HITACHI

GE Hitachi Nuclear Energy

Richard E. Kingston
Vice President, ESBWR Licensing

PO Box 780
3901 Castle Hayne Road, M/C A-55
Wilmington, NC 28402-0780 USA

T 910.819.6192
F 910.362.6192
rick.kingston@ge.com

MFN 08-920

Docket No. 52-010

December 12, 2008

U.S. Nuclear Regulatory Commission
11555 Rockville Pike
Document Control Desk
Rockville, MD 20852

Subject: **Response to Portion of NRC Request for Additional Information Letter No. 257 Related to ESBWR Design Certification Application - Instrumentation & Control Systems - RAI Numbers 7.1-109, 7.1-110, 7.1-111, 7.1-112, 7.1-113, 7.1-116, 7.1-121, 7.1-122, 7.1-123, 7.1-124, 7.1-125, 7.1-126, 7.2-68, 7.2-69, 7.2-70, 7.7-9, and 7.7-10**

Enclosures 1 and 2 contain the GE Hitachi Nuclear Energy (GEH) response to RAI Numbers 7.1-109, 7.1-110, 7.1-111, 7.1-112, 7.1-113, 7.1-116, 7.1-121, 7.1-122, 7.1-123, 7.1-124, 7.1-125, 7.1-126, 7.2-68, 7.2-69, 7.2-70, 7.7-9, and 7.7-10 from the U.S. Nuclear Regulatory Commission (NRC) Request for Additional Information (RAI) sent by NRC letter number 257, dated September 14, 2008 (Reference 1).

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

Sincerely,

Lee F. Dougherty for

Richard E. Kingston
Vice President, ESBWR Licensing

D068
NRO

Reference:

1. MFN 08-687, Letter from U.S. Nuclear Regulatory Commission to Robert E. Brown, *Request For Additional Information Letter No. 257 Related To ESBWR Design Certification Application*, dated September 14, 2008

Enclosures:

1. Response to Portion of NRC Request for Additional Information Letter No. 257 Related to ESBWR Design Certification Application - Instrumentation & Control Systems - RAI Numbers 7.1-109, 7.1-110, 7.1-111, 7.1-112, 7.1-113, 7.1-116, 7.1-121, 7.1-122, 7.1-123, 7.1-124, 7.1-125, 7.1-126, 7.2-68, 7.2-69, 7.2-70, 7.7-9, and 7.7-10

2. Response to Portion of NRC Request for Additional Information Letter No. 257 Related to ESBWR Design Certification Application - DCD Markups for RAI Numbers 7.1-110, 7.1-111, 7.1-112, 7.1-113, 7.1-121, 7.1-122, 7.1-123, 7.1-124, 7.1-125, 7.1-126, 7.2-68, 7.2-69, 7.7-9, and 7.7-10

cc:

AE Cubbage	USNRC (with enclosures)
RE Brown	GEH/Wilmington (with enclosures)
DH Hinds	GEH/Wilmington (with enclosures)
eDRF Sections:	0000-0092-1644 (RAI 7.1-109)
	0000-0091-8002 (RAI 7.1-110)
	0000-0091-7611 (RAI 7.1-111)
	0000-0093-3088 (RAI 7.1-112)
	0000-0091-7955 (RAI 7.1-113)
	0000-0092-0824 (RAI 7.1-116)
	0000-0092-9193 (RAI 7.1-121)
	0000-0091-8008 (RAI 7.1-122)
	0000-0092-0825 (RAI 7.1-123)
	0000-0092-1672 (RAI 7.1-124)
	0000-0093-1587 (RAI 7.1-125)
	0000-0091-7965 (RAI 7.1-126)
	0000-0092-7862 (RAI 7.2-68)
	0000-0092-7885 (RAI 7.2-69)
	0000-0092-7896 (RAI 7.2-70)
	0000-0094-8764 (RAI 7.7-9)
	0000-0094-8748 (RAI 7.7-10)

MFN 08-920

Enclosure 1

Response to Portion of NRC Request for Additional Information Letter No. 257 Related to ESBWR Design Certification Application

Instrumentation & Control Systems

RAI Numbers 7.1-109, 7.1-110, 7.1-111, 7.1-112, 7.1-113, 7.1-116, 7.1-121, 7.1-122, 7.1-123, 7.1-124, 7.1-125, 7.1-126, 7.2-68, 7.2-69, 7.2-70, 7.7-9, and 7.7-10

NRC RAI 7.1-109

See actual RAI letter No. 257 for accompanying graphic.

The scope section of IEEE Std 603 states, "The criteria contained in this standard establish minimum functional and design requirements for the power, instrumentation, and control portions of safety systems for nuclear power generating stations. To satisfy the criteria in this standard, interface requirements may be imposed on the other portions of the safety system as shown in Figure 1.

DCD Tier 1 or Tier 2 do not fully address the scope of IEEE Std 603 since they do not provide any discussion on mechanical process to sensor coupling. The DCD is primarily focused on instrumentation and provides limited information on sensing and actuation lines. For example, conformance to RG 1.151, "Instrument Sensing Lines," is stated in Tier 2 Section 7.1.6.4, however, no discussion is provided on separation, independence, single failure, etc. for sensing lines associated with reactor protection system (RPS), engineered safety feature system (ESF) instruments. This type of discussion should be provided under the "Instrumentation and Controls Requirements" subsections, such as 7.2.1.5, 7.3.3.5, etc.

GEH Response

GEH disagrees with the need to revise the DCD, as there is adequate discussion of separation/independence with regard to the RPS and ESF instrument sensing lines in the current revision.

The "mechanical process to sensor coupling" discussion for the RPS and ESF systems exists in DCD Tier 2, Revision 5, Subsection 7.2.1.2.4.2, Initiating Circuits (Nuclear Boiler System, Reactor Protection System).

Based on the above referenced discussion, the instrument sensing lines associated with the Reactor Protection System adhere to the scope of IEEE-603 with regards to separation, independence, and single failure. Additional discussion added to Subsections 7.2.1.5 and 7.3.3.5, "Instrumentation and Control Requirements", would be redundant.

DCD Impact

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

NRC RAI 7.1-110

Tier 2, Section 7.1.2 states that the Q-DCIS uses three diverse platforms, namely:

1. *Reactor Tip and Isolation Function (RTIF) function - NUMAC*
2. *Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) function - TRICON*
3. *Anticipated Transient without Scram/Standby Liquid Control (ATWS/SLC) and Vacuum Breaker Isolation Function (VBIF) functions - independent logic controllers*

There are a number of contradicting statements in Tier 1 and Tier 2 related to Q-DCIS platforms that require clarification. Some of the examples are:

- *DCD Tier 1 Table 2.15.1-1c, note 1 states that safety-related controls for VBIF are provided by control system independent of Q-DCIS [safety-related distributed control and information systems] and DPS [diverse protection system]. This statement can be interpreted to state that the independent logic controllers are not part of the Q-DCIS, which is inconsistent with DCD Tier 2 Section 7.1.2.*
- *Figure 7.1.2 and Section 7.1.2 indicate that ATWS/SLC and VBIF functions are being performed by the same platform. DCD Tier 2 Section 7.3.6.2 identifies that the VBIF automatic actuation logic is performed by a control system with components similar to those used in the ATWS/SLC control system. DCD Tier 2 Section 7.3.6.2 also identifies that each VB isolation function ATWS/SLC division can be placed into manual bypass status that is automatically indicated in the MCR. Clarify whether and how the ATWS/SLC and VBIF function are being implemented on a single platform. Identify any affects of combining the ATWS and containment cooling functions on the same platform on the topical report NEDO-33251, "ESBWR I&C Diversity and Defense-In-Depth Report," analyses.*
- *Per ATWS rule, the ATWS/SLC function is not required to be performed by safety grade components. For ESBWR, it appears that ATWS/SLC functions are being classified as safety-related. If such is the case then independent logic controllers must also comply with same regulations applicable to RTIF and SSLC/ESF platforms. For example, conformance to IEEE 603 for the ATWS function is not included in DCD Tier 2 Section 7.8.3.1.*

GEH Response

GEH agrees that statements in DCD Tier 1 Table 2.15.1-1c as well as Tier 2 Subsection 6.2.1.1.2 are in apparent contradiction with Tier 2 Subsection 7.1.2. The VB isolation function logic, like the ATWS/SLC logic, is safety-related and therefore part of Q-DCIS. The DCD Tier 1, Table 2.15.1-1c and Tier 2 Subsection 6.2.1.1.2 will be revised to support this concept.

The VB isolation function and ATWS/SLC logic are implemented on separate Independent Control Platforms (ICP) of the same type, i.e. platforms diverse from both

SSLC/ESF and RTIF/NMS. Figure 7.1-2 will be revised to show separate platforms of ICP for VB isolation function and ATWS/SLC. Since the ATWS/SLC and VB isolation function are not being implemented on a single platform, there is no impact to the topical report NEDO-33251, "ESBWR I&C Diversity and Defense-In-Depth Report," analyses.

GEH agrees that both the ATWS/SLC and the VB isolation function are safety-related and subject to IEEE Std. 603. The DCD will be revised to show conformance of ATWS/SLC to IEEE Std. 603 and additional General Design Criteria applicable to safety-related systems.

DCD Impact

DCD Tier 1, Table 2.15.1-1C will be revised in DCD Revision 6 as shown in Enclosure 2.

DCD Tier 2, Figure 7.1-2, Subsections 6.2.1.1.2, 7.1.3.4, 7.8.3.1, and 7.8.3.2 will be revised in DCD Revision 6 as shown in Enclosure 2.

DCD Tier 2, Tables 7.1-1 and 7.1-2 will be revised in Revision 6 to support the above response. The markup will be provided in a separate submittal in responses to RAI 7.1 99 and RAI 14.3-265, Supplement 1, respectively.

NRC RAI 7.1-111

In MFN 08-129, dated February 15, 2008, GEH committed to remove the TRICON licensing topical report (LTR), NEDO-33388, "ESBWR I&C TRICON (SSLC/ESF) Platform Application," Revision 0, September 2007 and the NUMAC LTR, NEDO-33288, "Application of Nuclear Measurement Analysis and Control (NUMAC) for the ESBWR Reactor Trip System," Revision 0, March 2007, from the design certification scope. This was to be completed in Revision 5 but was not done.

GEH Response

GEH concurs with the deletion of the TRICON and NUMAC licensing topical reports.

Per the GEH commitment of MFN 08-129 (submitted 2/15/2008), GEH will delete the following licensing topical reports (LTR) from the design certification scope:

- NEDO-33388, Class I (Non-proprietary), "ESBWR I&C TRICON (SSLC/ESF) Platform Application," and NEDE-33388P, Class III (Proprietary), "ESBWR I&C TRICON (SSLC/ESF) Platform Application," Revision 0, September 2007.
- NEDO-33288, "Application of Nuclear Measurement Analysis and Control (NUMAC) for the ESBWR Reactor Trip System," Revision 0, March 2007.

DCD Impact

DCD Tier 2, Table 1.6-1, Subsections 7.1.6.6.1.2, 7.2.2.1, 7.2.2.3.1, 7.2.5, 7.3.5.2, and 7.3.8 will be revised in DCD Revision 6 as shown in Enclosure 2.

NRC RAI 7.1-112

DCD Tier 2 Section 7.3.5.2 identifies that the SSLC/ESF architecture is presented in ESBWR DCD Tier 2 Reference 7.3-1, Triconex Topical Report 7286-545-1-a, "Qualification Summary Report." However, no additional discussion of the applicability of this report to the ESBWR design is provided. The applicant is requested to provide the deviations to the life cycle processes, hardware and software of the ESBWR SSLC/ESF platform from that which was originally provided by the staff in the Triconex Topical Report safety evaluation report (SER). Importantly, these proposed deviations should be evaluated in an analysis against appropriate regulatory criteria identifying why the deviations are acceptable. In lieu of identifying and evaluating deviations in the design certification, a commitment in the form of a specific DAC/ITAAC would be acceptable. Also, DAC/ITAAC should be provided for verifying the implementation of the plant specific requirements identified in section 5.2 of Triconex Topical Report SER.

GEH Response

The GEH Response to RAI 14.3-402 separately clarifies the DAC/ITAAC commitments for the development of the ESBWR SSLC/ESF hardware and software platforms.

GEH will delete reference to Triconex Topical Report 7286-545-1-a, "Qualification Summary Report", consistent with the deletion of all hardware-specific topical reports since the ESBWR DCD is platform-neutral for I&C hardware.

DCD Impact

DCD Tier 2, Table 1.6-2, Subsection 7.3.5.2, and Subsection 7.3.8 will be revised in DCD Revision 6 as shown in Enclosure 2.

