Common Set of DCD Markups for RAIs 7.1-99, 7.1-100, 7.1-101, and 14.3-265 Supplement 1

Table 2.2.15-1

IEEE Std. 603 Criterion System Applicability Matrix (1)(2)

Software projects		RTIF-NMS Platform							SSLC/ESF Platform										ICP	
		RTIF						NMS											VBIF	ATWS/SLC
Table 2.2.15-2, Item No.	IEEE Std. 603 Criterion	RTIF (2.2.10)	RPS (2.2.7)	LD&IS MSIV (2.2.12) [Note (4)]	CMS-SPTM (2.15.7)	NBS (2.1.2)	CRD (2.2.2)	NMS (2.2.5)	SSLC/ESF (2.2.13)	LD&IS non-MSIV (2.2.12) [Note (3)]	PRMS (2.3.1)	CMS non-SPTM (2.15.7) [Note (4)]	NBS (2.1.2)/ADS (N/A)	GDCS (2.4.2)	ICS (2.4.1)	SLC (2.2.4)	CBVS (2.16.2.2, 2.16.2.3) [Note (5)]	CRD (2.2.2)	VB Isolation Function (2.15.1)	ATWS/SLC (2.2.14)
1	4.1	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
2	4.4	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
3	4.5	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
4	4.6	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
5	4.7	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
6	4.8	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
7	4.9	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
8	5.1	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
9	5.2 and 7.3	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
10	5.6 and 6.3	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
11	5.7 and 6.5	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
12	5.9	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
13	5.10	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
14	5.11	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
15	5.12	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
16	6.1 and 7.1	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R

Table 2.2.15-1

IEEE Std. 603 Criterion System Applicability Matrix (1)(2)

Software projects		RTIF-NMS Platform							SSLC/ESF Platform										ICP	
		RTIF						NMS											VBIF	ATWS/SLC
Table 2.2.15-2, Item No.	IEEE Std. 603 Criterion	RTIF (2.2.10)	RPS (2.2.7)	LD&IS MSIV (2.2.12) [Note (4)]	CMS-SPTM (2.15.7)	NBS (2.1.2)	CRD (2.2.2)	NMS (2.2.5)	SSLC/ESF (2.2.13)	LD&IS non-MSIV (2.2.12) [Note (3)]	PRMS (2.3.1)	CMS non-SPTM (2.15.7) [Note (4)]	NBS (2.1.2)/ADS (N/A)	GDCS (2.4.2)	ICS (2.4.1)	SLC (2.2.4)	CBVS (2.16.2.2, 2.16.2.3) [Note (5)]	CRD (2.2.2)	VB Isolation Function (2.15.1)	ATWS/SLC (2.2.14)
17	6.2 and 7.2	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
18	6.4	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
19	6.6 and 7.4	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
20	6.7, 7.5, and 8.3	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
21	6.8	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
22	8.1	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R
23	8.2	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	C	R	R

Notes:

(1) R means the IEEE Std. 603 criterion compliance report(s) for the indicated software project (i.e., RTIF, NMS, SSLC/ESF, VB Isolation Function, and ATWS/SLC) include(s) the associated parts of the functional systems marked with a C or string of Cs, if any, immediately to the right of the R. C means compliance with the IEEE Std. 603 criterion is documented by one or more reports written against the first software project marked with an R, to the left of the C(s). For example, the report(s) for the RTIF software project will demonstrate compliance to IEEE Std. 603 criterion 5.1 for RPS, LD&IS MSIV, CMS-SPTM, NBS, and CRD.

(2) IEEE Std. 603 criteria apply only to the safety-related portions of the functional systems that perform sense, command, or execute functions.

(3) LD&IS non-MSIV functions control the safety-related actuators (isolation valves and isolation dampers) in the following nonsafety-related systems: RWCU/SDC, FAPCS, EFDS, CIS, CWS, HPNSS, SAS, RBVS, CBVS, FBVS.

(4) CMS (non-SPTM) provides sensor inputs for both LD&IS MSIV and LD&IS non-MSIV functions.

(5) CBVS includes the safety-related CB isolation dampers (see Note 3), EFU and CRHAVS. SSLC/ESF platform executes the CRHS function logic for the safety-related CBVS subsystems, CRHAVS and EFU.

~~Table 2.2.15-1~~

~~ITAAC Applicability Matrix (2)~~

~~IEEE Std. 603 Criterion~~	~~NBS (2.1.2)~~	~~CRDS (2.2.2)~~	~~SLC System (2.2.4)~~	~~NMS (2.2.5)~~	~~RSS (2.2.6)~~	~~RPS (2.2.7)~~	~~LD&IS (2.2.12)~~	~~SSLC/ESF (2.2.13)~~	~~PRMS (2.3.1)~~	~~ICS (2.4.1)~~	~~GDCS (2.4.2)~~	~~CS* (2.15.1)~~	~~CMS (2.15.7)~~	~~SPTM (2.15.7)~~	~~RBHVS (2.16.2.1)~~	~~CBHVS (2.16.2.2)~~	~~EFU (2.16.2.3)~~
~~5.1~~	-	-	-	X	-	X	X	X	-	X	X	X	-	-	X	X	X
~~5.2 and 7.3~~	-	-	-	-	-	X	X	X	-	-	-	X	-	-	-	-	-
~~5.3~~	(3)	(3)	(3)	(3)	(3)	(3)	(3)	(3)	(3)	(3)	(3)	-	(3)	(3)	(3)	(3)	(3)
~~5.4~~	X	X	X	X	X	X	X	X	X	X	X	-	X	X	X	X	X
~~5.5~~	X	X	X	X	X	X	X	X	X	X	X	-	X	X	X	X	X
~~5.6 and 6.3~~	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
~~5.7 and 6.5~~	X	X	X	X	-	X	X	X	X	X	X	X	X	X	X	X	X
~~5.8~~	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
~~5.9~~	-	-	-	X	X	X	X	X	-	-	-	-	-	-	-	-	-
~~5.10~~	X	X	X	X	X	X	X	X	X	X	X	-	X	X	X	X	X
~~5.11~~	X	X	X	X	X	X	X	X	X	X	X	-	X	X	X	X	X
~~5.12~~	-	-	-	X	-	X	X	X	-	X	X	-	-	-	X	X	X
~~5.13~~	-	-	-	X	-	X	X	X	-	X	X	-	-	-	-	-	-
~~5.14~~	X	X	X	X	X	X	X	X	X	X	X	-	X	X	X	X	X
~~5.15~~	X	X	X	X	X	X	X	X	X	X	X	-	X	X	X	X	X
~~6.1 and 7.1~~	-	-	-	X	-	X	X	X	X	-	-	-	-	-	X	X	X
~~6.2 and 7.2~~	-	-	-	X	-	X	X	X	X	-	-	X	-	-	X	X	X
~~6.4~~	X	X	X	X	X	X	X	X	X	X	X	-	X	X	X	X	X
~~6.6 and 7.4~~	-	-	-	X	-	X	-	X	-	-	-	-	-	-	-	-	-
~~6.7, 7.5, and 8.3~~	-	-	-	X	-	X	-	X	-	-	-	-	-	-	X	X	X
~~6.8~~	X	-	X	X	-	X	X	X	X	-	-	-	X	X	-	-	-
~~8.1~~	X	X	X	X	X	X	X	X	X	X	X	-	X	X	X	X	X
~~8.2~~	-	X	-	-	-	-	X	-	-	X	X	-	-	-	X	X	X

~~(1) A dash means not applicable.~~
~~(2) Safety-related portions only.~~
~~(3) No ITAAC is required for this criterion. See the description of the 10 CFR 50, Appendix B, Quality Assurance Program that is applied to the design, fabrication, construction, and test of the safety-related structures, systems, and components provided as part of the preliminary safety evaluation report as required by 10 CFR 50.34(a)(7).~~
~~*CS=Containment System~~

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1a. The Criterion 4.1 design bases for the software projects include a list of design basis events, the applicable reactor modes of operation, the initial conditions requiring protective action, and the allowable limits of plant conditions for each such event.	Inspection of the software projects design phase summary BRR will be performed for the identification of the design basis events. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR include a list of design basis events, the applicable reactor modes of operation, the initial conditions requiring protective action, and the allowable limits of plant conditions for each such event. {{Design Acceptance Criteria}}
1b. The Criterion 4.1 design bases for the as-built software projects include a list of design basis events, the applicable reactor modes of operation, the initial conditions requiring protective action, and the allowable limits of plant conditions for each such event.	Inspection of the as-built software projects of the installation phase summary BRR will be performed for the identification of the design basis events.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR include a list of design basis events, the applicable reactor modes of operation, the initial conditions requiring protective action, and the allowable limits of plant conditions for each such event.

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
2a. Criterion 4.4, Identification of variables monitored: The software projects design bases list: • The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action • The analytical limit associated with each variable • The ranges (normal, abnormal, and accident conditions) associated with each variable • The rates of change of these variables to be accommodated until proper completion of the protective action is ensured	Inspection of the software projects design phase summary BRR will be performed for identification of variables. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR identify: • The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action • The analytical limit associated with each variable • The ranges (normal, abnormal, and accident conditions) associated with each variable • The rates of change of these variables to be accommodated until proper completion of the protective action is ensured {{Design Acceptance Criteria}}

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
2b. Criterion 4.4, Identification of variables monitored: The as-built software projects design bases reconcile any changes to the list of: • The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action • The analytical limit associated with each variable • The ranges (normal, abnormal, and accident conditions) associated with each variable • The rates of change of these variables to be accommodated until proper completion of the protective action is ensured	Inspection of the software projects installation phase summary BRR will be performed for identification of variables.	Report(s) exist and conclude that the software projects installation phase summary BRR identify and comply with changes, deletions, and additions to: • The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action • The analytical limit associated with each variable • The ranges (normal, abnormal, and accident conditions) associated with each variable • The rates of change of these variables to be accommodated until proper completion of the protective action is ensured

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
3a. Criterion 4.5, Minimum criteria for manual initiation and control of protective actions subsequent to initiation: The software projects design bases list: • The points in time and the plant conditions during which manual control is allowed. • The justification for permitting initiation or control subsequent to initiation solely by manual means. • The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations will be performed. • The variables that will be displayed for the operator to use in taking manual action.	Inspection of the software projects design phase summary BRR will be performed for identification of the minimum criteria for manual initiation and control. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR identify: • The points in time and the plant conditions during which manual control is allowed. • The justification for permitting initiation or control subsequent to initiation solely by manual means. • The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations will be performed. • The variables that will be displayed for the operator to use in taking manual action. {{Design Acceptance Criteria}}

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
3b. Criterion 4.5, Minimum criteria for manual initiation and control of protective actions subsequent to initiation: The as-built software projects design bases list: • The points in time and the plant conditions during which manual control is allowed. • The justification for permitting initiation or control subsequent to initiation solely by manual means. • The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations will be performed. • The variables that will be displayed for the operator to use in taking manual action.	Inspection of the as-built software projects installation phase summary BRR will be performed for identification of the minimum criteria for manual initiation and control.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR identify and comply with applicable changes, deletions, and additions to: • The points in time and the plant conditions during which manual control is allowed. • The justification for permitting initiation or control subsequent to initiation solely by manual means. • The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations will be performed. • The variables that will be displayed for the operator to use in taking manual action.

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
4a. Criterion 4.6, Identification of the minimum number and location of sensors: The software projects design bases list the minimum number and locations of sensors for those variables that are required to perform a safety-related function and have a spatial dependence (i.e., where the variable varies as a function of position in a particular region).	Inspection of the software projects design phase summary BRR will be performed for the identification of the minimum number of sensors and locations of sensors for those variables that have a spatial dependence. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR identify the minimum number and locations of sensors for those variables that are required to perform a safety-related function and have a spatial dependence (i.e., where the variable varies as a function of position in a particular region). {{Design Acceptance Criteria}}
4b. Criterion 4.6, Identification of the minimum number and location of sensors: The as-built software projects design bases reconcile any changes to the list of the minimum number and locations of sensors for those variables that are required to perform a safety-related function and have a spatial dependence (i.e., where the variable varies as a function of position in a particular region).	Inspection of the as-built software projects installation phase summary BRR will be performed for the identification of the minimum number of sensors and locations of sensors for those variables that have a spatial dependence.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR identify and comply with changes, deletions, and additions to the applicable minimum number and locations of sensors for those variables that are required to perform a safety-related function and have a spatial dependence (i.e., where the variable varies as a function of position in a particular region).

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
5a. Criterion 4.7, Range of transient and steady-state conditions: The software projects design bases list the range of transient and steady state conditions of motive and control power and the environment (e.g., voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety-related system is to perform.	Inspection of the software projects design phase summary BRR will be performed for the identification of the range of transient and steady-state conditions of motive and control power and the environment. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR identify the range of transient and steady state conditions of motive and control power and the environment (e.g., voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety-related system will perform. {{Design Acceptance Criteria}}
5b. Criterion 4.7, Range of transient and steady-state conditions: The as-built software projects design bases reconcile any changes to the list of the range of transient and steady state conditions of motive and control power and the environment (e.g., voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety-related system is to perform.	Inspection of the as-built software projects installation phase summary BRR will be performed for the identification of the range of transient and steady state conditions of motive and control power and the environment.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR identify and comply with changes, deletions, and additions to the applicable range of transient and steady state conditions of motive and control power and the environment (e.g., voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety-related system will perform.

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
6a. Criterion 4.8, Identification of conditions having the potential for causing functional degradation of safety-related system's performance: The software projects design bases list the conditions having the potential to cause functional degradation of safety-related system performance.	Inspection of the software projects design phase summary BRR will be performed for the conditions having the potential for causing functional degradation of the safety-related system's performance. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR identify the conditions having the potential to cause functional degradation of safety-related system's performance. {{Design Acceptance Criteria}}
6b. Criterion 4.8, Identification of conditions having the potential for causing functional degradation of safety-related system's performance: The as-built software projects design bases reconcile any changes to the list: of the conditions having the potential to cause functional degradation of safety-related system performance.	Inspection of the as-built software projects installation phase summary BRR will be performed for the conditions having the potential for causing functional degradation of the safety-related system's performance.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR confirm that tests accounted for the applicable conditions having the potential to cause functional degradation of safety-related system's performance.

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
7a. Criterion 4.9, Identification of the methods used to determine reliability of the safety system design: The software projects design bases list the methods and any qualitative and quantitative reliability goals used to assess the reliability of the safety-related system design.	Inspection of the software projects design phase summary BRR will be performed of the applicable qualitative and quantitative reliability goals. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR identify that appropriate methods and qualitative and quantitative reliability goals were used to assess the reliability of the safety-related system design. {{Design Acceptance Criteria}}
7b. Criterion 4.9, Identification of the methods used to determine reliability of the safety system design: The as-built software projects design bases reconcile any changes to the list of the methods and any qualitative and quantitative reliability goals used to assess the reliability of the safety-related system design.	Inspection of the as-built software projects installation phase summary BRR will be performed of the applicable qualitative and quantitative reliability goals.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR confirm that the applicable qualitative and quantitative reliability goals were met.

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
8a. Criterion 5.1, Single-failure criterion: The software projects design bases show compliance with the single-failure criterion.	Inspection of the software projects' design phase summary BRR show that a Failures Mode and Effects Analysis (FMEA) have been completed. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show that a FMEA has been completed and show the software projects' safety-related functions required for design basis events can be performed in the presence of: • Single detectable failures within safety-related systems concurrent with identifiable but non-detectable failures; • Failures caused by the single failure; and • Failures and spurious system actions that cause or are caused by the DBE requiring the safety-related functions. {{Design Acceptance Criteria}}
8b. Criterion 5.1, Single-failure criterion: The as-built software projects comply with the results of the FMEA.	Inspection of the as-built software projects' installation phase summary BRR will be performed to show that the as-built software projects comply with the results of the FMEA.	Report(s) exist and conclude that the as-built software projects' installation phase summary BRR show that the as-built software projects test results confirm the results of the FMEA.

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
9a1. Criteria 5.2 and 7.3, Completion of Protective Actions: The software projects are designed so that once initiated (automatically or manually), the intended sequences of safety-related functions of the execute features continue until completion.	Inspections of the software projects design phase summary BRR verify that the design show "seal-in" features that are provided to enable system-level safety-related functions to go to completion. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show "seal-in" features. {{Design Acceptance Criteria}}
9a2. Criteria 5.2 and 7.3, Completion of Protective Actions: The software projects are designed so that after completion, deliberate operator action is required to return the safety-related systems to normal.	Inspections of the software projects design phase summary BRR verifies that the design show "manual reset" features that are provided to require deliberate operation action to return the safety-related systems to normal. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show "manual reset" features. {{Design Acceptance Criteria}}
9b1. Criteria 5.2 and 7.3, Completion of Protective Actions: The as-built software projects ensure that once initiated (automatically or manually), the intended sequences of safety-related functions of the execute features continue until completion.	Inspections of the as-built software projects installation phase summary BRR will be performed to show that test show that once initiated (automatically and manually), the intended sequences of safety-related functions of the "execute features" continue until completion.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR show that once initiated (automatically and manually), the intended sequences of safety-related functions of the "execute features" continue until completion.

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
9b2. Criteria 5.2 and 7.3, Completion of Protective Actions: The as-built software projects ensure that after completion, deliberate operator action is required to return the safety-related systems to normal.	Inspection of the as-built software projects installation phase summary BRR will be performed to verify that tests of the "manual reset" features have been completed.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR show that "manual reset" features, after completion, return the safety-related systems to normal.
10a1. Criteria 5.6 and 6.3, Independence: The software projects have four independent, redundant divisions.	Inspection of the software projects design phase summary BRR will be performed to verify that the design of the software projects have four independent, redundant divisions. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show that the software projects have four independent, redundant divisions. {{Design Acceptance Criteria}}
10a2. Criteria 5.6 and 6.3, Independence: The software projects' interdivisional communication systems have optically isolated fiber optic communication pathways.	Inspection of the software projects design phase summary BRR will be performed to verify that the design of the software projects' interdivisional communication systems have optically isolated fiber optic communication pathways. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show that the software projects' interdivisional communication systems have optically isolated fiber optic communication pathways. {{Design Acceptance Criteria}}

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
10a3. Criteria 5.6 and 6.3, Independence: The software projects' safety-related functions are performed independently of the existence and function of any nonsafety-related component, data, and communication channel.	Inspection of the software projects design phase summary BRR will be performed to verify that the software projects' safety-related functions are performed independently of the existence and function of any nonsafety-related component, data, and communication channel. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show that the software projects' safety-related functions are performed independently of the existence and function of any nonsafety-related component, data, and communication channel. {{Design Acceptance Criteria}}
10b1. Criteria 5.6 and 6.3, Independence: The as-built software projects have four independent, redundant divisions.	Inspection of the as-built software projects installation phase summary BRR will be performed to confirm that tests have been performed to show that the software projects have four independent, redundant divisions.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR show that the as-built software projects have four independent, redundant divisions.
10b2. Criteria 5.6 and 6.3, Independence: The as-built software projects' interdivisional communication systems have optically isolated fiber optic communication pathways.	Inspection of the as-built software projects installation phase summary BRR will be performed to confirm that tests have been performed to show that the software projects' interdivisional communication systems have optically isolated fiber optic communication pathways.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR show that the as-built software projects' interdivisional communication systems have optically isolated fiber optic communication pathways.

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
10b3. Criteria 5.6 and 6.3, Independence: The as-built software projects' safety-related functions are performed independently of the existence and function of any nonsafety-related component, data, and communication channel.	Inspection of the as-built software projects installation phase summary BRR will be performed to confirm that tests have been performed to show that the as-built software projects' safety-related functions are performed independently of the existence and function of any nonsafety-related component, data, and communication channel.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR show that the as-built software projects' safety-related functions are performed independently of the existence and function of any nonsafety-related component, data, and communication channel.
11a. Criteria 5.7 and 6.5, Capability for Test and Calibration: The software projects have maintenance bypasses that allow test and calibration of one out of four divisions while retaining their capability to accomplish their safety-related functions.	Inspection of the software projects design phase summary BRR will be performed to verify that tests of the maintenance bypasses allows test and calibration of one out of four divisions while retaining their capability to accomplish their safety-related functions. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show that the maintenance bypasses allow test and calibration of one out of four divisions while retaining their capability to accomplish their safety-related functions. {{Design Acceptance Criteria}}
11b1. Criteria 5.7 and 6.5, Capability for Test & Calibration: The as-built software projects' maintenance bypasses show that the divisions not in bypass status will accomplish their safety-related functions.	Inspection of the as-built software projects installation phase summary BRR will be performed to confirm that tests have been performed to show that the design allows for tripping and bypass of individual functions in each safety-related system division.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR confirm that test reports show that individual functions in each safety-related system division can be tripped and bypassed.

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11b2. Criteria 5.7 and 6.5, Capability for Test & Calibration: The as-built software projects' maintenance bypasses show that when one division is placed into maintenance bypass mode, the condition is alarmed in the MCR and the division logic automatically becomes a two-out-of-three voting scheme.	Inspection of the as-built software projects installation phase summary BRR will be performed to confirm that tests have been performed to show that when one division is placed into maintenance bypass mode, the condition is alarmed in the MCR and the division logic automatically becomes a two-out-of-three voting scheme.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR confirm that test reports show that when one division is placed into maintenance bypass mode, the condition is alarmed in the MCR and the division logic automatically becomes a two-out-of-three voting scheme.
12a. Criterion 5.9, Control of Access: The software projects are housed within cabinets with keylock doors, has keylock switches, and utilizes passwords that permit administrative control of access to safety-related system equipment.	Inspection of the software projects design phase summary BRR will be performed to confirm that software projects are housed within cabinets with keylock doors, has keylock switches, and utilizes passwords that permit administrative control of access to safety-related system equipment. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show that the software projects are housed within cabinets with keylock doors, has keylock switches, and utilizes passwords that permit administrative control of access to safety-related system equipment. {{Design Acceptance Criteria}}

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
12b. Criterion 5.9, Control of Access: The as-built software projects are housed within cabinets with keylock doors, has keylock switches, and utilizes passwords that permit administrative control of access to safety-related system equipment.	Inspection of the as-built software projects installation phase summary BRR will be performed to confirm that tests show the operation of the keylock doors, keylock switches, and passwords.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR confirm the operation of the keylock doors, keylock switches, and passwords.
13a. Criterion 5.10, Repair, The software projects have self-diagnostic features that facilitate the timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.	Inspection of the software projects design phase summary BRR will be performed of the self-diagnostic features. {{Design Acceptance Criteria}}.	Report(s) exist and conclude that the software projects design phase summary BRR confirm that the software projects periodic self-diagnostic functions locate failure to the component level. {{Design Acceptance Criteria}}
13b. Criterion 5.10, Repair, The as-built software projects have self-diagnostic features that facilitate the timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.	Inspection of the as-built software projects installation phase summary BRR will be performed of the self-diagnostic features.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR confirm that test confirm that periodic self-diagnostic functions locate failure to the component level.
14a. Criterion 5.11, Identification: The redundant portions of the software projects are distinctly identified.	Inspection of the software projects design phase summary BRR will be performed to ensure that the software projects' divisions are distinctly identified. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR confirm that the software projects' divisions are distinctly identified. {{Design Acceptance Criteria}}

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
14b. Criterion 5.11, Identification: The redundant portions of the as-built software projects are distinctly identified.	Inspection of the as-built software projects installation phase summary BRR will be performed to confirm that the redundant portions of the as-installed software projects are distinctly identified.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR confirm that the redundant portions of the as-installed software projects are distinctly identified.
15a. Criterion 5.12, Auxiliary Features: Other auxiliary features cannot degrade the software projects' performance below an acceptable level.	Inspection of the software projects design phase summary BRR will be performed to confirm that the Criterion 5.1 FMEA verifies that the designs of other auxiliary features of the software projects do not have failure modes that can degrade the software projects' performance below an acceptable level. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show that the designs of other auxiliary features of the software projects do not have failure modes that can degrade the software projects' performance below an acceptable level. {{Design Acceptance Criteria}}
15b. Criterion 5.12, Auxiliary Features: Other auxiliary features cannot degrade the as-built software projects' performance below an acceptable level.	Inspection of the as-built software projects' installation phase summary BRR will be performed to show that the as-built software projects comply with the results of the FMEA.	Report(s) exist and conclude that the as-built software projects' installation phase summary BRR show that the as-built software projects test results confirm the results of the FMEA.
16a. Criteria 6.1 and 7.1, Automatic Control: The software projects provides the means to automatically initiate and control the required safety-related functions.	Inspection of the software projects' design phase summary BRR will be performed to verify that the design automatically initiates and controls the required safety-related functions. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show that the design has the capability to automatically initiate and control the required safety-related functions. {{Design Acceptance Criteria}}

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
16b. Criteria 6.1 and 7.1, Automatic Control: The as-built software projects provide the means to automatically initiate and control the required safety-related functions.	Inspection of the as-built software projects installation phase summary BRR will be performed to confirm that tests of the as-built software projects using simulated signals and actuators automatically initiates and controls the required safety-related functions.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR confirm that tests of the as-built software projects using simulated signals and actuators automatically initiates and controls the required safety-related functions.
17a. Criteria 6.2 and 7.2, Manual Control: The software projects have features in the main control room to manually initiate and control the automatically initiated safety-related functions at the division level.	Inspection of the software projects design phase summary BRR will be performed to verify that they show main control room features that are capable of manually initiating and controlling automatically initiated safety-related functions at the division level. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show main control room features that are capable of manually initiating and controlling automatically initiated safety-related functions at the division level. {{Design Acceptance Criteria}}
17b. Criteria 6.2 and 7.2, Manual Control: The as-built software projects have features in the main control room to manually initiate and control the automatically initiated safety-related functions at the division level.	Inspection of the as-built software projects installation phase summary BRR will be performed to confirm that tests were performed to demonstrate that the as-built software projects have main control room features that manually initiate and control automatically initiated safety-related functions at the division level.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR confirm that tests of the as-built software projects using simulated signals and actuators show that the main control room features manually initiate and control automatically initiated safety-related functions at the division level.

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
18a. Criterion 6.4, Derivation of System Inputs: Sense and command feature inputs for the software projects are derived from signals that are direct measures of the desired variables specified in the design bases.	Inspection of the software projects design phase summary BRR will be performed to ensure that the sense and command feature inputs for the software projects are derived from signals that are direct measures of the desired variables specified in the design bases. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show that the sense and command feature inputs for the software projects are derived from signals that are direct measures of the desired variables specified in the design bases. {{Design Acceptance Criteria}}
18b. Criterion 6.4, Derivation of System Inputs: Sense and command feature inputs for the as-built software projects are derived from signals that are direct measures of the desired variables specified in the design bases.	Inspection of the as-built software projects installation phase summary BRR will be performed to confirm that the sense and command feature inputs for the as-built software projects are derived from signals that are direct measures of the desired variables specified in the design bases.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR confirm that the sense and command feature inputs for the as-built software projects are derived from signals that are direct measures of the desired variables specified in the design bases.
19a1. Criteria 6.6 and 7.4, Operating Bypasses: The software projects automatically prevent the activation of an operating bypass, whenever the applicable permissive conditions for an operating bypass are not met.	Inspections of the software projects design phase summary BRR will be performed to verify that the systems are capable of automatically preventing the activation of an operating bypass, whenever the applicable permissive conditions for an operating bypass are not met. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR confirm that the systems are capable of automatically preventing the activation of an operating bypass, whenever the applicable permissive conditions for an operating bypass are not met. {{Design Acceptance Criteria}}

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
19a2. Criteria 6.6 and 7.4, Operating Bypasses: The software projects automatically removes activated operating bypasses, if the plant conditions change so that an activated operating bypass is no longer permissible.	Inspection of the software projects design phase summary BRR will be performed to verify that they show removal of activated operating bypasses, if the plant conditions change so that an activated operating bypass is no longer permissible. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR confirm that the systems are removing activated operating bypasses, if the plant conditions change so that an activated operating bypass is no longer permissible. {{Design Acceptance Criteria}}
19b1. Criteria 6.6 and 7.4, Operating Bypasses: The as-built software projects automatically prevent the activation of an operating bypass, whenever the applicable permissive conditions for an operating bypass are not met.	Inspection of the as-built software projects installation phase summary BRR will be performed to confirm test results demonstrate that the software projects automatically prevent the activation of an operating bypass, whenever the applicable permissive conditions for an operating bypass are not met.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR confirm that test results demonstrate that the software projects automatically prevent the activation of an operating bypass, whenever the applicable permissive conditions for an operating bypass are not met.
19b2. Criteria 6.6 and 7.4, Operating Bypasses: The as-built software projects show that they automatically removes activated operating bypasses, if the plant conditions change so that an activated operating bypass is no longer permissible.	Inspection of the as-built software projects installation phase summary BRR will be performed to confirm test results demonstrate that the as-built software projects automatically remove activated operating bypasses, if the plant conditions change so that an activated operating bypass is no longer permissible.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR confirm that test results demonstrate that the as-built software projects automatically remove activated operating bypasses, if the plant conditions change so that an activated operating bypass is no longer permissible.

