



**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, Supplement 1

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 7.1-114, 7.1-115, 7.1-117, 7.1-118, 7.1-119, 7.1-120, 7.3-15, and 7.3-16**

Enclosures 1 and 2 contain the GE Hitachi Nuclear Energy (GEH) response to RAI Numbers 7.1-114, 7.1-115, 7.1-117, 7.1-118, 7.1-119, 7.1-120, 7.3-15, and 7.3-16 from the U.S. Nuclear Regulatory Commission (NRC) Request for Additional Information (RAI) sent by NRC letter number 257, dated September 14, 2008 (Reference1).

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

Sincerely,

*Lee F. Dougherty for*

Richard E. Kingston  
Vice President, ESBWR Licensing

DOG  
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 7.1-114, 7.1-115, 7.1-117, 7.1-118, 7.1-119, 7.1-120, 7.3-15, and 7.3-16
2. Response to Portion of NRC Request for Additional Information Letter No. 257 Related to ESBWR Design Certification Application - DCD Markups for RAI Numbers 7.1-115 and 7.3-15

cc:

AE Cabbage	USNRC (with enclosures)
RE Brown	GEH/Wilmington (with enclosures)
DH Hinds	GEH/Wilmington (with enclosures)
eDRF Sections:	0000-0092-0138 (RAI 7.1-114)
	0000-0092-0823 (RAI 7.1-115)
	0000-0091-7619 (RAI 7.1-117)
	0000-0092-1688 (RAI 7.1-118)
	0000-0092-1700 (RAI 7.1-119)
	0000-0091-8006 (RAI 7.1-120)
	0000-0092-6259 (RAI 7.3-15)
	0000-0092-6936 (RAI 7.3-16)

**MFN 08-920, Supplement 1**

**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 7.1-114, 7.1-115, 7.1-117, 7.1-118, 7.1-119,  
7.1-120, 7.3-15, and 7.3-16**

### **NRC RAI 7.1-114**

*DCD Tier 2 Section 7.1.3.4, Q-DCIS Testing and Inspection Requirements, states that the Q-DCIS meets the self-diagnostics for digital computer based protection recommended by IEEE Std. 7-4.3.2 but does not address all characteristics. For example, but not limited to, IEEE Std. 7-4.3.2 states, "The reliability requirements of the safety system shall be used to establish the need for self-diagnostics." The concern is diagnostics can adversely affect the system to perform its safety function. In many cases the diagnostics software is more complex and extensive than the safety function software itself. The standard does not address, nor advocate, the addition of diagnostics solely for the use to support surveillance testing. This should be addressed.*

*While DCD Tier 2 Section 7.1.6.5 identifies that the Q-DCIS design conforms to BTP HICB-17, DCD Tier 2 Section 7.1.3.4 does not mention BTP HICB-17 or discuss its applicable criteria. Address in DCD Tier 2 Section 7.1.3.4 the applicable self-diagnostics criteria identified in IEEE Std. 7-4.3.2 and BTP HICB-17.*

### **GEH Response**

GEH agrees that subsection 7.1.3.4 does not completely address Q-DCIS compliance with BTP HICB-17 and the applicable self-diagnostics criteria identified in both BTP HICB-17 and IEEE Std. 7-4.3.2. However, compliance with the applicable criteria identified in BTP HICB-17 is discussed in Subsections 7.2.1.4, 7.2.2.3.5, and 7.3.5.3.5. Therefore, no revision to subsection 7.1.3.4 is required.

All of the applicable requirements (including applicable self-diagnostics criteria) from BTP HICB-17 and IEEE Std. 7-4.3.2 are captured as part of the requirements phase documentation and carried through the software development life cycle as discussed in the ESBWR software program manuals: ESBWR Software Quality Assurance Program Manual, NEDE-33545P, Revision 3, and Section 5.7, *Requirements Phase*, of the ESBWR Software Management Program Manual, NEDE-33226P, Revision 3.

IEEE Std. 7-4.3.2 requires, as part of the reliability assessment, the use of self-diagnostic features in computer-based systems with multiple input and output states because the combination of just the input and output states quickly overwhelms the capability to manually detect fault states. For example, over 500,000 tests would be required to individually test all combinations of 20 inputs and outputs. IEEE Std. 7-4.3.2 requires that self-diagnostic features not adversely affect the capability of the system to perform its safety-related function and not cause spurious actuations of the safety-related functions.