NRC RAI 7.1-113

As noted in RAI 7.1-111, the NUMAC LTR will not be used to define the NUMAC used in the ESBWR application. However, several DCD Tier 2 sections continue to refer to the NUMAC platform. DCD Tier 2 should clarify that the NUMAC platform being proposed for the RTIF functions has not been previously submitted for review by the staff and should therefore be considered by the staff as a new platform. (Note that an entirely new platform dictates that an entire set of licensing documents should be submitted to the staff for review and approval to support a safety evaluation of the platform. Use of an existing platform allows safety analysis of the differences in addition to addressing any application specific items. The staff refers to the NRC DI&C TWG #6 for guidelines as what is to be submitted for new vs. NRC staff approved digital I&C platforms.)

No reference has been made to any of the previously NRC approved topical reports for a "NUMAC" platform. Importantly, no deviations, with the resulting "gap" analysis, or a commitment to do so, identifying the impact to the original safety evaluation of any NUMAC platform done by the NRC staff, have been submitted. When or if a reference is made, the utility or "plant specific" actions must also be addressed as identified in the last NUMAC SER.

GEH Response

Consistent with the GEH response to RAI 7.1-111, and commitment transmitted with MFN 08-129 (submitted 2/15/2008), GEH is deleting the NUMAC Licensing Topical Report (LTR), NEDO-33288, "Application of Nuclear Measurement Analysis and Control (NUMAC) for the ESBWR Reactor Trip System," Revision 0, March 2007 from the design certification scope.

Likewise, GEH committed in MFN 08-129 to the removal of the TRICON LTR, NEDE-33388P, "ESBWR I&C TRICON Platform Application," Revision 0, September 2007, from the design certification scope.

Consistent with the deletion of hardware-specific topical reports (noted in RAI 7.1-111) and because the ESBWR DCD is platform-neutral for I&C hardware, GEH will delete references to NUMAC and TRICON products and substitute:

- RTIF-NMS or RTIF-NMS platform for NUMAC.
- SSLC/ESF or SSLC/ESF platform for TRICON.

DCD Impact

DCD Tier 2, Subsections 7.1.2, 7.1.3.3.4, and 7.1.3.4 will be revised in DCD Revision 6 as shown in Enclosure 2.

NRC RAI 7.1-116

DCD Tier 2 Section 7.1.3.4 lists self-diagnostic "capabilities" then lists cyclically monitored items:

a) Is this a total listing of "capabilities" and actual diagnostics will be chosen from this list?

b) Does this mean all the self-diagnostics will not be cyclically monitored?

c) There is no identification of what self diagnostics take place during system initialization. IEEE Std. 7-4.3.2 identifies that when self-diagnostics are applied, self-diagnostics during computer system startup shall be incorporated into the system design. Clarify what self-diagnostics take place during system initialization.

GEH Response

a) *Is this a total listing of "capabilities" and actual diagnostics will be chosen from this list?*

No. This is a listing of minimum capabilities; actual diagnostic features will include these items.

b) *Does this mean all the self-diagnostics will not be cyclically monitored?*

Yes. Some diagnostics will be performed only upon system initialization.

c) *There is no identification of what self diagnostics take place during system initialization. IEEE Std. 7-4.3.2 identifies that when self-diagnostics are applied, self-diagnostics during computer system startup shall be incorporated into the system design. Clarify what self-diagnostics take place during system initialization.*

Details of self-diagnostic boot tests are beyond the scope of the DCD, but the second sentence of the sixth paragraph in Subsection 7.1.3.4 lists self-diagnostic features that are performed at system initialization and/or are performed cyclically. During startup power supply checks, microprocessor checks, system initialization, memory integrity checks, communication bus interfaces checks, and checks on the application program (checksum) will be performed. These features comply with IEEE Std. 7-4.3.2 (2003, Subsection 5.5.3, *Fault detection and self-diagnostics*), which requires "self-diagnostics during computer system startup" to be incorporated into the system design.

DCD Impact

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

NRC RAI 7.1-121

The discussion of "Logic System Functional Test" in this DCD Tier 2 Section 7.1.3.4 is different than that identified in the definition in Chapter 16 Section 1.1. The DCD should explain the differences.

GEH Response

GEH agrees to clarification. The "Logic System Function Test," as defined in DCD Tier 2, Chapter 7, Subsection 7.1.3.4 is the same "Logic System Function Test," as described in DCD Tier 2, Chapter 16, Section 1.1. However, to assure clarity and avoid differences in wording, DCD Tier 2, Chapter 7, Subsection 7.1.3.4 will be revised to be consistent with DCD Tier 2, Chapter 16, Section 1.1.

DCD Impact

DCD Tier 2, Chapter 7, Subsection 7.1.3.4 will be revised in DCD Revision 6 as shown in Enclosure 2.

NRC RAI 7.1-122

Failures detected by hardware, software, and surveillance testing should be consistent with the failure detectability assumptions of the single failure analysis and the failure modes and effects analysis. No comparable statement was found in DCD Tier 2 Section 7.1.3.4. This should be explicitly called out in the DCD.

GEH Response

GEH concurs with the staff's position concerning consistency between detected failures and assumptions for single failure analysis and FMEA. However, modification of Subsection 7.1.3.4 is not appropriate because the requirements that determine which self diagnostic features are to be provided is independent of the failure delectability assumptions of the single failure analysis and the FMEA. Instead, DCD Tier 2, Subsection 7.1.6.6.1.2 will be modified to add discussion stating that the FMEA is consistent with the failure modes detectable by the self-diagnostic features of the hardware/software platforms and those detected by periodic surveillance.

DCD Impact

DCD Tier 2, Section 7.1.6.6.1.2 will be revised in DCD Revision 6 as shown in Enclosure 2.

NRC RAI 7.1-123

DCD Tier 2 Section 7.1.5.4 states, "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 of I/O signals, buses, power supplies, processors, and interprocessor communications." However, DCD Tier 2 Section 7.1.3.4 does not discuss power supply diagnostics. Please clarify.

GEH Response

GEH agrees with the staff. Power supply diagnostics will be added to the list of self-diagnostic capabilities in Subsection 7.1.3.4.

DCD Impact

DCD Tier 2, Subsection 7.1.3.4 will be revised in DCD Revision 6 as shown in Enclosure 2.

NRC RAI 7.1-124

DCD Tier 2 Section 7.1.5.4 states, "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 use of the word "similar" is vague and implies that there may be differences. Clarify in the DCD the differences or at least where the potential for differences exist between Q-DCIS and N-DCIS online diagnostic features that support the technical specification surveillance requirements.

GEH Response

GEH concurs that the use of the word "similar" is vague; the DCD will be revised accordingly.

All references to Q-DCIS within subsection 7.1.5.4, "N-DCIS Testing and Inspection Requirements," will be removed to clarify and retain the online diagnostic features of the Q-DCIS (Subsection 7.1.3.4) and N-DCIS (Subsection 7.1.5.4) within their respective subsections.

The self-diagnostic routines are "similar" in that both the Q-DCIS and N-DCIS self-diagnostic routines were developed in part to:

- Satisfy surveillance requirements without requiring manual operator intervention, and
- Test for internal faults that cannot be found manually.

The detailed software requirements for Q-DCIS/N-DCIS online diagnostic features that support the Technical Specification surveillances will be developed as part of the ESBWR detailed design. Detailed software design will be implemented in accordance with the ESBWR - Software Management and Software Quality Assurance Program Manuals.

DCD Impact

DCD Tier 2, Subsection 7.1.5.4 will be revised in DCD Revision 6 as shown in Enclosure 2.

NRC RAI 7.1-125

Clarify in DCD Tier 2 Section 7.1.4.8.4, Plant Computer Functions Description Summary, that the item "MCR and RSS VDUs [main control room and remote shutdown system video display units]" is non-safety related.

GEH Response

GEH agrees to the Staff's request for clarification. Nonsafety-related Plant Computer Function information display and control capability are provided by nonsafety-related VDUs located in the MCR and RSS panels. The reference to MCR and RSS VDUs will be deleted from the lists in Subsections 7.1.4.8.2 and 7.1.4.8.4. The following sentence will be added at the end of Subsection 7.1.4.8.4: "PCF information display and control capability are provided by the nonsafety-related VDUs in the MCR and RSS panels."

DCD Impact

DCD Tier 2, Subsections 7.1.4.8.2 and 7.1.4.8.4 will be revised in DCD Revision 6 as shown in Enclosure 2.

NRC RAI 7.1-126

DCD Tier 2 Section 7.1.6.6.1.4 identifies that the safety related I&C systems "conform to the quality requirements described in IEEE Std. 7-4.3.2 as described in the software plans described in LTR, "ESBWR Man-Machine Interface System and Human Factors Engineering Implementation Plan, NEDO-33217 (Reference 7.1-13)." However, most of the information on the software plans was removed from NEDO-33217 in Revision 4. This section should instead reference the software LTRs, namely NEDE-33245P and NEDE-33226P.

GEH Response

GEH concurs and will delete reference to NEDO-33217, "ESBWR Man-Machine Interface System and Human Factors Engineering Implementation Plan". GEH will instead reference the following software LTRs:

- "ESBWR-Software Quality Assurance Program Manual," NEDO-33245, Class I (Non-proprietary); and "ESBWR-Software Quality Assurance Program Manual," NEDE-33245P Class III (Proprietary), Revision 3, July 2008
- "ESBWR-Software Management Program Manual," NEDO-33226, Class I (Non-proprietary); and "ESBWR-Software Management Program Manual," NEDE-33226P, Class III (Proprietary), Revision 3, June 2008

DCD Impact

DCD Tier 2, Subsections 7.1.6.6.1.4 and 7.1.8 will be revised in DCD Revision 6 as shown in Enclosure 2.

NRC RAI 7.2-68

In DCD Tier 2 Section 7.2.1.2.4.2 a new parameter was added in Rev. 5, namely: "Feedwater Temperature Biased Simulated Thermal Power." In this paragraph references are made to the RPS remote multiplexer units (RMU). Is this device same as the RTIF RMU? In Section 7.1, RPS designations have been replaced with RTIF when discussing the RMU, and Figure 7.1-2 only shows RTIF RMU. DCD Tier 2 Section 7.2.1.2.4.1 also discusses the RTIF RMU. GEH should verify that consistent device designations are presented in the DCD.

GEH Response

GEH concurs with your request. DCD Tier 2 subsection 7.2.1.2.4.2 will be revised to replace 'RPS' with 'RTIF' as appropriate. This includes references to remote multiplexer unit (RMU), digital trip modules (DTMs), trip logic units (TLUs) and bypass units (BPUs) in Section 7.2 for consistency of device designations presented in the DCD.

DCD Impact

DCD Tier 2 subsections 7.2.1.2.4.1, 7.2.1.2.4.2 and 7.2.1.5.2.2 will be revised in Revision 6 as shown in Enclosure 2.

NRC RAI 7.2-69

In DCD Tier 1 Table 2.2.7-2 and in the list of initiating circuits in DCD Tier 2 Section 7.2.1.2.4.2 (page 7.2-8), two new reactor scram initiators related to the simulated thermal power (STP) were added in Rev. 5, namely:

- High STP (feedwater temperature biased)

- FW temperature exceeding allowable STP vs. FW temperature domain

The associated description is provided in DCD Tier 2 Section 7.2.1.2.4.2 under the heading of Nuclear Boiler System in a paragraph titled "Feedwater Temperature Biased Simulated Thermal Power." However, only the 2nd reactor scram initiator is described. GEH should verify and provide a concise description of these parameters consistent with Tier 1.

GEH Response

GEH concurs with the request. ESBWR DCD Tier 2 Section 7.2.1.2.4.2 under the heading of "Nuclear Boiler System" will be revised to describe the two initiating circuits referenced in this Request for Additional Information and listed in DCD Tier 1 Table 2.2.7-2 and in the list of initiating circuits in DCD Tier 2 Section 7.2.1.2.4.2. RPS uses feedwater (FW) temperature from the Nuclear Boiler System (NBS) and simulated thermal power (STP) from the Neutron Monitoring System (NMS) to develop a STP setpoint that is a function of FW temperature (Feedwater Temperature Biased Simulated Thermal Power - High). In addition, the Reactor Protection System (RPS) uses FW temperature from NBS and STP from NMS to develop feedwater temperature high and feedwater temperature low setpoints that are functions of STP (Simulated Thermal Power Biased Feedwater Temperature - High and Simulated Thermal Power Biased Feedwater Temperature - Low, respectively).

DCD Impact

DCD Tier 2 subsections 7.2.1.2.4.2 will be revised in Revision 6 as shown in Enclosure 2.

NRC RAI 7.2-70

As described in DCD Tier 2 Section 7.2.1.2.4.2, some of the RPS scram initiating signals originate from the non-safety related components such as turbine stop valve (TSV), turbine closure valve (TCV), turbine bypass valve (TBV), main condenser, FW pump power sources, etc. While DCD Tier 2 Section 7.2.1.2.4.2 identifies the TSV and TBV position switches as part of the RPS, it is not clear that these switches are safety-related since they are attached to non-safety related components. The DCD should clarify the safety classification of these scram initiating sensors / circuits. The DCD should also describe any special treatment of the associated non-safety related components so as to prevent adverse impacts on the safety-related portions of the RPS. This discussion could be provided in Section 7.2.1.5, "Instrumentation and Control Requirements." Similar discussion should be provided for the pressure transmitters identified for the TCV hydraulics and the main condenser.