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
20a. Criteria 6.7, 7.5, and 8.3 Maintenance Bypasses: The software projects are capable of performing their safety-related functions, when one division is in maintenance bypass.	Inspections of the software projects design phase summary BRR will be performed to verify that they are capable of performing their safety-related functions, when one division is in maintenance bypass. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show that they are capable of performing their safety-related functions, when one division is in maintenance bypass. {{Design Acceptance Criteria}}
20b1. Criteria 6.7, 7.5, and 8.3, Maintenance Bypasses: The as-built software projects ensure that they are capable of performing their safety-related functions, when one division is in maintenance bypass.	Inspection of the as-built software projects installation phase summary BRR will be performed to confirm that tests demonstrate that they perform their safety-related functions, when one division is in maintenance bypass.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR confirm that test results demonstrate that they perform their safety-related functions, when one division is in maintenance bypass.
20b2. Criteria 6.7, 7.5, and 8.3, Maintenance Bypasses: The as-built software projects ensure that they are capable of performing their safety-related functions, when one power supply division is in maintenance bypass.	Inspection of the as-built software projects installation phase summary BRR will be performed to confirm that tests demonstrate that they perform their safety-related functions, when one power supply division is in maintenance bypass.	Report(s) exist and conclude that the as-built software projects installation phase summary BRR confirm that test results demonstrate that they perform their safety-related functions, when one power supply division is in maintenance bypass.
21a. Criterion 6.8, Setpoint: The software projects', setpoints for safety-related functions are defined, determined and implemented based on a defined setpoint methodology.	Inspection of the software projects design phase summary BRR will be performed to verify that a defined setpoint methodology exists. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show that a defined setpoint methodology exists. {{Design Acceptance Criteria}}

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
21b. Criterion 6.8, Setpoint: Any changes to the setpoints have been reconciled for the as-built software projects.	Inspection of the installation phase summary BRR setpoint analyses for the as-built software projects will be performed to verify that the setpoints for safety-related functions are defined, determined and implemented based on a defined setpoint methodology.	Report(s) exist and conclude that the installation phase summary BRR setpoints for safety-related functions for the as-built software projects were defined, determined and implemented using a defined setpoint methodology.
22a. Criterion 8.1, Power source requirements: The software projects' electrical components receive power from their respective, divisional, safety-related power supplies.	Inspection of the software projects design phase summary BRR will be performed to ensure that the software projects' electrical components receive power from their respective, divisional, safety-related power supplies. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR reference design documents that show that the software projects' electrical components receive power from their respective, divisional, safety-related power supplies. {{Design Acceptance Criteria}}
22b. Criterion 8.1, Power source requirements: The as-built software projects' as-built electrical components receive power from their respective, divisional, safety-related power supplies.	Inspection of the as-built software projects' installation phase summary BRR will be performed to confirm that tests have been performed on the as-built software projects' as-built electrical components by providing test signals in only one safety-related division at a time.	Report(s) exist and conclude that the as-built software projects' installation phase summary BRR confirm that the as-built software projects' as-built electrical components received test signals from a safety-related source in the same division.

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
23a. Criterion 8.2, Non-electrical Power Sources: The software projects' actuators receive non-electric power from safety-related sources.	Inspection of the software projects design phase summary BRR will be performed to ensure that safety-related systems and components that require non-electric power receive it from safety-related sources. {{Design Acceptance Criteria}}	Report(s) exist and conclude that the software projects design phase summary BRR show that safety-related systems and components that require non-electric power receive it from safety-related sources. {{Design Acceptance Criteria}}
23b. Criterion 8.2, Non-electrical Power Sources: The as-built software projects' actuators receive non-electric power from safety-related sources.	Inspection of the as-built software projects' installation phase summary BRR will be performed to confirm that tests have been performed on the as-built software projects' as-built mechanical installation of the as-built software projects' actuators to show that non-electric power is received from safety-related sources.	Report(s) exist and conclude that the as-built software projects' installation phase summary BRR confirm that the as-built software projects' actuators receive non-electric power from safety-related sources.

~~**Table 2.2.15-2**~~

~~**ITAAC For IEEE Std. 603 Compliance Confirmation**~~

~~**Design Commitment**~~	~~**Inspections, Tests, Analyses**~~	~~**Acceptance Criteria**~~
~~1. Criterion 5.1, Single Failure:~~ ~~The Criterion 5.1 systems listed in Table 2.2.15-1 are designed to ensure that safety-related functions required for design basis events (DBE) are performed in the presence of: (a) single detectable failures within safety-related systems concurrent with identifiable but non-detectable failures; (b) failures caused by the single failure; and (c) failures and spurious system actions that cause or are caused by the DBE requiring the safety-related functions, as identified in the applicable FMEA.~~	~~Block level FMEA of the Criterion 5.1 systems listed in Table 2.2.15-1 show that they perform safety-related functions required for design basis events in the presence of: (a) single detectable failures within safety-related systems concurrent with identifiable but non-detectable failures; (b) failures caused by the single failure; and (c) failures and spurious system actions that cause or are caused by the DBE requiring the safety-related functions, as identified in the applicable FMEA. {{Design Acceptance Criteria}}~~	~~Analysis report(s) conclude(s) that the systems identified in Table 2.2.15-1 for Criterion 5.1 ensure(s) that safety-related functions required for design basis events are performed in the presence of: (a) single detectable failures within safety-related systems concurrent with identifiable but non-detectable failures; (b) failures caused by the single failure; and (c) failures and spurious system actions that cause or are caused by the DBE requiring the safety-related functions, as identified in the applicable FMEA. {{Design Acceptance Criteria}}~~
~~2. Criteria 5.2 and 7.3, Completion of Protective Actions:~~ ~~The Criteria 5.2 and 7.3 systems listed in Table 2.2.15-1 are designed so that, (a) once initiated (automatically or manually), the intended sequences of safety-related functions of the execute features continue until completion, and (b) after completion, deliberate operator action is required to return the safety-related systems to normal.~~	~~a. Inspection of the current revision of the simplified logic diagrams (SLDs) for the Criteria 5.2 and 7.3 systems listed in Table 2.2.15-1 verifies that the design shows (a) "seal-in" features that are provided to enable system-level safety-related functions to go to completion, and (b) "manual reset" features that are provided to require deliberate operation action to return the safety-related systems to normal. {{Design Acceptance Criteria}}~~	~~a. Inspection report(s) conclude(s) that the current revision of the SLDs show (a) "seal-in" features, and (b) "manual reset" features. {{Design Acceptance Criteria}}~~

~~Table 2.2.15-2~~

~~ITAAC For IEEE Std. 603 Compliance Confirmation~~

~~Design Commitment~~	~~Inspections, Tests, Analyses~~	~~Acceptance Criteria~~
	~~b. Test(s) for the Criteria 5.2 and 7.3 systems listed in Table 2.2.15-1 will be performed to show that (a) once initiated (automatically or manually), the intended sequences of safety-related functions of the "execute features" continue until completion, and (b) after completion, deliberate operator action is required to return the safety-related systems to normal.~~	~~b. Test report(s) conclude(s) that for the Criteria 5.2 and 7.3 systems listed in Table 2.2.15-1, (a) once initiated (automatically and manually), the intended sequences of safety-related functions of the "execute features" continue until completion, and (b) after completion, deliberate operator action is required to return the safety-related systems to normal.~~
~~3. Criterion 5.4, Equipment Qualification: The listed systems in Table 2.2.15-1 are qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that the safety-related system will be capable of meeting, the performance requirements specified in the design basis through the equipment qualification process described in Section 3.8.~~	~~See Section 3.8~~	~~See Section 3.8~~

~~**Table 2.2.15-2**~~

~~**ITAAC For IEEE Std. 603 Compliance Confirmation**~~

~~**Design Commitment**~~	~~**Inspections, Tests, Analyses**~~	~~**Acceptance Criteria**~~
~~4. Criterion 5.5, System Integrity: The listed system's performance in Table 2.2.15-1 is adequate to ensure completion of protective actions over the range of transient and steady-state conditions of both the energy supply and the environment enumerated in the design basis through the equipment qualification process described in Section 3.8.~~	~~See Section 3.8~~	~~See Section 3.8~~

~~**Table 2.2.15-2**~~

~~**ITAAC For IEEE Std. 603 Compliance Confirmation**~~

~~Design Commitment~~	~~Inspections, Tests, Analyses~~	~~Acceptance Criteria~~
~~5. Criteria 5.6 and 6.3, Independence:~~ ~~For the Criteria 5.6 and 6.3 systems listed in Table 2.2.15-1, there is physical, electrical, and communications independence between redundant portions of a safety-related system, between safety-related systems and the effects of a DBE, and between safety-related systems and nonsafety-related systems, as identified in the applicable FMEA.~~	~~a. Block level FMEA will be performed to verify that the designs of the Criteria 5.6 and 6.3 systems listed in Table 2.2.15-1 have physical, electrical, and communications independence between redundant portions of a safety-related system, between safety-related systems and the effects of a DBE, and between safety-related systems and nonsafety-related equipment, as identified in the applicable FMEA. {{Design Acceptance Criteria}}~~ ~~b. Inspection(s) will be performed to demonstrate that the Criteria 5.6 and 6.3 systems listed in Table 2.2.15-1 have physical independence between redundant portions of a safety-related system, between safety-related systems and the effects of a DBE, and between safety-related systems and nonsafety-related equipment, as identified in the applicable FMEA. .~~	~~a. Analysis report(s) conclude(s) that the designs of the Criteria 5.6 and 6.3 listed in Table 2.2.15-1 have physical, electrical, and communications independence between redundant portions of a safety-related system, between safety-related systems and the effects of a DBE, and between safety-related systems and nonsafety-related equipment, as identified in the applicable FMEA. {{Design Acceptance Criteria}}~~ ~~b. Inspection report(s) conclude(s) that the Criteria 5.6 and 6.3 systems listed in Table 2.2.15-1 have physical independence between redundant portions of a safety-related system, between safety-related systems and the effects of a DBE, and between safety-related systems and nonsafety-related equipment, as identified in the applicable FMEA.~~

~~**Table 2.2.15-2**~~

~~**ITAAC For IEEE Std. 603 Compliance Confirmation**~~

~~Design Commitment~~	~~Inspections, Tests, Analyses~~	~~Acceptance Criteria~~
	~~c. Type test(s), test(s), and / or analysis(es) will be performed to demonstrate that the Criteria 5.6 and 6.3 systems communication interface modules listed in Table 2.2.15-1 have electrical and communications independence between redundant portions of a safety-related system, between safety-related systems and the effects of a DBE, and between safety-related systems and nonsafety-related equipment.~~	~~c. Type test(s), test(s), and / or analysis(es) report(s) conclude(s) that the Criteria 5.6 and 6.3 systems communication interface modules listed in Table 2.2.15-1 have electrical and communications independence between redundant portions of a safety-related system, between safety-related systems and the effects of a DBE, and between safety-related systems and nonsafety-related equipment.~~

~~Table 2.2.15-2~~

~~ITAAC For IEEE Std. 603 Compliance Confirmation~~

~~Design Commitment~~	~~Inspections, Tests, Analyses~~	~~Acceptance Criteria~~
~~6. Criteria 5.7 and 6.5, Capability for Test and Calibration:~~ ~~The Criteria 5.7 and 6.5 systems listed in Table 2.2.15-1 have the capability to have their equipment tested and calibrated while retaining their capability to accomplish their safety-related functions.~~	~~a. Inspection(s) of the current revision of the SLDs of the Criteria 5.7 and 6.5 systems listed in Table 2.2.15-1 will be performed to verify that both the automatic and manual circuitry have the capability to have the safety-related systems' equipment tested and calibrated while retaining the safety-related systems' capability to accomplish their safety-related functions. {{Design Acceptance Criteria}}~~	~~Inspection report(s) conclude(s) that the current revision of the SLDs of the Criteria 5.7 and 6.5 systems listed in Table 2.2.15-1 have the capability to have the safety-related systems' equipment tested and calibrated while retaining the safety-related systems' capability to accomplish their safety-related functions. {{Design Acceptance Criteria}}~~
	~~b. Test(s) of Criteria 5.7 and 6.5 systems listed in Table 2.2.15-1 will be performed to demonstrate that the design allows for tripping or bypass of individual functions in each safety-related system channel.~~	~~Test report(s) conclude(s) that for the Criteria 5.7 and 6.5 systems listed in Table 2.2.15-1 individual functions in each safety-related system channel can be tripped or bypassed.~~
	~~c. Test(s) of Criteria 5.7 and 6.5 systems listed in Table 2.2.15-1, will be performed to demonstrate that the digital computer-based I&C systems' self-test features confirm computer system operation on system initiation.~~	~~Test report(s) conclude(s) that for the Criteria 5.7 and 6.5 systems listed in Table 2.2.15-1, the digital computer-based I&C systems' self-test features confirm computer system operation on system initiation.~~

~~Table 2.2.15-2~~

~~ITAAC For IEEE Std. 603 Compliance Confirmation~~

~~Design Commitment~~	~~Inspections, Tests, Analyses~~	~~Acceptance Criteria~~
~~7. Criterion 5.8, Information Displays:~~ ~~Information display systems listed in Table 2.2.15-1 are designed to be accessible to the operators, display variables for manually controlled actions, display system status information, provide indication of bypasses, and display post-accident monitoring variables in accordance with the HFE process described in Section 3.3 and the post-accident monitoring design process described in Section 3.7.~~	~~See Sections 3.3 and 3.7~~	~~See Section 3.3 and 3.7~~
~~8. Criterion 5.9, Control of Access:~~ ~~The design of the Criterion 5.9 systems listed in Table 2.2.15-1 have features that permit administrative control of access to safety-related system equipment.~~	~~Inspection of system design specification(s) for the Criterion 5.9 systems listed in Table 2.2.15-1 will be performed to confirm that access control features are specified for safety-related systems equipment. {{Design Acceptance Criteria}}~~	~~Inspection report(s) conclude(s) that within the system design specification(s) of the Criterion 5.9 systems listed in Table 2.2.15-1, access control features are specified for safety-related systems equipment. {{Design Acceptance Criteria}}~~

~~**Table 2.2.15-2**~~

~~**ITAAC For IEEE Std. 603 Compliance Confirmation**~~

~~Design Commitment~~	~~Inspections, Tests, Analyses~~	~~Acceptance Criteria~~
~~9. Criterion 5.10, Repair:~~ ~~Safety-related systems listed in Table 2.2.15-1 are designed to facilitate the timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.~~	~~Inspection of system design specification(s) for the Criterion 5.10 systems listed in Table 2.2.15-1 will be performed to confirm that safety-related systems are designed to facilitate the timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.~~	~~Inspection report(s) conclude(s) that the system design specification(s) of the Criterion 5.10 systems listed in Table 2.2.15-1 are designed to facilitate the timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.~~
~~10. Criterion 5.11, Identification:~~ ~~The listed safety-related systems in Table 2.2.15-1 are distinctly identified for each redundant portion.~~	~~a. Inspection(s) will be performed of the "current revision" of the project design manual. {{Design Acceptance Criteria}}~~ ~~b. Inspection(s) will be performed of the as-installed safety-related systems identification system.~~	~~a. Inspection report(s) conclude(s) that the "current revision of the project design manual describes a method that distinctly identifies each redundant portion of the listed safety-related systems in Table 2.2.15-1 and that does not rely on separate reference material. {{Design Acceptance Criteria}}~~ ~~b. Inspection report(s) conclude that the redundant portions of the as-installed safety-related systems listed in Table 2.2.15-1 are identified.~~

~~**Table 2.2.15-2**~~

~~**ITAAC For IEEE Std. 603 Compliance Confirmation**~~

~~**Design Commitment**~~	~~**Inspections, Tests, Analyses**~~	~~**Acceptance Criteria**~~
~~11. Criterion 5.12, Auxiliary Features:~~ ~~Other auxiliary features cannot degrade the safety-related systems listed in Table 2.2.15-1, below an acceptable level.~~	~~Block level FMEA will be performed to verify that the designs of other auxiliary features of the Criterion 5.12 systems listed in Table 2.2.15-1 do not have failure modes that can degrade the safety-related systems below an acceptable level. {{Design Acceptance Criteria}}~~	~~Analysis report(s) conclude that the designs of other auxiliary features of the Criterion 5.12 systems listed in Table 2.2.15-1 do not have failure modes that can degrade the safety-related systems below an acceptable level. {{Design Acceptance Criteria}}~~

~~**Table 2.2.15-2**~~

~~**ITAAC For IEEE Std. 603 Compliance Confirmation**~~

~~**Design Commitment**~~	~~**Inspections, Tests, Analyses**~~	~~**Acceptance Criteria**~~
~~12.Criterion 5.13, Multi-Unit Stations:~~ ~~The operation or failure of structures, systems, and components shared between units at a multi-unit generating station do not affect the performance of the safety-related functions of the systems listed in Table 2.2.15-1.~~	~~Analysis(es) will be performed of the safety-related systems plant-specific interfaces with shared structures, systems, and components at a multi-unit generating station using the following nonconcurrent criteria for single-failure analysis for shared systems:~~ ~~The safety-related systems of all units shall be capable of performing their required safety-related functions with a single failure assumed within the shared systems or within the auxiliary supporting features or other systems with which the shared systems interface.~~ ~~b. The safety-related systems of each unit shall be capable of performing their required safety-related functions, with a single failure initiated concurrently in each unit within the systems that are not shared.~~	~~Analysis report(s) conclude that the operation or failure of shared structures, systems, and components at a multi-unit generating station do not affect the performance of the safety-related functions of the systems listed in Table 2.2.15-1.~~

~~Table 2.2.15-2~~

~~ITAAC For IEEE Std. 603 Compliance Confirmation~~

~~Design Commitment~~	~~Inspections, Tests, Analyses~~	~~Acceptance Criteria~~
~~13.Criterion 5.14, Human Factors Considerations:~~ ~~Human factors are incorporated in the design in accordance with the HFE design process described in Section 3.3.~~	~~See Section 3.3.~~	~~See Section 3.3.~~
~~14. Criterion 5.15, Reliability:~~ ~~Analysis of the adequacy of the reliability of the safety-related system(s) design listed in Table 2.2.15-1 is performed as part of the design reliability assurance program described in Section 3.6.~~	~~See Section 3.6.~~	~~See Section 3.6.~~
~~15. Criteria 6.1 and 7.1, Automatic Control:~~ ~~The Criteria 6.1 and 7.1 systems listed in Table 2.2.15-1 provide the means to automatically initiate and control the required safety-related functions.~~	~~Inspection(s) will be performed of the current revision of the SLDs for the Criteria 6.1 and 7.1 systems listed in Table 2.2.15-1 to verify that the design automatically initiates and controls the required safety-related functions. {{Design Acceptance Criteria}}~~ ~~b. Test(s) will be performed to demonstrate that the Criteria 6.1 and 7.1 systems listed in Table 2.2.15-1 automatically initiate and control the required safety-related functions.~~	~~Inspection report(s) conclude(s) that the current revision of the SLDs for the Criteria 6.1 and 7.1 systems listed in Table 2.2.15-1 show(s) that the design automatically initiates and controls the required safety-related functions. {{Design Acceptance Criteria}}~~ ~~b. Test report(s) conclude(s) that the Criteria 6.1 and 7.1 systems listed in Table 2.2.15-1 automatically initiate and control the required safety-related functions.~~

~~Table 2.2.15-2~~

~~ITAAC For IEEE Std. 603 Compliance Confirmation~~

~~Design Commitment~~	~~Inspections, Tests, Analyses~~	~~Acceptance Criteria~~
~~16. Criteria 6.2 and 7.2, Manual Control:~~ ~~The Criteria 6.2 and 7.2 systems listed in Table 2.2.15-1 have features in the main control room to manually initiate and control the automatically initiated safety-related functions at the division level.~~	~~a. Inspection(s) will be performed of the SLDs for the Criteria 6.2 and 7.2 systems listed in Table 2.2.15-1 to verify that they have main control room features that are capable of manually initiating and controlling automatically initiated safety-related functions at the division level. {{Design Acceptance Criteria}}~~ ~~b. Test(s) will be performed to demonstrate that the Criteria 6.2 and 7.2 systems listed in Table 2.2.15-1 have main control room features that manually initiate and control automatically initiated safety-related functions at the division level.~~	~~a. Inspection report(s) conclude(s) that the SLDs for the Criteria 6.2 and 7.2 systems listed in Table 2.2.15-1 have main control room features that are capable of manually initiating and controlling automatically initiated safety-related functions at the division level. {{Design Acceptance Criteria}}~~ ~~b. Test report(s) conclude(s) that the Criteria 6.2 and 7.2 systems listed in Table 2.2.15-1 have main control room features that manually initiate and control automatically initiated safety-related functions at the division level exist(s).~~
~~17. Criterion 6.4, Derivation of System Inputs:~~ ~~Sense and command feature inputs for the listed systems in Table 2.2.15-1 are derived from signals that are direct measures of the desired variables specified in the design bases.~~	~~Inspection(s) will be performed of the safety analyses and SLDs. {{Design Acceptance Criteria}}~~	~~Inspection report(s) conclude(s) that the sense and command feature inputs for the listed systems are derived from signals that are direct measures of the desired variables specified in the design bases. {{Design Acceptance Criteria}}~~

~~**Table 2.2.15-2**~~

~~**ITAAC For IEEE Std. 603 Compliance Confirmation**~~

~~Design Commitment~~	~~Inspections, Tests, Analyses~~	~~Acceptance Criteria~~
~~18. Criteria 6.6 and 7.4, Operating Bypasses:~~ ~~The Criteria 6.6 and 7.4 systems listed in Table 2.2.15-1 automatically (1) prevent the activation of an operating bypass, whenever the applicable permissive conditions for an operating bypass are not met, and (2) remove activated operating bypass(es), if the plant conditions change so that an activated operating bypass is no longer permissible.~~	~~a. Inspections(s) will be performed of the current revision of the SLDs for the Criteria 6.6 and 7.4 systems listed in Table 2.2.15-1 to verify that the systems are capable of automatically (1) preventing the activation of an operating bypass, whenever the applicable permissive conditions for an operating bypass are not met, and (2) removing activated operating bypasses, if the plant conditions change so that an activated operating bypass is no longer permissible. {{Design Acceptance Criteria}}~~ ~~b. Test(s) will be performed to demonstrate that the Criteria 6.6 and 7.4 systems listed in Table 2.2.15-1 automatically (1) prevent the activation of an operating bypass, whenever the applicable permissive conditions for an operating bypass are not met, and (2) remove activated operating bypass(es), if the plant conditions change so that an activated operating bypass is no longer permissible.~~	~~a. Inspection report(s) conclude that the current revision of the SLDs for the Criteria 6.6 and 7.4 systems listed in Table 2.2.15-1 show that the systems are capable of automatically (1) preventing the activation of an operating bypass, whenever the applicable permissive conditions for an operating bypass are not met, and (2) removing activated operating bypasses, if the plant conditions change so that an activated operating bypass is no longer permissible. {{Design Acceptance Criteria}}~~ ~~b. Test report(s) conclude(s) that the Criteria 6.6 and 7.4 systems listed in Table 2.2.15-1 automatically (1) prevent the activation of an operating bypass, whenever the applicable permissive conditions for an operating bypass are not met, and (2) remove activated operating bypass(es), if the plant conditions change so that an activated operating bypass is no longer permissible.~~

~~**Table 2.2.15-2**~~

~~**ITAAC For IEEE Std. 603 Compliance Confirmation**~~

~~Design Commitment~~	~~Inspections, Tests, Analyses~~	~~Acceptance Criteria~~
~~19. Criteria 6.7, 7.5, and 8.3 Maintenance Bypasses:~~ ~~The Criteria 6.7, 7.5, and 8.3 systems listed in Table 2.2.15-1 are capable of performing their safety-related functions, when one division is in maintenance bypass.~~	~~Inspections(s) will be performed of the current revision of the SLDs for the Criteria 6.7, 7.5 and 8.3 systems listed in Table 2.2.15-1 to verify that the safety-related systems are capable of performing their safety-related functions, when one division is in maintenance bypass. {{Design Acceptance Criteria}}~~ ~~Test(s) will be performed to demonstrate that the Criteria 6.7, 7.5 and 8.3 systems listed in Table 2.2.15-1 perform their safety-related functions, when one division is in maintenance bypass.~~ ~~c. Test(s) will be performed to demonstrate that the Criteria 6.7, 7.5, and 8.3 systems listed in Table 2.2.15-1 perform their safety-related functions, when one power supply division is in maintenance bypass. Criterion 5.15, Reliability:~~	~~a. Inspection report(s) conclude(s) that the current revision of the SLDs for the Criteria 6.7, 7.5, and 8.3 systems listed in Table 2.2.15-1 show that the safety-related systems are capable of performing their safety-related functions, when one division is in maintenance bypass. {{Design Acceptance Criteria}}~~ ~~b. Test report(s) conclude(s) that the Criteria 6.7, 7.5, and 8.3 systems listed in Table 2.2.15-1 perform their safety-related functions, when one division is in maintenance bypass.~~ ~~c. Test report(s) conclude(s) that the Criteria 6.7, 7.5, and 8.3 systems listed in Table 2.2.15-1 perform their safety-related functions, when one power supply division is in maintenance bypass.~~

~~Table 2.2.15-2~~

~~ITAAC For IEEE Std. 603 Compliance Confirmation~~

~~Design Commitment~~	~~Inspections, Tests, Analyses~~	~~Acceptance Criteria~~
~~20.Criterion 6.8, Setpoint:~~ ~~For the Criterion 6.8 systems listed in Table 2.2.15-1, setpoints for safety-related functions are defined, determined and implemented based on a defined setpoint methodology.~~	~~Inspection(s), test(s), and/or analysis(es) for the Criterion 6.8 systems listed in Table 2.2.15-1 will be performed to verify that the setpoints for safety-related functions are defined, determined and implemented based on a defined setpoint methodology.~~	~~Inspection(s), test(s), or analysis(es) report(s) for the Criterion 6.8 systems listed in Table 2.2.15-1 conclude(s) that the safety-related systems' setpoints for safety-related functions are defined, determined and implemented based on a defined setpoint methodology.~~
~~21.Criterion 8.1, Electrical Power Sources:~~ ~~The listed systems in Table 2.2.15-1 receive power from safety-related power supplies in the same division.~~	~~a. Inspection(s) will be performed of the "current revision" of the electrical one-line diagrams for the listed systems in Table 2.2.15-1. {{Design Acceptance Criteria}}~~ ~~b. Inspection(s) will be performed on the listed systems in table 2.2.15-1~~	~~a. Inspection report(s) conclude(s) that the "current revision" of the electrical one-line diagrams show the listed systems in Table 2.2.15-1, receive power from safety-related power supplies in the same division. {{Design Acceptance Criteria}}~~ ~~b. Inspection report(s) conclude(s) that the listed systems in Table 2.2.15-1, receive power from safety-related power supplies in the same division.~~

~~**Table 2.2.15-2**~~

~~**ITAAC For IEEE Std. 603 Compliance Confirmation**~~

~~**Design Commitment**~~	~~**Inspections, Tests, Analyses**~~	~~**Acceptance Criteria**~~
~~22.Criterion 8.2, Non-electrical Power Sources:~~ ~~The listed systems in Table 2.2.15-1 receive non-electric power from safety-related sources.~~	~~a. Inspection(s) will be performed on the "current revision" of the P&ID of the listed systems in Table 2.2.15-1. {{Design Acceptance Criteria}}~~ ~~b. Inspection(s) will be performed on the as-built mechanical installation of the listed systems in Table 2.2.15-1.~~	~~a. Inspection report(s) conclude(s) that the "current revision" of the P&ID of the listed systems in Table 2.2.15-1 show non-electric power from safety-related sources. {{Design Acceptance Criteria}}~~ ~~b. Inspection report(s) conclude(s) that the listed systems in Table 2.2.15-1 receive non-electric power from safety-related sources.~~

~~assurance requirements for the DCIS and address the Nuclear Regulatory Commission (NRC) review guidance provided in the Standard Review Plan.~~

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

7.1.2 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~~ Reactor Trip Isolation Function-Neutron Monitoring System (RTIF-NMS) ~~functions~~, ~~TRICON for~~ Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) ~~functions~~, and the independent control platform. The independent control platform provides independent logic controllers for the Anticipated Transient Without Scram/Standby Liquid Control (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 contain equipment for both the RTIF platform and the independent control platform. These cabinets include the following systems and functions:
  - **RTIF Platform 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)~~,~~; and
    - ~~Anticipated Transient Without Scram/Standby Liquid Control (ATWS/SLC) functions (Refer to Subsection 7.4.1),~~
    - Suppression Pool Temperature Monitoring (SPTM) ~~subsystem~~ function of the Containment Monitoring System (CMS) (Refer to Subsection 7.2.3).~~, and~~
  - **Independent Control Platform Systems and Functions**
    - VB isolation function of the containment system (Refer to Subsection 7.3.6);~~.~~ and
    - ATWS/SLC functions (Refer to Subsection 7.4.1 and 7.8.1).
- ~~Neutron Monitoring System (~~NMS~~)~~ (Refer to Subsection 7.2.2) which includes:
  - Startup Range Neutron Monitor (SRNM) functions and
  - Power Range Neutron Monitor (PRNM) functions that include:
    - Local Power Range Monitor (LPRM) functions,
    - Average Power Range Monitor (APRM) functions, and
    - Oscillation Power Range Monitor (OPRM) functions.

SSLC/ESF protection systems are designed so that no safety-related function depends on the existence or function of any nonsafety-related component, data, or communication channel.

The Q-DCIS uses RMUs for data acquisition for the RTIF, NMS, and SSLC/ESF protection systems and for safety-related displays in the MCR and Remote Shutdown System (RSS). These data acquisition units are either distributed within the division or reside in specific chassis and are not dedicated to specific RTIF, NMS, or SSLC/ESF systems (for example, GDCS, ICS, and ADS).

For added reliability and diversity, the architecture of the RTIF and NMS protection systems is different from the architecture of the SSLC/ESF protection system (refer to Figure 7.1-3 and Figure 7.1-4). These systems operate automatically under normal conditions, without operator input.