The self-diagnostics are part of the overall Q-DCIS application program for the Q-DCIS platforms that finds potential problems and notifies the operator to take action if required. The self-diagnostics are another "function" of the Q-DCIS hardware and

software. As such the self-diagnostics are equally subject to the controls applicable to the safety function logic (quality, management, lifecycle, etc.) described in the referenced ESBWR software plans. Self-diagnostics are not provided solely to support surveillance testing. The self-diagnostic features supplement the Generic Technical Specification (GTS) instrumentation surveillance requirements. The performance of the surveillance requirements required by the GTS are ultimately the responsibility of the operator and do not depend solely on the self-diagnostic features; however, the Human Factors Engineering (HFE) processes and future plant procedure development may elect to utilize the capability of the self-diagnostic features to report on channel performance as a tool to assist the operator in satisfying surveillance requirements required by the GTS.

### **DCD Impact**

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

**NRC RAI 7.1-115**

- a) *DCD Tier 2 Section 7.1.3.4 identifies NUMAC having "a" watchdog timer. Developed digital I&C platforms have watchdog timers, for example, in the Bus Controllers, CPUs, and I/O modules. Clarify the watchdog timers used in NUMAC.*
- b) *The NUMAC watchdog timer discussion identifies a "channel trip and alarm" while the instrument resets. This incorrectly suggests the channel is resetting by itself. (IEEE Std. 603-1991, Criterion 5.2)*

**GEH Response**

- a) GEH agrees to clarify the use of watchdog timers. The watchdog timers used in the NMS and RTIF equipment are not single entities/processors; there is one for each logic processor or logic function (RMU, SPTM, OLU, DTM, TLU, etc.) running the application code for that equipment. As part of the self-diagnostics, the application code for the equipment includes watchdog timer functions to ensure that each of the application functions is executed within its allotted time and to ensure that the entire application code sequence is always executed completely (that it has not become suspended or "hung up").
- b) GEH agrees to clarify the word "instrument" in the phrase "while the instrument is resetting." A single division resetting automatically is permissible by IEEE Std. 603, Criterion 5.2, provided that a reactor trip (SCRAM) initiation sequence has not started. This is explained in detail below; however, the following clarification text is beyond the scope of the ESBWR DCD.

The use of "affected instrument" in Subsection 7.1.3.4 refers to the affected logic processor or logic function. Automatically resetting a division is permissible in accordance with IEEE Std. 603, Criterion 5.2, because the protection system makes a reactor trip (SCRAM) decision based on two-out-of-four division logic. A single division indicating a trip resulting from a watchdog timer critical fault is not a protection system reactor trip (SCRAM) initiation signal by itself. IEEE Std. Criterion 5.2 is, therefore, not invoked and the individual logic processor or logic function within the division may be reset automatically (by itself). Resetting the individual NMS or RPS logic processor or logic function allows the application code to restart. If the watchdog timer continues to indicate a critical fault (including resulting from the logic function's/processor's application code not restarting), the affected safety-related division will produce a trip signal. Until the watchdog timer has completed resetting and the application code has successfully restarted, a division critical fault and associated division trip signal exist. Once the application code has successfully restarted, the fault is automatically cleared and the division trip signal no longer exists. If, during the reset period, there is a trip signal from another division, the protection system will initiate a reactor trip (SCRAM) and seal-in the trip signals. If

the logic function's/processor's application code is later successfully restarted, the operator must manually reset the sealed-in protection system reactor trip (SCRAM). If the watchdog timer is still indicating a critical fault (which may include the critical fault resulting from the logic function's/processor's application code not restarting) the division's trip cannot be reset.

**DCD Impact**

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

**NRC RAI 7.1-117**

*DCD Tier 2 Section 7.1.3.4 does not identify which diagnostics have equipment vs operator initiated capabilities. Please clarify.*

**GEH Response**

GEH does not concur with the necessity to clarify. The DCIS equipment is capable of automatically initiating all diagnostics described in DCD Tier 2, subsection 7.1.3.4. Describing the diagnostics as “self-diagnostics” and “continuous automatic online diagnostics” identifies this equipment capability. The DCIS is also capable of allowing the operator to initiate diagnostics. As with all operator tasks, the determination of which diagnostics should have operator initiated capability, will be determined by the HFE design process identified in DCD Tier 2, Chapter 18 and DCD Tier1, Section 3.3.