DCD Tier 2 Section 7.2.1.2.4.2, in the discussion under the heading "Loss of Power Generation Bus" does not identify any associated RPS interface for the FW pump power sources. Identify the RPS component that interfaces with the power generation bus.

GEH Response

GEH agrees that subsection 7.2.1.2.4.2 is not clear that the TSV and TBV position switches as part of the RPS are safety-related, since they are attached to non-safety related components. However as per DCD Tier 2 Table 3.2-1 "Classification Summary," and subsection 7.2.1.2.2, all functions and components of the RPS are safety-related unless otherwise indicated. DCD Tier 2 subsection 7.2.1.2.4.2 and Table 7.2-1 describes the scram initiating sensors including TSV and TBV position switches, TCV hydraulic trip system oil pressure transmitter, main condenser pressure transmitter and power generation bus voltage detectors as components of the RPS and are safety-related. DCD Tier 2 subsection 7.2.1.5.1 under section 7.2.1.5 "Instrumentation and Control Requirements," refers to subsection 7.2.1.2.4.2 for discussions of the scram initiating sensors including TCV fast closure and main condenser and the systems that apply to them.

As per DCD Tier 2, subsection 10.3.1.1, Turbine Main Steam System piping from the seismic interface restraint to the main stop valves and main turbine bypass valves are designed as Seismic Category II and are analyzed to demonstrate structural integrity under Safe Shutdown Earthquake (SSE) loading conditions. Also, per subsection 7.2.1.3 "Safety Evaluation," RPS design conforms to RG 1.89 and complies with the criteria set forth in IEEE Std. 603 to prevent any adverse impacts on the safety-related component by their associated non-safety components.

As described in DCD Tier 2, subsection 7.2.1.2.4.2 under "Loss or Power Generation Bus (Loss of Feedwater Flow)," each plant electrical system 13.8 kV power generation bus is equipped with sensors to detect a low voltage. Loss of more than one power generation bus (i.e., less than three power generation buses operating), as indicated by low voltage, is indicative of a loss of the FW pumps and flow.

DCD Impact

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

NRC RAI 7.7-9

In ESBWR DCD Tier 2, with Revision 5 changes, Section 7.7.3.2.1 states, "If a fault tolerant digital controller (FTDC) channel detects a discrepancy between the field voter output and the FTDC channel output, a "lock-up" signal is sent to a "lock-up" voter which causes the feed pump adjustable speed drive (ASD) to maintain the current pump speed and activates an alarm in the main control room (MCR)." DCD Tier 1 Revision 5, Table 2.2.3-2 has added the one way blocking function of the high pressure feedwater heater bypass valves and the one-way blocking of the seventh feedwater heater heating valves, but does not mention the "lock-up" voter function. Revise Tier 1 Table 2.2.3-2 to add the "lock-up" voter function described in Section 7.7.3.2.1 to assure that this important protective function is verified in ITAAC testing.

GEH Response

GEH agrees with adding the "lock-up" function for ITAAC testing. However, instead of adding the "lock-up" function to DCD Tier 1,Table 2.2.3-2 that is requested by the staff, GEH will add the "lock-up" function to Item 5 (FWCS controllers are fault tolerant) in Table 2.2.3-4, ITAAC For Feedwater Control System, since the "lock-up" is related to FWCS controller fault.

DCD Impact

DCD Tier 1, Table 2.2.3-4 will be revised in DCD Revision 6 as shown in Enclosure 2.

NRC RAI 7.7-10

DCD Rev. 5 added significant information to Tier 2, Section 7.7.3 on the feedwater control system (FWCS) FW temperature control functions including the required temperature measurement signals. However, this information is not reflected in DCD Tier 2, Section 7.7.3.5.2, Equipment. Revise DCD Tier 2, Section 7.7.3.5.2 to address the missing components of the FWCS.

GEH Response

GEH concurs with the staff's request. DCD Tier 2, subsection 7.7.3.5.2 will be revised to add the FW temperature signals.

DCD Impact

DCD Tier 2, subsection 7.7.3.5.2 will be revised in DCD Revision 6 as shown in Enclosure 2.

MFN 08-920

Enclosure 2

Response to Portion of NRC Request for Additional Information Letter No. 251 Related to ESBWR Design Certification Application

DCD Markups for RAI Numbers 7.1-110, 7.1-111, 7.1-112, 7.1-113, 7.1-121, 7.1-122, 7.1-123, 7.1-124, 7.1-125, 7.1-126, 7.2-68, 7.2-69, 7.7-9, and 7.7-10

DCD Markups for
RAI 7.1-110

Table 2.15.1-1c

Electrical Equipment

Equipment Name (Description)	Equipment Identifier See Figure 2.15.1-1	Control Q-DCIS/ DPS	Seismic Category I	Safety-Related	Safety-Related Display	Active Safety Function	Remotely Operated	Containment Isolation Valve Actuator
Vacuum Breaker	11(A)	-	Yes	Yes	Yes	Open/Close	No	No
Vacuum Breaker Isolation Valve	11a(A)	Yes/No~~Note 1~~	Yes	Yes	Yes	Open/Close	Yes	No
Vacuum Breaker	11(B)	-	Yes	Yes	Yes	Open/Close	No	No
Vacuum Breaker Isolation Valve	11a(B)	Yes/No~~Note 1~~	Yes	Yes	Yes	Open/Close	Yes	No
Vacuum Breaker	11(C)	-	Yes	Yes	Yes	Open/Close	No	No
Vacuum Breaker Isolation Valve	11a(C)	Yes/No~~Note 1~~	Yes	Yes	Yes	Open/Close	Yes	No
Containment System Logic Controllers	-	Yes/No~~Note 1~~	Yes	Yes	Yes	Open/Close Vacuum Breaker Isolation Valves on signals	Yes	No

~~Notes:~~

~~1. Safety-related control provided by control system independent of Q-DCIS and DPS~~

while the second vacuum breaker provides single failure protection for opening. On the upstream side of each vacuum breaker, pneumatically operated fail-as-is safety-related isolation valves are provided to isolate a leaking or stuck open vacuum breaker. During a LOCA, when the vacuum breaker opens and allows the flow of gas from WW to DW to equalize the DW and WW pressure and subsequently does not completely close as detected by the proximity sensors, a control signal closes the upstream isolation valve to prevent bypass leakage through the vacuum breaker and therefore maintain the pressure suppression capability of the containment. In addition to the proximity sensors, there are temperature sensors located between the vacuum breaker and the isolation valve. These sensors detect a rise in temperature due to the hot DW gas bypass, relative to the WW gas, which generates another control signal to close the isolation valve. ~~The safety-related logic and control of the isolation valve is independent of the safety-related Safety-Related Distributed Control and Information System (Q-DCIS).~~ Each isolation valve logic subsystem is located in physically separate divisional rooms or compartments that have appropriate fire barriers between them. The isolation valve can also be manually opened or closed. For more discussion on the logic control of the vacuum breaker isolation valves, see Subsection 7.3.6. The design WW-to-DW pressure difference and the vacuum breaker opening differential pressure are given in Table 6.2-1.

The vacuum breaker and vacuum breaker isolation valves are protected from pool swell loads by structural shielding/debris screen designed for pool swell loads determined based on the Mark II/III containment design. Both valves are located in the DW and connected to the WW gas space by a penetration through the diaphragm floor. The structural shielding/debris screen is located in the WW gas space at the inlet side of the penetration.

A safety-related PCCS is incorporated into the design of the containment to remove decay heat from DW following a LOCA. The PCCS uses six elevated heat exchangers (condensers) that are an integral part of the containment boundary located in large pools of water outside the containment at atmospheric pressure to condense steam that has been released to the DW following a LOCA. This steam is channeled to each of the condenser tube-side heat transfer surfaces where it condenses and the condensate returns by gravity flow to the GDCS pools. Noncondensable gases are purged to the suppression pool via vent lines. The PCCS condensers are an integral part of the containment boundary, do not have isolation valves, and start operating immediately following a LOCA. These low pressure PCCS condensers provide a thermally efficient heat removal mechanism. No forced circulation equipment is required for operation of the PCCS. Steam produced, due to boil-off in the pools surrounding the PCCS condensers, is vented to the atmosphere. There is sufficient inventory in these pools to handle at least 72 hours of decay heat removal. The PCCS is described and discussed in detail in Subsection 6.2.2.

The containment design includes a Drywell Cooling System (DCS) to maintain DW temperatures during normal operation within acceptable limits for equipment operation as described in Subsection 9.4.8.

Protection against the dynamic effects from the piping systems is provided by the DW structure. The DW structure provides protection against the dynamic effects of plant-generated missiles (Section 3.5).

An equipment hatch for removal of equipment during maintenance and an air lock for entry of personnel are provided in both the lower and upper DW. These access openings are sealed under

loss of one power feed or power supply does not affect any safety-related system function (IEEE Std. 603, Section 8.1).

The Q-DCIS includes the safety-related hardware and software for the RTIF, NMS, and SSLC/ESF protection functions and parallels the four-division design of those systems. No failure of any two divisions prevents a safety-related action, such as a detection or a trip, from being accomplished successfully. Component self-testing reconfigures the system to the approved safe state upon detection of uncorrectable errors. The capability for off-line test and calibration of the Q-DCIS components is designed into the system. An individual division can be disconnected for maintenance and calibration through the use of bypasses within the safety-related logic division without compromising the operations of the other divisions. Only one division can be bypassed at any one time and the existence of a bypass is alarmed in the MCR.

7.1.3.3.8 Acceptance Criteria, Guidance, and Conformance

The regulatory acceptance criteria and guidance applicable to each of the Q-DCIS systems identified in the "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants", NUREG-0800 are stated in Table 7.1-1, "Regulatory Requirements Applicability Matrix". Sections 7.2 through Section 7.8 contain regulatory conformance discussions for each specific system. The degree of applicability and conformance, along with 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 Q-DCIS uses ~~two~~ three diverse safety-related platforms;; ~~NUMAC for~~ RTIF-NMS ~~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)~~ICP.

~~Both~~The RTIF-NMS and SSLC/ESF 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~~RTIF-NMS and ~~TRICON~~SSLC/ESF 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~~RTIF-NMS and ~~TRICON~~SSLC/ESF have self-diagnostic features that check the validity of input signals. An analog input outside expected limits creates an alarm.

The ~~NUMAC~~RTIF-NMS 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~~SSLC/ESF platform~~,~~ is a Triple Modular Redundant (TMR) system, ~~has~~ with 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~~RTIF-NMS and ~~TRICON~~SSLC/ESF are cyclically tested from the sensor input point to logic contact output. The self-diagnostic capabilities include power supply checks, 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~~SSLC/ESF platform),
- Inter-divisional communication between RPS and NMS instruments (~~NUMAC~~RTIF-NMS platform),~~and~~
- Functionality of the output contact by momentarily reversing its state and confirming readiness to change state on demand (~~TRICON~~SSLC/ESF platform)~~.~~, and
- Power supplies.

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~~RTIF-NMS~~/~~ or ~~TRICON~~SSLC/ESF 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 ICP is similar to the RTIF-NMS and SSLC/ESF platforms in that it contains self-diagnostic capabilities to ensure that the platform is functioning properly. The ICP self-diagnostics contain the ability to:

- Detect data transmission errors,
- Detect hardware failures, and
- Check platform operability.

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~~the safety-related platforms, in conjunction with

the TSM, accomplish the channel check requirements for detecting unacceptable deviations by automatic cyclic comparison of channel outputs. TSM 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 the safety-related platforms~~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 the safety-related platforms~~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.