The RTIF and NMS status is monitored on the divisional Q-DCIS safety-related MCR and RSS VDUs that are connected to the SSLC/ESF (the N-DCIS VDUs also have the capability to independently monitor the RTIF and NMS statuses but only after appropriate isolation and with no capability to control the Q-DCIS). The RTIF and NMS process data are sent per division through the required safety-related isolation and via a one-way dedicated communication path (datalink and gateway if necessary) for display on the corresponding divisional safety-related VDU. The RTIF, NMS, and SSLC/ESF operate independently of the VDUs, they continue to perform their safety-related functions if there is a failure of the VDU network and the VDUs have no capability to control the RTIF or the NMS. Safety-related VDUs are provided in the MCR and at the RSS and operate independently of one another. The safety-related VDUs provide data display capability for the RTIF, NMS, and SSLC/ESF safety-related systems but manual control capability only for the SSLC/ESF safety-related systems in the same division as the safety-related VDU, all in a Human Factors Engineering (HFE) approved format.

The divisional Q-DCIS components outside of the MCR are located in physically separate DCIS divisional rooms or compartments in the Reactor Building (RB) and Control Building (CB) that have appropriate fire barriers between them.

The divisional Q-DCIS components are powered by redundant, independent, and separated uninterruptible power supplies (UPS) dedicated to their division with battery backup (per division) for at least 72 hours. After 72 hours, the Q-DCIS can operate continuously on power from diesel generators or from off-site power (Refer to Chapter 8 for additional information about the power sources for the isolation load centers and safety-related uninterruptible AC power).

The Q-DCIS provides self-diagnostics that monitor communication, power, and processors to the replaceable card, module, or chassis level. Process diagnostics include system alarms and the capability to identify sensor failures. Process and self-diagnostic system alarms are provided to the MCR.

7.1.2.1 Q-DCIS Safety-Related Design Bases Summary

The safety-related design bases applicable to the Q-DCIS are found in IEEE Std. 603, Sections 4.1, 4.2, 4.5, 4.8, and 4.10. They specifically address reading signals, performing signal

- Provide secure data communication to all authorized external systems, including the technical support center (TSC), the emergency operating facility (EOF), and the emergency response data system (ERDS).
- Provide gateway interfaces to control and logic processing equipment supplied by parties other than the primary N-DCIS equipment supplier;
- Perform various PCF that include calculations, displays, and alarms;
- Provide for report generation; and
- Provide for a Plant Configuration Database (PCD).

7.1.4.3 N-DCIS Safety Evaluation Summary

The N-DCIS is used as the primary control, monitoring, and data communication system with power production applications. The N-DCIS is not required for safety-related purposes, nor is its operability required during or after any DBE. The system is required to operate in the normal plant environment and is relied on for data communications and power production applications. The N-DCIS provides an isolated alternate path for safety-related data to be presented to the plant operators. The N-DCIS network that supports the dual/triple, fault-tolerant digital controllers and communication scheme is diverse from the Q-DCIS network design in both hardware and software.

The N-DCIS equipment is located throughout the plant and is subject to the environment of each area. RMUs are typically located throughout the plant and auxiliary buildings. Computer equipment and peripherals are typically located mainly in the CB (MCR and Back Panel areas), Radwaste Building, TSC, EOF, and other auxiliary buildings.

The N-DCIS panels and components are designed to maintain structural integrity, during and after a DBE, and do not prevent any safety-related equipment in their area from performing its safety-related function.

Table 7.1-1 identifies the Q-DCIS systems and N-DCIS segments and the associated codes and standards applied, in accordance with the SRP. The following subsection summarizes N-DCIS conformance to regulatory requirements, guidelines, and industry standards.

7.1.4.4 N-DCIS Regulatory Requirements Conformance Summary

As shown in Table 7.1-1 and/or described in Subsection 7.1.6 the N-DCIS meets applicable portions of: .

- 10 CFR 50.55a(a)(1);
- 10 CFR 50.34(f)(2)(iii)[I.D.1];
- 10 CFR 50.34(f)(2)(iv)[I.D.2];
- 10 CFR 50.34(f)(2)(v)[I.D.3];

- 10 CFR 50.34(f)(2)(xv)[II.E.4.4];
- 10 CFR 50.34(f)(2)(xvii)[II.F.1];
- 10 CFR 50.34(f)(2)(xviii)[II.F.2];
- 10 CFR 50.34(f)(2)(xix)[II.F.3];
- 10 CFR 50.34(f)(2)(xxi)[II.K.1.22];
- 10 CFR 50.34(f)(2)(xxiv)[II.K.3.23];
- 10 CFR 50.34(f)(2)(xxvi)[III.D.1.1];
- 10 CFR 50.34(f)(2)(xxvii)[III.D.3.3];
- 10 CFR 50.49;
- 10 CFR 50.62;
- 10 CFR 52.47(a)(21);
- 10 CFR 52.47(b)(1);
- 10 CFR 52.47;

~~NUREG 0694, 0718, and 0737;~~

- IEEE Std. 7-4.3.2, 338, 497, 518, 603, 828, 829, 830, 1008, 1012, 1028, 1050, 1074;
- ANSI/ISA S67.02.01 (RG 1.151) and S67.04.01 (RG 1.105);
- GDC 1, 2, 4, 12, 13, 19, ~~and~~ 24, 25, 26, 27, 28, 29, 33, 38, 41, 42, 43, 63, and 64;
- SRM II.Q and II.T on SECY 93-087;
- RGs 1.89, 1.97, 1.100, 1.105, 1.152, 1.168, 1.169, 1.170, 1.171, 1.172, 1.173, 1.180, and ~~1.204~~1.209; and
- BTPs HICB-1, 10, ~~11, 12, 14,~~ 16, and ~~17, 18,~~ 19~~, and 21~~.

7.1.4.5 N-DCIS Testing and Inspection Requirements Summary

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 elements are performed before fuel loading and startup testing to ensure that the system functions as designed and that actual system performance is within specified criteria.

The N-DCIS controllers, displays, monitoring and input and output communication interfaces function continuously during normal power operation. Abnormal operation of these components can be detected during plant operation. In addition, the controllers are equipped with on-line diagnostic capabilities to identify and isolate failure of I/O signals, buses, power supplies,

processors, and inter-processor communications. These on-line diagnostics can be performed without interrupting the normal operation of the N-DCIS.

7.1.4.6 N-DCIS Operator Interface Requirements Summary

The N-DCIS VDUs allow operator control and monitoring of the N-DCIS systems. However, they allow only monitoring of safety-related system data, through appropriate isolation. The VDUs are also segmented so that the network segments can be monitored and controlled independently. During normal operation the segments are not apparent to the operators. The N-DCIS supplies alarm and annunciation information to the operator and a permanent overview mimic display for important plant information.

7.1.4.7 N-DCIS System Boundaries

The N-DCIS includes no Q-DCIS components. The N-DCIS does not include the sensors or the sensor wiring to the RMUs or the RMU output wiring to the actuators.

7.1.4.8 N-DCIS Major Systems Description Summary

The N-DCIS systems and components are nonsafety-related entities of the DCIS. The N-DCIS major system summary descriptions follow.

7.1.4.8.1 GENE Systems Description Summary

The GENE network segment comprises of workstations, triple-redundant controllers, and dual-redundant controllers, that execute the following functionssystems include:

- Workstations:;3D MONICORE that calculates three dimensional power distribution and thermal limits for the reactor core;
  - 3D MONICORE, and
  - SPDS.
- Dual-Redundant ControllersSystems that control and monitor control rod motion, including the RC&IS, ATLM, rod worth minimizer (RWM), MRBM, and signal interface unit (SIU):;
  - RC&IS (includes RSPC, RAPI, FCM),
  - ATLM,
  - Rod worth minimizer (RWM), and
  - Signal interface unit (SIU).
- Triple-Redundant ControllersThe logic for the Safety Parameter Display System (SPDS);:
  - DPS,

- Steam Bypass and Pressure Control (SB&PC),
- Feedwater Control System,
- Feedwater Temperature Control System, and
- Turbine-Generator Control System.

~~The DPS that provides diverse backup to the RPS and SSLC/ESF functions;~~

~~The nonsafety-related datalinks and gateways that translate and distribute data between the Q-DCIS and the N-DCIS;~~

~~Operator control and monitoring from the MCR VDUs; and~~

~~The nonsafety-related portion of the NMS that includes the AFIP subsystem and the MRBM subsystem.~~

7.1.4.8.2 Plant Investment Protection Systems (Train A and Train B) Description Summary

~~The N-DCIS for~~ T~~t~~he Plant Investment Protection (PIP) network segment comprises two channels (A and B) of dual-redundant controllers that execute the following functions:~~systems (Train A and Train B) provides the control logic for the~~:

- Control Rod Drive (CRD) System,
- Reactor Water Cleanup and Shutdown Cooling (RWCU/SDC) System,
- FAPCS,
- Nonsafety-related RSS ,
- 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),
- Nonsafety-related post accident monitoring (PAM) systems,
- Nonsafety-related LD&IS systems,
- PCCS Ventilation Fans,
- Ancillary and standby diesel generators,
- 6.9 KV plant electrical power system,

- Low voltage electrical system, and
- Nonsafety-related ~~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) network segments comprise a single channel of dual-redundant controllers that execute the following functions: ~~provide the logic for systems involved in power generation. These systems control/protect:~~

~~Reactor pressure;~~

~~RPV water level;~~

~~The Feedwater controlFWCS, including RPV level and feedwater temperature control;~~

- ~~The PASPlant automation~~Turbine auxiliary;
- ~~The SB&PC System~~Generator auxiliary controller;
- ~~The turbine and generator~~Electrical system main transformer/Unit Auxiliary Transformer (UAT) controller;
- ~~The m~~Main condenser ~~and normal heat sink~~controller;
- ~~The nonsafety-related plant electrical systems, including protective relaying, that are non-PIP~~Electrical system Reserve Auxiliary Transformer (RAT) controller;
- ~~Power generation components such as the moisture separator reheater (MSR) and the CPS~~Normal heat sink controller;
- ~~The~~ Condensate~~ and~~ /Feedwater ~~System~~ (~~C&FS~~FW)/drains/extraction controller, including extraction and level control; ~~and~~
- ~~Vendor-furnished BOP systems~~Water systems controller;~~.~~
- Service air/containment inerting/floor drains controller; and
- Miscellaneous HVAC controller.

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 Plant Configuration Database (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.

7.1.4.8.5 Nonsegment-Based Equipment

Equipment shared among segments are listed below:

- Nonsafety-related VDU/MCRP;
- Gateways;
- Datalinks; and

- Safety Parameter Display System (SPDS) logic.

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 simplified network functional ~~network~~ diagram of the DCIS appears as ~~part of~~ Figure 7.1-1~~2~~, ~~which~~ and 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 signals to the RMUs include transmitters, contact closures and other sensors or process

The N-DCIS equipment is located throughout the plant and is subject to the environment of each area. Specifically:

- RMUs are located throughout the plant and auxiliary buildings; and
- Computer equipment and peripherals are located mainly in the CB in the MCR and Back Panel areas. They are also located in other areas such as the EOF, Radwaste Building, TSC, Auxiliary Fuel Building, Auxiliary Fuel Building roof area, or alternate building designations specific to the plant design.

The N-DCIS panels and components are designed to retain their structural integrity during and after DBEs so that proximate safety-related equipment is not prevented from performing its safety-related function.

Table 7.1-1 identifies the N-DCIS elements and the associated regulatory requirements, guidelines, and codes and standards applied. The N-DCIS major subsystems are summarized in Subsection 7.1.4.8. The following subsections address I&C systems conformance to regulatory requirements, guidelines, and industry standards.

General DCIS conformance to regulatory requirements, guidelines, and industry standards is also addressed in Subsection 7.1.6.

7.1.5.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety, and 10 CFR 50.55a(h) Protection and Safety Systems, compliance with IEEE Std. 603:

- Conformance: The N-DCIS design complies with the above requirements.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(iv)[I.D.2], Safety parameter display system:

- Conformance: The N-DCIS design conforms to these requirements.

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

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xv)[II.E.4.4], Purge System Isolation Under Accident Conditions:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)[II.K.1.22], Auxiliary Heat Removal Systems:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxiv)[II.K.3.23], Central Reactor Vessel Water Level Recording:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxvi)[III.D.1.1], Leakage Control and Detection in Design Systems Outside Containment:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of In-plant Airborne Radioactivity:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.49, Environmental Qualifications of Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants:

- Conformance: The design has ATWS mitigation functions, as described in Section 7.8.

10 CFR 52.47(a)~~(1)(iv)~~(21), Resolution of Unresolved and Generic Safety-Related Issues:

- Conformance: The N-DCIS is nonsafety-related. Resolution of unresolved and generic safety issues is discussed in Section 1.11.

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

- Conformance: Inspection, Test, Analyses, and Acceptance Criteria (ITAAC) for the N-DCIS are identified in Tier 1.

10 CFR 52.47(a)~~(1)(vii)~~(25), Interface Requirements:

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

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided within the DCD conforms to this regulation.

10 CFR 52.47 (c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.1.5.3.2 General Design Criteria

GDC 1, 2, 4, 12, 13, 19, ~~and~~ 24, 25, 26, 27, 28, 29, 33, 38, 41, 42, 43, and 64:

- Conformance: The N-DCIS design conforms to these GDCs. Refer to Subsections 3.1.2 and 3.1.3 for a general discussion of each GDC.

7.1.5.3.3 Staff Requirements Memorandum

SRM, SECY-93-087, Item II.Q, Defense Against Common Mode Failures in Digital Instrumentation and Control Systems:

- Conformance: SRM on SECY 93-087, II.Q, states 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, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

  The N-DCIS provides diverse functionality via the DPS and associated interface systems. The nonsafety-related portions of the systems that conform to this guidance are~~,~~ further discussed in Section 7.8 and in Reference 7.1-4.

SRM, SECY-93-087, Item II.T, Control Room Alarm Reliability:

- Conformance: The N-DCIS AMS follows guidance in the above document for redundancy, independence, and separation so that the "alarm system" is considered redundant, has its own redundant processors and uses signals from distributed and redundant controllers. Alarm points are sent through a dual network to redundant processors that have dual power feeds. 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 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.97.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.151, Instrument Sensing Lines:

- Conformance: RG 1.151 is not applicable to the N-DCIS. The N-DCIS receives signals from nonsafety-related sensors in various systems in the plant that are supplied by~~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.
- Subsection 7.1.6.4.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The N-DCIS design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The Q-DCIS conforms to IEEE Std. 603.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The N-DCIS design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems

- Conformance: The N-DCIS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.1.5.3.5 Branch Technical Positions

BTP HICB-1, Guidance on Isolation of the Low Pressure Systems from the High Pressure Reactor Coolant System:

- Conformance: The N-DCIS conforms to BTP HICB-1.

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: N-DCIS conforms to BTP HICB-10. Details of design implementation are discussed in Section 7.5.

~~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.

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

- Conformance: The nonsafety-related portions of the systems that conform to BTP HICB-19 are discussed in Section 7.8 and in Reference 7.1-4.

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

- Zinc Injection System (ZNIS), an optional system.

7.1.6 General DCIS Conformance to Regulatory Requirements, Guidelines and Industry Codes and Standards

Table 7-1 of NUREG 0800 lists the Code of Federal Regulations (CFR)~~,~~ including GDC, SRM, RGs, and Instrumentation and Controls Branch ~~Memoranda~~ Technical Positions (HICB) that provide acceptance criteria or guidelines for each subsection of Chapter 7. Additional acceptance criteria or guidelines are delineated in the (NUREG-0800) SRP Chapter 7 sections.

The specific regulatory acceptance criteria and guideline requirements applicable to each of these systems (safety-related or nonsafety-related but significant for plant operation) identified in the SRP are tabulated in Table 7.1-1. The regulatory requirements and guidelines applicability matrix for Table 7.1-1 is followed in Sections 7.2 through 7.8 by a regulatory conformance discussion for each specific system. The degree of applicability and conformance, along with any clarifications or justification for exceptions, are presented in the safety evaluation sections for each specific system. Requirements and guidelines not applicable to the ESBWR design are delineated in Tables 1.9-7, 1.9-20, and 1A-1. General Q-DCIS and N-DCIS conformance is discussed in the following subsections.

7.1.6.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety~~, and10 CFR 50.55a(h) Protection and Safety Systems, compliance with IEEE Std. 603~~:

- Conformance: The Q-DCIS and N-DCIS designs comply~~ies~~ with the above requirements.

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

- Conformance: The Q-DCIS design conforms to IEEE Std. 603.

10 CFR 50.34(f), Conformance to Three Mile Island (TMI) Action Plan Requirements:

- ~~The response to~~ TMI-~~-~~related requirements~~matters is~~are generically addressed in Appendix 1A. Applicable TMI~~-~~-related~~action plan~~ requirements are identified for the systems in Table 7.1-1. The applicable systems are designed to conform. ~~However, because of the design features, several of these~~Those TMI-related requirements that are not applicable are not included in Table 7.1-1. The relevant TMI-related requirements that are resolved by the ESBWR Q-DCIS and N-DCIS design~~These~~ are identified as follows:

  ~~II.K.3.13 – HPCI and RCIC Initiation Levels,~~

  – ~~II.K.3.15 - Isolation of HPCI and RCIC (Turbine Driven),~~II.K.3.18 – ADS Actuation. ADS is designed for automatic operation.

  – II.K.3.21 - Automatic Restart of LPCS and LPCI~~,~~. ~~and~~ There are no automatic restart requirements based on the ECCS design.

~~II.K.3.22 - RCIC Automatic Switchover of Suction Supply.~~

The TMI action items applicable to the I&C systems are:

- 10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design,
- 10 CFR 50.34(f)(2)(iv)[I.D.2], Safety parameter display system, (see Subsection 7.1.5.2.4.1),
- 10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication,
- 10 CFR 50.34(f)(2)(viii)[II.B.3], Compatibility to Promptly Obtain and Analyze Containment Atmosphere Samples,
- 10 CFR 50.34(f)(2)(x)[II.D.1], Relief and Safety Valve Test Requirements,
- 10 CFR 50.34(f)(2)(xi)[II.D.3], Direct Indication of Relief and Safety Valve Position in the Control Room,
- 10 CFR 50.34(f)(2)(xv)[II.E.4.4], Purge System Isolation Under Accident Conditions,
- 10 CFR 50.34(f)(2)(xvii) [II.F.1], Accident Monitoring Instrumentation,
- 10 CFR 50.34(f)(2)(xviii) [II.F.2], Inadequate Core Cooling Instrumentation,
- 10 CFR 50.34(f)(2)(xiv) [II.E.4.2], Containment Isolation Systems,
- 10 CFR 50.34(f)(2)(xix) [II.F.3], Instruments for Monitoring Plant Conditions Following Core Damage,
- 10 CFR 50.34(f)(2)[II.K.1.22], Auxiliary Heat Removal Systems,
- 10 CFR 50.34(f)(2)(xxiii) [II.K.2.10], Anticipatory Reactor Trip,
- 10 CFR 50.34(f)(1)(v)[II.K.3.13], HPCI and RCIC Initiation Levels,
- 10 CFR 50.34(f)(1)(x)[II.K.3.28], Automatic Depressurization System Functioning During/Following an Accident Situation.
- 10 CFR 50.34(f)(2)(xxiv) [II.K.3.23], Central Reactor Vessel Water Level Recording,
- 10 CFR 50.34(f)(2)(xxvi)[III.D.1.1], Leakage Control and Detection in Design Systems Outside Containment,
- 10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of In-plant Airborne Radioactivity, and
- 10 CFR 50.34(f)(2)(xxviii)[III.D.3.4], Control Room Habitability Problems Under Accident Conditions.

10 CFR 50.44(c)(4), Combustible Gas Control For Nuclear Power Reactors, Monitoring:

- Conformance: The SSLC/ESF and CMS design complies with this requirement.

10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants:

- Conformance: The Q-DCIS and N-DCIS design has ATWS mitigation functions, as described in Section 7.8.

10 CFR 50.63, Loss of All Alternating Current Power:

- Conformance: The Q-DCIS design conforms to these standards, as described in Sections 7.2, 7.3, and 7.4.

10 CFR 52.47(a)~~(1)(iv),~~ (21), 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)~~(b)(1), ITAAC in Design Certification Applications:

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

10 CFR 52.47(a)~~(1)(vii)~~(25), 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 within the DCD conforms to this regulation.

10 CFR 52.47~~(b)(2)(i)~~(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

10 CFR 50.49, Environmental Qualifications of Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The Q-DCIS systems are designed to meet the equipment qualification requirements set forth in 10 CFR 50.49. Details are discussed in Section 3.11

7.1.6.2 General Design Criteria

In accordance with Table 7.1-1, the following GDC are addressed for the Q-DCIS:

GDC 1, 2, 4, 10, 12, 13, 15, 16, 19, 20, 21, 22, 23, 24, 25, 26, 27, ~~and~~ 29, 30, 33, 34, 35, 37, 41, 43, 44, and 64.

- Conformance: The Q-DCIS design complies with these GDC. Specific conformance of the I&C systems themselves is addressed in Sections 7.2 through 7.8.

GDC 1, 2, 4, 12, 13, 19, 24, 25, 26, 27, 28, 29, 33, 38, 41, 42, 43 and 64.

- Conformance: The N-DCIS design complies with these GDC. Specific conformance of the I&C systems themselves is addressed in Sections 7.2 through 7.8.

7.1.6.3 Staff Requirements Memorandum

SRM on SECY 93-087 II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems:

- Conformance: To minimize exposure to common-mode failures, the digital I&C systems are designed for high reliability, with the application of quality assurance requirements as specified in 10 CFR 50.55a(a)(1). Additionally, ~~T~~the digital I&C is designed ~~with~~ applying principles of defense-in-depth and diversity ~~for~~ defense against common mode failures. Section 7.8 includes the description of the diverse I&C systems that specifically addresses the requirements of this SRM.

SRM on SECY 93-087 II.T, Control Room Annunciator/Alarm Reliability:

- Conformance: The AMS follows guidance in the above document for redundancy, independence, and separation because the "alarm system" is considered redundant. Alarm points are sent through dual networks to redundant message processors on dual power supplies. The processors are dedicated to only doing alarm processing. The alarms are displayed on multiple independent VDUs that each have dual power supplies. The alarm tiles, or their equivalent, are driven by redundant datalinks (with dual power). There are redundant alarm processors. There are no alarms that require manually controlled actions for safety-related systems to accomplish their function. Thus the requirements for safety-related equipment and circuits are not applicable.

7.1.6.4 Regulatory Guides

A discussion of the general conformance of the I&C equipment to RGs is provided below.

RG 1.22, Periodic Testing of Protection System Actuation Functions:~~.~~

- Conformance: Safety-related systems have provision for periodic testing. Proper functioning of analog sensors is verified by channel cross-comparison and is done continuously by the PCF. Some actuators and digital sensors, because of their locations, cannot be fully tested during actual reactor operation. Such equipment is identified and provisions for meeting the guidance of Paragraph D.4 (per BTP HICB-8) are discussed in the Safety Evaluation subsections within Sections 7.2 through 7.8.

RG 1.45, Reactor Coolant Pressure Boundary Leakage Detection Systems:

- Conformance: Provisions are made to detect and monitor identified and unidentified leakage of reactor coolant consistent with the guidance of this RG.

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

- Conformance: Bypass indications are designed to satisfy the guidance of IEEE Std. 603, Paragraph 5.8.3, and RG 1.47. The design of the bypass indications allows testing during normal operation and is used to supplement administrative procedures by providing indications of safety-related systems status.

Bypass indications use isolation devices that preclude the possibility of any adverse electrical effect of the bypass indication circuits on the plant safety-related system.

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

- Conformance: The safety-related systems are organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy for the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related systems designs' conformance to the single-failure criterion. ~~designs conform to the single failure criterion; additionally the design meets N-2 conditions.~~

RG 1.62, Manual Initiation of Protective Actions:~~.~~

- Conformance: The applicable I&C systems are designed to comply with RG 1.62. Specific conformance of the I&C systems is addressed in Sections 7.2 through 7.4.~~Manual initiation of the protective action is provided at the system level for safety-related systems conditions. An exception to RG 1.62, Regulatory Positions C.4 and C.5 is taken for the two of four divisional manual trip switches for ADS (SRV and DPV), GDCS, ICS, and SLC manual initiation. These switches are indirectly connected to the squib valve load drivers or valve solenoids through the SSLC/ESF. The DPS manual trip switches are independently connected to the squib valve load drivers or valve solenoids, through DPS logic.~~

RG 1.75, Physical Independence of Electric Systems:~~.~~

- Conformance: The safety-related system designs conform to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electronic Equipment Important to Safety for Nuclear Power Plants~~.~~:

- Conformance: The safety-related system design conforms to RG 1.89.

RG 1.97, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident:~~.~~

- Conformance: The ~~I&C system~~Q-DCIS and N-DCIS are~~is~~ designed to meet the guidance of RG 1.97. Details of design implementation are discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants~~.~~:

- Conformance: The Q-DCIS systems are designed to meet the ~~requirements~~ guidance set forth in RG 1.100. Details are discussed in Section 3.11.

RG 1.105, Instrument Setpoints for safety-related Systems:~~.~~

- Conformance: The ~~I&C systems~~Q-DCIS and N-DCIS are consistent with the guidance of RG 1.105. The applicable analytical or design basis limit (technical specification limit), as well as the nominal trip setpoint (instrument setpoint) and any "as-found tolerance" and, "as left tolerance" are provided in separate documentation. These parameters are appropriately separated from each other based on instrument accuracy, calibration capability and design drift (estimated) allowance data. The setpoints are within the instrument best-accuracy range. The established setpoints provide margin to satisfy safety-related requirements and plant availability objectives.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:~~.~~

- Conformance: The I&C systems are consistent with the guidance of RG 1.118.

RG 1.151, Instrument Sensing Lines:~~.~~

- Conformance: The instrument sensing lines are designed to satisfy the guidance of RG 1.151. These lines are used to perform safety-related and nonsafety-related functions. There are four redundant, separate sets of instrument lines, each having safety-related instruments associated with one of the four electrical safety-related divisions. The RPS logic requires any two-out-of-four trip signals to scram. If a division is bypassed, the logic is two-out-of-three. Also, emergency core cooling functions are redundant throughout the four divisions and the feedwater system is designed with triple fault-tolerant digital controllers (FTDC) that use sensors separate from the safety-related sensors. Therefore, the systems are designed so that no single failure or two-division failure can cause a DBE and at the same time, the systems provide mitigating action for the event. Sections of endorsed standard ANSI/ISA-S67.02.01 on design practices for tubing, vents, and drains also apply to nonsafety-related instrumentation.

RG 1.152, Computer Software Used in Safety-related Systems:~~.~~

- Conformance: The guidelines of RG 1.152 are a basis for design procedures established for programmable digital equipment. As the principleRG for digital computers in safety-related systems in nuclear power plants, it endorses and refers to IEEE Std. 603 for specific criteria details. This RG also contains discussions on digital I&C equipment common mode failure issues. The concern is related to the possibility that a design error in the software in redundant divisions of a safety-related system could lead to common cause or common mode failure of the safety-related system function. It is possible for conditions to exist where some form of diversity is necessary that provides additional assurance beyond that which is provided by the design and quality assurance (QA) programs that incorporate software QA and V&V. The design techniques of functional diversity, design diversity, diversity in operation, and diversity within the four echelons of defense-in-depth can be applied as defense against common-cause failures. The justification for equipment diversity, or for the diversity of related system software such as a real-time operation system, must extend to equipment components to ensure that actual diversity exists. Claims for diversity based on different manufacturers are insufficient without consideration of the above. Other considerations such as functional and signal diversity, that lead to different software requirements form a stronger basis for diversity. The following sections are noted in IEEE Std. 7-4.3.2 as specifically addressed by the NRC in RG 1.152:

- The main text portions of IEEE Std. 7-4.3.2 are similar to those in the 1993 version, with more extensive requirements incorporated for software development, V&V, software configuration management, equipment qualification, self-diagnostics, independence, and reliability. There is no specific detail on diverse method requirements.
- Annex B, "Diversity Requirements Determination" is essentially unchanged from the 1993 version. This annex provides a methodology for determining the need for diversity. RG 1.152 does not endorse Annex B.
- Annex C, "Dedication of existing commercial computers" is similar to the 1993 version.
- Annex E, "Communication Independence" is similar to the annex in the 1993 version. The NRC does not endorse Annex E.
- Annex F, "Computer reliability" is similar to the annex in 1993 the version. The NRC states that quantitative reliability goals are not the only means, and does not endorse this method as the sole means of meeting the regulations for reliability of digital computers. The NRC acceptance is based on deterministic criteria.
- Safety I&C System compliance with IEEE Std. 7-4.3.2

Additionally, RG 1.152 includes guidance applicable to the Q-DCIS. Compliance is summarized as follows:

- Defense against software common mode failures: GEH has evaluated BTP HICB-19 guidelines including the acceptance criteria on defense-in-depth and diversity and defense against common mode failures, on the four echelons of defense against common mode failures. The four echelons are control systems, reactor trip system, Engineered Safety Features Actuation System (ESFAS), and monitoring and indicator functions. To fully address the guidelines of BTP HICB-19 on defense-in-depth and diversity and defense against common mode failures, the DPS backs up the primary safety-related I&C system protection functions. The DPS is implemented with hardware and software that is totally separate and independent from the primary safety-related I&C protection systems (RTIF, NMS, and SSLC/ESF). The DPS is implemented in addition to the ATWS/SLC system function. A detailed description of the DPS and the description of defense-in-depth and diversity and defense against common mode failure are included in Section 7.8.
- Software development process: The software development process of the Q-DCIS (including control systems key to plant operation) follows the guidelines of BTP HICB-14. Software development process plans for the DCIS design implementation include the Software Management Plan (SMP), Software Development Plan (SDP), Software Verification and Validation Plan (SVVP), Software Configuration Management Plan (SCMP), Software Safety Plan (SSP), as required by guidance in BTP HICB-14 and are described in References 7.1-10 and 7.1-12. Actual detailed hardware and software design implementation follows the guidelines specified by these plans as part of the design acceptance criteria process.