**DCD Impact**

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

### **NRC RAI 7.1-118**

*DCD Tier 2 Section 7.1.3.4 states the technical specifications monitor (TSM) uses a hardware / software platform different from NUMAC and TRICON. DCD Tier 2 Section 7.1.5.2.4 indicates that the TSM is part of the plant computer function (PCF). However, the TSM is not listed with the PCF on DCD Tier 2 Figure 7.1-4, ESBWR Hardware / Software (Architecture) Diversity Diagram. Identify and describe the TSM hardware and software in the DCD. Include the TSM in DCD Tier 2 Figure 7.1-4.*

*DCD Tier 2 Section 7.1.3.4, under the heading, "Channel Check," indicates that the self-diagnostic features of NUMAC / TRICON, in conjunction with the TSM, perform the technical specification surveillances. As the TSM is nonsafety related, clarify measures to ensure that the TSM performs the technical specification surveillances properly and to detect degradation in performance or failure of the TSM.*

### **GEH Response**

GEH concurs that the Technical Specifications Monitor (TSM) is part of the plant computer function (PCF) as described in DCD Tier 2, subsection 7.1.5.2.4.5. However, the TSM hardware and software requirements will not be described in the DCD because these will be determined as part of the HFE design process and detailed design of the TSM. DCD Tier 2, figure 7.1-4 is revised, per RAI 7.1-100, to remove all subsystems from this figure. The PCF subsystems will only be described in subsection 7.1.5.2.4.

In addition, DCD Tier 2, subsection 7.1.5.2.4 also identifies that the PCF is an integral part of the HFE process. The allocation of functions accommodates human capabilities and limitations, fault detection and recovery capabilities are provided, and an acceptable operator workload is not exceeded. The TSM applications and requirements will be specified, validated, verified and tested as part of the ESBWR HFE design process, the software management program manual (SMPM), NEDE-33226, and the software quality assurance program manual (SQAPM), NEDE-33245.

DCD Tier 2, subsection 7.1.3.3 provides additional information on communications between Q-DCIS and N-DCIS. All communications between the Q-DCIS and the N-DCIS are through safety-related communication interface modules via data links and fiber optic cable. A degradation of the TSM will not create a failure of a safety-related system.

As described in DCD Tier 2, subsection 7.1.3.4, the Q-DCIS has self-diagnostic capabilities that include automatic cyclic comparison of channel outputs and monitoring of unacceptable deviations. Similarly, DCD Tier 2, subsection 7.1.5.4 describes the self-diagnostics capabilities of the N-DCIS. The nonsafety-related TSM provides a log of the results, and provides operator notification (alarms) of out-of-limits conditions.

GEH Generic Technical Specifications (GTS) provides Surveillance Requirements for periodic performance of Channel Checks for specified instrumentation systems. The Channel Checks performed by the online self-diagnostic features described in DCD Tier 2, subsection 7.1.3.4 supplement the GTS-required Channel Checks with automatic cyclic checks. The performance of the Channel Checks required by the GTS are ultimately the responsibility of the operator and do not depend on the TSM; however, the HFE processes and future plant procedure development may elect to utilize the capability of the TSM to report on channel performance as a tool to assist the operator in satisfying the GTS-required Channel Checks.

### **DCD Impact**

DCD Tier 2, figure 7.1-4 will be revised in DCD Revision 6 to remove the PCF subsystems. The markup will be provided in a separate submittal in responses to RAI 7.1-100.

**NRC RAI 7.1-119**

*DCD Tier 2 Section 7.1.3.4 describes the periodic testing performed to support surveillance requirements of the Technical Specifications, including channel checks, functional tests, logic system functional tests or response times. However, DCD Tier 2 Section 7.1.3.4 does not identify the required durations and frequencies of the individual self-diagnostics. Also, this section does not identify the overall time it takes to complete the series of diagnostics or which diagnostics are necessary to complete a channel check, functional test, logic system functional test or response time test. Provide this information to support the values included in the technical specifications.*

**GEH Response**

GEH concurs that the DCD Tier 2 Section 7.1.3.4 describes that periodic testing is performed to support surveillance requirements of the Technical Specifications. The Channel Functional Test frequencies are currently specified in DCD Chapter 16 Technical Specifications.

GEH Generic Technical Specifications (GTS) provides Surveillance Requirements for periodic performance of Channel Checks for specified instrumentation systems. The Channel Checks performed by the online self-diagnostic features described in DCD Tier 2, subsection 7.1.3.4 supplement the GTS-required Channel Checks with automatic cyclic checks.

As described in DCD Tier 2, subsection 7.1.3.4, the Q-DCIS has self-diagnostic capabilities that include automatic cyclic comparison of channel outputs and monitoring of unacceptable deviations. The self-diagnostics will be specified to meet the requirements of the traditional, manual surveillance tests; these specifications will include the self-diagnostics intervals. It is anticipated that the self-diagnostic test intervals will match the cycle time of the application/logic. Any manual surveillance of the self-diagnostic features will be performed on an interval that does not exceed the surveillance intervals defined in Chapter 16 Technical Specifications.