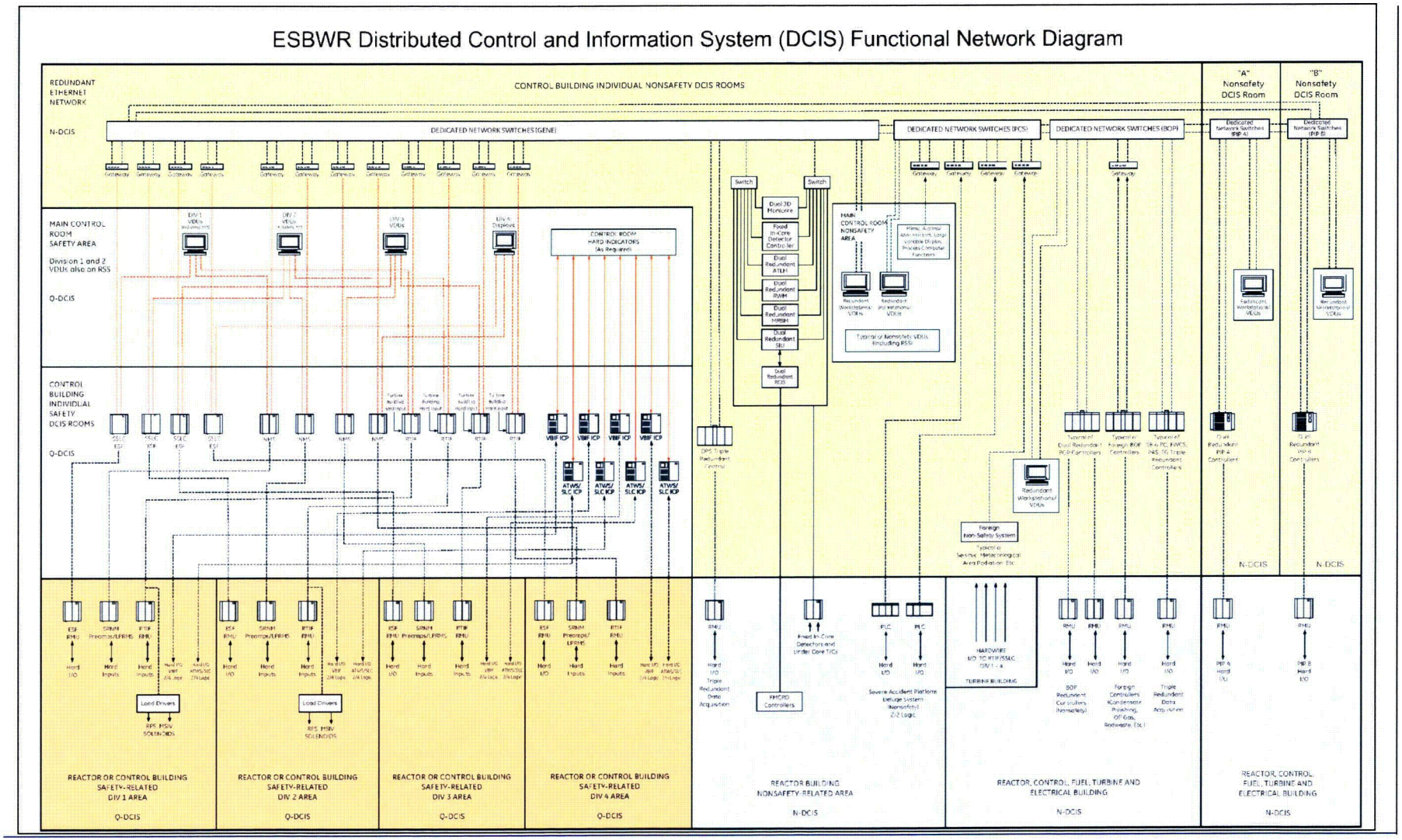
Logic System Functional Test

A LOGIC SYSTEM FUNCTIONAL TEST shall be a test of all logic components required for OPERABILITY of a logic circuit, from as close to the sensor as practicable up to, but not including, the actuated device, to verify OPERABILITY. The LOGIC SYSTEM FUNCTIONAL TEST may be performed by means of any series of sequential, overlapping, or total system steps so that the entire logic system is tested. ~~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 safety-related platforms~~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.


ESBWR Distributed Control and Information System (DCIS) Functional Network Diagram
REDUNDANT ETHERNET NETWORK
N-DCIS
CONTROL BUILDING INDIVIDUAL NONSAFETY DCIS ROOMS
DEDICATED NETWORK SWITCHES (GENE)
DEDICATED NETWORK SWITCHES (PCS)
DEDICATED NETWORK SWITCHES (BOP)
"A" Nonsafety DCIS Room
"B" Nonsafety DCIS Room
MAIN CONTROL ROOM SAFETY AREA
Division 1 and 2 VDUs also on RSS
Q-DCIS
CONTROL ROOM HARD INDICATORS (As Required)
MAIN CONTROL ROOM NONSAFETY AREA
CONTROL BUILDING INDIVIDUAL SAFETY DCIS ROOMS
Q-DCIS
REACTOR OR CONTROL BUILDING SAFETY-RELATED DIV 1 AREA
Q-DCIS
REACTOR OR CONTROL BUILDING SAFETY-RELATED DIV 2 AREA
Q-DCIS
REACTOR OR CONTROL BUILDING SAFETY-RELATED DIV 3 AREA
Q-DCIS
REACTOR OR CONTROL BUILDING SAFETY-RELATED DIV 4 AREA
Q-DCIS
REACTOR BUILDING NONSAFETY-RELATED AREA
N-DCIS
REACTOR, CONTROL, FUEL, TURBINE AND ELECTRICAL BUILDING
N-DCIS
REACTOR, CONTROL, FUEL, TURBINE AND ELECTRICAL BUILDING
N-DCIS

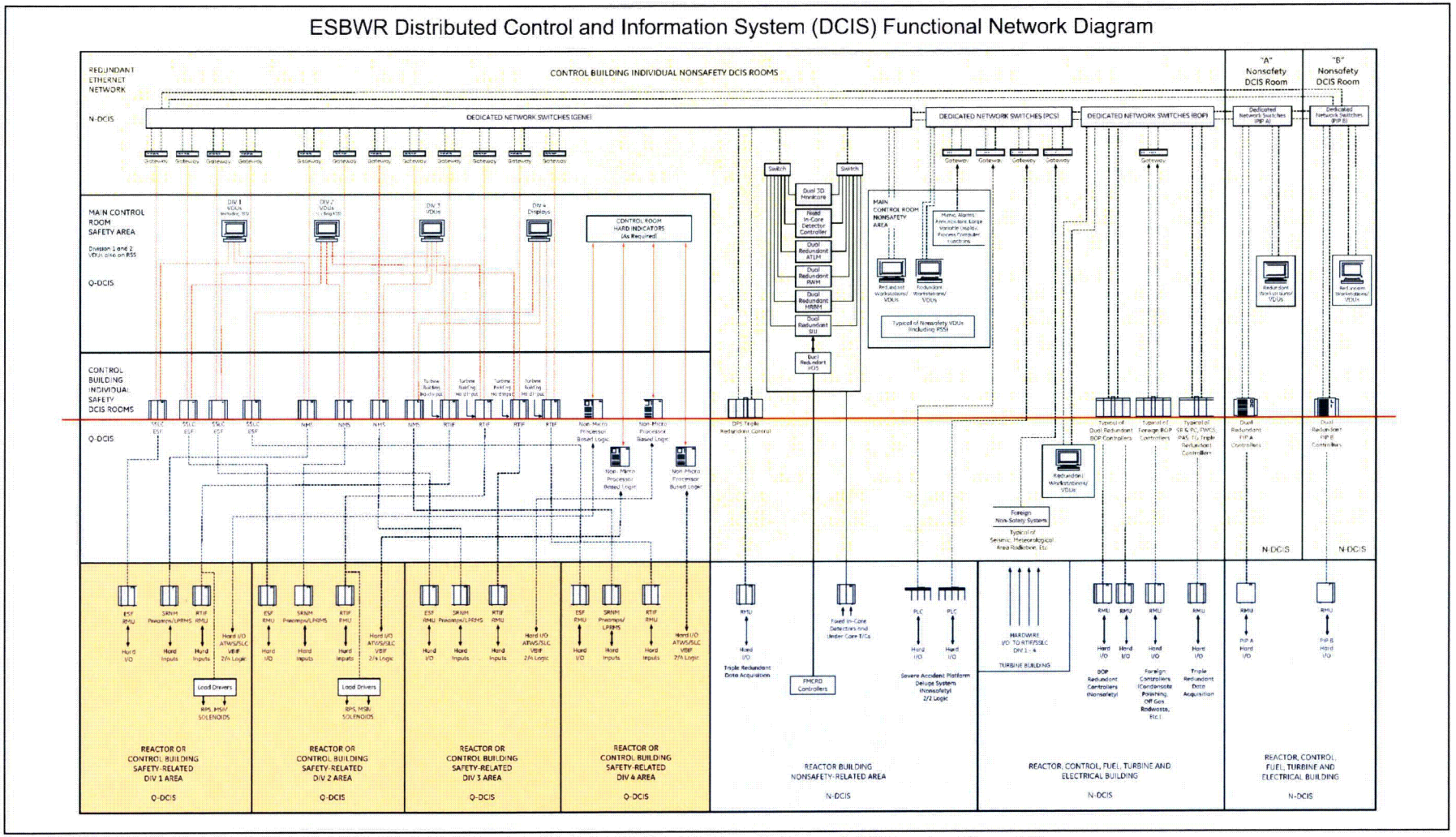


Figure 7.1-2. ESBWR Distributed Control and Information System (DCIS) Functional Network Diagram

10 CFR 50.55a(h), Protection and Safety Systems, compliance with IEEE Std. 603:

- Conformance: Safety-related systems are in conformance with RG 1.153 and IEEE Std. 603. Separation and isolation is preserved both mechanically and electrically in accordance with IEEE Std. 603, Section 5.6 and RG 1.75. The ATWS/SLC function is divisionalized and designed with redundancy so failure of any instrument will not prevent the system operation. Electrical separation is maintained between the redundant divisions.

For the diverse I&C systems, the applicable requirements are from IEEE Std. 603, Section 5.6, 'Independence'. Q-DCIS inter-divisional and cross-platform signal transmission is performed via fiber optic cables. Signal transmission between the systems of the Q-DCIS and the nonsafety-related control systems, including the DPS, is performed via fiber optic cables. The safety-related fiber optic communication interface module (CIM) provides the required isolation.

The diverse I&C have electrical surge withstand capability and can withstand the electromagnetic interference, radio frequency, and electrostatic discharge conditions that exist at their locations in the plant.

The diverse I&C equipment withstands the room ambient temperature, humidity conditions, radiation levels, and seismic accelerations that exist at their locations at the times for which they are required to be operational or required to fail in a safe mode.

10 CFR 50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication:

- Conformance: The diverse I&C systems conform to these requirements by providing automatic indication of bypassed and inoperable status.

10 CFR 50.62, Requirements for reduction of risk from ATWS events for light-water cooled nuclear power plants:

- Conformance: The ATWS mitigation functions described in Subsection 7.8.1.1 are designed in accordance with the requirements of 10 CFR 50.62.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAACs are provided for the diverse I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47(a)(2), Level of Detail:

- Conformance: The level of detail provided for the diverse I&C functions within the DCD conforms to this requirement.

7.8.3.2 General Design Criteria

General Design Criteria (GDC) 1, 2, 4, 13, 19, 20, 21, 22, 23, and 24:

- Conformance: The diverse I&C systems design conforms to these GDC.

The design of the diverse I&C systems does not compromise the ability of the RPS and SSLC/ESF actuation system to meet the requirements of 10 CFR 50 Appendix A, "General Design Criteria for Nuclear Power Plants," Section III, "Protection and Reactivity Control Systems."

7.8.3.3 Staff Requirements Memorandum

Item II.Q, (Defense Against Common-Mode Failures in Digital Instrument and Control Systems) of SECY-93-087 and SRM on SECY 93-087 (Policy, Technical, and Licensing Issues Pertaining to Evolutionary and ALWR Designs):

- Conformance: The SRM requirements applicable to the diverse I&C functions state that, "If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure as the safety system shall be required to perform either the same function as the safety system function that is vulnerable to common mode failure or a different function." It also states, "The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary functions under the associated event conditions." With respect to manual control and display functions, it states, "A set of displays and controls located in the main control room shall be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer systems."

  The implementation of the DPS and the ATWS mitigation features as described in Subsection 7.8.1, in conjunction with the RPS and ESF designs, conforms to the above SRM requirements.