- Equipment qualification, self-diagnostics, independence, and reliability: IEEE Std. 603 states that these requirements are applicable to safety-related I&C system equipment. The Q-DCIS meets the requirements of IEEE Std. 603, and the above requirements in areas applicable to digital computer-based equipment.

- Security: The security guidelines included in RG 1.152 are evaluated and incorporated as appropriate and necessary in the DCIS design, both on plant hardware security measures and software security measures. The software development process plans are developed with the security requirements incorporated for actual detailed design implementation.

RG 1.153, Criteria for Safety Systems:

- Conformance: Safety-related systems are designed to satisfy the requirements of IEEE Std. 603, as endorsed by RG 1.153.

RG 1.168, Verification, Validation, Reviews, and Audits For Digital Computer Software Used In Safety Systems of Nuclear Power Plants:

- Conformance: This RG endorses IEEE Std. 1012, IEEE Standard for SVVPs, and IEEE Std. 1028, IEEE Standard for Software Reviews and Audits. IEEE Std. 1012 is acceptable for providing high functional reliability and design quality in software used in safety-related systems. IEEE Std. 1028 is acceptable for carrying out software reviews, inspections, walkthroughs, and audits subject to certain provisions. Safety-related systems use the guidance in these standards, as discussed in Reference 7.1-10, to develop portions of the overall SDP and thus comply with RG 1.168.

RG 1.169, Configuration Management Plans For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants:

- Conformance: RG 1.169 endorses IEEE Std. 828, IEEE Standard for SCMPs, and ANSI/IEEE Std. 1042, IEEE Guide to Software Configuration Management. These standards, with the clarifications provided in the Regulatory Position, describe acceptable methods for providing high functional reliability and design quality in software used in safety-related systems. Safety-related systems use the guidance in these standards, as discussed in Reference 7.1-10, to develop portions of the overall SDP and thus comply with RG 1.169.

RG 1.170, Software Test Documentation For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants:

- Conformance: The guidance contained in IEEE Std. 829, IEEE Standard for Software Test Documentation, provides an acceptable approach for meeting the requirements of 10 CFR Part 50 as they apply to the test documentation of safety-related system software subject to the provisions in this guide. Safety-related systems use the guidance in these standards to develop portions of the overall SDP and thus comply with RG 1.170.

RG 1.171, Software Unit Testing For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants:

- Conformance: RG 1.171 endorses IEEE Std. 1008, IEEE Standard for Software Unit Testing, subject to the provisions in this guide. This standard defines an acceptable method for planning, preparing for, conducting, and evaluating software unit testing. Safety-related systems use the guidance in this standard to develop, as discussed in Reference 7.1-10, portions of the overall SDP and, thus, comply with RG 1.171.

RG 1.172, Software Requirements Specifications For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants:

- Conformance: RG 1.172 endorses IEEE Std. 830, Recommended Practice for Software Requirements Specifications, as amended in the Regulatory Position. This standard describes current practices for writing software requirements specifications for a wide variety of systems. It is not specifically aimed at safety-related applications; however, it does provide guidance on the development of software requirements specifications that exhibit characteristics important for developing safety-related system software. This is consistent with the goal of ensuring high-integrity software in reactor safety-related systems. Safety-related systems use the guidance in this standard, as described in the References 7.1-10 and 7.1-12, to develop portions of the overall software development plan and thus comply with RG 1.172.

RG 1.173, Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants:

- Conformance: RG 1.173 endorses IEEE Std. 1074. The standard describes, in terms of inputs, development, verification or control processes, and outputs, a set of processes and constituent activities that are commonly accepted as composing a controlled and well-coordinated software development process. It describes inter-relationships among activities by defining the source activities that produce the inputs and the destination activities that receive the outputs. The standard specifies activities that must be performed and their inter-relationships; it does not specify complete acceptance criteria for determining whether the activities themselves are properly designed. Therefore, the standard is used in conjunction with guidance from other appropriate RGs, standards, and software engineering literature. Safety-related systems use the guidance in this standard, as described in References 7.1-10 and 7.1-12, to develop portions of the overall SDP and thus comply with RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems:

- Conformance: Electrical and electronic components in the I&C safety-related systems are qualified for anticipated levels of EMI at their as-installed locations. EMC of I&C equipment is verified through factory testing and site-specific testing for both individual equipment and interconnected systems to meet EMC requirements for protection against the following:
  - EMI,
  - RFI,
  - Electrostatic discharge, and

- Electrical surge.

  EMI qualifications, including methods of evaluating EMI operating envelopes, follow the requirements defined in Mil Std. 461E and IEC 61000-4. Q-DCIS equipment is qualified to perform continuously within specified ranges even when exposed to EMI environmental limits at the hardware mounting location. To that end, EMI qualifications for safety-related systems meet the proposed requirements of RG 1.180, Rev 1 "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems."

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The surge withstanding capability of the safety-related I&C design conforms with IEEE Std. 1050. See Subsection 8A.1.2 for detailed information about the lightning protection system and conformance to RG 1.204.

RG 1.209, Guidelines For Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The safety-related system design conforms to RG 1.209.

7.1.6.5 Branch Technical Positions

BTPs that are applicable to the I&CDCIS systems are identified relative to the I&C systems in Table 7.1-1. BTPs that are not applicable to the I&C design are identified in Table 1.9-7. BTPs are guidance documents; the I&C systemsDCIS are is generally designed to conform to the BTPs. The degree of conformance, along with any clarifications or exceptions, is discussed in the safety evaluation subsections of Sections 7.1 through 7.8.

The following BTPs are not applicable to the ESBWR design:

BTP HICB-3, Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service. Reactor coolant pumps are not used in the design and Position B.1 does not apply.

BTP HICB-6, Guidance on Design of Instrumentation and Controls Provided to Accomplish changeover from Injection to Recirculation Mode. No recirculation pumps and ECCS pumps are used in the design.

BTP HICB-13, Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors. RTDs are not used in safety-related applications.

The following BTPs are applicable:

BTP HICB-1, Guidance on Isolation of the Low Pressure Systems from the High Pressure Reactor Coolant System. The GDCS and interlock systems PIP A/B segment of N-DCIS design conforms to BTP HICB-1.

BTP HICB-8, Guidance on Application of RG 1.22. The Q-DCIS is fully functional during reactor operation and is tested in conjunction with the SSLC/ESF. Therefore, the Q-DCIS design

conforms to BTP HICB-8. The DPVs, SRVs, and squib valves are not tested during reactor operation.

BTP HICB-9, Guidance on Requirements for RPS Anticipatory Trips. The Q-DCIS conforms to BTP HICB-9.

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97. ~~I&C~~The Q-DCIS and N-DCIS design conforms to BTP HICB-10. Details of design implementation are discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices. The Q-DCIS design conforms to BTP HICB-11.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints. The Q-DCIS design conforms to BTP HICB-12.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-based I&C Safety Systems. Refer to Subsections 7.1.2.4, Reference 7.1-10 and 7.1-12 discussions. The Q-DCIS design conforms to BTP HICB-14.

The Q-DCIS and N-DCIS follow a development process that is in accordance with BTP HICB-14. As part of the Certification activity, the software development process plans require NRC review and approval.

Safety-related I&C systems (RTIF, NMS and SSLC/ESF) use computers for their logic functions. A description of the Q-DCIS design, together with the description of the DPS is included in Section 7.8, and specifically addresses the issues of defense-in-depth and diversity and defense against common mode failures.

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52. BTP HICB-16 is applicable to all sections of Chapter 7 of the Design Control Document and all sections conform to it.

BTP HICB-16 states that the application should:

- Describe the resolution of unresolved and generic safety issues applicable to the I&C systems,
- Describe the interface requirements to be met by portions of the plant for which the application does not seek certification and which are necessary to ensure proper functioning of the I&C system, and
- Identify and describe the validation of innovative means of accomplishing I&C system safety-related functions.

Applications that propose the use of computers for systems with safety-related uses should describe the computer system development process. Applications that propose the use of computers for RTS and ESFAS functions should also describe the design of the overall I&C systems with respect to defense-in-depth and diversity requirements.

The I&C design has no unresolved or generic safety-related issues applicable to I&C systems. In Section 1.11, unresolved and generic safety-related issues are discussed. There are several new generic issues that are related to I&C systems, such as failure of protective devices on safety-related equipment, electromagnetic pulse, identification of protection system instrument sensing lines, and protection system testability. These issues either are not applicable to safety-related I&C systems or are addressed by the safety-related I&C design. Within the scope of the DCD submitted for certification application, there are no interface requirements described here that fall into this category.

The design uses the voluminous data available from operating plants and from the testing and licensing efforts performed to license the predecessor designs and individual plants. The I&C design does not use innovative means for accomplishing safety functions.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions in Digital Computer-based I&C Systems. Refer to Subsection 7.2.1.3.5 and 7.3.4.3 discussions. The Q-DCIS design conforms to BTP HICB-17.

BTP HICB-18, Guidance on Use of Programmable Logic Controllers in Digital Computer-based I&C System. The Q-DCIS design conforms to BTP HICB-18.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems (Item II.Q of SECY-93-087). The Q-DCIS, DPS and associated N-DCIS interfacing systems design conform~~s~~ to BTP HICB-19. The implementation of an additional diverse instrumentation and control system is described in Section 7.8.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance. The Q-DCIS design conforms to BTP HICB-21.

7.1.6.6 Industry Standards

The safety evaluation subsections throughout Chapter 7 address the RGs identified by the SRP. The IEEE standards that are endorsed by RGs are not addressed separately.

Some codes or standards that are not mentioned in the SRP are used in specific system applications. These are identified in the system description and the corresponding reference section. In accordance with the SRP format, the following IEEE standards applicable to the I&C equipment are addressed in other chapters.

IEC 61000-4 series. The design conforms to this series of standards.

IEEE Std. 323, "Qualifying safety-related Equipment for Nuclear Power Generating Stations." Safety-related systems are designed to meet the requirements of IEEE Std. 323. Environmental qualification is addressed in Section 3.11.

IEEE Std. 344, "Recommended Practices for Seismic Qualification of Safety-related Equipment for Nuclear Power Generating Stations". Safety-related I&C equipment is classified as Seismic Category I and designed to withstand the effects of the safe shutdown earthquake (SSE). It remains functional during normal and accident conditions. Qualification and documentation

procedures used for Seismic Category I equipment and systems satisfy the provisions of IEEE Std. 344 as indicated in Section 3.10.

IEEE Std. 379, "IEEE Standard for the Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems." The Q-DCIS platforms, RTIF-NMS, SSLC/ESF, ATWS/SLC logic controllers, and VBIF logic controllers, are organized into four physically and electrically isolated divisions that use principles of redundancy and independence to conform to the single failure criterion.

IEEE Std. 383, "IEEE Standard for Type Test of Safety-related Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations." Electric cable conforms to this standard. Fiber optic cable insulation/covering/jacketing also conforms to the requirements for flame tests in IEEE Std. 383.

IEEE Std. 384, "IEEE Standard Criteria for Independence of Safety-related Equipment and Circuits". See the discussion of RG 1.75 in Subsection 7.1.6.4.

IEEE Std. 497, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations." Accident monitoring instrumentation is discussed in Section 7.5.

IEEE Std. 518, "IEEE Guide for the Installation of Electrical Equipment to Minimize Electrical Noise Inputs to Controllers from External Sources". The design conforms to IEEE Std. 518.

IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations". Conformance to IEEE Std. 603 is discussed in Subsection 7.1.6.6.1.

IEEE Std. 1050, "IEEE Guide for Instrumentation Control Equipment Grounding in Generating Stations". The design conforms to IEEE Std. 1050.

7.1.6.6.1 IEEE Std. 603 – IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

The scope of IEEE Std. 603 includes safety-related I&C systems that are described in Sections 7.1 through 7.8. IEEE Std. 603 does not directly apply to nonsafety-related systems, other than to require independence between nonsafety-related systems and safety-related systems. IEEE Std. 603 provides design criteria for safety systems. ESBWR divides safety systems into two parts: the Q-DCIS platforms, and the subsystems that contain the sensors and actuators used by the Q-DCIS platforms. This section describes how the IEEE Std. 603 criteria are allocated to the different Q-DCIS platforms and subsystems. For convenience, some of these requirements may also be adopted as design bases for some nonsafety-related I&C components and systems such as for accident monitoring instrumentation, in accordance with RG 1.97. Compliance with the requirements of IEEE Std. 603 is also identified as compliance with the requirements and guidance contained within the federal regulations, GDC, SRM, and RGs, as described throughout Section 7.1. The safety-related I&C design comprises the Q-DCIS which includes the equipment in the RTIF, NMS, and SSLC/ESF cabinets. The design conforms to IEEE Std. 603. ITAACs are provided for the major attributes for compliance with IEEE Std. 603 and are not intended to limit the scope of compliance.

When the IEEE Std. 603 design criteria are applied to platforms relying on the use of software to perform their safety-related functions, additional criteria from IEEE Std. 7-4.3.2, which augments the IEEE Std. 603 criteria, also apply to the platform as described under the applicable IEEE Std. 603 criterion. The evaluation of Q-DCIS platforms for compliance with IEEE Std. 603 and IEEE Std. 7-4.3.2 criteria includes the examination of the effects that the associated sensors and actuators have on the performance of the safety-related function.

In accordance with the software development process described in Subsection 14.3.3.2 and the defense-in-depth and diversity strategy described in Section 7.8, the protection systems are executed as software projects on particular Q-DCIS platforms. The software projects are named RTIF, NMS, SSLC/ESF, VB Isolation Function, and ATWS/SLC.

Table 14.3-4 show the relationship between the Q-DCIS platforms and their corresponding software projects. As shown, the RTIF-NMS platform has two software projects: RTIF and NMS. The SSLC/ESF platform has one software project: SSLC/ESF. The Independent Control Platform has two software projects: VBIF and ATWS/SLC.

7.1.6.6.1.1 Safety System Designation (IEEE Std. 603, Section 4, et al)

IEEE Std. 603, Section 4, requires that a specific basis be established for the design of each safety-related system. The DBEs applicable to the safety-related control systems are shown in Table 15.0-2. DBEs comprise Anticipated Operational Occurrences (AOO), infrequent events, accidents, and special events.

Criterion 4.1 requires identification of the DBEs applicable to each mode of operation of the plant along with the initial conditions and allowable limits of plant conditions for each such event. Table 1.3-1 defines the reactor system design characteristics. Tables 15.0-3, 15.0-4, 15.0-5, and 15.0-6 define the safety-related analysis acceptance criteria for the AOOs, infrequent events, special events, and accidents. Table 15.1-2 defines the ESBWR operating modes for the entire operating envelope. Table 15.1-3 defines the ESBWR abnormal events with applicable operating modes. Table 15.2-1 defines the input parameters, initial conditions, and assumptions for AOO events and infrequent events. Table 15.5-2 defines the initial conditions and bounding limits for ATWS events.~~The plant operating conditions applicable to each DBE are shown in Tables 15.1-2 and 15.1-3. The safety-related analysis acceptance criteria for the AOOs, infrequent events, and accidents are shown in Tables 15.0-3, 15.0-4, 15.0-5, and 15.0-6. Special events are evaluated in Subsections 15.5.1 through 15.5.7.~~ Credited systems, interlocks, and functions for each DBE are described in Sections 15.2, 15.3, 15.4, and 15.5. Additional details about the specific safety-related or nonsafety-related interfacing system design bases, interlocks, and functions are found in Sections 4.6, 5.2, 5.4, 6.2, 6.3, 8.3, 9.1, 9.3, 9.4, 10.2, 10.3, and 10.4. Information provided for each design basis item enables the detailed design of the system to be carried out. Safety-related system design basis descriptions are included in the various sections of this chapter as indicated below.

- Reactor Trip System;
  - RPS (Subsection 7.2.1),
  - NMS (Subsection 7.2.2), and

  - Suppression Pool Temperature Monitoring (Subsection 7.2.3).
- SSLC/ESF (Subsection 7.3.5);
  - ECCS (Subsection 7.3.1):
    - ADS (Subsection 7.3.1.1),
    - GDCS (Subsection 7.3.1.2),
    - ICS (Subsection 7.4.4), and
    - SLC system (Subsection 7.4.1).
- PCCS (Subsection 7.3.2);
- LD&IS non-MSIV functions (Subsection 7.3.3) (MSIV functions of the LD&IS are located in the RTIF cabinets);
- CRHS (Subsection 7.3.4);
- RSS (Subsection 7.4.2);
- RWCU/SDC (Subsection 7.4.3);
- PAM system (Subsection 7.5.1);
- CMS (Subsection 7.5.2);
- PRMS (Subsection 7.5.3);
- ATWS/SLC (7.8.1);
- CRHS (7.5.2); and
- VB isolation function (7.3.6).

Criterion 4.2 requires identification of the safety-related functions and corresponding protective actions of the execute features for each event evaluated in the Nuclear Safety Operational Analysis (NSOA). Table 15.1-5 defines the execute systems required to respond to each event. Table 15.1-6 defines the automatic safety-related instrument trips in response to each event. Additionally, safety-related design bases for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

Criterion 4.3 requires identification of the permissive conditions for each operating bypass capability that is to be provided. Additionally, the permissive conditions for each operating bypass for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

Criterion 4.4 requires identification of the variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper

completion of the protective action is ensured. The minimum list of such variables and combinations of variables to be monitored is determined as part of the HFE design process described in Chapter 18. The variables and combinations of variables that are associated with each event are discussed in the relevant subsection describing the event as defined in Table 15.1-7.

Criterion 4.5 requires identification of (1) the points in time and the plant conditions during which manual control is allowed, (2) the justification for permitting initiation or control subsequent to initiation solely by manual means, (3) the range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations are performed, and (4) the variables identified by Criterion 4.4 that are displayed for the operator to use in taking manual action, for each action identified by Criterion 4.2 whose operation may be controlled by manual means initially or subsequent to initiation. The minimum list of variables and combinations of variables to be monitored is determined as part of the HFE design process described in Chapter 18.

Criterion 4.6 requires identification of the minimum number and locations of sensors required for protective purposes for those variables identified by Criterion 4.4 that have spatial dependence. The minimum list of variables and combinations of variables to be monitored is determined as part of the HFE design process described in Chapter 18. The variables and combinations of variables that have spatial dependence are described within each applicable subsection of this chapter.

Criterion 4.7 requires identification of the range of transient and steady-state conditions of both motive and control power and the environment during normal, abnormal, and accident circumstances throughout which the safety system performs. Safety-related mechanical equipment and electrical equipment (which comprises electrical power and instrumentation and controls equipment) is qualified in accordance with the equipment qualification program described in Section 3.11. Environmental conditions for the zones where qualified equipment is located are calculated for normal, AOO, test, accident and post-accident conditions and are documented in Appendix 3H, Equipment Qualification Environmental Design Criteria.

Criterion 4.8 requires identification of the conditions having the potential for functional degradation of safety system performance and for which provisions are incorporated to retain the capability for performing the safety functions. Safety-related mechanical equipment and electrical equipment (which comprises electrical power and instrumentation and controls equipment) is qualified in accordance with the equipment qualification program described in Sections 3.9 through 3.11. Environmental conditions for the zones where qualified equipment is located are calculated for normal, AOO, test, accident and post-accident conditions and are documented in Appendix 3H, Equipment Qualification Environmental Design Criteria.

Criterion 4.9 requires identification of the methods to be used to determine that the reliability of each safety system design is appropriate and any qualitative or quantitative reliability goals that may be imposed on the system design. The ESBWR Design Reliability Assurance Program (D-RAP) is a program utilized during detailed design and specific equipment selection phases to assure that the important ESBWR reliability assumptions of the Probabilistic Risk Assessment (PRA) are addressed throughout the plant life. The D-RAP is described in Section 17.4.

Criterion 4.10 requires identification of the critical points in time or the plant conditions, after the onset of a design basis event, including: (1) the point in time or plant conditions for which the protective actions of the safety system are initiated, (2) the point in time or plant conditions that define the proper completion of the safety function, (3) the point in time or the plant conditions that require automatic control of protective actions, and (4) the point in time or the plant conditions that allow returning a safety system to normal. The relevant points in time and plant conditions associated with each event, except for the allowable conditions for returning a plant to normal, are discussed in the relevant subsection describing the event as defined in Table 15.1-7. The allowable conditions for returning a plant to normal (i.e., return to service conditions) are described in Chapter 16, Technical Specifications.

Criterion 4.11 requires identification of the equipment protective provisions that prevent the safety systems from accomplishing their safety functions. The safety-related systems are designed to accomplish their safety-related functions in accordance with the single-failure criterion, IEEE Std. 603, Section 5.1. Failure modes and effects analyses are performed on the safety-related system final design to ensure that no equipment protective provisions preclude correctly performing any safety-related function.

Criterion 4.12 requires identification of any other special design basis that may be imposed on the system design (e.g., diversity, interlocks, regulatory agency criteria). The design bases for each subsystem (including bases for diversity, interlocks, regulatory agency criteria) are identified within each applicable subsection of this chapter.

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

The safety-related system designs are organized into four physically and electrically isolated divisions that use the principle of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally the design meets N-2 conditions (see Subsection 7.1.3.3.6).

The safety-related control systems include sufficient redundancy~~, diversity,~~ and independence to fulfill their intended safety function even when~~meet system performance requirements if the system is~~ degraded by any single credible failure. ~~In t~~The ~~RPS~~RTIF - ~~,~~ NMS, ~~and~~ SSLC/ESF, and independent control platform implement the single failure criterion of IEEE Std. 603 Section 5.1 using four independent and redundant channels, which are provided in two-out-of-four ~~redundancy and~~ trip logic. This ensures no single failure of or within any division prevents the system from performing its safety function or causing either an inadvertent reactor scram or an ECCS actuation~~a single failure from inhibiting a scram or reactor core cooling safety-related function. They also prevent a single failure from causing either an inadvertent reactor trip or an ECCS action~~. Redundancy begins with the sensors monitoring the variables and continues through the signal processing, output devices, and actuators.

Independence is implemented as described in Subsections 7.1.6.6.1.7 and 7.1.6.6.1.20.

Failure modes and effects analyses (FMEA) complying with IEEE Std. 379 are used to confirm the safety-related system designs' conformance to the single-failure criterion.~~More than one diverse sensor and control system initiates most protective actions. No single failure or two-~~

~~division failure within the safety-related system causes an AOO to degrade to an Infrequent Event or an Infrequent Event to degrade to an Accident.~~

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

Equipment is provided in accordance with a proscribed quality assurance plan as described in Subsection 7.1.6.6.1.4.

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. Additionally, completion of protective actions for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).~~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.~~

7.1.6.6.1.4 Quality (IEEE Std. 603, Section 5.3)

The Quality criterion requires that the Q-DCIS be consistent with minimum maintenance requirements and low failure rates and be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Q-DCIS meets this requirement through the application of the ESBWR Quality Assurance Program described in Chapter 17.

IEEE Std. 7-4.3.2 has additional quality assurance requirements related to software. Refer to LTRs "ESBWR Software Management Program Manual," NEDE-33226P (Reference 7.1-12), and "ESBWR Software Quality Assurance Program Manual," NEDE-33245P (Reference 7.1-10) for a description of the software plans that control the additional IEEE Std. 7-4.3.2 criteria related to the following hardware and software quality assurance requirements.

- IEEE Std. 7-4.3.2, Criterion 5.3.1, Software Development. The quality of software development activities is assured in accordance with the Software Quality Assurance Plan (SQAP).
- IEEE Std. 7-4.3.2, Criterion 5.3.2, Software Tools. Software tools are controlled in accordance with the Software Configuration Management Plan (SCMP).
- IEEE Std. 7-4.3.2, Criterion 5.3.3, Verification and Validation (V&V). Software V&V is performed in accordance with the Software V&V Plan (SVVP).
- IEEE Std. 7-4.3.2, Criterion 5.3.4, Independent V&V (IV&V). Software IV&V is performed in accordance with the Software V&V Plan (SVVP).
- IEEE Std. 7-4.3.2, Criterion 5.3.5, Software Configuration Management. Software configuration is controlled in accordance with the Software Configuration Management Plan (SCMP).
- IEEE Std. 7-4.3.2, Criterion 5.3.6, Software Project Risk Management: Software project risk management is managed in accordance with the Software Management Plan (SMP).

Safety-related~~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)

The Equipment Qualification criterion requires the referencing platform to be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that the safety-related system is capable of meeting the performance requirements specified in the design basis. The Q-DCIS meets the Equipment Qualification requirements through the application of the Equipment Qualification program that is described in Sections 3.9 through 3.11. Refer to Table 3.11-1 for a list of electrical and mechanical equipment and conformance criteria for Equipment Qualification.

IEEE Std. 7-4.3.2 has additional Equipment Qualification requirements related to SSC using software. Refer to LTRs "ESBWR Software Management Program Manual," NEDE-33226P (Reference 7.1-12), and "ESBWR Software Quality Assurance Program Manual," NEDE-33245P (Reference 7.1-10) for a description of the software plans that control the additional IEEE Std. 7-4.3.2 criteria related to the following hardware and software equipment qualification requirements.

- IEEE Std. 7-4.3.2, Criterion 5.4.2, Qualification of existing commercial computers is performed in accordance with the commercial-off-the-shelf (COTS) dedication process in accordance with the Software Development Plan.
- IEEE Std. 7-4.3.2, Criterion 5.4.1, The referencing platform qualification testing is performed with the referencing system functioning with software and diagnostics that are representative of those used in actual operation in accordance with the Software Test Plan.

~~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.~~

~~Radiation: The Q-DCIS components are designed to be qualified (by analysis) to perform safety-related functions over their service life under the specified radiation conditions. The design ensures that the maximum radiation levels at the equipment locations do not exceed the allowed limits.~~

~~Seismic Qualification: The Q-DCIS components are designed to be qualified, by type testing and analysis, to perform safety-related functions correctly when operated within the specified seismic limits, and when mounted in accordance with the specified methods. The Q-DCIS components are qualified in accordance with the requirements of RG 1.100 (IEEE Std. 344). The design ensures that the maximum seismic accelerations at the mounting locations of the equipment do not exceed the allowed limits.~~

~~EMI Qualification: The Q-DCIS components are designed to be qualified by type testing and analysis to perform all safety-related functions when operated within the specified EMI limits. The Q-DCIS components are qualified in conformance to RG 1.180, when mounted in accordance with the specified methods. The Q-DCIS equipment is designed to not be susceptible to electromagnetic disturbances from neighboring modules or cause electromagnetic disturbances to neighboring modules. The EMI qualification design follows the requirements specified in Mil Std. 461E and IEC 61000-4, depending on the specific requirement conditions. The Q-DCIS equipment is qualified to perform within its specifications continuously while exposed to EMI environmental limits at the hardware mounting location. The EMI susceptibility and emissions testing is performed by type testing. In addition to the equipment design considerations, plant-specific actions are required to establish practices to control emission sources, maintain good grounding practices, and maintain equipment and cable separation.~~

7.1.6.6.1.6 System Integrity (IEEE Std. 603, Section 5.5)

The System Integrity criterion requires that the referencing platform's features be adequate to ensure completion of protective actions over the range of transient and steady-state conditions of both the energy supply and the environment enumerated in the design basis. The Q-DCIS meets this requirement through the application of the Equipment Qualification program described in Sections 3.9 through 3.11, and Subsection 7.1.6.6.1.5.

IEEE Std. 7-4.3.2 has additional system integrity requirements related to SSC using software. Refer to LTRs "ESBWR Software Management Program Manual," NEDE-33226P (Reference 7.1-12), and "ESBWR Software Quality Assurance Program Manual," NEDE-33245P (Reference 7.1-10) for a description of the software plans that control the additional IEEE Std. 7-4.3.2 criteria related to the following hardware and software system integrity requirements:

- IEEE Std. 7-4.3.2, Criterion 5.5.1, Design for computer integrity: The referencing system is designed to perform its safety-related function when subjected to design basis conditions.

- IEEE Std. 7-4.3.2, Criterion 5.5.2, Design for test and calibration: The referencing system is designed to perform its safety-related function when undergoing test and calibration in accordance with the Software Development Plan.
- IEEE Std. 7-4.3.2, Criterion 5.5.3, Fault detection and self-diagnostics: Fault detection and self-diagnostics (as performed by platform self-test features) do not adversely affect the capability of the referencing system to perform its safety-related functions in accordance with the Software Development Plan.

The Q-DCIS systems are required to accomplish their safety-related functions under the full range of applicable conditions enumerated in the design bases. Other areas addressed as requirements include adequate system real-time performance for digital computer-based systems to ensure completion of protective action, evaluation of hardware integrity and software integrity (software safety-related analysis, as part of BTP HICB-14 requirements), failure to a safe state upon loss of energy or adverse environmental conditions, and the requirements for manual reset.