NRC RAI 16.2-145, Supplement 1, requests that GEH revise the surveillance frequencies for instrumentation channel checks and channel functional tests to be consistent with the standard technical specifications. Channel check and channel functional test surveillance frequencies and justification for these surveillance frequencies will be addressed in response to RAI 16.2-145, Supplement 1. Therefore, information supporting the values included in the technical specifications is not provided in this response to RAI 7.1-119.

**DCD Impact**

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

**NRC RAI 7.1-120**

*IEEE Std. 7-4.3.2 identifies that when self-diagnostics are applied, periodic self-diagnostics while the computer system is operating shall be incorporated into the system design. DCD Tier 2 Section 7.1.3.4 does not identify if the capability exists to periodically test and calibrate the automatic test equipment within the cabinets. Please clarify.*

**GEH Response**

GEH agrees to supply the following clarification. There is no automatic test equipment that requires periodic calibration within the cabinets. The self-diagnostics features are designed into the various systems. Modern electronics are self-regulating with no internal adjustment capability. Clock time is verified as part of the board design and later using other microprocessors in the system. There is no further need to periodically check clock time because absolute clock time is not important to the operation of the system.

**DCD Impact**

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

**RAI 7.3-15**

*Discussion provided in Section 7.3 does not clearly define the boundaries of the ESF systems. In Rev. 5, the VBIF was added as Section 7.3.6; however, there is no leading / introductory discussion in Section 7.3 that establishes this function as a part of the ESF systems.*

**GEH Response**

GEH concurs with the request.

The introduction to DCD Tier 2, Revision 5, Section 7.3 notes that Figure 7.1-1 provides a simplified block diagram indicating "the relationships of the ESF systems with their safety-related peers...," including the Vacuum Breaker Isolation Function (VBIF). The VBIF logic is performed on an Independent Control Platform. DCD Tier 2 Figures 7.1-1 and 7.3-5 indicate the VBIF boundaries and interfaces; DCD Tier 2 Figure 7.1-2 will be revised by the GEH response to RAI 7.1-110 to provide additional interface information.

DCD Tier 2, Revision 5, Section 7.3.6 will be revised to indicate that the VBIF is an Independent Control Platform and to reference the DCD Tier 2 Figures 7.1-1 and 7.1-2 to indicate system interfaces.

**DCD Impact**

DCD Tier 2, Section 7.3.6 will be revised in DCD Revision 6 as shown in Enclosure 2.

DCD Tier 2, Figure 7.1-2, will be revised in DCD Revision 6 as described above. The markup will be provided in a separate submittal in responses to RAI 7.1-110.

### **RAI 7.3-16**

Section 7.3.6.1 does not provide the functional design bases for the VBIF. DCD Tier 2 Section 6.2.2.2.1 identifies that the DW and WW vacuum breaker must fully close after each demand to support the PCCS operation. If the vacuum breaker does not close, a backup isolation valve closes. However, no additional details are provided, and this function is not discussed in DCD Tier 2 Section 7.3.6. If the VBIF function is to assure passive containment cooling, then identify the relevant performance requirements, such as isolation initiating logic, isolation valve reset / open logic to allow for vacuum breaker functionality, response time, power supply requirements, etc. GEH should also provide the basis for selecting an independent digital I&C platform for this application, and need for hardwired manual controls for these VB isolation valves.

### **GEH Response**

GEH concurs with the request.

Details of the Vacuum Breaker Isolation Function (VBIF) and the associated logic are described in DCD Tier 2, Revision 5, Subsection 7.3.6.2. Additional details on the automatic and manual functions of the VBIF logic are provided in the GEH response to RAI 7.1-106 (MFN 08-742, Supplement 1).

DCD Tier 2, Revision 5, subsection 7.3.6.1, describes the Design Bases for the VBIF. This subsection notes the automatic and manual logic requirements, the use of divisional power supplies (which will meet N-2 requirements), and other requirements. A specific response time requirement is not noted since the applicable LOCA event sequences associated with the use of the VBIF develop slowly (many minutes).

The basis for selecting an independent digital I&C platform for this application is provided in the GEH response to RAI 7.1-105 (MFN 08-742, Supplement 1).

Manual controls for the VBIF are provided to allow the Operator to control the vacuum breaker isolation valve during post-DBA conditions. The use of hard-wired controls allows independence from other Q-DCIS platforms and associated potential common cause failures. Additional detail on the use of manual controls is provided in the GEH response to RAI 7.1-106 (MFN 08-742, Supplement 1).