7.8.3.4 Regulatory Guides

RG 1.22, (Safety Guide 22) Periodic Testing of Protection System Actuation Functions:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in RG 1.22. This RG is not applicable to the nonsafety-related DPS.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in RG 1.47. Automatic indication is provided in the MCR to inform the operator that the system is inoperable or a division is bypassed. This RG is not applicable to the nonsafety-related DPS.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

DCD Markups for
RAI 7.1-111

Table 1.6-1

Referenced GE / GEH Reports

Report No.	Title	Section No.
NEDO-33275	GE Hitachi Nuclear Energy, "ESBWR Training Development Implementation Plan," NEDO-33275, Class I (Non-proprietary), Revision 2, May 2008.	18.10
NEDO-33276	GE Hitachi Nuclear Energy, "ESBWR HFE Verification and Validation Implementation Plan," NEDO-33276, Class I (Non-proprietary), Revision 2, May 2008.	18.11
NEDO-33277	GE Hitachi Nuclear Energy, "ESBWR HFE Human Performance Monitoring Implementation Plan," NEDO-33277, Class I (Non-proprietary), Revision 3, May 2008.	18.13
NEDO-33278	GE Hitachi Nuclear Energy, "ESBWR HFE Design Implementation Plan," NEDO-33278, Class I (Non-proprietary), Revision 3, May 2008.	18.12
NEDE-33279P NEDO-33279	GE Energy – Nuclear, "ESBWR Containment Fission Product Removal Evaluation Model," NEDE-33279P, Class III (Proprietary), Revision 1, August 2007.	15.4, 15C
(Deleted)~~NEDO-33288~~	~~GE Energy – Nuclear, "Application of Nuclear Measurement Analysis and Control (NUMAC) for the ESBWR Reactor Trip System," NEDO-33288, Class I (Non-proprietary), Revision 0, March 2007.~~	~~7.2~~
NEDO-33289	GE Hitachi Nuclear Energy, "NP2010 COL Demonstration Project, Reliability Assurance Program Plan," NEDO-33289, Class I (Non-proprietary), Revision 1, December 2007.	17.4
NEDE-33295P NEDO-33295	GE Energy – Nuclear, "ESBWR Cyber Security Program Plan," NEDE-33295P, Class III (Proprietary), and NEDO-33295, Class I (Non-proprietary), Revision 0, October 2007.	7.1

Table 1.6-1

Referenced GE / GEH Reports

Report No.	Title	Section No.
NEDC-33374P NEDO-33374	GE-Hitachi Nuclear Energy, "Criticality Analysis for ESBWR Fuel Racks," NEDC-33374P, Class II (Proprietary), and NEDO-33374, Class I (Non-proprietary), November 2007.	9.1
(Deleted)~~NEDE-33388P~~ ~~NEDO-33388~~	~~GE Hitachi Nuclear Energy, "ESBWR I&C TRICON (SSLC/ESF) Platform Application," NEDE-33388P, Class III (Proprietary), and NEDO-33388, Class I (Non-proprietary), Revision 0, September 2007.~~	~~7.3~~
NEDE-33391	GE Hitachi Nuclear Energy, "ESBWR Safeguards Assessment Report," NEDE-33391, Revision 0, November 2007 – Safeguards Information.	13.6
NEDC-33408P NEDO-33408	GE Hitachi Nuclear Energy, "ESBWR Steam Dryer – Plant Based Load Evaluation Methodology," NEDC-33408P, Class III (Proprietary), and NEDO-33408, Class I (Non-proprietary), February 2008.	3L
NEDO-33411	GE Hitachi Nuclear Energy, "Risk Significance of Structures, Systems and Components for the Design Phase of the ESBWR," NEDO-33411, Class I (Non-proprietary), Revision 0, March 2008.	17.4

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 cable.

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 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 transmissions. The two-out-of-four voting logic treats the absence of an interdivisional trip signal as a trip 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 failure mode and effects analysis (FMEA) is performed of the complete safety-related reactor protection, ESF, and DPS designs. The FMEA is consistent with the failure modes detectable by the self-diagnostic features of the hardware/software platforms and those detected by periodic surveillance. ~~In addition, the NUMAC and TRICON platform specific LTRs (References 7.2-2 and 7.3-5, respectively) include analysis summaries of the architecture's conformance to the requirements of IEEE Std. 603.~~

7.1.6.6.1.3 Completion of Protective Action (IEEE Std. 603, Sections 5.2 and 7.3)

After initiation by either automatic or manual means, the protective actions go to completion in conformance to IEEE Std. 603, Section 5.2. They go to completion by using one of the following: seal-in logic, non-resettable squib valves, manually reset valves, diverse functions, or a combination of logic, valves and functions. Deliberate operator action is required to reset the safety-related systems. Control rod insertion is performed hydraulically if there is loss of power to both scram pilot valve solenoids, the three scram air header dump valves, or both pairs of ARI solenoid valves. The loss of power mode is latched at the load drivers by seal-in logic or by a maintained-open switch. The FMCRD mechanism provides a diverse means to hold the control rods in the fully inserted position if the loss of power signal is maintained long enough to allow the FMCRD to reach the fully inserted position. Specific descriptions are included in Subsections 7.2.1.1, 4.6.1, 4.6.2, and in other subsections as shown in Table 7.1-2.

7.2.1.5.9 Reactor Mode Switch In Shutdown Position Scram Bypass Switches

Two manual control switches are used to bypass the scram signal when moving the Reactor Mode Switch to its Shutdown position. This bypass only would be permitted during an outage condition when the reactor already is shutdown.

7.2.1.5.10 Maintenance Bypass Switches

Requirements for RPS-related maintenance bypass switches are addressed in Subsection 7.2.1.5.2.2. The maintenance bypasses are:

- Four division-of-sensor maintenance bypass switches; and
- Four division-out-of-service maintenance bypass switches.

7.2.1.5.11 Test Switches

Test switches to aid in surveillance testing during reactor operations are provided in the RPS design.

7.2.2 Neutron Monitoring System

The NMS monitors reactor core thermal neutron flux from the startup source range to beyond rated power and provides trip signals initiating reactor scrams under excessive neutron flux or excessive rates of change in neutron flux (short period) conditions.

7.2.2.1 System Design Bases

The subsystems comprising the NMS are:

- Startup Range Neutron Monitor (SRNM),
- Power Range Neutron Monitor (PRNM),
- Automatic Fixed In-Core Probe (AFIP), and
- Multi-Channel Rod Block Monitor (MRBM)

The PRNM subsystem includes the Local Power Range Monitor (LPRM), APRM functions, and the OPRM.

The SRNM and PRNM subsystems are safety-related and are discussed below. The nonsafety-related AFIP subsystem and the MRBM are addressed in Subsection 7.7.6. The application of this non-safety to safety interface is described in Subsection 7.1.3.3~~and in detail in Reference 7.2-2. This Topical Report addresses the CIM function, communication data link, data flow, and isolation requirements of IEEE Std. 603.~~ The CIM uses a one-way fiber optic communication data link and provides required safety-related isolation when passing data from nonsafety-related systems to safety-related systems.

7.2.2.3 Safety Evaluation

This evaluation covers the safety-related SRNM, LPRM, APRM, and OPRM functions of the NMS.

The evaluation of the trip inputs from the NMS to the RPS is discussed in Subsection 7.2.1.

The AFIP subsystem and the MRBM are nonsafety-related subsystems of the NMS, and are evaluated in Subsection 7.7.6.

Table 7.1-1 identifies the NMS and the associated codes and standards applied, in accordance with the Standard Review Plan NUREG-0800. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.2.2.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The NMS design conforms to these standards.

10 CFR 50.55a(h), "Protection and Safety Systems," compliance with ANS/IEEE Std. 603:

- Conformance: Safety-related systems are designed to conform to RG 1.153 and IEEE Std. 603. Separation and isolation are preserved both mechanically and electrically in accordance with IEEE Std. 603, Section 5.6 and RG 1.75. The NMS is divisionalized and designed with redundancy so that failure of any instrument does not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

  There are 64 LPRM assemblies uniformly distributed in the core. There are four LPRM detectors within each LPRM assembly, equally spaced from near the bottom of the active fuel region to near the top of the active fuel region (Figure 7.2-8). The 256 detectors are assigned to four divisions comprising the four APRM channels. Any single LPRM detector is assigned to one APRM division. Each set of 64 LPRM detector signals is assigned to one APRM channel with these signals averaged and normalized to form an APRM signal representing the average core power. Electrical and physical separation of the division is maintained and optimized to fulfill the safety-related system requirement.

  With the four divisions redundancy requirements are met, because a scram signal still can be initiated with a postulated single failure of one APRM channel under allowable APRM bypass conditions.

  Components used for the safety-related functions are qualified for the environments in which they are located. ~~Additional information on NMS equipment qualification is included in Reference 7.2-2.~~

10 CFR 50.34(f)(2)(v) [I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The NMS design of bypass and inoperable status indication conforms to this requirement, consistent with conformance of the NMS design to RG 1.47. In

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 ~~Plan~~Program Manual," NEDO-33226, Class I (Non-proprietary); and "ESBWR ~~I&C~~ Software Management ~~Plan~~Program Manual," NEDE-33226P, Class III (Proprietary), Revision ~~2~~3, ~~July~~June ~~2007~~2008.

7.2-4 GE Hitachi 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 ~~2~~3, July ~~2007~~2008.

- Testability,
- Separation and independence, and
- Bypass of certain functions and indication thereof.

7.3.5.2 System Description

SSLC/ESF is the decision-making control logic segment for the ESF systems. The SSLC/ESF processes automatic and manual demands for ESF system actuations, based upon sensed plant process parameters or at operator request. The SSLC/ESF includes the I&C implementing the non-MSIV isolation functions of the LD&IS, the ADS functions of the NBS for SRV and DPV control, the ECCS functions of the GDCS and SLC system, the ECCS and shutdown cooling functions of the ICS, and the control room isolation function of the CRHS. ~~The SSLC/ESF architecture is presented Reference 7.3-1 and Reference 7.3-5.~~

7.3.5.2.1 General SSLC/ESF Arrangement

The SSLC/ESF resides in four independent and separated instrumentation divisions. The SSLC/ESF integrates the control logic of the safety-related systems in each division into firmware or microprocessor-based, software-controlled, processing modules located in divisional cabinets in the safety-related equipment rooms of the CB. The SSLC/ESF runs without interruption in all modes of plant operation to support required safety functions.

The SSLC/ESF consists of the non-MSIV isolation functions of the LD&IS, the ECCS functions, and the isolation function of the CRHS. The ESF/ECCS part includes the functions of SRV and DPV initiation, GDCS initiation, SLC initiation, and the core cooling and shutdown cooling logic functions of the ICS. There are separate multiplexing networks for RTIF and SSLC/ESF functions within each division. Figure 7.3-4 shows a functional block diagram of the SSLC/ESF portion of the system. The RPS function is discussed in Subsection 7.2.1, with the RPS functional block diagram shown in Figure 7.2-1. The ATWS/SLC mitigation function is discussed in Subsection 7.8.1.1.

Most SSLC/ESF input data are process variables multiplexed by the Q-DCIS in four physically and electrically isolated redundant instrumentation divisions (Subsection 7.1.3). Each of the four independent and separated Q-DCIS channels feeds separate and independent trains of SSLC/ESF equipment in the same division.

7.3.5.2.2 Signal Logic Processing

Signals that must meet time response constraints and signals from system logic that are proximal to the SSLC/ESF cabinets are directly connected to the divisional cabinets in the safety-related equipment rooms in the CB. These signals are derived from sensors that are redundant in the four divisions (for each sensed variable).

All input data are processed within the RMU function of the Q-DCIS. The sensor data are transmitted through the DCIS network to the SSLC/ESF Digital Trip Module (DTM) function for setpoint comparison. A trip (or non-trip) signal is generated from this function. Processed

Management ~~Plan~~Program Manual," NEDE-33226P, Class III (Proprietary), Revision ~~2~~3, ~~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 ~~2~~3, 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.~~

DCD Markups for
RAI 7.1-112

Table 1.6-2

Referenced non-GE / GEH Topical Reports

Report No.	Title	Section No.
BC-TOP-3-A	Bechtel, "Tornado and Extreme Wind Design Criteria for Nuclear Power Plants," Topical Report BC-TOP-3-A, Revision 3, August 1974	3.3
BC-TOP-9A	Bechtel, "Design of Structures for Missile Impact," Topical Report BC-TOP-9A, Revision 2, September 1974.	3.5
(Deleted)~~7286-545-1-a~~	~~Triconex, "Qualification Summary Report," Topical Report 7286-545-1-a, March 8, 2002.~~	~~7.3~~

– Bypass of certain functions and indication thereof.

7.3.5.2 System Description

SSLC/ESF is the decision-making control logic segment for the ESF systems. The SSLC/ESF processes automatic and manual demands for ESF system actuations, based upon sensed plant process parameters or at operator request. The SSLC/ESF includes the I&C implementing the non-MSIV isolation functions of the LD&IS, the ADS functions of the NBS for SRV and DPV control, the ECCS functions of the GDCS and SLC system, the ECCS and shutdown cooling functions of the ICS, and the control room isolation function of the CRHS. ~~The SSLC/ESF architecture is presented Reference 7.3-1 and Reference 7.3-5~~.

7.3.5.2.1 General SSLC/ESF Arrangement

The SSLC/ESF resides in four independent and separated instrumentation divisions. The SSLC/ESF integrates the control logic of the safety-related systems in each division into firmware or microprocessor-based, software-controlled, processing modules located in divisional cabinets in the safety-related equipment rooms of the CB. The SSLC/ESF runs without interruption in all modes of plant operation to support required safety functions.

The SSLC/ESF consists of the non-MSIV isolation functions of the LD&IS, the ECCS functions, and the isolation function of the CRHS. The ESF/ECCS part includes the functions of SRV and DPV initiation, GDCS initiation, SLC initiation, and the core cooling and shutdown cooling logic functions of the ICS. There are separate multiplexing networks for RTIF and SSLC/ESF functions within each division. Figure 7.3-4 shows a functional block diagram of the SSLC/ESF portion of the system. The RPS function is discussed in Subsection 7.2.1, with the RPS functional block diagram shown in Figure 7.2-1. The ATWS/SLC mitigation function is discussed in Subsection 7.8.1.1.

Most SSLC/ESF input data are process variables multiplexed by the Q-DCIS in four physically and electrically isolated redundant instrumentation divisions (Subsection 7.1.3). Each of the four independent and separated Q-DCIS channels feeds separate and independent trains of SSLC/ESF equipment in the same division.