The Q-DCIS meets the integrity requirements described in IEEE Std. 603, Section 5.5. The ~~RPS~~ RTIF – NMS platform functions fail to the tripped state. The SSLC/ESF platform and the independent control platform fail~~s~~ to a state where the actuated component remains "as-is" to prevent a control system induced LOCA. Hardware and software failures detected by self-diagnostics cause a trip signal to be generated in the RPS division in which the failure occurs and no trip signal is generated if the failure occurs in a SSLC/ESF or independent control platform division. Single failures of hardware and software do not inhibit manual initiation of protective functions. ~~and complete failures of hardware and software do not inhibit manual initiation of reactor scram, MSIV closure or SLC injection. available in the MCR in accordance with More details of system integrity design considerations are included in the system description subsections of the respective safety-related systems as outlined in Table 7.1-2.~~

7.1.6.6.1.7 Independence (IEEE Std. 603, Section 5.6)

The required independence between redundant portions of a safety-related system, between safety-related systems and the effects of DBEs, and between safety-related systems and other systems is defined. Three aspects of independence are addressed in each case: physical independence, electrical independence, and communication independence. The Q-DCIS design meets these requirements.

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 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 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.

Physical Independence

The Q-DCIS systems have four redundant and independent divisions that are physically independent and separated and that have independent electrical power sources applied to them. Except where fiber optic cable is used, there are no common switches shared by the four divisions. The sensors used for each of the four divisions, are independent and physically separated from one another. All wiring and electrical components are physically separated via isolation barriers or spacing (see Subsection 7.1.3.3.1).~~Communication directly between the four divisions is limited to the minimum, such as trip signals and bypass status signals, and is through proper isolation devices.~~

Electrical Independence

Independence between ~~the~~ safety-related systems ~~and the effects of DBEs~~ is achieved through proper equipment qualification and isolation. ~~Safety-related equipment is qualified for continuous functional capability in the environment at the equipment location, for which DBE conditions are considered.~~ Safety-related systems are totally separated and independent from nonsafety-related systems. When system interfacing is required, electrical isolation is provided via isolation devices (qualified per IEEE Std. 384) and by the use of fiber optic cables.

Communication Independence

Communication between redundant safety channels is limited to a minimum, such as trip signals and bypass status signals, and is through proper isolation devices. In accordance with IEEE Std. 379, 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.) In addition, loss of communication or communication upsets are contained within a single channel and cannot inhibit the ability of redundant channels to perform their functions. Optical couplers and fiber optic cable provide the route for communications.

Communication between safety-related systems and nonsafety-related systems is carried out via fiber optic cable through the required qualified safety-related signal isolation devices (CIMs), and data pathways such as datalinks and gateways (when necessary). Communication from nonsafety-related systems to safety-related systems is prohibited, with the exception of time tagging and NMS calibration data. Additional discussion on this subject is included in Subsection 7.1.3.3. The RTIF, NMS, and SSLC/ESF protection functions have priority over data transmissions, so that data transmissions do not interfere with the RTIF, NMS, or SSLC/ESF protection functions. .~~More details of safety-related system independence design are included in the system description subsections of the respective safety-related systems as outlined in Table 7.1-2.~~

7.1.6.6.1.8 Capability for Testing and Calibration (IEEE Std. 603, Section 5.7)

The capability for testing and calibration of safety-related system equipment is provided during power operation and duplicates the performance of the safety-related function as closely as practicable, as discussed in Sections 7.2 through 7.8. Tests ~~can~~ are capable of being performed

in overlapping segments when testing one safety-related function. Maintenance bypasses of individual functions are provided in the safety-related system channels to enable testing during power operation. For example, the safety-related functions of each safety-related division can be tested on-line with the tested division bypassed from the two-out-of-four voting trip logic. The I&C equipment has built-in self-diagnostic functions to identify critical failures such as loss of power and data errors. The Q-DCIS meets the requirements outlined in this section. (See Subsections 7.1.3.3.6, 7.1.3.3.7, 7.1.3.4 and 7.1.3.5)~~More details of system testing and calibration are included in the system description subsections of the respective safety-related systems as outlined in Table 7.1-2.~~

Safety-related sensors are designed with the capability for test and calibration during reactor operation.~~,~~ Additionally, any exceptions for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).~~with the following two exceptions in the RPS:~~

~~MSIV limit switches, and~~

~~Turbine stop valve (TSV) limit switches.~~

~~These limit switches are not accessible during reactor operation. Although they are tested/checked for operability during reactor operation, they cannot be calibrated until the reactor is shut down.~~

7.1.6.6.1.9 Information Displays (IEEE Std. 603, Section 5.8)

The Information Displays criterion requires that information displays for the referencing platform be designed to be accessible to the operators, display variables for manually controlled actions, display system status information, provide indication of bypasses, and display post-accident monitoring variables in accordance with the HFE process. The Q-DCIS information displays, including displays for manually controlled actions, meet this requirement by the application ~~The information display design is part~~ of the HFE design process described in Chapter 18. This process includes the steps to ensure compliance with regulatory requirements. The information display design conforms to the ~~It also includes~~ guidance offered in RG 1.47 for bypassed and inoperable status indication~~ and in RG 1.97 for PAM instruments as discussed in Section 7.5.1~~.

System Status Indication: The safety-related and nonsafety-related I&C systems are provided with system status information that meets the requirements of IEEE Std. 603, Section 5.8. All pertinent system trip/logic status, parameter data values, equipment functional status and ESF actuator status are displayed to the operator upon request. For safety-related systems, this information is available for each division. Certain information, key to plant operation and status monitoring, is permanently displayed on the large WDP in the MCR. Alarm and annunciation indications are also available in the MCR in accordance with system design requirements. All information available within a division, including post accident monitoring information, can be viewed in a safety-related manner on the VDUs associated with that division. The same divisional information and all nonsafety-related information can be viewed on the nonsafety-related VDUs and WDP.

Indication of Bypasses: For safety-related system protection functions, bypass status is continuously displayed to the operator. ~~in accordance with system design requirements including those for alarms. More details of system bypass and alarm conditions are included in the system description subsections of the respective safety-related systems as outlined in Table 7.1-2.~~

Locations of Displays: Displays in the MCR are either on the main control console or on the large WDP visible and accessible to the operator. The man-machine interface system design includes design requirements and specifications for the classification of locations of displays in the MCR. More detailed descriptions of requirements for the locations of displays are included in Chapter 18.

7.1.6.6.1.10 Control of Access (IEEE Std. 603, Section 5.9)

Administrative control is used to implement access control to vital areas of the plant, including the MCR. Physical security and electronic security devices are provided to ensure only authorized ~~so that~~ and qualified plant personnel are allowed to have access to the Q-DCIS cabinets and consoles. Physical security is described in Section 13.6. In addition to the plant physical security, the Q-DCIS equipment has its own access control devices. Q-DCIS cabinets have doors with keylocks and position switches. Q-DCIS components within the cabinets have keylock switches that are used to control access to special functions (such as, the INOP/OP switch).~~keys to doors, cabinets, and keylock switches and passwords to obtain access to safety-related systems and equipment. Only qualified plant personnel are allowed to exercise operations such as change of setpoints, instrument calibration, equipment testing, and logic bypass operation. Only qualified plant personnel are allowed access to other plant operation switches.~~

Keys, passwords, and other security devices (following the guidance of RG 1.152) are used ~~by qualified plant personnel~~ to ~~enter~~ control access to specific rooms; open specific equipment cabinets; obtain permission for access to enter specific electronic instruments for calibration, testing, and setpoint changes; and, gain access to safety-related system software and data. Safety-related software is not routinely changed at the plant site.

~~An o~~Opening a Q-DCIS cabinet door produces an alarm in the MCR.

There is no access to safety-related system equipment and control through the network from nonsafety-related system equipment. Computer-related access controls and authorization are part of the cyber-security program plan, which is described in the LTRs, "ESBWR Cyber Security Program Plan," NEDO-33295, (Non-Proprietary); and "ESBWR Cyber Security Program Plan," NEDE-33295-P, (Proprietary), (Reference 7.1-8). `

7.1.6.6.1.11 Repair (IEEE Std. 603, Section 5.10)

The Q-DCIS systems provide timely recognition of location, replacement, repair, and adjustment of malfunctioning equipment. Periodic self-diagnostic functions locate the failure to the component level. Through individual division bypassing, the failed component is replaced or repaired on line without affecting the safety-related system protection function. During repairs the trip logic is two-out-of-three so that the single failure criterion is still met. ~~Although it is not~~

~~possible to bypass more than one division at a time, the Q-DCIS system performs its safety-related functions with three out of four divisions available, in the presence of a single failure.~~

7.1.6.6.1.12 Identification (IEEE Std. 603, Section 5.11)

The Q-DCIS system equipment conforms to the identification requirements specified in IEEE Std. 603, Section 5.11. Color-coding is used as one of the major methods of identification. Safety-related equipment is distinctly marked in each redundant division of a safety-related system. Hardware component or equipment units have an identification label or nameplate. See Subsection 8.3.1.3 for additional details. For digital computer-based system equipment, versions of computer hardware, programs, and software are distinctly identified. Configuration management formalizes system component and software identification.

IEEE Std. 7-4.3.2 has additional identification requirements related to SSC using software. Refer to LTRs "ESBWR Software Management Program Manual," NEDE-33226P (Reference 7.1-12), and "ESBWR Software Quality Assurance Program Manual," NEDE-33245P (Reference 7.1-10) for a description of the software plans that control the additional IEEE Std. 7-4.3.2 requirement for the identification and retrieval of software identification using software maintenance tools.

7.1.6.6.1.13 Auxiliary Features (IEEE Std. 603, Section 5.12)

Safety-related I&C system auxiliary supporting features~~, such as safety-related electrical system equipment including batteries and inverters, satisfy the requirements of~~ conform to IEEE Std. 603, Section 5.12 where applicable and maintain the supported safety-related system performance at an acceptable level.

The Q-DCIS is supported by four divisions of safety-related uninterruptible power as described in Subsection 8.3.2. DC batteries supply power if there is a loss of off-site and on-site AC power.

HVAC, whether active or passive is a key auxiliary supporting system that maintains the necessary environmental conditions for both the safety-related and nonsafety-related I&C equipment. Under normal operating conditions when offsite power is available or when diesel generators are running, HVAC systems control the temperature and humidity of all I&C equipment. Under a loss of power condition, including Station Blackout (SBO), batteries provide continuous safety-related I&C operation for 72 hours, and continued operation of the nonsafety-related I&C equipment for two hours. However, during a loss of power condition, active HVAC is not available to the safety-related CB or RB equipment, except in the CRHA as noted below.

The Q-DCIS and its safety-related battery-operated support equipment remain powered and the heat generated is removed passively (except possibly by small chassis mounted fans); the Q-DCIS and support equipment is qualified to the worst case anticipated ~~for the expected~~ temperature rise. Battery-backed N-DCIS equipment is only powered for two hours if offsite and diesel generator power is lost; during that interval the batteries supplying the N-DCIS also power nonsafety-related HVAC in the CRHA. If the nonsafety-related redundant HVAC is not available, safety-related temperature sensors with two-out-of-four logic trip the control room

power that feeds the nonsafety-related I&C. The safety-related I&C that remains operable is qualified for the resulting temperature rise with passive heat removal. This scheme protects the equipment and maximizes operator comfort. Additional description of the HVAC design, including the use of room coolers powered by the ancillary diesel generators is included in Chapter 8, Chapter 9, and Appendix 19A.

7.1.6.6.1.14 Multi-Unit Stations (IEEE Std. 603, Section 5.13)

The multi-unit station criteria do not apply to the standard single unit plant design submitted for NRC certification. ~~For multiple unit designs only the N-DCIS would have common network components as necessary to control and monitor common hardware and systems. The Q-DCIS of multiple units would have neither shared components nor shared divisions. The operation or failure of shared N-DCIS components does not affect the performance of the Q-DCIS.~~

7.1.6.6.1.15 Human Factors Considerations (IEEE Std. 603, Section 5.14)

The I&C system design includes a HFE design process that is consistent with the requirements outlined in NUREG-0711, "Human Factors Engineering Program Review Model." The HFE process defines a comprehensive, iterative design approach for the development of a human-centered control and information infrastructure and is described in Chapter 18.

7.1.6.6.1.16 Reliability (IEEE Std. 603, Section 5.15)

The degree of redundancy, diversity, testability, and quality of the safety-related I&C design achieves the necessary functional reliability. Safety-related equipment is provided under GEH's 10 CFR 50 Appendix B quality program. The BTP HICB-14 and IEEE 7.4.3.2 (as endorsed by RG 1.152) guidance followed for software development processes achieves reliable software design and implementation. The Design Reliability Assurance Program (D-RAP) described in Section 17.4 confirms that any quantitative or qualitative reliability goals established for the protection systems have been met. To achieve defense against common mode failure, the design includes defense-in-depth and diversity measures including the incorporation of the DPS described in Section 7.8. Reference 7.1-4 provides specific information on the redundancy and diversity used in safety-related I&C systems. The Q-DCIS is included in the consideration of the probabilistic risk assessment (PRA). (Refer to Chapter 19.)

7.1.6.6.1.17 Automatic Control (IEEE Std. 603, Sections 6.1 and 7.1)

The RTIF- ~~and~~ NMS, and ATWS/SLC logic automatically initiates reactor trip and the RTIF for LD&IS (non-MSIV), SSLC/ESF and VBIF logic automatically actuates the ESF that mitigate the consequences of ~~AOOs and~~ DBEs. These automatic protection actions are implemented through two-out-of-four voting logic whenever one or more process variables reach their actuation setpoint. Variables are monitored and measured by each of the RTIF -~~,~~ NMS, ATWS/SLC, ~~and~~ SSLC/ESF, and VBIF divisions.

Plant-specific setpoint analyses determine the protection systems' instrument setpoints using the methodology described in Reference 7.1-9. The GEH setpoint methodology uses plant-specific setpoint analyses to ensure that the combination of characteristics of the instruments such as

range, accuracy and resolution provide the required high probability that the analytical limits in Chapter 15 analyses are not exceeded for the safety-related control system components and systems of the safety-related I&C. The response times of the I&C systems are assumed in the safety-related analyses and verified by plant specific surveillance testing or system analyses. The Q-DCIS application software, hardware processing rates, and internal and external communication system design ensures that the real-time performance of the safety-related control systems is deterministic.

7.1.6.6.1.18 Manual Control (IEEE Std. 603, Sections 6.2 and 7.2)

Each protective action can be manually initiated at the system level, in conformance to RG 1.62, and at the division level in conformance to IEEE Std. 603, Sections 6.2 and 7.2. The manual initiation satisfies divisional rules for independence and separation. Two manual actions, each in a separate division, are required in order to satisfy the two-out-of-two system logic or the two-out-of-four division logic that initiates a reactor trip in the RPS and ESF functions in the SSLC/ESF systems.

The operator can manually initiate the ESF functions by actuating manual switches in two-out-of-four divisions; thus, satisfying the two-out-of-two system initiation logic. The ESF functions that use squib valves use a redundant two-step arm and fire sequence. This prevents single failures from firing or from inhibiting the firing of the squib valves. The squib valves are the GDCS pool injection valves, the suppression pool injection valves, the GDCS deluge valves, the ADS DPV, and the SLC injection valves. To manually initiate the GDCS short-term and long-term injection systems, a low-pressure signal must be present in the RPV. This prevents inadvertent manual initiation of the system during normal reactor operation.

The operator can manually initiate reactor emergency shutdown, reactor trip, with control rods by using any of three different methods using redundant or diverse controls. The manual reactor trip occurs independently of the automatic trip logic and sensor status.

The two manual scram switches, the Reactor Mode Switch, and the four divisional manual trip switches (per protective system) are located in the MCR and are easily accessible to the operator.

The two MCR manual scram switches, the RSS manual scram switches share no equipment with the automatic controls and require no software for their operation, and the DPS manual scram switches share a minimum of equipment with the automatic controls. The MCR and RSS manual scram switches are directly connected to the power feed for the load drivers that are, in turn, connected directly to the scram pilot valve solenoids. The DPS manual scram switches directly control the scram air header dump valves

After manual initiation, the protective actions go to completion in conformance to IEEE Std. 603, Section 5.2 as described in Subsection 7.1.6.6.1.3. The manual initiation of a protective action performs all actions carried out by automatic initiation.

In the Q-DCIS design, there are no protective actions that have not been selected of automatic control. There are also no manual actions necessary to maintain safe conditions after the completion of protective actions for 72 hours after a DBE.

The manual controls are designed so that the information provided, display content and location are taken into consideration for easy operator access and action in the MCR. Further information about the design of manual controls and HFE considerations, as well as plant manual operation procedure requirements, are included in Chapter 18. Additionally, manual controls for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h)~~Additional details of automatic and manual controls at system levels (RTIF, NMS, and SSLC/ESF) are included in Subsections 7.2.1, 7.2.2, and 7.3.5, respectively~~.

7.1.6.6.1.19 Interaction Between the Sense and Command Features and Other Systems (IEEE Std. 603, Section 6.3)

The Q-DCIS protection systems are totally separate and independent from the nonsafety-related control systems, in accordance with GDC 24. Any failure of nonsafety-related systems does not affect safety-related protection systems or prevent them from performing their safety-related functions. If one safety-related division fails, any nonsafety-related control system can be isolated from the failure by using data validation techniques to select a valid control input from the three other remaining divisions. The communication path broadcasts one way - from the protection system to the N-DCIS. A failure of communication does not affect the protection function. Therefore, providing additional redundancy to isolate the protection system from communication failure is not required and not applied. For further detail on communication between the Q-DCIS and the N-DCIS (including transmission of time tagging signals) see Subsection 7.1.3.3.

Sensors used by safety-related I&C systems are not shared with nonsafety-related control systems. Calculated safety-related signals such as APRMs can be used, after isolation, by nonsafety-related control systems.~~ Additional descriptions of the RTIF, NMS, and SSLC/ESF are included in Subsections 7.2.1, 7.2.2, and 7.3.5, respectively.~~

7.1.6.6.1.20 Derivation of System Inputs (IEEE Std. 603, Section 6.4)

To the extent feasible, the protection system inputs are derived from signals that directly measure the designated process variables. ~~The two RPS sensing inputs that are not~~An example of an in direct measure~~s of the variables are the RPV water level and~~is the loss of feedwater flow in the RPS scram logics. ~~The RPV water level is measured by the differential pressure derived from the sensing line with a reference point. This method is a proven technology in the BWR applications.~~ The loss of the feedwater flow variable is represented by the loss of the power generation bus signal. When the power to the feedwater pump motor is lost, the feedwater flow is also immediately lost. The use of loss of power generation bus signals to represent the loss of feedwater flow signal meets the requirements of the safety-related analysis of Chapter 15, because it is the only credible way that all feedwater flow can be lost. Additionally, derivation of system inputs for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).~~The RPS initiating circuits and SSLC/ESF logics are described in Subsections 7.2.1 and 7.3.5, respectively.~~

7.1.6.6.1.21 Capability for Testing and Calibration (IEEE Std. 603, Section 6.5)

The operational availability of the protection system sensors can be checked by perturbing the monitored variables, by cross-checking between redundant channels that have a known relationship with each other and that have read-outs available, or by introducing and varying a substitute input to the sensor of the same nature as the measured variable. The four-division RTIF~~,~~ -NMS, ~~and~~ SSLC/ESF, and independent control platform logic provides at least two valid divisions for crosschecking of monitored variables. The third division also has the capability to be available for crosschecking, depending on the maintenance bypass status. When one division is placed into maintenance bypass mode, the condition is alarmed in the MCR and the division logic automatically becomes a two-out-of-three voting scheme. Most sensors and actuators are provisioned for actual testing and calibration during power operation with the exceptions described in Sections 7.2 through 7.8. See Subsections 7.1.3.3.5, 7.1.3.3.6, 7.1.3.3.7, and 7.1.3.5 for additional details.

In the Q-DCIS design a 24 month calibration periodicity is implemented to ensure accuracy and integrity of signal development, transmission and processing. Digital I&C equipment utilized in the I&C design is qualified for the environment in which it is located so that it retains its calibration during the post accident time period. Additionally, capability for testing and calibration for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.22 Operating Bypasses (IEEE Std. 603, Sections 6.6 and 7.4)

Operating bypasses are implemented in the Q-DCIS. One example of such operating bypasses is associated with the trip function dependence on reactor operating mode. The requirements of IEEE Std. 603 are met by the safety-related I&C operating bypass design. Specific descriptions of safety-related system operating bypasses are included in Subsections 7.2.1.5 and 7.3.5.2. Operating bypasses are automatically removed as described in Subsections 7.2.1.5 and 7.3.5.2. Additionally, operating bypasses for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.23 Maintenance Bypass (IEEE Std. 603, Sections 6.7 and 7.5)

Maintenance bypass capability is incorporated in the design of the Q-DCIS. This permits equipment maintenance, testing, and repair of one individual division with the plant operating and without initiating any protection functions. The single failure criterion is met under this bypass condition. Although it is possible to bypass only one division at a time, the Q-DCIS design is able to supply its safety-related functions even with a two-division failure. Maintenance bypass is always alarmed or indicated in the MCR. Maintenance bypass for safety-related I&C systems is typically applied through a joystick bypass switch with exclusive logic that allows only one division, out of four, to be bypassed at any given time. Maintenance bypasses are initiated manually by the plant operator per administrative control. Additionally, maintenance bypasses for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h). ~~Specific descriptions of safety-related system maintenance bypasses are included in Subsections 7.2.1.5.2.2 and 7.3.5.2.~~

7.1.6.6.1.24 Setpoints (IEEE Std. 603, Section 6.8)

For automatic protective devices, safety-related setpoints and setpoints having significant safety functions for the Technical Specification required limiting safety system settingsInstrument setpoints are determined by the methodology described in Reference 7.1-9, which is based on the previously NRC-approved GE Setpoint Methodology, NEDC-31336P-A (Reference 7.1-11), as updated to reflect a graded approach as provided in BTP HICB-12 and information contained in Regulatory Information Summary (RIS) 2006-017, "NRC Staff Position on the Requirements of 10 CFR 50.36, 'Technical Specifications,' Regarding Limiting Safety System Settings During Periodic Testing and Calibration of Instrument Channels." The GEH setpoint methodology uses plant-specific setpoint analyses to ensure that the instruments' range, accuracy, and resolution meet the performance requirements assumed in the safety-related analyses in Chapter 15 for the safety-related control system components and systems. This methodology meets the requirements of IEEE Std. 603, Section 6.8. The response times of the I&C systems assumed in the safety-related analyses are verified by plant specific surveillance testing or system analyses.

7.1.6.6.1.25 Electrical Power Sources (IEEE Std. 603, Section 8.1)

The Q-DCIS protection system cabinets and components are supported by two independent power sources. Each division of safety-related I&C is powered by two UPS that can supply 120 VAC from either offsite power, diesel generator power, or safety-related batteries (for 72 hours). Either of the two power sources allows Q-DCIS operation. These power sources comply with IEEE 603 as described in Subsection 7.1.6.6.1. See Subsection 7.1.3.3.7 for additional description. Two divisions of the uninterruptible 120 VAC are also used as the power sources for the solenoids of the scram pilot valves. Two divisions of power sources are used for the backup scram valves solenoids, for scram reset permissive logic. Specific dDescriptions of safety-related system power sources are included in Subsections 7.2.1.2 and 7.2.2.2, as well as in Chapter 8.

7.1.6.6.1.26 Non-electrical Power Sources (IEEE Std. 603, Section 8.2)

To perform the scram protection function, each HCU furnishes pressurized water for the hydraulic scram, following a signal from the RPS. With low CRD HCU Accumulator Charging Pressure, the CRD system sounds an alarm in the MCR. A loss of nitrogen decreases the nitrogen pressure and actuates a pressure switch. Additionally, a float type level switch actuates an alarm if water leaks past the piston barrier and collects in the accumulator instrumentation block. An alarm is issued for low CRD charging header pressure that keeps the individual accumulators charged; if the CRD pressure decreases further the reactor is automatically scrammed while there is still hydraulic pressure to do so.

The SLC system injection status is provided by the MCR indication of accumulator pressure. Operation of the accumulator nitrogen charging and makeup to accommodate small losses is manual. MCR alarms are provided for high, low, and low-low conditions of accumulator pressure and low and low-low conditions of accumulator solution level. If a non-electrical power source is required for a safety function, then the source of the power is classified as safety-related and complies with IEEE 603 as described in Subsection 7.1.6.6.1. Additionally,

non-electrical power sources for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.27 Maintenance Bypass (IEEE Std. 603, Section 8.3)

The Q-DCIS components are powered by redundant, independent, and separated uninterruptible power supplies appropriate to their division with battery backup (per division) for at least 72 hours. The UPS have both an automatic static transfer switch and a manual maintenance switch and either supply (per division) can operate its Q-DCIS division. Using the inverter's automatic or manual bypass and shutting down either the associated batteries, chargers or inverters technically makes the division inoperable but, in fact the division remains fully functional, losing only the ability to operate for 72 hours should offsite or diesel power be lost (it operates for approximately 36 hours under those circumstances). Operation of the Q-DCIS when one of its power supplies is in maintenance bypass is appropriately alarmed. In the very unlikely event that an entire division is without power the failsafe RTIF/NMS interprets the condition as a trip (unless bypassed) and the SSLC/ESF does not assume a trip. Because only two divisions are necessary to satisfy the safety requirements, no functionality is lost. The condition of a division without power triggers an alarm. Refer to the discussion of GDC 18 in DCD Subsection 8.3.1.2.1 for maintenance provisions of safety-related power supplies. Further discussion of the safety-related power supplies is provided ~~in~~throughout Chapter 8.

A single non-electrical redundant power source (e.g., one of two parallel accumulators, one of two squibs) may be taken to "maintenance bypass" (i.e., isolated) without adversely impacting the safety function of any system.

For those non-electrical power sources having a degree of redundancy of one, taking it to maintenance bypass does not adversely impact the reliability of any safety-related system to perform its safety functions. Additionally, manual bypassing of power sources for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.28 Cyber Security (IEEE Std. 7-4.3.2)

The security measures included in RG 1.152 are evaluated and incorporated in the Q-DCIS design and include plant hardware and software security measures. The software development process plans are developed with the security measures.

The comprehensive cyber security program plan (Reference 7.1-8) identifies security risks and outlines appropriate procedures. The plant ensures that hardware, controls, and data networks comprising the control network cannot be disrupted, interrupted, or negatively affected by unauthorized users or external systems. Reference 7.1-8 documents the design commitments, which meet the applicable guidance of RG 1.152, Section C.2, and Positions 2.1 through 2.9.