### **DCD Impact**

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

**MFN 08-920, Supplement 1**

**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 7.1-115 and 7.3-15**

**DCD Markups for  
RAI 7.1-115**

diagnostic alarms can be viewed in the MCR while a single failure and most multiple failures exist. The Q-DCIS failures are alarmed in the MCR (IEEE Std. 603, Section 5.7 and 6.5).

The Q-DCIS components and cabinets have redundant power supplies that are supplied by redundant uninterruptible power feeds within each division. These power feeds support the Q-DCIS operation for 72 hours with neither diesel-generator nor offsite power available. The 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 NUMACRTIF-NMS and TRICONSSLC/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 NUMACRTIF-NMS and TRICONSSLC/ESF have self-diagnostic features that check the validity of input signals. An analog input outside expected limits creates an alarm.

The NUMACRTIF-NMS hardware has a watchdog timers for various logic processors and logic functions that monitors the execution of the software. If the software stops executing (suspending the self-diagnostics), the its watchdog timer resets the affected logic processor or

logic functioninstrument. This results in a channel trip and alarm while the logic processor or logic functioninstrument is resetting.

The ~~TRICONSSLC/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 ~~NUMACRTIF-NMS~~ and ~~TRICONSSLC/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 (~~TRICONSSLC/ESF platform~~),
- Inter-divisional communication between RPS and NMS logic processors or logic functionsinstruments (~~NUMACRTIF-NMS platform~~), and logic processors or logic functionsinstruments (~~NUMACRTIF-NMS platform~~), and
- Functionality of the output contact by momentarily reversing its state and confirming readiness to change state on demand (~~TRICONSSLC/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 ~~NUMACRTIF-NMS/ or TRICONSSLC/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 logic processor or logic functioninstrument self-diagnostics and the TSM support the performance of the response time test for the safety-related platforms ~~NUMAC/TRICON~~. Watchdog timers monitor logic processor or logic functioninstrument internal clocks and alarms for out-of-limit conditions and the completion of application code per logic processor or logic functioninstrument cycle. Since the clocks set the response time, there is no mechanism for the response time to change without alarm or trip. All

**DCD Markups for  
RAI 7.3-15**

The SSLC/ESF component design accommodates electrostatic discharge (ESD) withstand capability. Administrative controls ensure that the associated channel is bypassed prior to opening any system cabinet. Alternatively, administrative actions consistent with standard electronics ESD control practices are required prior to opening a cabinet. These practices implement manufacturer recommendations.

Logic and controls for SSLC/ESF are located on each divisional SSLC/ESF cabinet in the secure Q-DCIS equipment rooms in the CB, with controls and system operating status available on the operator interface section in the MCR. The SSLC/ESF controls are used infrequently. Such controls are available for operator action during plant operation or during accident or transient conditions, and are also used to support testing and maintenance. The SSLC/ESF cabinets are accessible for maintenance and testing. Access to the SSLC/ESF cabinets is administratively controlled. If required the affected division's sensors are bypassed such that they do not provide trip inputs to other divisions, and the division can be disconnected from its actuators so that its logic remains functional. After maintenance or other access the affected division's diagnostics, self-testing, and actuator/sensor monitoring confirm correct operation.

The minimum required SSLC/ESF displays provided in the MCR (per division) are:

- Division-of-sensors in bypass,
- SSLC/ESF controller inoperative (DTM or VLU), and
- Communication Interface Module (CIM) inoperative.

### 7.3.6 Containment System Wetwell-to-Drywell Vacuum Breaker Isolation Function

The Vacuum Breaker Isolation Function (VBIF) is an Independent Control Platform that, upon detection of excessive vacuum breaker (VB) leakage, ~~the VB isolation function~~ prevents the loss of long-term containment integrity. Figures 7.1-1, 7.1-2, and 7.3-5 indicate VBIF interfaces.

#### 7.3.6.1 System Design Bases

The wetwell-to-drywell VB isolation function has the following safety-related requirements (IEEE Std. 603, Sections 4.1, 4.2, 4.5, 5.1, 5.6, 5.8, 6.2, 7.2, and 7.3) and 10 CFR 50.2 Design Bases.

- Automatically isolates an excessively leaking VB using a VB isolation valve.
- The VB and VB isolation valve are qualified for a harsh environment inside the drywell.
- Manual opening and closing of a VB isolation valve is provided for in the design.
- No single control logic and instrumentation failure opens/closes more than one VB isolation valve.
- VB and VB isolation valve positions are displayed in the MCR.