7.3.5.2.2 Signal Logic Processing

Signals that must meet time response constraints and signals from system logic that are proximal to the SSLC/ESF cabinets are directly connected to the divisional cabinets in the safety-related equipment rooms in the CB. These signals are derived from sensors that are redundant in the four divisions (for each sensed variable).

All input data are processed within the RMU function of the Q-DCIS. The sensor data are transmitted through the DCIS network to the SSLC/ESF Digital Trip Module (DTM) function for setpoint comparison. A trip (or non-trip) signal is generated from this function. Processed trip signals from a division and trip signals from the other three divisions are transmitted through the communication interface and are processed in the VLU function for two-out-of-four voting.

7.3.6.5 Instrumentation and Control Requirements

The performance and effectiveness of the VB isolation function in a postulated accident is verified by observing the following MCR indications (IEEE Std. 603, Section 5.8) (additional discussion on the VB isolation function instrumentation is contained in Subsection 7.3.6.1 and in Subsection 6.2.1.1.5):

- Status indication of VB position;
- Status indication of VB isolation valve position;
- Drywell and wetwell pressure indication;
- 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 ~~2~~3, ~~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 ~~2~~3, 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~~

DCD Markups for
RAI 7.1-113

- Communications between the systems.

Figure 7.1-1 shows a simplified functional block diagram of the ESBWR I&C system. The data communication systems embedded in the DCIS perform the data communication functions that are part of or support the systems described in Sections 7.2 through 7.8. A network diagram of the DCIS appears as Figure 7.1-2, which is a functional representation of the design.

The Q-DCIS and N-DCIS architectures, their relationships, and their acceptance criteria are further described throughout Section 7.1.

The Q-DCIS and N-DCIS functions are implemented with diverse power and sensors as indicated in Figure 7.1-3 and diverse hardware and software architectures as shown in Figure 7.1-4. These are discussed in Reference 7.1-4, the Licensing Topical Report (LTR), "ESBWR I&C Defense-In-Depth And Diversity Report," NEDO-33251.

The software for the Q-DCIS and N-DCIS is designed and developed in accordance with 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 7.1-12 and 7.1-10, respectively.) These plans describe the managerial, design, development, and software quality assurance requirements for the DCIS and address the Nuclear Regulatory Commission (NRC) review guidance provided in the Standard Review Plan.

7.1.2 Q-DCIS General Description Summary

The Q-DCIS, which performs the safety-related control and monitoring functions of the DCIS, is organized into four physically and electrically isolated divisions. The Q-DCIS uses three diverse platforms: ~~NUMAC for the~~ RTIF NMS ~~functions~~, ~~TRICON for~~ SSLC/ESF ~~functions~~, and independent logic controllers for the ATWS/SLC and vacuum breaker (VB) isolation function. Each division is segmented into systems; segmentation allows, but does not require, the systems to operate independently of each other. The Q-DCIS major cabinets, systems, and functions are:

- Reactor Trip and Isolation Function (RTIF) cabinets. These cabinets include the following systems and functions:
  - Reactor Protection System (RPS) (Refer to Subsection 7.2.1),
  - Main Steam Isolation Valve (MSIV) functions of the Leak Detection and Isolation System (LD&IS) (Refer to Subsection 7.3.3),
  - Anticipated Transient Without Scram/Standby Liquid Control (ATWS/SLC) functions (Refer to Subsection 7.4.1),
  - Suppression Pool Temperature Monitoring (SPTM) subsystem of the Containment Monitoring System (CMS) (Refer to Subsection 7.2.3), and
  - VB isolation function of the containment system (Refer to Subsection 7.3.6).
- Neutron Monitoring System (NMS) (Refer to Subsection 7.2.2) which includes:
  - Startup Range Neutron Monitor (SRNM) functions and

PRNM systems already licensed for some U.S. nuclear power plants, which is done manually and is rigorously controlled. Before the ~~NUMAC chassis~~RTIF-NMS platform can accept new calibration data, even if it has been continuously sent by 3D MONICORE, the operator must use a keylock switch to make the particular chassis inoperable (INOP). If the operator has not additionally put the corresponding division in bypass, the INOP is interpreted as an NMS trip. It is physically impossible to simultaneously bypass more than one division. Trips and bypasses are alarmed in the MCR.

After the chassis has been made INOP, the operator reviews the download received by the chassis being calibrated. Additionally, the operator can determine that a checkback signal interchange indicates that the ~~NUMAC chassis~~RTIF-NMS platform has correctly received the 3D MONICORE data. If a checkback signal is utilized, it is initiated by the ~~NUMAC~~ RTIF-NMS equipment and sent to 3D MONICORE. 3D MONICORE receives the checkback signal, verifies/validates that the information received by the ~~NUMAC~~ RTIF-NMS equipment is what was sent, and then sends a signal back to the ~~NUMAC~~ RTIF-NMS equipment confirming that the data was received accurately. There is no automatic/automated system response to a good or bad checkback signal. Only after the operator is satisfied that the calibration data are accurate and correct (through manual verification of the data and/or the use of a confirming electronic checkback signal) can the operator instruct the ~~NUMAC~~ RTIF-NMS platform~~chassis~~ that it is acceptable to use the downloaded data. This process is equivalent, but more convenient and accurate, to carrying the calibration data to the RTIF-NMS platform~~NUMAC chassis and~~ then entering it manually. The manual process is still possible. After the download is accepted by the RTIF-NMS platform~~NUMAC~~, the operator uses the keylock switch to make the instrument operable (removing it from the INOP state) and then resets the bypass for the division.

7.1.3.3.5 Dataflow, RMUs, Processor Cabinets, and VDUs

Dataflow within each of the four divisions of the Q-DCIS is from the RMUs located in the CB, RB, and possibly Fuel Building (FB) in areas appropriate to their division; there are no safety-related RMUs in any other building. Data such as that from transducers and switches is acquired by the RMUs, the signal appropriately conditioned, and sent via the redundant fiber optic cable communication links (datalinks) along with diagnostic data to the RTIF, NMS and SSLC/ESF cabinets. The RTIF, NMS, and SSLC/ESF cabinets are either centralized control processors or are various cabinets distributed throughout the division to perform the logic required by the safety-related systems.

There are always RTIF, NMS, and SSLC/ESF cabinets located in the MCR back panel area where there are four Q-DCIS rooms, one per division. The back panel area is where the interdivisional communication is physically performed to support the two-out-of-four voting that initiates safety-related action. Additionally RTIF, NMS, and SSLC/ESF safety-related fiber optic CIMs are used to operate the safety-related VDUs in that division and to provide isolation between the Q-DCIS and the N-DCIS. Finally, calculated outputs from the RTIF, NMS, and SSLC/ESF cabinets are sent via the redundant Q-DCIS communication system to the RMUs that provide outputs to the safety-related actuators (i.e., solenoids, explosive squib valves, etc.) via load drivers. Note that some outputs are hardwired directly to the final actuators if higher speeds are required.

loss of one power feed or power supply does not affect any safety-related system function (IEEE Std. 603, Section 8.1).

The Q-DCIS includes the safety-related hardware and software for the RTIF, NMS, and SSLC/ESF protection functions and parallels the four-division design of those systems. No failure of any two divisions prevents a safety-related action, such as a detection or a trip, from being accomplished successfully. Component self-testing reconfigures the system to the approved safe state upon detection of uncorrectable errors. The capability for off-line test and calibration of the Q-DCIS components is designed into the system. An individual division can be disconnected for maintenance and calibration through the use of bypasses within the safety-related logic division without compromising the operations of the other divisions. Only one division can be bypassed at any one time and the existence of a bypass is alarmed in the MCR.

7.1.3.3.8 Acceptance Criteria, Guidance, and Conformance

The regulatory acceptance criteria and guidance applicable to each of the Q-DCIS systems identified in the "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants", NUREG-0800 are stated in Table 7.1-1, "Regulatory Requirements Applicability Matrix". Sections 7.2 through Section 7.8 contain regulatory conformance discussions for each specific system. The degree of applicability and conformance, along with 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 Q-DCIS uses ~~two~~ three diverse safety-related platforms~~:~~: ~~NUMAC for~~ RTIF-NMS ~~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)~~ICP.

~~Both~~The RTIF-NMS and SSLC/ESF 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~~RTIF-NMS and ~~TRICON~~SSLC/ESF 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~~RTIF-NMS and ~~TRICON~~SSLC/ESF have self-diagnostic features that check the validity of input signals. An analog input outside expected limits creates an alarm.

The ~~NUMAC~~RTIF-NMS 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~~SSLC/ESF platform~~,~~ is a Triple Modular Redundant (TMR) system, ~~has~~ with 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~~RTIF-NMS and ~~TRICON~~SSLC/ESF are cyclically tested from the sensor input point to logic contact output. The self-diagnostic capabilities include power supply checks, 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~~SSLC/ESF platform),
- Inter-divisional communication between RPS and NMS instruments (~~NUMAC~~RTIF-NMS platform), ~~and~~
- Functionality of the output contact by momentarily reversing its state and confirming readiness to change state on demand (~~TRICON~~SSLC/ESF platform)~~.~~, and
- Power supplies.

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~~RTIF-NMS~~/~~ or ~~TRICON~~SSLC/ESF 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 ICP is similar to the RTIF-NMS and SSLC/ESF platforms in that it contains self-diagnostic capabilities to ensure that the platform is functioning properly. The ICP self-diagnostics contain the ability to:

- Detect data transmission errors,
- Detect hardware failures, and
- Check platform operability.

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~~the safety-related platforms, in conjunction with

DCD Markups for
RAI 7.1-121

The channel check is a qualitative assessment of channel behavior during operation. The online self-diagnostic features of ~~NUMAC/TRICON~~the safety-related platforms, in conjunction with the TSM, accomplish the channel check requirements for detecting unacceptable deviations by automatic cyclic comparison of channel outputs. TSM 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 the safety-related platforms~~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 the safety-related platforms~~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

A LOGIC SYSTEM FUNCTIONAL TEST shall be a test of all logic components required for OPERABILITY of a logic circuit, from as close to the sensor as practicable up to, but not including, the actuated device, to verify OPERABILITY. The LOGIC SYSTEM FUNCTIONAL TEST may be performed by means of any series of sequential, overlapping, or total system steps so that the entire logic system is tested. ~~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 safety-related platforms~~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.

DCD Markups for
RAI 7.1-122

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 cable.

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 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 transmissions. The two-out-of-four voting logic treats the absence of an interdivisional trip signal as a trip 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 failure mode and effects analysis (FMEA) is performed of the complete safety-related reactor protection, ESF, and DPS designs. The FMEA is consistent with the failure modes detectable by the self-diagnostic features of the hardware/software platforms and those detected by periodic surveillance. ~~In addition, the NUMAC and TRICON platform specific LTRs (References 7.2-2 and 7.3-5, respectively) include analysis summaries of the architecture's conformance to the requirements of IEEE Std. 603.~~

7.1.6.6.1.3 Completion of Protective Action (IEEE Std. 603, Sections 5.2 and 7.3)

After initiation by either automatic or manual means, the protective actions go to completion in conformance to IEEE Std. 603, Section 5.2. They go to completion by using one of the following: seal-in logic, non-resettable squib valves, manually reset valves, diverse functions, or a combination of logic, valves and functions. Deliberate operator action is required to reset the safety-related systems. Control rod insertion is performed hydraulically if there is loss of power to both scram pilot valve solenoids, the three scram air header dump valves, or both pairs of ARI solenoid valves. The loss of power mode is latched at the load drivers by seal-in logic or by a maintained-open switch. The FMCRD mechanism provides a diverse means to hold the control rods in the fully inserted position if the loss of power signal is maintained long enough to allow the FMCRD to reach the fully inserted position. Specific descriptions are included in Subsections 7.2.1.1, 4.6.1, 4.6.2, and in other subsections as shown in Table 7.1-2.

DCD Markups for
RAI 7.1-123

Both ~~NUMAC~~RTIF-NMS and ~~TRICON~~SSLC/ESF are cyclically tested from the sensor input point to logic contact output. The self-diagnostic capabilities include power supply checks, 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~~SSLC/ESF platform),
- Inter-divisional communication between RPS and NMS instruments (~~NUMAC~~RTIF-NMS platform), ~~and~~
- Functionality of the output contact by momentarily reversing its state and confirming readiness to change state on demand (~~TRICON~~SSLC/ESF platform)~~.~~, and
- Power supplies.

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~~RTIF-NMS~~/~~ or ~~TRICON~~SSLC/ESF 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 ICP is similar to the RTIF-NMS and SSLC/ESF platforms in that it contains self-diagnostic capabilities to ensure that the platform is functioning properly. The ICP self-diagnostics contain the ability to:

- Detect data transmission errors,
- Detect hardware failures, and
- Check platform operability.