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

Table 7.1-1

I&C Systems Regulatory Requirements Applicability Matrix

System																													
Applicable Criteria Guidelines: SRP NUREG 0800, Section 7.1	Reference Standard	RPS (Q)	NMS (Q)	SPTM Function (Q)	ADS (Q)	GDCS (Q)	LD&IS (Q & N)	CRHS (Q)	SSLC /ESF (Q)	VB Isolation Function (Q)	SLC (Q)	RSS (Q & N)	RWCU /SDC (N)	ICS (Q)	PAM (Q & N)	CMS (Q &N)	PRMS (Q &N)	ARMS (N)	Interlock Systems (N)	NBS (Q & N)	RC&IS (N)	FWCS (N)	PAS (N)	SB&PC (N)	NMS (N)	CIS(N)	DPS(N) ATWS/SLC (Q)	Q DCIS (Q)	N DCIS (N)
10 CFR																													
50.55a(a)(1)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
50.55a(h)	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X			X							X	X	
50.34(f)(2)(v)(I.D.3)		X	X	X	X	X	X	X	X	X	X			X	X	X	X			X							X	X	
50.34(f)(2)(xvii)(II.F.1)															X	X	X	X											
50.34(f)(2)(xviii)(II.F.2)															X					X									
50.34(f)(2)(xiv)(II.E.4.2)					X	X	X	X	X	X																			
50.34(f)(2)(xix)(II.F.3)															X	X	X	X											
50.34(f)(2)(xxiv)(II.K.3.23)															X														
50.44(c)(4)																X													
50.62											X										X	X					X#	X	
52.47(a)(1)(iv)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
52.47(a)(1)(vi)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
52.47(a)(1)(vii)		N/A																											
52.47(a)(2)		X	X	X	X	X	X	X	X	X	X	X		X	X	X	X		X	X							X	X	
52.47(b)(2)(i)		N/A																											
50.34(f)(2) xii [II.E.1.2]		N/A																											
50.34(f)(2) xx [II.G.1]		N/A																											
50.34(f)(2) xxii [II.K.2.9]		N/A																											
50.34(f)(2) xxiii [II.K.2.10]		X							X					X															
52.79(c)		N/A																											

Table 7.1-1

I&C Systems Regulatory Requirements Applicability Matrix

System																													
Applicable Criteria Guidelines: SRP NUREG 0800, Section 7.1	Reference Standard	RPS (Q)	NMS (Q)	SPTM Function (Q)	ADS (Q)	GDCS (Q)	LD&IS (Q & N)	CRHS (Q)	SSLC /ESF (Q)	VB Isolation Function (Q)	SLC (Q)	RSS (Q & N)	RWCU /SDC (N)	ICS (Q)	PAM (Q & N)	CMS (Q &N)	PRMS (Q &N)	ARMS (N)	Interlock Systems (N)	NBS (Q & N)	RC&IS (N)	FWCS (N)	PAS (N)	SB&PC (N)	NMS (N)	CIS(N)	DPS(N) ATWS/SLC (Q)	Q DCIS (Q)	N DCIS (N)
General Design Criteria																													
1		X	X	X	X	X	X	X	X	X	X	X		X	X	X	X		X	X							X	X	X
2	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								X	X
4	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								X	X
13	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
19		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
20	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X			X														X	
21	IEEE Std. 603 & IEEE Std. 338	X	X	X	X	X	X	X	X	X	X			X														X	
22	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X			X														X	
23	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X			X														X	
24	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
25	IEEE Std. 603	X	X	X															X									X	
29	IEEE Std. 603	X	X	X																	X							X	
SRM on SECY 93-087																													
II.Q	BTP HICB 19	X	X	X	X	X	X	X	X	X	X			X						X							X	X	X
II.T															X	X	X											X	X
Regulatory Guides (RG)																													
1.22		X	X	X	X	X	X	X	X	X	X			X													X	X	
1.47	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X			X		X	X										X	X	
1.53	IEEE Std. 379 IEEE Std. 603	X	X	X	X	X	X	X	X	X	X	X		X		X	X										X	X	
1.62	IEEE Std. 603	X		X	X	X	X	X	X	X	X			X													X	X	

~~Table 7.1-1~~

~~I&C Systems Regulatory Requirements Applicability Matrix~~

~~System~~																													
~~Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1~~	~~Reference Standard~~	~~RPS (Q)~~	~~NMS (Q)~~	~~SPTM Function (Q)~~	~~ADS (Q)~~	~~GDCS (Q)~~	~~LD&IS (Q & N)~~	~~CRHS (Q)~~	~~SSLC /ESF (Q)~~	~~VB Isolation Function (Q)~~	~~SLC (Q)~~	~~RSS (Q & N)~~	~~RWCU /SDC (N)~~	~~ICS (Q)~~	~~PAM (Q & N)~~	~~CMS (Q &N)~~	~~PRMS (Q &N)~~	~~ARMS (N)~~	~~Interlock Systems (N)~~	~~NBS (Q & N)~~	~~RC&IS (N)~~	~~FWCS (N)~~	~~PAS (N)~~	~~SB&PC (N)~~	~~NMS (N)~~	~~CIS(N)~~	~~DPS(N) ATWS/SLC (Q)~~	~~Q DCIS (Q)~~	~~N DCIS (N)~~
~~1.75~~	~~IEEE Std. 384~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~		~~X~~		~~X~~	~~X~~		~~X~~	~~X~~							~~X~~	~~X~~	
~~1.89~~	~~IEEE Std. 323~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~			~~X~~						~~X~~							~~X~~	~~X~~	
~~1.97~~	~~IEEE Std. 497~~		~~X~~	~~X~~											~~X~~	~~X~~	~~X~~	~~X~~										~~X~~	~~X~~
~~1.100~~		~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~		~~X~~	~~X~~	~~X~~	~~X~~			~~X~~							~~X~~	~~X~~	
~~1.105~~	~~ANSI/ISA-S67.04.01~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~			~~X~~		~~X~~	~~X~~		~~X~~	~~X~~							~~X~~	~~X~~	
~~1.118~~	~~IEEE Std. 338~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~		~~X~~		~~X~~	~~X~~		~~X~~								~~X~~	~~X~~	
~~1.151~~	~~ANSI/ISA-S67.02.01~~[@]					~~X~~					~~X~~		~~X~~	~~X~~		~~X~~			~~X~~	~~X~~		~~X~~				~~X~~	~~X~~		
~~1.152*~~	~~IEEE Std. 7-4.3.2~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~			~~X~~		~~X~~	~~X~~			~~X~~							~~X~~	~~X~~	~~X~~
~~1.153~~	~~IEEE Std. 603~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~		~~X~~		~~X~~	~~X~~			~~X~~							~~X~~	~~X~~	
~~1.168*~~	~~IEEE Std. 1012~~ ~~IEEE Std. 1028~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~			~~X~~		~~X~~	~~X~~			~~X~~							~~X~~	~~X~~	~~(1)~~
~~1.169*~~	~~IEEE Std. 828~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~			~~X~~		~~X~~	~~X~~			~~X~~							~~X~~	~~X~~	~~(1)~~
~~1.170*~~	~~IEEE Std. 829~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~			~~X~~		~~X~~	~~X~~			~~X~~							~~X~~	~~X~~	~~(1)~~
~~1.171*~~	~~IEEE Std. 1008~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~			~~X~~		~~X~~	~~X~~			~~X~~							~~X~~	~~X~~	~~(1)~~
~~1.172*~~	~~IEEE Std. 830~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~			~~X~~		~~X~~	~~X~~			~~X~~							~~X~~	~~X~~	~~(1)~~
~~1.173*~~	~~IEEE Std. 1074~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~			~~X~~		~~X~~	~~X~~			~~X~~							~~X~~	~~X~~	~~(1)~~
~~1.180~~	~~IEEE Std. 1050~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~[‡‡]	~~X~~[‡‡]	~~X~~	~~X~~[‡‡]	~~X~~[‡‡]	~~X~~[‡‡]	~~X~~[‡‡]	~~X~~[‡‡]	~~X~~	~~X~~[‡‡]	~~X~~[‡‡]	~~X~~[‡‡]	~~X~~[‡‡]	~~X~~[‡‡]	~~X~~[‡‡]	~~X~~[‡‡]	~~X~~	~~X~~[‡‡]
~~1.204~~	~~IEEE Std. 1050~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~1.209~~	~~IEEE Std. 323~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~		~~X~~	~~X~~	~~X~~	~~X~~			~~X~~							~~X~~	~~X~~	
~~Branch Technical Positions (BTP)~~																													
~~BTP HICB-1~~	~~IEEE Std. 603~~					~~X~~													~~X~~									~~X~~	
~~BTP HICB-3~~	~~IEEE Std. 603~~	~~N/A~~																											

Table 7.1-1

I&C Systems Regulatory Requirements Applicability Matrix

		System																											
Applicable Criteria Guidelines: SRP NUREG 0800, Section 7.1	Reference Standard	RPS (Q)	NMS (Q)	SPTM Function (Q)	ADS (Q)	GDCS (Q)	LD&IS (Q & N)	CRHS (Q)	SSLC /ESF (Q)	VB Isolation Function (Q)	SLC (Q)	RSS (Q & N)	RWCU /SDC (N)	ICS (Q)	PAM (Q & N)	CMS (Q &N)	PRMS (Q &N)	ARMS (N)	Interlock Systems (N)	NBS (Q & N)	RC&IS (N)	FWCS (N)	PAS (N)	SB&PC (N)	NMS (N)	CIS(N)	DPS(N) ATWS/SLC (Q)	Q DCIS (Q)	N DCIS (N)
BTP HICB-4		N/A																											
BTP HICB-6	IEEE Std. 603	N/A																											
BTP HICB-8	Refer to RG 1.22	X	X	X	X	X	X	X	X	X	X			X													X	X	
BTP HICB-9	Refer to RG 1.153	X																										X	
BTP HICB-10	Refer to RG 1.97		X	X											X		X	X										X	X
BTP HICB-11	Refer to RG1.75 RG 1.153	X	X	X	X	X	X	X	X	X	X	X		X		X	X		X	X							X	X	X
BTP HICB-12	Refer to RG 1.105	X	X	X	X	X	X	X	X	X	X			X		X	X			X							X	X	X
BTP HICB-13	Refer to RG 1.153	N/A																											
BTP HICB-14*	Refer to RG 1.152	X	X	X	X	X	X	X	X	X	X	X		X		X	X			X							X	X	X
BTP HICB-16		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
BTP HICB-17*	Refer to RG 1.22, 1.47, 1.53, 1.118, 1.152 & 1.153	X	X	X	X	X	X	X	X	X	X	X		X		X	X		X	X							X	X	X
BTP HICB-18*	Refer to RG 1.152	X	X	X	X	X	X	X	X	X	X	X		X		X	X		X	X							X	X	X
BTP HICB-19*	NUREG/CR-6303	X	X	X	X	X	X	X	X	X	X			X						X		X					X	X	X
BTP HICB-21*	NUREG/CR-6083	X	X	X	X	X	X	X	X	X	X	X		X		X	X			X							X	X	X

Notes:
Q=Safety-related, N=Nonsafety-related
X = The code or regulation is applicable to the specified system.
N/A = The code or regulation is not applicable to the ESBWR design.
(1) = Parts or all of this code or regulation are voluntarily invoked for the specified system..
*These criteria are addressed with the digital computer-related functions of the Q DCIS
††N DCIS hardware uses industrial methods for EMI/EMF compliance
#Initiates the 10 CFR 50.62 ARI, SLC and FW runback and trip functions as described in Section 7.8.
@ Sections of the ANSI/ISA standard that are not specific to safety-related systems, but provide guidance on design practices for tubing, vents, & drains apply to identified (N) systems.

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																			N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform		Network Segments			
	RTIF						NMS																
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	GENE	PIP A/B	BOP	PCF
10 CFR																							
50.55a(a)(1)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
50.55a(h)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
50.34(f)(1)(v) [II.K.3.13]								X				X	X	X									
50.34(f)(1)(x) [II.K.3.28]												X											
50.34(f)(2)(iii) [I.D.1]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
50.34(f)(2)(iv) [I.D.2]																				X			
50.34(f)(2)(v) [I.D.3]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				X
50.34(f)(2)(viii) [II.B.3]								X			X												
50.34(f)(2)(x) [II.D.1]								X			X												
50.34(f)(2)(xi) [II.D.3]								X				X											
50.34(f)(2)(xiv) [II.E.4.2]	X		X					X	X														

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																			N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform		Network Segments			
	RTIF						NMS																
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	GENE	PIP A/B	BOP	PCF
50.34(f)(2)(xv) [II.E.4.4]								X	X													X	
50.34(f)(2)(xvii) [II.F.1]								X		X	X												X
50.34(f)(2)(xviii) [II.F.2]							X	X				X											X
50.34(f)(2)(xix) [II.F.3]								X		X	X	X											X
50.34(f)(2)(xxi) [II.K.1.22]	X	X						X						X							X		
50.34(f)(2)(xxiii) [II.K.2.10]		X						X						X									
50.34(f)(2)(xxiv) [II.K.3.23]																							X
50.34(f)(2)(xxvi) [III.D.1.1]								X	X														X
50.34(f)(2)(xxvii) [III.D.3.3]								X		X	X												X
50.34(f)(2)(xxviii) [III.D.3.4]								X		X						X							
50.44(c)(4)								X			X												

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																			N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform		Network Segments			
	RTIF						NMS																
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	GENE	PIP A/B	BOP	PCF
50.49	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																						
50.62							X	X						X					X	X	X	X	
50.63	X	X	X			X		X	X				X	X		X							
52.47(a)(21)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
52.47(b)(1)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
52.47(a)(25)	NA																						
52.47	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
52.47(c)(2)	NA																						
GENERAL DESIGN CRITERIA																							
1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																			N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform		Network Segments			
	RTIF						NMS																
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	GENE	PIP A/B	BOP	PCF
4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
10	X	X					X																
12	X	X					X													X			
13	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
15	X		X					X	X			X											
16	X		X					X	X									X					
19	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
20	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
21	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
22	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
23	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																			N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform		Network Segments			
	RTIF						NMS																
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	GENE	PIP A/B	BOP	PCF
24	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
25	X	X					X													X			
26	X	X				X	X												X	X			
27	X	X				X	X												X	X			
28																	X			X			
29	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
30								X	X			X											
33								X				X	X	X							X		
34								X						X									
35								X				X	X	X	X				X				
37								X				X	X	X	X				X				

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																			N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform		Network Segments			
	RTIF						NMS																
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	GENE	PIP A/B	BOP	PCF
38																					X		
41								X			X											X	
42																						X	
43								X			X											X	
44														X									
63								X															X
64								X		X	X												X
SRM on SECY 93-087																							
II.Q	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
II.T								X												X			X
Regulatory Guides (RG)																							
1.22	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																			N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform		Network Segments			
	RTIF						NMS																
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	GENE	PIP A/B	BOP	PCF
1.45								X	X	X	X												
1.47	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.53	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.62	X	X	X					X	X			X	X	X		X		X	X				
1.75	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.89	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																						
1.97(10)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.100	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																						
1.105	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
1.118	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.151 (8)		X		X	X	X			X		X	X	X	X	X				X		X	X	
1.152(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																			N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform		Network Segments			
	RTIF						NMS																
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	GENE	PIP A/B	BOP	PCF
1.153	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.168(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.169(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.170(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.171(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.172(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.173(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.180(9)	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																						
1.204	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.209	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																						
Branch Technical Positions (BTP)																							
BTP HICB-1								X					X								X		

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																			N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform		Network Segments			
	RTIF						NMS																
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	GENE	PIP A/B	BOP	PCF
BTP HICB-3	N/A																						
BTP HICB-6	N/A																						
BTP HICB-8	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
BTP HICB-9	X	X				X																	
BTP HICB-10(10)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
BTP HICB-11	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
BTP HICB-12	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
BTP HICB-13	N/A																						
BTP HICB-14(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
BTP HICB-16	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
BTP HICB-17(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
BTP HICB-18(7)	X	X					X	X										X	X				

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																			N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform		Network Segments			
	RTIF						NMS																
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	GENE	PIP A/B	BOP	PCF
BTP HICB-19(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
BTP HICB-21(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				

Notes:

(1) LD&IS (non-MSIV) controls the safety-related actuators (for the isolation valves and dampers) associated with the following nonsafety-related systems: RWCU/SDC, FAPCS, EFDS, CIS, CWS, CMS, HPNSS, RBVS, and FBVS. RWCU/SDC provides safety-related sensor inputs to LD&IS (non-MSIV). The regulatory requirements associated with these actuators and sensors are addressed as part of LD&IS.

(2) CBVS includes the CRHS and CRHAVS subsystems and EFUs.

(3) SSLC/ESF includes RSS, MCRP and safety-related VDUs.

(4) Includes the NBS sensors associated with ATWS/SLC.

(5) SSLC/ESF platform column for CRD includes safety-related sensors associated with control rod separation detection.

(6) The following safety-related systems have logic implemented on multiple platforms in support of their protective functions: CMS, CRD, LD&IS, NBS and SLC. Refer to DCD Sections 7.2, 7.3, 7.4, and 7.5 for detailed descriptions of the system functions.

(7) These criteria are addressed with digital computer-related functions of the Q-DCIS and N-DCIS.

(8) Sections of the ANSI/ISA standard that are not specific to safety-related systems, but provide guidance on design practices for tubing, vents and drains apply to the systems associated with the N-DCIS network segments.

(9) Hardware associated with the N-DCIS network segments uses industrial methods for EMI/EMF/RFI/EMC compliance.

(10) The ESBWR I&C conforms to RG 1.97 and applies the guidance in IEEE std. 497. RG 1.97 endorses IEEE Std. 497 (with clarifications and exceptions stated in RG 1.97) and the use of the HFE development process to determine the human actions during and following accident scenarios. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

Table 7.1-2

I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference

		Q-DCIS																		
		RTIF - NMS PLATFORM							SSLC/ESF PLATFORM										INDEPENDENT CONTROL PLATFORM	
		RTIF						NMS												
IEEE Std. 603 Section	Functions (1)	RTIF	RPS	LD&IS (MSIV Only) (6)	CMS (includes SPTM) (6)	NBS (6)	CRD (6)	NMS (3)	SSLC/ESF (4)	LD&IS (Non-MSIV) (2)&(6)	PRMS	CMS (6)	NBS (includes ADS) (6)	GDCS	ICS	SLC (6)	CBVS (7)	CRD (6)	VBIF	ATWS / SLC (5),(6)&(7)
4.1	Design basis events	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.2	Safety-related functions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1 7.5.5.3.1	7.1.6.6.1.1 7.5.5.3.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.3	Permissive conditions for operating bypasses	7.1.6.6.1.1	7.1.6.6.1.1 7.2.1.3.1	7.1.6.6.1.1 7.3.3.3.1	7.1.6.6.1.1 7.2.3.3.1	7.1.6.6.1.1 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.1	7.1.6.6.1.1 7.2.2.3.1	7.1.6.6.1.1 7.3.5.3.1	7.1.6.6.1.1 7.3.3.3.1	7.1.6.6.1.1 7.5.3.3.1	7.1.6.6.1.1 7.5.2.3.1	7.1.6.6.1.1	7.1.6.6.1.1 7.3.1.2.3.1	7.1.6.6.1.1 7.4.4.3.1	7.1.6.6.1.1 7.4.1.3.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1 7.3.6.3.1	7.1.6.6.1.1
4.4	Monitored variables, and associated analytical limits	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.5	Minimum criteria for manual actions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.6	Spatially dependent variables	7.1.6.6.1.1	7.1.6.6.1.1 7.2.1.3.1	7.1.6.6.1.1 7.3.3.3.1	7.1.6.6.1.1 7.2.3.3.1	7.1.6.6.1.1 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.1	7.1.6.6.1.1 7.2.2.3.1	7.1.6.6.1.1 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.1 7.3.3.3.1	7.1.6.6.1.1 7.5.3.3.1	7.1.6.6.1.1 7.5.2.3.1	7.1.6.6.1.1	7.1.6.6.1.1 7.3.1.2.3.1	7.1.6.6.1.1 7.4.4.3.1	7.1.6.6.1.1 7.4.1.3.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1 7.3.6.3.1	7.1.6.6.1.1
4.7	Range of transient and steady-state conditions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.8	Adverse environmental conditions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.9	Reliability methods	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.10	DBE critical times / conditions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.11	Equipment protective provisions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1

Table 7.1-2

I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference

		Q-DCIS																		
		RTIF - NMS PLATFORM							SSLC/ESF PLATFORM										INDEPENDENT CONTROL PLATFORM	
		RTIF						NMS												
IEEE Std. 603 Section	Functions (1)	RTIF	RPS	LD&IS (MSIV Only) (6)	CMS (includes SPTM) (6)	NBS (6)	CRD (6)	NMS (3)	SSLC/ESF (4)	LD&IS (Non-MSIV) (2)&(6)	PRMS	CMS (6)	NBS (includes ADS) (6)	GDCS	ICS	SLC (6)	CBVS (7)	CRD (6)	VBIF	ATWS / SLC (5),(6)&(7)
4.12	Special design basis	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
5.1	Single failure criterion	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2
5.2	Completion of protective action	7.1.6.6.1.3	7.1.6.6.1.3 7.2.1.3.1	7.1.6.6.1.3 7.3.3.3.1	7.1.6.6.1.3 7.2.3.3.1	7.1.6.6.1.3 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.2.2.3.1	7.1.6.6.1.3 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.3 7.3.3.3.1	7.1.6.6.1.3 7.5.3.3.1	7.1.6.6.1.3 7.5.2.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.3.1.2.3.1	7.1.6.6.1.3 7.4.4.3.1	7.1.6.6.1.3 7.4.1.3.1	7.1.6.6.1.3	7.1.6.6.1.3	7.1.6.6.1.3 7.3.6.3.1	7.1.6.6.1.3
5.3	Quality	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4
5.4	Equipment qualification	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5
5.5	System Integrity	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6
5.6	Independence	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7
5.7	Capability for test and calibration	7.1.6.6.1.8	7.1.6.6.1.8 7.2.1.3.1	7.1.6.6.1.8 7.3.3.3.1	7.1.6.6.1.8 7.2.3.3.1	7.1.6.6.1.8 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.8	7.1.6.6.1.8 7.2.2.3.1	7.1.6.6.1.8 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.8 7.3.3.3.1	7.1.6.6.1.8 7.5.3.3.1	7.1.6.6.1.8 7.5.2.3.1	7.1.6.6.1.8	7.1.6.6.1.8 7.3.1.2.3.1	7.1.6.6.1.8 7.4.4.3.1	7.1.6.6.1.8 7.4.1.3.1	7.1.6.6.1.8	7.1.6.6.1.8	7.1.6.6.1.8 7.3.6.3.1	7.1.6.6.1.8
5.8	Information displays	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9
5.9	Control of Access	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10
5.10.	Repair	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11
5.11	Identification	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12
5.12	Auxiliary features	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13
5.13	Multi-unit stations	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14
5.14	Human factors considerations	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15
5.15	Reliability	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16

Table 7.1-2

I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference

		Q-DCIS																		
		RTIF - NMS PLATFORM							SSLC/ESF PLATFORM										INDEPENDENT CONTROL PLATFORM	
		RTIF						NMS												
IEEE Std. 603 Section	Functions (1)	RTIF	RPS	LD&IS (MSIV Only) (6)	CMS (includes SPTM) (6)	NBS (6)	CRD (6)	NMS (3)	SSLC/ESF (4)	LD&IS (Non-MSIV) (2)&(6)	PRMS	CMS (6)	NBS (includes ADS) (6)	GDCS	ICS	SLC (6)	CBVS (7)	CRD (6)	VBIF	ATWS / SLC (5),(6)&(7)
6.1	Automatic Control	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17
6.2	Manual control	7.1.6.6.1.18	7.1.6.6.1.18 7.2.1.3.1	7.1.6.6.1.18 7.3.3.3.1	7.1.6.6.1.18 7.2.3.3.1	7.1.6.6.1.18 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.18	7.1.6.6.1.18 7.2.2.3.1	7.1.6.6.1.18 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.18 7.3.3.3.1	7.1.6.6.1.18 7.5.3.3.1	7.1.6.6.1.18 7.5.2.3.1	7.1.6.6.1.18	7.1.6.6.1.18 7.3.1.2.3.1	7.1.6.6.1.18 7.4.4.3.1	7.1.6.6.1.18 7.4.1.3.1	7.1.6.6.1.18	7.1.6.6.1.18	7.1.6.6.1.18 7.3.6.3.1	7.1.6.6.1.18
6.3	Interaction between the sense and command features and other systems	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19
6.4	Derivation of system inputs	7.1.6.6.1.20	7.1.6.6.1.20 7.2.1.3.1	7.1.6.6.1.20 7.3.3.3.1	7.1.6.6.1.20 7.2.3.3.1	7.1.6.6.1.20 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.20	7.1.6.6.1.20 7.2.2.3.1	7.1.6.6.1.20 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.20 7.3.3.3.1	7.1.6.6.1.20 7.5.3.3.1	7.1.6.6.1.20 7.5.2.3.1	7.1.6.6.1.20	7.1.6.6.1.20 7.3.1.2.3.1	7.1.6.6.1.20 7.4.4.3.1	7.1.6.6.1.20 7.4.1.3.1	7.1.6.6.1.20	7.1.6.6.1.20	7.1.6.6.1.20 7.3.6.3.1	7.1.6.6.1.20
6.5	Capability for testing and calibration	7.1.6.6.1.21	7.1.6.6.1.21 7.2.1.3.1	7.1.6.6.1.21 7.3.3.3.1	7.1.6.6.1.21 7.2.3.3.1	7.1.6.6.1.21 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.21	7.1.6.6.1.21 7.2.2.3.1	7.1.6.6.1.21 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.21 7.3.3.3.1	7.1.6.6.1.21 7.5.3.3.1	7.1.6.6.1.21 7.5.2.3.1	7.1.6.6.1.21	7.1.6.6.1.21 7.3.1.2.3.1	7.1.6.6.1.21 7.4.4.3.1	7.1.6.6.1.21 7.4.1.3.1	7.1.6.6.1.21	7.1.6.6.1.21	7.1.6.6.1.21 7.3.6.3.1	7.1.6.6.1.21
6.6	Operating bypasses	7.1.6.6.1.22	7.1.6.6.1.22 7.2.1.3.1	7.1.6.6.1.22 7.3.3.3.1	7.1.6.6.1.22 7.2.3.3.1	7.1.6.6.1.22 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.22	7.1.6.6.1.22 7.2.2.3.1	7.1.6.6.1.22 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.22 7.3.3.3.1	7.1.6.6.1.22 7.5.3.3.1	7.1.6.6.1.22 7.5.2.3.1	7.1.6.6.1.22	7.1.6.6.1.22 7.3.1.2.3.1	7.1.6.6.1.22 7.4.4.3.1	7.1.6.6.1.22 7.4.1.3.1	7.1.6.6.1.22	7.1.6.6.1.22	7.1.6.6.1.22 7.3.6.3.1	7.1.6.6.1.22
6.7	Maintenance bypass	7.1.6.6.1.23	7.1.6.6.1.23 7.2.1.3.1	7.1.6.6.1.23 7.3.3.3.1	7.1.6.6.1.23 7.2.3.3.1	7.1.6.6.1.23 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.23	7.1.6.6.1.23 7.2.2.3.1	7.1.6.6.1.23 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.23 7.3.3.3.1	7.1.6.6.1.23 7.5.3.3.1	7.1.6.6.1.23 7.5.2.3.1	7.1.6.6.1.23	7.1.6.6.1.23 7.3.1.2.3.1	7.1.6.6.1.23 7.4.4.3.1	7.1.6.6.1.23 7.4.1.3.1	7.1.6.6.1.23	7.1.6.6.1.23	7.1.6.6.1.23 7.3.6.3.1	7.1.6.6.1.23
6.8	Setpoints	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24

Table 7.1-2

I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference

		Q-DCIS																		
		RTIF - NMS PLATFORM							SSLC/ESF PLATFORM										INDEPENDENT CONTROL PLATFORM	
		RTIF						NMS												
IEEE Std. 603 Section	Functions (1)	RTIF	RPS	LD&IS (MSIV Only) (6)	CMS (includes SPTM) (6)	NBS (6)	CRD (6)	NMS (3)	SSLC/ESF (4)	LD&IS (Non-MSIV) (2)&(6)	PRMS	CMS (6)	NBS (includes ADS) (6)	GDCS	ICS	SLC (6)	CBVS (7)	CRD (6)	VBIF	ATWS / SLC (5),(6)&(7)
7.1	Automatic Control	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17
7.2	Manual control	7.1.6.6.1.18	7.1.6.6.1.18 7.2.1.3.1	7.1.6.6.1.18 7.3.3.3.1	7.1.6.6.1.18 7.2.3.3.1	7.1.6.6.1.18 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.18	7.1.6.6.1.18 7.2.2.3.1	7.1.6.6.1.18 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.18 7.3.3.3.1	7.1.6.6.1.18 7.5.3.3.1	7.1.6.6.1.18 7.5.2.3.1	7.1.6.6.1.18	7.1.6.6.1.18 7.3.1.2.3.1	7.1.6.6.1.18 7.4.4.3.1	7.1.6.6.1.18 7.4.1.3.1	7.1.6.6.1.18	7.1.6.6.1.18	7.1.6.6.1.18 7.3.6.3.1	7.1.6.6.1.18
7.3	Completion of protective action	7.1.6.6.1.3	7.1.6.6.1.3 7.2.1.3.1	7.1.6.6.1.3 7.3.3.3.1	7.1.6.6.1.3 7.2.3.3.1	7.1.6.6.1.3 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.2.2.3.1	7.1.6.6.1.3 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.3 7.3.3.3.1	7.1.6.6.1.3 7.5.3.3.1	7.1.6.6.1.3 7.5.2.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.3.1.2.3.1	7.1.6.6.1.3 7.4.4.3.1	7.1.6.6.1.3 7.4.1.3.1	7.1.6.6.1.3	7.1.6.6.1.3	7.1.6.6.1.3 7.3.6.3.1	7.1.6.6.1.3
7.4	Operating bypass	7.1.6.6.1.22	7.1.6.6.1.22 7.2.1.3.1	7.1.6.6.1.22 7.3.3.3.1	7.1.6.6.1.22 7.2.3.3.1	7.1.6.6.1.22 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.22	7.1.6.6.1.22 7.2.2.3.1	7.1.6.6.1.22 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.22 7.3.3.3.1	7.1.6.6.1.22 7.5.3.3.1	7.1.6.6.1.22 7.5.2.3.1	7.1.6.6.1.22	7.1.6.6.1.22 7.3.1.2.3.1	7.1.6.6.1.22 7.4.4.3.1	7.1.6.6.1.22 7.4.1.3.1	7.1.6.6.1.22	7.1.6.6.1.22	7.1.6.6.1.22 7.3.6.3.1	7.1.6.6.1.22
7.5	Maintenance bypass	7.1.6.6.1.23	7.1.6.6.1.23 7.2.1.3.1	7.1.6.6.1.23 7.3.3.3.1	7.1.6.6.1.23 7.2.3.3.1	7.1.6.6.1.23 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.23	7.1.6.6.1.23 7.2.2.3.1	7.1.6.6.1.23 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.23 7.3.3.3.1	7.1.6.6.1.23 7.5.3.3.1	7.1.6.6.1.23 7.5.2.3.1	7.1.6.6.1.23	7.1.6.6.1.23 7.3.1.2.3.1	7.1.6.6.1.23 7.4.4.3.1	7.1.6.6.1.23 7.4.1.3.1	7.1.6.6.1.23	7.1.6.6.1.23	7.1.6.6.1.23 7.3.6.3.1	7.1.6.6.1.23
8.1	Electrical power sources	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25
8.2	Non-electrical power sources	7.1.6.6.1.26	7.1.6.6.1.26 7.2.1.3.1	7.1.6.6.1.26 7.3.3.3.1	7.1.6.6.1.26 7.2.3.3.1	7.1.6.6.1.26 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.26	7.1.6.6.1.26 7.2.2.3.1	7.1.6.6.1.26 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.26 7.3.3.3.1	7.1.6.6.1.26 7.5.3.3.1	7.1.6.6.1.26 7.5.2.3.1	7.1.6.6.1.26	7.1.6.6.1.26 7.3.1.2.3.1	7.1.6.6.1.26 7.4.4.3.1	7.1.6.6.1.26 7.4.1.3.1	7.1.6.6.1.26	7.1.6.6.1.26	7.1.6.6.1.26 7.3.6.3.1	7.1.6.6.1.26

Table 7.1-2

I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference

		Q-DCIS																		
		RTIF - NMS PLATFORM							SSLC/ESF PLATFORM										INDEPENDENT CONTROL PLATFORM	
		RTIF						NMS												
IEEE Std. 603 Section	Functions (1)	RTIF	RPS	LD&IS (MSIV Only) (6)	CMS (includes SPTM) (6)	NBS (6)	CRD (6)	NMS (3)	SSLC/ESF (4)	LD&IS (Non-MSIV) (2)&(6)	PRMS	CMS (6)	NBS (includes ADS) (6)	GDCS	ICS	SLC (6)	CBVS (7)	CRD (6)	VBIF	ATWS / SLC (5),(6)&(7)
8.3	Maintenance Bypass	7.1.6.6.1.27	7.1.6.6.1.27 7.2.1.3.1	7.1.6.6.1.27 7.3.3.3.1	7.1.6.6.1.27 7.2.3.3.1	7.1.6.6.1.27 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.27	7.1.6.6.1.27 7.2.2.3.1	7.1.6.6.1.27 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.27 7.3.3.3.1	7.1.6.6.1.27 7.5.3.3.1	7.1.6.6.1.27 7.5.2.3.1	7.1.6.6.1.27	7.1.6.6.1.27 7.3.1.2.3.1	7.1.6.6.1.27 7.4.4.3.1	7.1.6.6.1.27 7.4.1.3.1	7.1.6.6.1.27	7.1.6.6.1.27	7.1.6.6.1.27 7.3.6.3.1	7.1.6.6.1.27

Notes:

(1) The IEEE Std. 603 criteria apply to the safety-related portions of the systems identified in this table.

