupling of the control rod is carried out to actuate the corresponding separation switches and validate the rod block functionality.

7.1.5.5 N-DCIS Instrumentation and Control Requirements

7.1.5.5.1 Uninterruptible Nonsafety-Related AC Power Supply

The N--DCIS components and cabinets that are key to power generation are supplied with either dual redundant or triple redundant power supplies and power feeds. The sources of this power are three independent UPS inverters, normally supported by AC power. If off-site power fails and the diesel generators fail, the N--DCIS inverters receive power from three independent battery systems. All of these AC power feeds are well regulated and supply 120 ±10% volt AC, 60 Hz. Inverter operation-- Ffrequency, voltages, currents, and battery and charger operation are monitored and alarmed. The N--DCIS panel is designed so that the loss of one power supply or incoming power source does not affect the N--DCIS or its functional or plant operation.

7.1.5.5.2 Lighting and Service Power System

The LSP supplies 120 VAC power to the N--DCIS for lighting and maintenance equipment. This includes internal cabinet lighting and convenience outlets.

7.1.5.6 N-DCIS Major System Interfaces

The N--DCIS has interfaces with almost all of the I&C and electrical nonsafety-related plant systems. Safety-related system information acquired by the Q--DCIS is available to N--DCIS through qualified isolation devices that are part of the Q--DCIS. System interfaces with nonsafety-related systems, or portions of systems, and systems acquiring Q--DCIS data through isolation devices/gateways/datalinks include:

- ARMS;
- Auxiliary Boiler System (ABS);
- C&FS;
- Chilled Water System;
- CIRC;
- Condensate Storage and Transfer System;
- ~~Containment Inerting System;~~
- CMS;
- CB HVAC;
- CPS;
- CRD system;