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

DCD Markups for
RAI 7.1-124

The alarm processors are dedicated, redundant, and conservatively sized. The alarms can be displayed on multiple independent VDUs, each with dual power supplies. Alarms are driven by redundant data links to the AMS. The alarm processors are redundant. There is one horn and one voice speaker. Test buttons test the horn and the lights.

7.1.5.3.4 Regulatory Guides

RG 1.151, Instrument Sensing Lines:

- Conformance: RG 1.151 is not applicable to the N-DCIS. The N-DCIS receives signals from sensors in various systems in the plant that are from instrument sensing lines from nonsafety-related instrumentation but the N-DCIS itself does not contain instrument sensing lines.
- For details on conformance to the Regulatory Guides listed in subsection 7.1.4.4, refer to Subsection 7.1.6.4.

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 design conforms to the intent of BTP HICB-14 as outlined in References 7.1-8, 7.1-10, and 7.1-12 for 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 in this subsection (7.1.5) conforms to BTP HICB-16.

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

Testing and inspection requirements for N-DCIS systems 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, t~~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 is detected and alarmed. ~~In addition, similar to the functionality of the Q-DCIS platforms described in Section 7.1.3.4, t~~The N-DCIS controllers are equipped with on-line diagnostic capabilities for cyclically monitoring the operability of I/O signals, buses, power supplies, processors, and inter-

processor communications. On-line diagnostics are performed without interrupting the normal 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 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.

~~Like the Q-DCIS, t~~The 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, AFIP, MRBM, ATLM, and 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

DCD Markups for
RAI 7.1-125

- Control Rod Drive (CRD) System,
- Reactor Water Cleanup and Shutdown Cooling (RWCU/SDC) System,
- FAPCS,
- Reactor Component Cooling Water System (RCCWS),
- Plant Service Water System (PSWS),
- PSWS cooling towers,
- Nuclear Island Chilled Water System (NICWS),
- Drywell cooling nonsafety-related electrical systems,
- Instrument Air System (IAS),
- Ancillary and standby diesel generators,
- 6.9 KV plant electrical power system,
- Low voltage electrical system, and
- Uninterruptible power supplies (UPS)~~, and~~

~~MCR and RSS panel displays.~~

The N-DCIS segments in PIP A and PIP B allow for operator control and monitoring from the MCR nonsafety-related VDUs and the RSS VDUs. The A and B segments can operate independently of one another.

During loss of offsite power events, the N-DCIS for PIP A and PIP B is powered by its respective nonsafety-related batteries for two hours and then by diesel generators and can therefore operate without offsite power.

7.1.4.8.3 Balance Of Plant Systems Description Summary

The balance of plant (BOP) segments provide the logic for systems involved in power generation. These systems control/protect:

- Reactor pressure;
- RPV water level;
- The FWCS, including RPV level and feedwater temperature control;
- The PAS;
- The SB&PC System;
- The turbine and generator;

- The main condenser and normal heat sink;
- The nonsafety-related plant electrical systems, including protective relaying, that are non-PIP;
- Power generation components such as the moisture separator reheater (MSR) and the CPS;
- The Condensate and Feedwater System (C&FS), including extraction and level control; and
- Vendor-furnished BOP systems.

Segments in the BOP systems allow for operator control and monitoring from the MCR nonsafety-related VDUs.

7.1.4.8.4 Plant Computer Functions Description Summary

The PCF provide:

- Performance monitoring and control (PMC) functions, prediction calculations, visual display control, point log and alarm processing, surveillance test support, and automation;
- Core thermal power/flow calculations;
- The plant Alarm Management System (AMS) that alerts the operator to process deviations and equipment/instrument malfunctions;
- Fire Protection System (FPS) data through datalinks and gateways (if necessary);
- The Historian function, that stores data for later analysis and trending;
- Control of the main mimic on the MCR Wide Display Panel (WDP);
- Support functions for printers and the secure data communications to the TSC, EOF, ERDS, and potential links to the Simulator;
- Online procedures (OLP) to guide the operator during normal and abnormal operations, and to verify and record compliance;
- Transient recording;
- Nonsafety-related PAM displays;
- ~~MCR and RSS VDUs;~~
- Report generators to allow the operator, technician, or engineer to create historical or real time reports for performance analysis and maintenance activities;
- The PCD to document, manage, and configure components of the N-DCIS;
- Gateways to vendor-supplied nonsafety-related systems such as seismic, meteorological, and radiation monitoring; and
- Nonsafety-related process and area radiation monitoring.

PCF information display and control capability are provided by nonsafety-related VDUs in the MCR and RSS panels.

7.1.5 N-DCIS Specifics

The N-DCIS data communication systems are embedded in the DCIS that performs the data communication functions that are part of and support the nonsafety-related systems described in Sections 7.2 through 7.8 and support the Q-DCIS to N-DCIS communications for the safety-related systems described in Sections 7.2 through 7.8. A functional network diagram of the DCIS appears as part of Figure 7.1-2, which indicates the elements of the N-DCIS and the Q-DCIS.

The N-DCIS architecture, its relationships, and its acceptance criteria are further described in this subsection.

7.1.5.1 N-DCIS Design Bases

7.1.5.1.1 N-DCIS Safety-Related Design Bases

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

7.1.5.1.2 N-DCIS Nonsafety-Related Design Bases

The N-DCIS is used as the primary control, monitoring, and data communication system for power production applications. The design bases for the N-DCIS include the requirements to:

- Segment the N-DCIS display and control of the two PIP Systems (A&B) and the BOP systems so they can operate independently of one other;
- Segment the major reactor control systems (FWCS, SB&PC System, TGCS and PAS) so they can operate independently of one another and from the DPS;
- Perform closed loop control and system logic independently of the MCR VDUs and Ethernet networks. Operability of the RSS panels, and their VDUs is independent of the operation or existence of the MCR displays;
- Ensure that no single failure of an N-DCIS component affects power generation;
- Provide a communication path for nonsafety-related data gathered and distributed throughout the plant, including datalink interfaces to control systems. The communication paths are redundant and include both the "native" control systems and "foreign", vendor supplied or prepackaged control systems (condensate purification, offgas, radwaste, area radiation monitoring, and meteorological monitoring, for example);
- Reliably transfer to or from the plant areas, in digital format, analog or binary information that has been collected and digitized from nonsafety-related RMUs. The RMUs include transmitters, contact closures and other sensors or process activation signals, generated elsewhere for the control of remote devices such as pumps, valves or solenoids;

DCD Markups for
RAI 7.1-126

to both scram pilot valve solenoids, the three scram air header dump valves, or both pairs of ARI solenoid valves. The loss of power mode is latched at the load drivers by seal-in logic or by a maintained-open switch. The FMCRD mechanism provides a diverse means to hold the control rods in the fully inserted position if the loss of power signal is maintained long enough to allow the FMCRD to reach the fully inserted position. Specific descriptions are included in Subsections 7.2.1.1, 4.6.1, 4.6.2, and in other subsections as shown in Table 7.1-2.

7.1.6.6.1.4 Quality (IEEE Std. 603, 5.3)

All equipment is provided under the GEH 10 CFR 50, Appendix B quality assurance program. The NRC-accepted GEH Quality Assurance Program with its implementing procedures, constitutes the Quality Assurance system that is applied to the Q-DCIS design. It satisfies all applicable requirements of the following: 1) 10 CFR 50 Appendix B; 2) ANSI/ASME NQA-1; and 3) ISO 9001. Safety-related I&C systems employing digital computers, software, firmware, and software tools conform to the quality requirements ~~described~~ in IEEE Std. 7-4.3.2 as described in ~~the software plans described in LTR, "ESBWR Man Machine Interface System and Human Factors Engineering Implementation Plan," NEDO-33217~~ (References 7.1-1~~3~~0 and 7.1-12~~)~~. Software tools used to support software development processes and V&V processes are controlled under a configuration management program. The software tool configuration management process ensures that software tools are part of a test tool validation process. The software test tool validation process confirms by one or both of the following methods that software tools are suitable for use.

- Software tools are subjected to a test tool validation program.
- Software tools are used in a manner such that defects not detected by the software tool are detected by V&V activities.

7.1.6.6.1.5 Equipment Qualification (IEEE Std. 603, Section 5.4)

It is required that safety-related equipment be designed to meet the safety-related functional performance requirements over the range of normal, abnormal, and DBA environmental conditions for the area in which it is located. Equipment qualification typically includes EMI qualification, seismic qualification, and other environmental condition qualification such as temperature, humidity, radiation, and pressure. The Q-DCIS systems are designed to meet the equipment qualification requirements set forth in 10 CFR 50.49, RG 1.209, RG 1.89, RG 1.100, IEEE Std. 603, IEEE Std. 323, and IEEE Std. 344. Equipment qualification is discussed in Section 3.11. The Q-DCIS components are designed to be qualified to operate in the normal, abnormal, and DBA environments in which they are located.

For environmental qualification, the following conditions are addressed:

Temperature and Humidity: The Q-DCIS components are designed to be qualified using type testing as the preferred method and analysis to demonstrate that the components perform all specified functions correctly when operated within the specified temperature range and relative humidity range.

Pressure: The Q-DCIS components are designed to be qualified (by analysis) to perform safety-related functions for any absolute pressure in the range specified.

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 PlanProgram Manual," NEDO-33226, Class I (Non-proprietary); and "ESBWR I&C Software Management PlanProgram Manual," NEDE-33226P, Class III (Proprietary), Revision 32, July June 20078.

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.*

DCD Markups for
RAI 7.2-68

The software associated with RPS channel trip and trip system coincident logic decisions installed in these modules is RPS unique. The number of sensors used in the functional performance of the RPS is shown in Table 7.2-1 (IEEE Std. 603, Section 4.4).

Q-DCIS equipment within a single division of sensor channels is powered from the safety-related power source of the same division. However, different pieces of equipment are powered from separate low-voltage DC power supplies within the panels belonging to the same division. Within a sensor channel, the sensors themselves are components of the RPS or components of an interfacing system. Signal conditioning and distribution performed by the RMUs are functions of the Q-DCIS.

Components within each of the four RPS sensor channels are separated physically and are independent from components of other sensor channels (fulfilling the independence requirement of IEEE Std. 603, Section 5.6). The RPS equipment is independent and physically separated from other safety-related or nonsafety-related systems fulfilling the requirements of IEEE Std. 603, Section 5.6.

Any signal communication between the RPS and other systems is through the required safety-related isolation devices (the safety-related fiber optic communication interface modules [CIMs]). There are no signal inputs from other systems affecting the safety function of the RPS. The application of this nonsafety-to-safety interface is described in Subsection 7.1.3.3. The transfer of data between the safety-related system and nonsafety-related system is one-way..

Divisions of Trip Logic: Equipment within an RPS division of trip logic consists of TLUs, manual switches, Bypass Units (BPUs), and Output Logic Units (OLUs).

The TLUs perform the automatic scram initiation logic checking for two-out-of-four coincidence of trip conditions in any set of instrument channel signals coming from the four divisions of DTMs, or when a NMS-isolated digital trip signal (voted two-out-of-four in the NMS TLU) is received. The automatic scram initiation logic for any trip is based on the reactor operating mode switch status, channel trip conditions, NMS trip input, and bypass conditions. Each TLU, in addition to receiving the signals described above, also receives digital input signals from the BPU and other control interfaces in the same division. Signals from one RPS division to another RPS division are isolated optically 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~~ RTIF 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~~ RTIF 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.

7.2.1.2.4.2 Initiating Circuits

The RPS logic initiates a reactor scram in the individual sensor channels when any one or more of the conditions listed below exist (IEEE Std. 603, Section 4.1, 4.2 and 4.4). The system monitoring the process condition is indicated in parentheses. These conditions are:

- High drywell pressure (CMS),
- Turbine stop valve (TSV) closure (RPS),
- Turbine control valve (TCV) fast closure (RPS),
- NMS-monitored SRNM and APRM conditions exceed acceptable limits (NMS),
- High reactor pressure (NBS),
- Low reactor pressure vessel (RPV) water level (Level 3) decreasing (NBS),
- High RPV water level (Level 8) increasing (NBS),
- Main steam line isolation valve (MSIV) closure (Run mode only) (NBS),
- Low control rod drive HCU accumulator charging header pressure (CRDS),
- High suppression pool temperature (CMS),
- High condenser pressure (RPS),
- Power generation bus loss (Loss of all feedwater [FW] flow)(Run mode only) (RPS),
- High simulated thermal power (FW temperature biased) (NBS and NMS),
- Feedwater temperature exceeding allowable simulated thermal power vs. FW temperature domain (NBS),
- Operator-initiated manual scram (RPS), and
- Reactor Mode Switch in Shutdown position (RPS).

With the exception of the NMS outputs, the MSIV closure, TSV closure and TCV fast-closure, loss of all FW flow due to ~~a loss of~~ power generation bus loss, main condenser pressure high, and manual scram outputs, systems provide sensor outputs through the ~~RPS~~ RTIF RMU.