(2) LD&IS (non-MSIV) controls the safety-related actuators (for the isolation valves and dampers) associated with the following nonsafety-related systems: RWCU/SDC, FAPCS, EFDS, CIS, CWS, CMS, HPNSS, RBVS, and FBVS. RWCU/SDC provides safety-related sensor inputs to LD&IS (non-MSIV). The regulatory requirements associated with these actuators and sensors are addressed as part of LD&IS.

(3) NMS has Q and N parts. The Q parts are SRNM, LPRM, APRM, and OPRM. The N parts are AFIP and MRBM.

(4) SSLC/ESF includes the RSS, MCRP, and safety-related VDUs.

(5) Includes the NBS sensors associate with ATWS/SLC.

(6) The following safety-related systems have logic implemented on multiple platforms in support of their protective functions: CMS, CRD, LD&IS, NBS and SLC. Refer to DCD Sections 7.2, 7.3, 7.4, and 7.5 for detailed descriptions of the system functions.

(7) CBVS includes the CRHS and CRHAVS subsystems and EFUs.

~~Table 7.1-2~~

~~Section Roadmap of I&C Systems Conformance to Evaluation of IEEE Std. 603 Specific Criteria Compliance~~

~~Subject~~		~~Instrumentation & Control Systems~~	~~Reactor Trip Systems~~	~~Engineered Safety Features~~	~~Safe Shutdown Systems~~	~~Information Systems~~	~~Interlock Systems~~	~~Control Systems~~	~~Diverse Instrumentation and Control Systems~~
~~IEEE Std. 603 Section~~	~~Functions [1]~~	~~Q-DCIS, N-DCIS~~	~~RPS, NMS [2], SPTM [3], MSIV (for LD&IS)~~	~~SSLC/ESF ECCS [4], PCCS [5], LD&IS (except MSIV) CRHS, VBIF~~	~~Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)~~	~~Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)~~	~~HP/LP SI (N)~~	~~NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)~~	~~ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)~~
~~4~~	~~Safety System Designation~~	~~7.1.2.1 7.1.3.1.1 7.1.6.6.1.1 Table 15.0-2 Table 15.1-2 Table 15.1-3~~	~~7.1.6.6.1.1 Table 15.0-2 Table 15.1-2 Table 15.1-3~~	~~7.1.6.6.1.1 Table 15.0-2 Table 15.1-2 Table 15.1-3~~	~~7.1.6.6.1.1 Table 15.0-2 Table 15.1-2 Table 15.1-3~~	~~7.1.6.6.1.1 Table 15.0-2 Table 15.1-2 Table 15.1-3~~	~~-~~	~~7.1.6.6.1.1 Table 15.0-2 Table 15.1-2 Table 15.1-3~~	~~Table 15.0-2 Table 15.1-2 Table 15.1-3~~
~~4.1 4.2 4.3 4.4 4.5~~	~~DBE, safety-related functions, permissive conditions for operating bypasses, monitored variables, analytical limits, minimum criteria for manual actions~~	~~7.1.6.6.1.1 7.1.2.1 7.1.3.1.1~~	~~7.2.1.1 (RPS) 7.2.1.2.4.1 7.2.1.2.4.2 Table 15.0-2~~	~~7.3.1.2.1 (GDCS) 7.4.4.1 (ICS) 7.4.4.5 7.4.1.1 (SLC) 7.3.6.1 (VBIF)~~	~~7.4.1.1 (SLC) 7.4.1.2 7.4.2.2.2 (RSS) 7.4.3.1.1 (RWCU/SDC) 7.4.4.1 (ICS) 7.4.4.5~~	~~7.5.2.1 (CMS)~~	~~-~~	~~7.7.1.1.1 (NBS)~~	~~-~~
~~4.6~~	~~Spatially dependent variables, identification, number and location~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~
~~4.7~~	~~Range of transient and steady-state conditions~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~

~~Table 7.1-2~~

~~Section Roadmap of I&C Systems Conformance to Evaluation of IEEE Std. 603 Specific Criteria Compliance~~

~~Subject~~		~~Instrumen-tation & Control Systems~~	~~Reactor Trip Systems~~	~~Engineered Safety Features~~	~~Safe Shutdown Systems~~	~~Information Systems~~	~~Interlock Systems~~	~~Control Systems~~	~~Diverse Instrumen-tation and Control Systems~~
~~IEEE Std. 603 Section~~	~~Functions [1]~~	~~Q-DCIS, N-DCIS~~	~~RPS, NMS [2], SPTM [3], MSIV (for LD&IS)~~	~~SSLC/ESF ECCS [4], PCCS [5], LD&IS (except MSIV) CRHS, VBIF~~	~~Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)~~	~~Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)~~	~~HP/LP SI (N)~~	~~NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)~~	~~ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)~~
~~4.8~~	~~Adverse environmental conditions~~	~~7.1.2.1 7.1.3.1.1~~	~~-~~	~~7.4.4.3 (ICS) 7.4.1.1 (SLC) 7.4.1.3 7.4.4.3 (ICS)~~	~~7.4.1.1 (SLC) 7.4.1.3 7.4.4.3 (ICS)~~	~~-~~	~~-~~	~~7.7.1.1.1 (NBS) 7.7.1.3~~	~~-~~
~~4.10~~	~~DBE critical times / conditions~~	~~7.1.2.1 7.1.3.1.1~~	~~-~~	~~-~~	~~7.4.1.1 (SLC) 7.4.4.3 (ICS)~~	~~-~~	~~-~~	~~7.7.1.1.1 (NBS)~~	~~-~~
~~4.12~~	~~Special design basis~~	~~-~~	~~-~~	~~7.3.1.1.4 (ADS)~~		~~-~~	~~-~~	~~-~~	~~-~~

~~Table 7.1-2~~

~~Section Roadmap of I&C Systems Conformance to Evaluation of IEEE Std. 603 Specific Criteria Compliance~~

~~Subject~~		~~Instrumentation & Control Systems~~	~~Reactor Trip Systems~~	~~Engineered Safety Features~~	~~Safe Shutdown Systems~~	~~Information Systems~~	~~Interlock Systems~~	~~Control Systems~~	~~Diverse Instrumentation and Control Systems~~
~~IEEE Std. 603 Section~~	~~Functions [1]~~	~~Q-DCIS, N-DCIS~~	~~RPS, NMS [2], SPTM [3], MSIV (for LD&IS)~~	~~SSLC/ESF ECCS [4], PCCS [5], LD&IS (except MSIV) CRHS, VBIF~~	~~Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)~~	~~Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)~~	~~HP/LP SI (N)~~	~~NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)~~	~~ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)~~
~~5.1~~	~~Single failure criterion~~	~~7.1.3.3~~ ~~7.1.6.6.1.2~~	~~7.1.6.6.1.2~~ ~~7.2.1.1 (RPS)~~ ~~7.2.1.2.4~~ ~~7.2.1.3.4~~ ~~7.2.2.2.4.3 (NMS)~~ ~~7.2.2.2.4.6~~ ~~7.2.2.2.6.4~~	~~7.1.6.6.1.2~~ ~~7.3.1.1.2 (ADS)~~ ~~7.3.1.1.3~~ ~~7.3.1.1.3.4~~ ~~7.3.1.2.1 (GDCS)~~ ~~7.3.1.2.2~~ ~~7.3.1.2.3~~ ~~7.3.1.2.3.4~~ ~~7.3.3.1 (LD&IS)~~ ~~7.3.3.2~~ ~~7.3.4.2 (CRHS)~~ ~~7.3.5.2.2 (SSLC/ESF)~~ ~~7.3.5.3.4~~ ~~7.4.4.3 (ICS)~~ ~~7.3.6.1 (VBIF)~~ ~~7.3.6.3.4 (VBIF)~~ ~~7.4.1.3 (SLC)~~	~~7.1.6.6.1.2~~ ~~7.4.1.3 (SLC)~~ ~~7.4.2.2.1 (RSS)~~ ~~7.4.2.3.1~~ ~~7.4.2.3.3~~ ~~7.4.4.3 (ICS)~~	~~7.1.6.6.1.2~~	~~-~~	~~7.1.6.6.1.2~~ ~~7.7.1.3 (NBS)~~	~~-~~

~~Table 7.1-2~~

~~Section Roadmap of I&C Systems Conformance to Evaluation of IEEE Std. 603 Specific Criteria Compliance~~

~~Subject~~		~~Instrumentation & Control Systems~~	~~Reactor Trip Systems~~	~~Engineered Safety Features~~	~~Safe Shutdown Systems~~	~~Information Systems~~	~~Interlock Systems~~	~~Control Systems~~	~~Diverse Instrumentation and Control Systems~~
~~IEEE Std. 603 Section~~	~~Functions [1]~~	~~Q-DCIS, N-DCIS~~	~~RPS, NMS [2], SPTM [3], MSIV (for LD&IS)~~	~~SSLC/ESF ECCS [4], PCCS [5], LD&IS (except MSIV) CRHS, VBIF~~	~~Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)~~	~~Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)~~	~~HP/LP SI (N)~~	~~NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)~~	~~ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)~~
~~5.2~~	~~Completion of protective action~~	~~7.1.6.6.1.3~~	~~7.1.6.6.1.3~~ ~~7.2.1.1 (RPS)~~ ~~7.2.1.3.4~~	~~7.1.6.6.1.3~~ ~~7.3.1.1.2 (ADS)~~ ~~7.3.1.2.2 (GDCS)~~ ~~7.3.3.1 (LD&IS)~~ ~~7.3.3.3~~ ~~7.3.5.2.2 (SSLC/ESF)~~ ~~7.4.1.2.2 (SLC)~~	~~7.1.6.6.1.3~~ ~~7.4.1.2.2 (SLC)~~	~~7.1.6.6.1.3~~	~~-~~	~~7.1.6.6.1.3~~	~~-~~
~~5.3~~	~~Quality~~	~~7.1.6.6.1.4~~	~~7.1.6.6.1.4~~	~~7.1.6.6.1.4~~	~~7.1.6.6.1.4~~	~~7.1.6.6.1.4~~	~~-~~	~~7.1.6.6.1.4~~	~~-~~
~~5.4~~	~~Equipment qualification~~	~~7.1.6.6.1.5~~	~~7.1.6.6.1.5~~ ~~7.2.1.3.5 (RPS)~~	~~7.1.6.6.1.5~~ ~~7.4.1.3 (SLC)~~	~~7.1.6.6.1.5~~ ~~7.4.1.3 (SLC)~~	~~7.1.6.6.1.5~~	~~-~~	~~7.1.6.6.1.5~~	~~7.8.3 (CMF defenses within SSD)~~
~~5.5~~	~~System Integrity~~	~~7.1.6.6.1.6~~	~~7.1.6.6.1.6~~	~~7.1.6.6.1.6~~ ~~7.3.4.2 (CRHS)~~	~~7.1.6.6.1.6~~	~~7.1.6.6.1.6~~	~~-~~	~~7.1.6.6.1.6~~	

~~Table 7.1-2~~

~~Section Roadmap of I&C Systems Conformance to Evaluation of IEEE Std. 603 Specific Criteria Compliance~~

~~Subject~~		~~Instrumentation & Control Systems~~	~~Reactor Trip Systems~~	~~Engineered Safety Features~~	~~Safe Shutdown Systems~~	~~Information Systems~~	~~Interlock Systems~~	~~Control Systems~~	~~Diverse Instrumentation and Control Systems~~
~~IEEE Std. 603 Section~~	~~Functions [1]~~	~~Q-DCIS, N-DCIS~~	~~RPS, NMS [2], SPTM [3], MSIV (for LD&IS)~~	~~SSLC/ESF ECCS [4], PCCS [5], LD&IS (except MSIV) CRHS, VBIF~~	~~Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)~~	~~Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)~~	~~HP/LP SI (N)~~	~~NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)~~	~~ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)~~
~~5.6~~	~~Independence~~	~~7.1.6.6.1.7~~ ~~7.1.3.3~~	~~7.1.6.6.1.7~~ ~~7.2.1.1 (RPS)~~ ~~7.2.1.2.4.1~~ ~~7.2.1.3.1~~ ~~7.2.1.3.4~~ ~~7.2.2.2.4.3 (NMS)~~ ~~7.2.2.2.5.3~~ ~~7.2.2.2.6.4~~ ~~7.2.2.3.1~~ ~~7.2.3.3.1 (SPTM)~~	~~7.1.6.6.1.7~~ ~~7.3.1.1.3.1 (ADS)~~ ~~7.3.1.2.3.1 (GDCS)~~ ~~7.3.3.1 (LD&IS)~~ ~~7.3.3.2~~ ~~7.3.3.3.1~~ ~~7.3.4.2 (CRHS)~~ ~~7.3.5.2.2 (SSLC/ESF)~~ ~~7.4.1.3 (SLC)~~ ~~7.4.4.3.1(ICS)~~ ~~7.3.6.3.1 (VBIF)~~	~~7.1.6.6.1.7~~ ~~7.4.1.3 (SLC)~~ ~~7.4.2.2.1 (RSS)~~ ~~7.4.2.3.1~~ ~~7.4.2.3.3~~ ~~7.4.4.3.1 (ICS)~~	~~7.1.6.6.1.7~~ ~~7.5.2.2 (CMS)~~ ~~7.5.2.3.1~~ ~~7.5.3.3.1 (PRMS)~~	-	~~7.1.6.6.1.7~~ ~~7.7.2.2.7.4 (RC&IS)~~ ~~7.7.3.1.2 (FWCS)~~ ~~7.7.4.2 (PAS)~~ ~~7.7.5.1.2 (SB&PC)~~	~~7.8.3~~ ~~7.8.3.1~~

~~Table 7.1-2~~

~~Section Roadmap of I&C Systems Conformance to Evaluation of IEEE Std. 603 Specific Criteria Compliance~~

~~Subject~~		~~Instrumentation & Control Systems~~	~~Reactor Trip Systems~~	~~Engineered Safety Features~~	~~Safe Shutdown Systems~~	~~Information Systems~~	~~Interlock Systems~~	~~Control Systems~~	~~Diverse Instrumentation and Control Systems~~
~~IEEE Std. 603 Section~~	~~Functions [1]~~	~~Q-DCIS, N-DCIS~~	~~RPS, NMS [2], SPTM [3], MSIV (for LD&IS)~~	~~SSLC/ESF ECCS [4], PCCS [5], LD&IS (except MSIV) CRHS, VBIF~~	~~Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)~~	~~Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)~~	~~HP/LP SI (N)~~	~~NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)~~	~~ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)~~
~~5.7~~	~~Capability for test and calibration~~	~~7.1.6.6.1.8~~ ~~7.1.3.3~~ ~~7.1.3.4~~ ~~7.1.3.5~~ ~~7.1.6.4~~	~~7.1.6.6.1.8~~ ~~7.2.1.3.4 (RPS)~~ ~~7.2.1.4.1~~	~~7.1.6.6.1.8~~ ~~7.3.1.1.4 (ADS)~~ ~~7.3.1.2.4 (GDCS)~~ ~~7.3.3.1 (LD&IS)~~ ~~7.3.3.4.2~~ ~~7.3.5.4 (SSLC/ESF)~~ ~~7.4.4.4 (ICS)~~ ~~7.4.4.5~~ ~~7.4.1.3 (SLC)~~ ~~7.4.1.4~~ ~~7.3.6.4 (VBIF)~~	~~7.1.6.6.1.8~~ ~~7.4.1.3 (SLC)~~ ~~7.4.1.4~~ ~~7.4.3.4 (RWCU/SDC)~~ ~~7.4.4.4 (ICS)~~ ~~7.4.4.5~~	~~7.1.6.6.1.8~~ ~~7.5.3.4 (PRMS)~~	~~–~~	~~7.1.6.6.1.8~~ ~~7.7.1.4 (NBS)~~	~~-~~

~~Table 7.1-2~~

~~Section Roadmap of I&C Systems Conformance to Evaluation of IEEE Std. 603 Specific Criteria Compliance~~

~~Subject~~		~~Instrumentation & Control Systems~~	~~Reactor Trip Systems~~	~~Engineered Safety Features~~	~~Safe Shutdown Systems~~	~~Information Systems~~	~~Interlock Systems~~	~~Control Systems~~	~~Diverse Instrumentation and Control Systems~~
~~IEEE Std. 603 Section~~	~~Functions [1]~~	~~Q-DCIS, N-DCIS~~	~~RPS, NMS [2], SPTM [3], MSIV (for LD&IS)~~	~~SSLC/ESF ECCS [4], PCCS [5], LD&IS (except MSIV) CRHS, VBIF~~	~~Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)~~	~~Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)~~	~~HP/LP SI (N)~~	~~NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)~~	~~ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)~~
~~5.8~~	~~Information displays~~	~~7.1.2.6~~ ~~7.1.3.5~~ ~~7.1.6.6.1.9~~	~~7.1.6.6.1.9~~ ~~7.2.1.2.4.3 (RPS)~~ ~~7.2.1.3.1~~ ~~7.2.1.3.4~~ ~~7.2.2.3.1 (NMS)~~ ~~7.2.2.5.1~~	~~7.1.6.6.1.9~~ ~~7.3.1.1.2 (ADS)~~ ~~7.3.1.1.5~~ ~~7.3.1.2.1 (GDCS)~~ ~~7.3.1.2.2~~ ~~7.3.1.2.3.1~~ ~~7.3.1.2.5~~ ~~7.3.3.3.1 (LD&IS)~~ ~~7.3.4.2 (CRHS)~~ ~~7.3.5.3.1 (SSLC/ESF)~~ ~~7.4.4.5 (ICS)~~ ~~7.4.1.3 (SLC)~~ ~~7.4.1.5~~ ~~7.3.6.1 (VBIF)~~ ~~7.3.6.3.1~~ ~~7.3.6.5~~	~~7.1.6.6.1.9~~ ~~7.4.1.3 (SLC)~~ ~~7.4.1.5~~ ~~7.4.2.2.1 (RSS)~~ ~~7.4.4.5 (ICS)~~	~~7.1.6.6.1.9~~ ~~7.5.2.1 (CMS)~~	~~–~~	~~7.1.6.6.1.9~~ ~~7.7.1.5 (NBS)~~	~~-~~
~~5.9~~	~~Control of Access~~	~~7.1.6.6.1.10~~	~~7.1.6.6.1.10~~ ~~7.2.1.1 (RPS)~~	~~7.1.6.6.1.10~~ ~~7.3.3.1 (LD&IS)~~	~~7.1.6.6.1.10~~ ~~7.4.2.2.1 (RSS)~~	~~7.1.6.6.1.10~~	~~-~~	~~7.1.6.6.1.10~~	~~-~~

~~Table 7.1-2~~

~~Section Roadmap of I&C Systems Conformance to Evaluation of IEEE Std. 603 Specific Criteria Compliance~~

~~Subject~~		~~Instrumentation & Control Systems~~	~~Reactor Trip Systems~~	~~Engineered Safety Features~~	~~Safe Shutdown Systems~~	~~Information Systems~~	~~Interlock Systems~~	~~Control Systems~~	~~Diverse Instrumentation and Control Systems~~
~~IEEE Std. 603 Section~~	~~Functions [1]~~	~~Q-DCIS, N-DCIS~~	~~RPS, NMS [2], SPTM [3], MSIV (for LD&IS)~~	~~SSLC/ESF ECCS [4], PCCS [5], LD&IS (except MSIV) CRHS, VBIF~~	~~Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)~~	~~Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)~~	~~HP/LP SI (N)~~	~~NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)~~	~~ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)~~
~~5.10.~~	~~Repair~~	~~7.1.3.5~~ ~~7.1.6.6.1.11~~	~~7.1.6.6.1.11~~ ~~7.2.1.2.4.4 (RPS)~~ ~~7.2.2.2.4.6 (NMS)~~ ~~7.2.2.2.6.6~~	~~7.1.6.6.1.11~~	~~7.1.6.6.1.11~~	~~7.1.6.6.1.11~~	~~-~~	~~7.1.6.6.1.11~~	~~-~~
~~5.11~~	~~Identification~~	~~7.1.6.6.1.12~~	~~7.1.6.6.1.12~~	~~7.1.6.6.1.12~~	~~7.1.6.6.1.12~~	~~7.1.6.6.1.12~~	~~-~~	~~7.1.6.6.1.12~~	~~-~~
~~5.12~~	~~Auxiliary features~~	~~7.1.6.6.1.13~~	~~7.1.6.6.1.13~~ ~~7.2.1.1 (RPS)~~	~~7.1.6.6.1.13~~ ~~7.4.1.2.1 (SLC)~~	~~7.1.6.6.1.13~~ ~~7.4.1.2.1 (SLC)~~	~~7.1.6.6.1.13~~	~~—~~	~~7.1.6.6.1.13~~	~~-~~
~~5.13~~	~~Multi-unit stations~~	~~7.1.6.6.1.14~~	~~7.1.6.6.1.14~~	~~7.1.6.6.1.14~~	~~7.1.6.6.1.14~~	~~7.1.6.6.1.14~~	~~-~~	~~7.1.6.6.1.14~~	~~-~~
~~5.14~~	~~Human factors considerations~~	~~7.1.6.6.1.15~~	~~7.1.6.6.1.15~~	~~7.1.6.6.1.15~~	~~7.1.6.6.1.15~~	~~7.1.6.6.1.15~~	~~-~~	~~7.1.6.6.1.15~~	~~-~~
~~5.15~~	~~Reliability~~	~~7.1.6.6.1.16~~	~~7.1.6.6.1.16~~	~~7.1.6.6.1.16~~	~~7.1.6.6.1.16~~	~~7.1.6.6.1.16~~	~~-~~	~~7.1.6.6.1.16~~	~~-~~
~~6.1~~	~~Automatic Control~~	~~7.1.6.6.1.17~~	~~7.1.6.6.1.17~~	~~7.1.6.6.1.17~~ ~~7.3.1.1.2 (ADS)~~ ~~7.3.3.1 (LD&IS)~~	~~7.1.6.6.1.17~~	~~7.1.6.6.1.17~~	~~-~~	~~7.1.6.6.1.17~~	~~-~~

~~Table 7.1-2~~

~~Section Roadmap of I&C Systems Conformance to Evaluation of IEEE Std. 603 Specific Criteria Compliance~~

~~Subject~~		~~Instrumentation & Control Systems~~	~~Reactor Trip Systems~~	~~Engineered Safety Features~~	~~Safe Shutdown Systems~~	~~Information Systems~~	~~Interlock Systems~~	~~Control Systems~~	~~Diverse Instrumentation and Control Systems~~
~~IEEE Std. 603 Section~~	~~Functions [1]~~	~~Q-DCIS, N-DCIS~~	~~RPS, NMS [2], SPTM [3], MSIV (for LD&IS)~~	~~SSLC/ESF ECCS [4], PCCS [5], LD&IS (except MSIV) CRHS, VBIF~~	~~Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)~~	~~Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)~~	~~HP/LP SI (N)~~	~~NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)~~	~~ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)~~
~~6.2~~	~~Manual control~~	~~7.1.6.6.1.18~~	~~7.1.6.6.1.18~~ ~~7.2.1.1 (RPS)~~ ~~7.2.1.3.4~~	~~7.1.6.6.1.18~~ ~~7.3.1.1.2 (ADS)~~ ~~7.3.1.2.1 (GDCS)~~ ~~7.3.1.2.2~~ ~~7.3.3.3 (LD&IS)~~ ~~7.3.4.2 (CRHS)~~ ~~7.3.5.3.1 (SSLC/ESF)~~ ~~7.4.4.5 (ICS)~~ ~~7.3.6.1 (VBIF)~~	~~7.1.6.6.1.18~~ ~~7.4.4.5 (ICS)~~	~~7.1.6.6.1.18~~	~~-~~	~~7.1.6.6.1.18~~	~~-~~
~~6.3~~	~~Interaction between the sense and command features and other systems~~	~~7.1.3.3~~ ~~7.1.6.6.1.19~~	~~7.1.6.6.1.19~~ ~~7.2.1.3.1 (RPS)~~ ~~7.2.2.3.1 (NMS)~~	~~7.1.6.6.1.19~~ ~~7.4.4.3.1 (ICS)~~	~~7.1.6.6.1.19~~ ~~7.4.2.2.1 (RSS)~~ ~~7.4.2.3.1~~ ~~7.4.2.3.3~~ ~~7.4.4.3.1 (ICS)~~	~~7.1.6.6.1.19~~	~~--~~	~~7.1.6.6.1.19~~	~~-~~
~~6.4~~	~~Derivation of system inputs~~	~~7.1.6.6.1.20~~	~~7.1.6.6.1.20~~	~~7.1.6.6.1.20~~	~~7.1.6.6.1.20~~	~~7.1.6.6.1.20~~	~~-~~	~~7.1.6.6.1.20~~	~~-~~

~~Table 7.1-2~~

~~Section Roadmap of I&C Systems Conformance to Evaluation of IEEE Std. 603 Specific Criteria Compliance~~

~~Subject~~		~~Instrumentation & Control Systems~~	~~Reactor Trip Systems~~	~~Engineered Safety Features~~	~~Safe Shutdown Systems~~	~~Information Systems~~	~~Interlock Systems~~	~~Control Systems~~	~~Diverse Instrumentation and Control Systems~~
~~IEEE Std. 603 Section~~	~~Functions [1]~~	~~Q-DCIS, N-DCIS~~	~~RPS, NMS [2], SPTM [3], MSIV (for LD&IS)~~	~~SSLC/ESF ECCS [4], PCCS [5], LD&IS (except MSIV) CRHS, VBIF~~	~~Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)~~	~~Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)~~	~~HP/LP SI (N)~~	~~NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [2] (N) CIS (N)~~	~~ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)~~
~~6.5~~	~~Capability for testing and calibration~~	~~7.1.3.3~~ ~~7.1.3.5~~ ~~7.1.6.6.1.21~~	~~7.1.6.6.1.21~~ ~~7.2.1.3.4 (RPS)~~ ~~7.2.1.4.1~~	~~7.1.6.6.1.21~~ ~~7.3.1.1.4 (ADS)~~ ~~7.3.1.2.4 (GDCS)~~ ~~7.3.3.4.2 (LD&IS)~~ ~~7.3.5.4 (SSLC/ESF)~~ ~~7.4.4.4 (ICS)~~ ~~7.4.4.5~~ ~~7.4.1.3 (SLC)~~ ~~7.3.6.4 (VBIF)~~	~~7.1.6.6.1.21~~ ~~7.4.1.3 (SLC)~~ ~~7.4.3.4 (RWCU/SDC)~~ ~~7.4.4.4 (ICS)~~ ~~7.4.4.5~~	~~7.1.6.6.1.21~~ ~~7.5.2.4 (CMS)~~ ~~7.5.3.4 (PRMS)~~	~~—~~	~~7.1.6.6.1.21~~	~~-~~
~~6.6~~	~~Operating bypasses~~	~~7.1.6.6.1.22~~	~~7.1.6.6.1.22~~ ~~7.2.1.5.2.1 (RPS)~~	~~7.1.6.6.1.22~~	~~7.1.6.6.1.22~~	~~7.1.6.6.1.22~~	~~-~~	~~7.1.6.6.1.22~~	~~-~~
~~6.7~~	~~Maintenance bypass~~	~~7.1.6.6.1.23~~	~~7.1.6.6.1.23~~ ~~7.2.1.2.4 (RPS)~~ ~~7.2.1.5.2.2~~	~~7.1.6.6.1.23~~ ~~7.4.1.3 (SLC)~~	~~7.4.1.3 (SLC)~~	~~-~~	~~-~~	~~-~~	~~-~~

~~Table 7.1-2~~

~~Section Roadmap of I&C Systems Conformance to Evaluation of IEEE Std. 603 Specific Criteria Compliance~~