The MSIV Closure, TSV closure and TCV fast-closure, loss of power generation bus, manual scram output, and main condenser pressure high signals are provided to the RPS through hardwired connections. The NMS trip signal is provided to the RPS through fiber optic cable. The systems and equipment providing trip and scram initiating inputs to the RPS for these conditions are discussed in the following subsections.

Neutron Monitoring System

The separate and isolated NMS digital Startup Range Neutron Monitor (SRNM) trip signals, and Average Power Range Monitor (APRM) trip signals from each of the four divisions of the NMS equipment are provided to their divisions of RPS trip logic as shown on Figure 7.2-1.

SRNM Trip Signals: The safety-related SRNM subsystem provides trip signals to the RPS to cover the range of plant operation from source range through startup range (more than 10% of reactor rated power). Three SRNM conditions, monitored as a function of the NMS, comprise the SRNM trip logic output to the RPS. These conditions are:

- SRNM upscale (high count rate or high thermal neutron flux level),
- Short (fast) period, and
- SRNM inoperative.

The three trip conditions from every SRNM associated with a NMS division are combined into a single SRNM trip signal for that division. The specific condition causing the SRNM trip output state is identified by the NMS, and is not detectable within the RPS. The SRNM trip functions are summarized in Table 7.2-2. SRNM trip signals are summarized in Table 7.2-3.

APRM Trip Signals: The APRM trip signals cover the range of plant operation from a few percent of reactor rated power to greater than rated power. Three APRM conditions, monitored as a function of the NMS, comprise the APRM trip logic output to the RPS. These conditions are:

- APRM high thermal neutron flux,
- High simulated reactor thermal power, and
- APRM inoperative.

The APRM trip functions are summarized in Table 7.2-4.

Within the safety-related APRM subsystem there is the Oscillation Power Range Monitor (OPRM) function, which is capable of generating a trip signal in response to core thermal neutron flux oscillation conditions, and thermal-hydraulic instability fast enough to prevent cladding thermal limit violation and fuel damage. This OPRM trip signal is combined with the other three APRM trip signals to form the final APRM trip signal to the RPS. The NMS also provides the RPS with a simulated reactor thermal power signal to support the load rejection bypass algorithm.

Nuclear Boiler System

Reactor Pressure: Reactor pressure is measured by four physically separate pressure transmitters mounted on separate divisional local racks in the safety envelope within the Reactor Building (RB). Each transmitter is on a separate instrument line and is associated with a separate RPS electrical division. Each transmitter provides an analog output signal to the ~~RPS~~ RTIF RMU, which digitizes and conditions the signal before sending it to the appropriate ~~RPS~~ RTIF

DTM in one of the four RPS divisional sensor channels. The four pressure transmitters and associated instrument lines are components of the NBS.

Reactor Pressure Vessel Water Level: RPV water level is measured by four physically separate level (differential pressure) transmitters mounted on separate divisional local racks in the safety envelope within the RB. Each transmitter is on a separate pair of instrument lines and is associated with a separate RPS electrical division. Each transmitter provides an analog output signal to the ~~RPS~~ RTIF RMU, which digitizes and conditions the signal before sending it to the appropriate DTM in one of the four RPS divisional sensor channels. The four separate level transmitters and associated instrument lines are components of the NBS.

Main Steamline Isolation Valve Closure: Each of the four Main Steam Lines (MSLs) can be isolated by closing either its inboard or outboard isolation valve. Position (limit) switches are mounted on both isolation valves of each MSL. These switches provide output to the appropriate DTM in one of the four RPS divisional trip channels using hard-wired connections. On each MSL, two position switches are mounted on each inboard isolation valve and each outboard isolation valve. Each of the two position switches on any one MSL isolation valve is associated with a different RPS divisional sensor channel. A reactor scram is initiated by either the inboard or outboard valve closure on two or more of the MSLs. The eight MSIVs and the 16 position switches supplied with these valves (for RPS use) are components of the NBS.

Feedwater Temperature Biased Simulated Thermal Power: FW temperature is measured by four separate temperature sensors mounted on each FW line in the MSL tunnel area within the RB. Each sensor is connected to a separate channel and is associated with a separate RPS electrical division. Each sensor provides a temperature signal to the ~~RPS~~ RTIF RMU, which digitizes and conditions the signal before sending it to the appropriate ~~RPS~~ RTIF DTM. The eight temperature sensors (four on each FW line) are components of the NBS. The RPS uses FW temperature from NBS to develop a STP high setpoint that is a function of FW temperature. ~~The RPS initiates a scram when the FW temperature further departs from the area allowed by the thermal power vs. FW temperature domain.~~

Simulated Thermal Power Biased Feedwater Temperature: The RPS uses the STP signal from NMS and feedwater temperature from NBS as described in the paragraph above to generate a high/low feedwater temperature setpoint that is a function of STP. The RPS initiates a scram when the FW temperature further departs from the area allowed by the thermal power vs. FW temperature domain.

Control Rod Drive System

Locally mounted pressure transmitters measure the CRDS accumulator charging header pressure at four physically separate locations. Each transmitter is associated with a separate RPS division and is on a separate instrument line. Each transmitter provides an analog output signal to the RMU, which digitizes and conditions the signal before sending it to the appropriate DTM (in one of the four RPS divisional trip channels). The four pressure transmitters and associated instrument lines are components of the CRDS. This is an anticipatory scram because it initiates a scram before the HCUs accumulators have time to depressurize ~~the reactor~~.

Reactor Protection System

two-out-of-three trip. Loss of communication with a bypass switch is interpreted as a "no bypass" signal.

This bypass permits any one of the safety-related RPS components of the input sensor channels of one division to be repaired, replaced, or maintained off-line.

- TLU output (division-out-of-service) bypass (alarmed maintenance bypass): A manually-operated bypass switch with interlock capability (for example, a joystick-type switch) is installed in the MCR to bypass the RPS trip output logic of one RPS electrical division at a time. This bypass is effective at the TLU trip input to the OLU and permits the ~~RPS~~ RTIF TLU of the associated division to be repaired, replaced, or maintained off-line. Loss of communication with the bypass switch is interpreted as a "no bypass" signal.

  The interlock ensures that the output signals of only one TLU (of one division) can be bypassed at any one time. Once a bypass of one division of trip logic has been established, bypasses of any of the remaining three division trip logics are inhibited. When a division-out-of-service bypass switch is placed in the bypass position, there is an alarm in the MCR indicating which division is out of service. With a division-out-of-service bypass in effect, the operator still is able manually to trip that division.

- The division-of-sensors maintenance bypass function and the division-out-of-service maintenance bypass function are independent. Thus, bypassing one division of sensors (taken out of service at the sensor channels level) and, simultaneously removing from service the same division or any other division at the RPS trip system level is allowed. In all cases, the RPS system remains able to trip the reactor if any two (or more) un-bypassed parameters exceed their trip values.

7.2.1.5.3 Requirements for Manual Controls

Operator action by means of manual controls is limited to:

- Initiation of scram by manual scram switches,
- Reactor Mode Switch operation (results in scram if placed in the Shutdown position),
- Reset of automatic trip systems after trip input signals clear,
- Reset of manual trip systems (preferably after reset of the automatic trip systems),
- Manual bypasses for conditions that are specifically permitted, and
- Manual initiation of selected trip systems or trip actuators using trip logic test switches.

7.2.1.5.4 Reactor Mode Switch

A multi-function, multi-bank, control switch placed on the MCR console provides mode selection for the necessary interlocks associated with the various plant modes: Shutdown, Refuel, Startup, and Run. This Reactor Mode Switch provides both electrical and physical separation

DCD Markups for
RAI 7.2-69

DTM in one of the four RPS divisional sensor channels. The four pressure transmitters and associated instrument lines are components of the NBS.

Reactor Pressure Vessel Water Level: RPV water level is measured by four physically separate level (differential pressure) transmitters mounted on separate divisional local racks in the safety envelope within the RB. Each transmitter is on a separate pair of instrument lines and is associated with a separate RPS electrical division. Each transmitter provides an analog output signal to the ~~RPS~~ RTIF RMU, which digitizes and conditions the signal before sending it to the appropriate DTM in one of the four RPS divisional sensor channels. The four separate level transmitters and associated instrument lines are components of the NBS.

Main Steamline Isolation Valve Closure: Each of the four Main Steam Lines (MSLs) can be isolated by closing either its inboard or outboard isolation valve. Position (limit) switches are mounted on both isolation valves of each MSL. These switches provide output to the appropriate DTM in one of the four RPS divisional trip channels using hard-wired connections. On each MSL, two position switches are mounted on each inboard isolation valve and each outboard isolation valve. Each of the two position switches on any one MSL isolation valve is associated with a different RPS divisional sensor channel. A reactor scram is initiated by either the inboard or outboard valve closure on two or more of the MSLs. The eight MSIVs and the 16 position switches supplied with these valves (for RPS use) are components of the NBS.

Feedwater Temperature Biased Simulated Thermal Power: FW temperature is measured by four separate temperature sensors mounted on each FW line in the MSL tunnel area within the RB. Each sensor is connected to a separate channel and is associated with a separate RPS electrical division. Each sensor provides a temperature signal to the ~~RPS~~ RTIF RMU, which digitizes and conditions the signal before sending it to the appropriate ~~RPS~~ RTIF DTM. The eight temperature sensors (four on each FW line) are components of the NBS. The RPS uses FW temperature from NBS to develop a STP high setpoint that is a function of FW temperature. ~~The RPS initiates a scram when the FW temperature further departs from the area allowed by the thermal power vs. FW temperature domain.~~

Simulated Thermal Power Biased Feedwater Temperature: The RPS uses the STP signal from NMS and feedwater temperature from NBS as described in the paragraph above to generate a high/low feedwater temperature setpoint that is a function of STP. The RPS initiates a scram when the FW temperature further departs from the area allowed by the thermal power vs. FW temperature domain.

Control Rod Drive System

Locally mounted pressure transmitters measure the CRDS accumulator charging header pressure at four physically separate locations. Each transmitter is associated with a separate RPS division and is on a separate instrument line. Each transmitter provides an analog output signal to the RMU, which digitizes and conditions the signal before sending it to the appropriate DTM (in one of the four RPS divisional trip channels). The four pressure transmitters and associated instrument lines are components of the CRDS. This is an anticipatory scram because it initiates a scram before the HCUs accumulators have time to depressurize ~~the reactor~~.

Reactor Protection System

DCD Markups for
RAI 7.7-9

Table 2.2.3-4

ITAAC For Feedwater Control System

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
	failure of each FWCS level controller.	conclude ~~document~~ that failure of any one FWCS level controller will not affect FWCS output.
	iii. Test(s) will be performed simulating discrepancy between field voter output and FTDC output of each FWCS level controller.	iii. Test report(s) exist and conclude that "Lock-up" signal will be sent to ASD following discrepancy between field voter output and FTDC output of each FWCS level controller.
	iv. Test(s) will be performed simulating discrepancy between field voter output and FTDC output of each FWCS temperature controller.	iv. Test report(s) exist and conclude that "Lock-Up" signal will be sent to the modulating steam admission valves of the seventh stage feedwater heater, and the modulating heater bypass valves following discrepancy between field voter output and FTDC output of each FWCS temperature controller.

DCD Markups for
RAI 7.7-10

7.7.3.4 Testing and Inspection Requirements

The FTDC self-test and on-line diagnostic test features are capable of identifying and isolating failures of process sensors, Input/Output (I/O) cards, power buses, power supplies, processors and inter-processor communication paths. These features identify the presence of a fault and determine the location of the failure down to the module level.

The FWCS components and critical components of interfacing systems are tested to ensure that specified performance requirements are satisfied. Preoperational testing of the FWCS is performed before fuel loading and startup testing to ensure that the system functions as designed and that stated system performance is within specified criteria.

7.7.3.5 Instrumentation and Control Requirements

7.7.3.5.1 Power Sources

Redundant UPS power the FWCS digital controllers and process measurement equipment. No single power source or single power supply failure results in the loss of FWCS functions.

7.7.3.5.2 Equipment

The FWCS consists of:

- The FTDC that contains the software and processors for execution of the control algorithms;
- FW flow rate signals that provide for the measurement of the total flow rate of FW into the RPV;
- Steam flow rate signals that provide for the measurement of the total flow rate of steam leaving the RPV;
- Feed water pump discharge flow rate signals that provide for the measurement of the discharge flow rate of each feed pump;
- The LFCV differential pressure transmitters that provide for the measurement of the pressure drop across the LFCV, for LFCV gain control; ~~and~~
- The LFCV flow transmitters that provide for the measurement of the flow rate through the LFCV, for both LFCV control and low thermal power calculations; and
- FW temperature signals that provide for the measurement of the FW temperature at the point prior to the FW penetration to the reactor building.

7.7.3.5.3 Reactor Vessel Water Level Measurement

Reactor vessel narrow-range water level is measured by at least three identical, independent sensing systems. For each level measurement channel, a differential pressure transmitter senses the difference between the pressure caused by a constant reference column of water and the pressure caused by the variable height of water in the RPV. The differential pressure