~~Subject~~		~~Instrumentation & Control Systems~~	~~Reactor Trip Systems~~	~~Engineered Safety Features~~	~~Safe Shutdown Systems~~	~~Information Systems~~	~~Interlock Systems~~	~~Control Systems~~	~~Diverse Instrumentation and Control Systems~~
~~IEEE Std. 603 Section~~	~~Functions [1]~~	~~Q-DCIS, N-DCIS~~	~~RPS, NMS [2], SPTM [3], MSIV (for LD&IS)~~	~~SSLC/ESF ECCS [4], PCCS [5], LD&IS (except MSIV) CRHS, VBIF~~	~~Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)~~	~~Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)~~	~~HP/LP SI (N)~~	~~NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)~~	~~ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)~~
~~6.8~~	~~Setpoints~~	~~7.1.6.6.1.24~~	~~7.1.6.6.1.24~~ ~~7.2.2.1.1.1 (NMS)~~ ~~7.2.2.2.4.5~~ ~~7.2.2.2.4.6~~	~~7.1.6.6.1.24~~ ~~7.3.3.1 (LD&IS)~~	~~7.1.6.6.1.24~~	~~7.1.6.6.1.24~~	~~-~~	~~7.1.6.6.1.24~~	~~-~~
~~7.1~~	~~Automatic Control~~	~~7.1.6.6.1.17~~	~~7.1.6.6.1.17~~	~~7.1.6.6.1.17~~ ~~7.3.1.1.2 (ADS)~~	~~7.1.6.6.1.17~~	~~7.1.6.6.1.17~~	~~-~~	~~7.1.6.6.1.17~~	~~-~~
~~7.2~~	~~Manual control~~	~~7.1.6.6.1.18~~	~~7.1.6.6.1.18~~	~~7.1.6.6.1.18~~ ~~7.3.1.1.2 (ADS)~~ ~~7.3.1.2.1 (GDCS)~~ ~~7.3.1.2.2~~ ~~7.3.3.2 (LD&IS)~~ ~~7.3.3.3 (LD&IS)~~ ~~7.3.4.2 (CRHS)~~ ~~7.3.5.3.1 (SSLC/ESF)~~ ~~7.4.4.5 (ICS)~~ ~~7.3.6.1 (VBIF)~~	~~7.1.6.6.1.18~~ ~~7.4.4.5 (ICS)~~	~~7.1.6.6.1.18~~	~~–~~	~~7.1.6.6.1.18~~	~~-~~

~~Table 7.1-2~~

~~Section Roadmap of I&C Systems Conformance to Evaluation of IEEE Std. 603 Specific Criteria Compliance~~

~~Subject~~		~~Instrumentation & Control Systems~~	~~Reactor Trip Systems~~	~~Engineered Safety Features~~	~~Safe Shutdown Systems~~	~~Information Systems~~	~~Interlock Systems~~	~~Control Systems~~	~~Diverse Instrumentation and Control Systems~~
~~IEEE Std. 603 Section~~	~~Functions [1]~~	~~Q-DCIS, N-DCIS~~	~~RPS, NMS [2], SPTM [3], MSIV (for LD&IS)~~	~~SSLC/ESF ECCS [4], PCCS [5], LD&IS (except MSIV) CRHS, VBIF~~	~~Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)~~	~~Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)~~	~~HP/LP SI (N)~~	~~NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)~~	~~ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)~~
~~7.3~~	~~Completion of protective action~~	~~-~~ ~~7.1.6.6.1.3~~	~~-~~	~~7.3.1.2.1 (GDCS)~~ ~~7.3.6.1 (VBIF)~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~
~~7.4~~	~~Operating bypass~~	~~7.1.6.6.1.22~~	~~7.1.6.6.1.22~~ ~~7.2.1.5.2.1 (RPS)~~	~~7.1.6.6.1.22~~	~~7.1.6.6.1.22~~	~~7.1.6.6.1.22~~	~~-~~	~~7.1.6.6.1.22~~	~~-~~
~~7.5~~	~~Maintenance bypass~~	~~7.1.6.6.1.23~~	~~7.1.6.6.1.23~~ ~~7.2.1.2.4 (RPS)~~ ~~7.2.1.5.2.2~~	~~7.1.6.6.1.23~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~
~~8.1~~	~~Electrical power sources~~	~~7.1.3.3~~ ~~7.1.6.6.1.25~~	~~7.1.6.6.1.25~~	~~7.1.6.6.1.25~~ ~~7.4.4.3 (ICS)~~ ~~7.4.1.2.1 (SLC)~~	~~7.1.6.6.1.25~~ ~~7.4.1.2.1 (SLC)~~ ~~7.4.4.3 (ICS)~~	~~7.1.6.6.1.25~~	~~-~~	~~7.1.6.6.1.25~~	~~-~~
~~8.2~~	~~Non-electrical power sources~~	~~7.1.6.6.1.26~~	~~-~~	~~7.4.1.2.1 (SLC)~~	~~7.4.1.2.1 (SLC)~~	~~-~~	~~-~~	~~-~~	~~-~~
~~8.3~~	~~Maintenance Bypass~~	~~7.1.6.6.1.27~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~

~~Table 7.1-2~~

~~Section Roadmap of I&C Systems Conformance to Evaluation of IEEE Std. 603 Specific Criteria Compliance~~

~~Subject~~		~~Instrumentation & Control Systems~~	~~Reactor Trip Systems~~	~~Engineered Safety Features~~	~~Safe Shutdown Systems~~	~~Information Systems~~	~~Interlock Systems~~	~~Control Systems~~	~~Diverse Instrumentation and Control Systems~~
~~IEEE Std. 603 Section~~	~~Functions [1]~~	~~Q-DCIS, N-DCIS~~	~~RPS, NMS [2], SPTM [3], MSIV (for LD&IS)~~	~~SSLC/ESF ECCS [4], PCCS [5], LD&IS (except MSIV) CRHS, VBIF~~	~~Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)~~	~~Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)~~	~~HP/LP SI (N)~~	~~NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [2] (N) CIS (N)~~	~~ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)~~

~~1.All systems are safety-related (Q) unless shown as nonsafety-related (N)~~

~~2.NMS has Q and N parts. The Q parts are SRNM, LPRM, APRM, and OPRM. The N parts are AFIP and MRBM.~~

~~3.SPTM is part of the RTS, ref. 7.2.3.~~

~~4.The SSLC/ESF ECCS comprises the ADS, GDCS, ICS, and SLC, ref. 7.3.1.~~

~~5.Passive system which does not require any control system interface to perform its safety-related function~~

~~* CMF: Common Mode Failure~~
~~DIC: Diverse Instrumentation and Control~~
~~DMCD: Diverse Manual Controls and Displays~~
~~PMS: Pool Monitoring Subsystems~~
~~SSD: Safety-Related System Design~~
~~D: Defense~~
~~WTDVBM: Wetwell to Drywell Vacuum Breaker Monitoring~~
~~IS: Information Systems~~
~~SS: Safe Shutdown~~
~~VBIF: Vacuum Breaker Isolation Function~~

confirmed by two-out-of-four coincidence of division trip outputs. A separate and diverse manual trip method is provided in the form of two independent manual trip channels. Actuation of both manual trip systems is required for a full reactor scram. Availability is enhanced because any one division can be bypassed at one time to allow online repair without degrading operability. This satisfies the repair requirement of IEEE Std. 603, Section 5.10 while maintaining plant availability.

The RPS consists of four redundant divisions identical in design and independent in operation. Although each division constitutes a separate trip system, normally each division can make two-out-of-four trip decisions with or without a division of sensors being bypassed. There are four instrument channels provided for each process variable being monitored, one for each RPS division. Four sensors, one per division, are provided for each variable. When more than four sensors are required to monitor a variable the outputs of the sensors are combined into only four instrument channels. The logic in each division does not depend on absolute time of day and is asynchronous with respect to the other divisions. No division depends on the correct operation of another division. There is no combination of MCR-initiated bypasses that can unacceptably degrade the RPS.

7.2.1.3 Safety Evaluation

Table 7.1-1 identifies the RPS 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.

7.2.1.3.1 Code of Federal Regulations

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

- Conformance: The RPS conforms to these standards.

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

- Conformance: The RPS conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the RPS conforms to IEEE Std. 603 is discussed below.~~Safety-related systems are designed to conform to Regulatory Guide (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 RPS is divisionalized and is designed with redundancy so that failure of any instrument does not interfere with the system operation. Electrical separation is maintained between the redundant divisions~~
  - Section 4.2 (Safety-related Functions): See Subsection 7.2.1.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are discussed in Sections 7.2.1.1, 7.2.1.2.4, and 7.2.1.5.2.1.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to the RPS.

- Section 5.2 (Completion of Protective Actions): See Subsections 7.2.1.1 and 7.2.1.3.4.
- Section 5.7 (Capability for Test and Calibration): Subsections 7.2.1.4.1 and 7.2.1.4.2 describe testing of the RPS. Additional information can be found in subsections 7.2.1.3.4, 7.2.1.5.2.2, and 7.2.1.5.11.
- Section 6.2 and 7.2 (Manual Control): See Subsections 7.2.1 1 and 7.2.1.3.4 for discussion of RPS manual control.
- Section 6.4 (Derivation of System Inputs): The two RPS sensing inputs that are not direct measures of the variables are the RPV water level and the loss of feedwater flow in the RPS scram logics. The RPV water level is measured by the differential pressure derived from the sensing line with a reference point. This method is a proven technology in the BWR applications. The loss of the feedwater flow variable is represented by the loss of the power generation bus signal. When the power to the feedwater pump motor is lost, the feedwater flow is also immediately lost. The use of loss of power generation bus signals to represent the loss of feedwater flow signal meets the requirements of the safety-related analysis of Chapter 15, because it is the only credible way that all feedwater flow can be lost.
- Section 6.5 (Capability of Test and Calibration): Subsections 7.1.2.1.4.1 and 7.2.1.4.2 describe testing of the RPS. Additional information can be found in subsections 7.2.1.3.4, 7.2.1.5.2.2, and 7.2.1.5.11.
- Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the RPS are described in Subsections 7.2.1.2.4.1 and 7.2.1.5.2.1.
- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the RPS are described in Subsections 7.2.1.2.4 and 7.2.1.5.2.2.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the RPS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the RPS are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The RPS design conforms to these requirements.

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

- Conformance: The RPS design of bypass and inoperable status indication conforms to these requirements and is consistent with the conformance of the RPS design to RG 1.47. ~~It also conforms to the requirements for control and protection system interaction, as described in IEEE Std. 603, Sections 5.8 and 6.3~~

10 CFR 50.34(f)(2)[II.K.1.22], Auxiliary Heat Removal Systems:

- Conformance: The RPS conforms to these requirements.

10 CFR 50.34(f)(2)(xxiii)[II.K.2.10], Anticipatory Reactor Trip:

- Conformance: The reactor will trip in response to a Loss of All Feedwater Flow Event. This is an anticipatory trip actuated on a power generation bus loss event~~loss of power to two of the four main FW pumps~~. The reactor will also trip on a turbine trip only if an insufficient number of bypass valves opens within a prescribed time period.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The RPS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.63, Loss of All Alternating Current Power:

- Conformance: The RPS conforms to these requirements.

10 CFR 52.47(a)~~(1)(iv)~~(21), 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)~~(b)(1)~~(vi)~~, ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for Instrumentation and Control (I&C) systems and equipment in Tier 1.

10 CFR 52.47(a)~~(1)(vii)~~(25), 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 RPS within the DCD documents conforms to this requirement.

10 CFR 52.47~~(b)~~(c)(2)~~(i)~~, Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.2.1.3.2 General Design Criteria

GDC 1, 2, 4, 10, 12, 13, 19, 20, 21, 22, 23, 24, 25, 26, 27 and 29:

- Conformance: The RPS design conforms to these GDC.

7.2.1.3.3 Staff Requirements Memorandum

Item II.Q of SECY-93-087, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The Reactor Trip (Protection) System design conforms to Item II.Q of SECY-93-087 NRC Branch Technical Position (BTP HICB-19) by the implementation of an additional Diverse Instrumentation and Control System described in Section 7.8.

7.2.1.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Actuation Functions - This includes conformance to BTP HICB-8:

- Conformance: The system is capable of being tested, from sensor device to final actuator device, during plant operation. The tests must be performed in overlapping stages so an actual reactor scram would not occur as a result of the testing. ~~The portions of the protection systems subject to periodic testing are designed in accordance with IEEE Std. 603, Sections 5.7 and 6.5, which supersedes IEEE Std. 279~~

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

- Conformance: Automatic indication that a system is out of service is provided in the MCR~~ (IEEE Std. 603, Section 5.8)~~. Indicators show which part of a system is not operable and which division is bypassed. Annunciator test switches are provided in the MCR.

  Individual indicators are arranged together in the MCR to indicate which function of the system is out of service, bypassed, or otherwise inoperable. These automatic indicators remain available, and cannot be cleared until the function is operable~~ (IEEE Std. 603, Sections 5.2 and 5.8)~~.

  A manual switch or push button is provided for manual bypass actuation, which annunciates out-of-service conditions~~ (IEEE Std. 603, Section 5.8)~~.

  These display provisions serve to supplement administrative controls and aid the operator in assessing the availability of component and system-level protective actions~~ (IEEE Std. 603, Section 5.8)~~. These displays do not perform a safety-related function~~ (IEEE Std. 603, Section 5.7)~~.

  System out-of-service alarm circuits are electrically isolated from the plant safety-related systems to prevent adverse effects~~ (IEEE Std. 603, Section 5.7)~~.

  Testing is included on a periodic basis when equipment associated with the display is tested.

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

- Conformance: The RPS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy for the single failure

criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related systems designs' conformance to the single-failure criterion. ~~Compliance with RG 1.53 is satisfied by specifying, designing, and constructing the RPS to meet the single-failure criterion of IEEE Std. 603, Section 5.1, and IEEE Std. 379. Redundant sensors are used and the logic is arranged to ensure that a failure in a sensing element, decision logic, or an actuator does not prevent protective action. Separate channels are employed so a fault affecting one channel does not prevent the other channels from operating properly.~~

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: Means are provided for manual initiation of reactor scram through the use of two control switches and the Reactor Mode Switch ~~(IEEE Std. 603, Section 6.2)~~. Reactor scram is accomplished by operation of both pushbutton switches, or by placing the Reactor Mode Switch in the Shutdown position. These controls are located on the MCR console.

  The common equipment required for initiation of both manual scram and automatic scram is limited to actuator load power sources, actuator loads, and cabling between the two. There is no shared trip or scram logic equipment for manual scram and automatic scram ~~(IEEE Std. 603, Sections 5.6 and 6.2)~~. No single failure in the manual, automatic, or common portions of the protection system would prevent initiation of reactor scram by manual or automatic means.

  Manual initiation of reactor scram, once initiated, goes to completion as required by IEEE Std. 603, Section 5.2.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The RPS design complies with the criteria set forth in IEEE Std. 603, Section 5.6, and RG 1.75~~, which endorses IEEE Std. 384~~. Safety-related circuits and safety-related associated circuits are identified and separated from redundant and nonsafety-related circuits. Isolation devices are provided where an interface exists between redundant safety-related divisions and between safety-related or safety-related associated circuits and nonsafety-related circuits. See Subsection 8.3.1.4.1 for RPS separation requirements.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Setpoints for Safety-Related Instrumentation:

- Conformance: The RPS initiation setpoints are consistent with this guide. Reference 7.2-1 provides a detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection System:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by~~The RPS design complies with~~ RG 1.118~~ as amplified in IEEE Std. 338~~. The RPS is designed so its individual elements can periodically and independently be tested to demonstrate system reliability is being maintained. Safety-related RPS equipment allows for inspection and testing during periodic shutdowns and refueling.

RG 1.151, Instrument Sensing Lines:

- Conformance: NBS provides the measurement inputs to RPS. The NBS instrument sensing lines conform to the guidelines of RG 1.151 and ISA-67.02.01. Flow restrictors are provided inside containment on instrument lines connected to the RCPB. Accessible manual isolation valves and self-actuating excess flow check valves are provided outside the drywell. The mechanical design guidelines as defined by ISA-67.02.01 and RG 1.151 are met as applicable for each installation.

RG 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design complies with RG 1.152. The hardware and software for the RPS function and other safety-related systems are developed in compliance with RG 1.152, which endorses IEEE Std. 7-4.3.2. The structured development plan for the RPS includes conformance to all software standards referenced in IEEE Std. 7-4.3.2. Hardware and software are integrated into a final assembly validated by testing against input requirements.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The ~~configuration of the~~ RPS design ~~and other safety-related systems regarding independence, separation, and the single-failure criterion~~ conforms to ~~the guidance of RG 1.153, which endorses IEEE Std. 603~~10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.168 as implemented on the RTIF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.169 as implemented on the RTIF platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.170 as implemented on the RTIF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.171 as implemented on the RTIF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.172 as implemented on the RTIF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.173 as implemented on the RTIF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The RPS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.2.1.3.5 Branch Technical Positions

~~BTP HICB-3, Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service:~~

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

BTP HICB-8, Guidance on Application of RG 1.22:

- Conformance: The RPS design conforms to BTP HICB-8.

BTP HICB-9, Guidance on Requirements for RPS Anticipatory Trips:

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

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The RPS design conforms to this position. The RPS logics use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

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

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

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

  The digital RPS trip setpoints do not drift and any changes are reported to the N-DCIS as alarms. The analog-to-digital converters are self-calibrating, and the RPS uses self-diagnostics, all of which are reported to the N-DCIS through the required safety-related isolation. It is expected that all of the variability in the parameter channel will be attributable to the field sensor. The established setpoints provide margin to fulfill both safety requirements and plant availability objectives.

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

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

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.~~ The NMS conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the NMS conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsections 7.2.2.1.1.2, 7.2.2.1.2.1, 7.2.2.1.3.1, and 7.2.2.1.4.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): See Subsections 7.2.2, Tables 7.2-2 and 7.2-4 for a description of the NMS system Operating Bypasses and Permissive Conditions.
  - Section 4.6 (Spatially Dependent Variables): See Subsections 7.2.2.2.4.3, 7.2.2.2.5.3, 7.2.2.2.6.3, and Tables 7.2-6 through 7.2-10 for a description of the NMS system sensor and location information.
  - Section 5.2 (Completion of Protective Actions): Completion of Protective Actions are not applicable beyond that discussed in subsection 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): See Subsections 7.2.2.4.1 through 7.2.2.4.2.4 for NMS Test and Calibration Capability.
  - Section 6.2 and 7.2 (Manual Control): Manual Control is not applicable to NMS.

- Section 6.4 (Derivation of System Inputs): The NMS derives its sense and command features from direct measurements.
- Section 6.5 (Capability of Test and Calibration): See Subsections 7.2.2.4.1 through 7.2.2.4.2.4 for NMS Test and Calibration Capability.
- Section 6.6 and 7.4 (Operating Bypasses): See Section 7.2.2, Tables 7.2-2 and 7.2-4 for a description of the NMS system Operating Bypasses and Permissive Conditions.
- Section 6.7 and 7.5 (Maintenance Bypasses): See Subsections 7.2.2.2.4.6, 7.2.2.2.5.6, 7.2.2.2.6.6, 7.2.2.2.7.5 for a description of NMS Maintenance Bypasses.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the NMS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the NMS power sources are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

~~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)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The NMS design conforms to these requirements.

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 addition, the design conforms to the requirements of control and protection system interaction as described in IEEE Std. 603, Sections 5.8 and 6.3.~~

The 12 SRNM channels are divided into four divisions and are independently assigned to four bypass groups such that bypass of up to four SRNM channels at any one time is allowed while still providing the required monitoring and protection capability (with any three of the four divisions of safety-related power available).

10 CFR 50.34 (f) (2) (xviii) [II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: The LPRM assemblies contain thermocouples that are available for monitoring core cooling. The discussion of the thermocouples for LPRM is addressed in Subsection 7.2.2.2.5.3.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The NMS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants:

- Conformance: The NMS conforms to these requirements.

10 CFR 52.47(a)~~(1)(iv)~~(21), 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)~~(b)(1)~~(vi)~~, ITAAC in Design Certification Applications:

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

10 CFR 52.47(a)~~(1)(vii)~~(25), 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 NMS within the DCD documents conforms to this requirement.

10 CFR 52.47(c)~~(b)~~(2)~~(i)~~, Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.2.2.3.2 General Design Criteria

GDC 1, 2, 4, 10, 12, 13, 19, 20, 21, 22, 23, 24, 25, 26, 27, and 29:

- Conformance: The NMS design complies with these GDC.

7.2.2.3.3 Staff Requirements Memorandum

Item II.Q of SECY-93-087, (Defense Against Common-Mode Failures in Digital Instrument and Control Systems):

- Conformance: The NMS design, as part of the safety-related system, minimizes the likelihood of common mode failures, and conforms to this requirement by the

implementation of additional Diverse Instrumentation and Control System capabilities, described in Section 7.8.

7.2.2.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Actuation Functions:

- Conformance: The NMS design conforms to RG 1.22.

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

- Conformance: The NMS design conforms to RG 1.47.

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

- Conformance: The NMS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single-failure criterion.~~The NMS design conforms to RG 1.53.~~

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The NMS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants~~Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident~~:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.~~The NMS design conforms to RG 1.97.~~

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Instrument Setpoints for Safety-Related Systems:

- Conformance: The NMS design conforms to RG 1.105. Reference 7.2-1 provides a detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: ~~The NMS design conforms to~~Periodic testing of the protection systems is performed in accordance with IEE Std. 338, as modified by RG 1.118.

RG 1.152, Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation and Control Portions of Safety Systems:

- Conformance: The NMS design conforms ~~to RG 1.153~~10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.168 as implemented on the NMS platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.169 as implemented on the NMS platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.170 as implemented on the NMS platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.171 as implemented on the NMS platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.172 as implemented on the NMS platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.173 as implemented on the NMS platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The NMS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.2.2.3.5 Branch Technical Positions

~~BTP HICB-3, Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service:~~

~~Conformance: Because there is no reactor coolant pump BTP HICB-3 does not apply.~~

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The NMS design conforms to BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5~~There are four divisional safety-related subsystems of the NMS. Each division is entirely redundant and identical in design. The divisions are independent of each other, and each is capable of providing indication of neutron flux for the required range. The NMS equipment is qualified to the requirements of IEEE Std. 323. Therefore, the NMS complies with BTP HICB-10~~.

BTP HICB~~P~~-11, Guidance for Application and Qualification of Isolation Devices:

- Conformance: The NMS design conforms to BTP HICB~~P~~-11. The NMS equipment uses safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices to meet the requirements of RG 1.75 and RG 1.153.

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

- Conformance: The analytical limits of the safety-related setpoints of the NMS are determined from safety analyses for each reactor fuel cycle to ensure the reactor core is protected from any rising neutron flux potentially exceeding these values. The nominal setpoints are calculated to be consistent with the GEH standard setpoint methodology (Reference 7.2-1), which conforms to RG 1.105. The setpoint margin calculated by this method also has considered additional uncertainties with the calibration interval. Therefore, the NMS meets BTP HICB-12.

divisional Q-DCIS to the RPS. Safety-related protective actions are generated by the RPS. Abnormal status alarms, data display, and recording are provided.

7.2.3.3 Safety Evaluation

Table 7.1-1 identifies the SPTM function 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.

7.2.3.3.1 Code of Federal Regulations

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

- Conformance: The SPTM function complies with these standards

10 CFR 50.55a(h), Protection and Safety Systems, compliance with 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 SPTM portion of CMS consists of four redundant divisions so failure of any single temperature element does not interfere with the system operation. Electrical separation is maintained between the redundant divisions.~~The SPTM function conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the SPTM function conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 7.2.3.1.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable to the SPTM function.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency requirements of the SPTM function are described in Subsection 7.2.1.2.4.2.
  - Section 5.2 (Completion of Protective Actions): Completion of Protective Actions are not applicable beyond that discussed in subsection 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): Subsection 7.2.3.4 describes testing requirements specific to the SPTM function.
  - Section 6.2 and 7.2 (Manual Control): Manual Control is not applicable to the SPTM function.
  - Section 6.4 (Derivation of System Inputs): SPTM inputs are derived from direct measures.
  - Section 6.5 (Capability of Test and Calibration): Subsection 7.2.3.4 describes testing requirements specific to the SPTM function.

- Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses are not applicable to the SPTM function.
- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the SPTM function are adequately described in Subsection 7.1.6.6.1.24.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the SPTM function are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the SPTM function are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The SPTM function conforms to these requirements.

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

- Conformance: The SPTM function complies by providing automatic indication of bypassed and inoperable status.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The SPTM function conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)~~(1)(iv)~~(21), 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)~~(b)(1)~~(vi)~~, ITAAC in Design Certification Applications:

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

10 CFR 52.47(a)~~(1)(vii)~~(25), 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 SPTM function within the DCD documents conforms to this requirement.

10 CFR 52.47~~(b)~~(c)(2)~~(i)~~, Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.2.3.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, ~~25,~~ and 29:

- Conformance: The SPTM function complies with these GDC.

7.2.3.3.3 Staff Requirements Memorandum

Item II.Q, (Defense Against Common-Mode Failures in Digital Instrument and Control Systems):

- Conformance: The SPTM ~~subsystem design~~function conforms to item II.Q of SECY-93-087 (BTP HICB-19) by the implementation of diverse instrumentation and control~~,~~ described in Section 7.8.

7.2.3.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Actuation Function:

- Conformance: The SPTM ~~design~~ function conforms to RG 1.22.

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

- Conformance: The SPTM ~~design~~ function conforms to RG 1.47.

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

- Conformance: ~~The SPTM design conforms to RG 1.53.~~ The SPTM is organized into four physically and electrically-isolated divisions that use the principle of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single-failure criterion.

~~RG 1.62, Manual Initiation of Protective Actions:~~

~~Conformance: The SPTM design conforms to RG 1.62.~~

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The SPTM ~~design~~ function conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The SPTM ~~design~~ function conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants~~Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident~~:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.~~The SPTM design conforms to RG 1.97~~.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The SPTM ~~design~~ function conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Setpoints for safety-related Instrumentation:

- Conformance: The SPTM ~~design~~ function conforms to RG 1.105. Reference 7.2-1 provides a detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection System:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEE Std. 338, as modified by ~~The SPTM design conforms to~~ RG 1.118.

RG 1.151, Instrument Sensing Lines:

- Conformance: The SPTM function conforms to RG 1.151.

RG 1.152, Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants:

- Conformance: The SPTM function~~design~~ conforms to RG 1.152.

RG 1.153, Power Instrumentation & Control Portions of Safety Systems:

- Conformance: The SPTM ~~design~~ function conforms to ~~RG 1.153~~10 CFR 50.55a(h).

RG 1.168, Verification, Validation Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM ~~design~~ function conforms to RG 1.168 as implemented on the RTIF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM ~~design~~ function conforms to RG 1.169 as implemented on the RTIF platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM ~~design~~ function conforms to RG 1.170 as implemented on the RTIF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM ~~design~~ function conforms to RG 1.171 as implemented on the RTIF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM ~~design~~ function conforms to RG 1.172 as implemented on the RTIF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM ~~design~~ function conforms to RG 1.173 as implemented on the RTIF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The SPTM ~~design~~ function conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The SPTM ~~design~~ function conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The SPTM ~~design~~ function conforms to RG 1.209~~.~~ See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.2.3.3.5 Branch Technical Positions

~~BTP HICB-3, Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service:~~

~~Conformance: Because there is no reactor coolant pump BTP HICB-3 does not apply.~~

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The SPTM ~~design~~ function conforms to BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5~~The SPTM design conforms to BTP HICB-10~~.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The SPTM ~~design~~ function conforms to BTP HICB-11. RTIF logic controllers for the SPTM use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

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

- Conformance: The SPTM ~~design~~ function conforms to BTP HICB-12.

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

- ~~Conformance: Because the SPTM uses thermocouple-type temperature sensors BTP HICB-13 does not apply.~~

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

- Conformance: The SPTM ~~design~~ function conforms to BTP HICB-14.

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

- Conformance: The SPTM ~~design~~ function conforms to BTP HICB-16.

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

- Conformance: The SPTM ~~design~~ function conforms to BTP HICB-17.

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

- ~~Conformance: The SPTM design conforms to BTP HICB-18.~~

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

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

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

- Conformance: The SPTM ~~design~~ function conforms to BTP HICB-21.

Table 7.1-1 identifies the ADS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.3.1.1.3.1 Code of Federal Regulations

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

- Conformance: The ADS design complies with 10 CFR 50.55a(a)(1).

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

- Conformance: ~~The ADS design complies with 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 ADS is divisionalized and designed with redundancy so failure of any instrument will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.~~ The ADS design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the ADS design conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 7.3.1.1.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses See Subsection 7.3.1.1.2.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to ADS.
  - Section 5.2 (Completion of Protective Actions): See Subsection 7.3.1.1.2.
  - Section 5.7 (Capability for Test and Calibration): See Subsections 7.3.1.1.2.
  - Section 6.2 and 7.2 (Manual Control): See Subsection 7.3.1.1.2.
  - Section 6.4 (Derivation of System Inputs): Derivation of System Inputs for the DPS are not applicable beyond that discussed in Subsection 7.1.6.6.1.20.
  - Section 6.5 (Capability of Test and Calibration): See Subsection 7.3.1.1.2.
  - Section 6.6 and 7.4 (Operating Bypasses): See Subsection 7.3.1.1.2.
  - Section 6.7 and 7.5 (Maintenance Bypasses): See Subsection 7.3.1.1.2.
  - Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the DPS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
  - Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the DPS are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(1)(v)[II.K.3.13], HPCI and RCIC Initiation Levels:

- Conformance: The ADS design conforms to these requirements.

10 CFR 50.34(f)(1)(x)[II.K.3.28], Automatic Depressurization System Functioning During/Following an Accident Situation:

- Conformance: The ADS design conforms to these requirements.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The ADS design conforms to these requirements.

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

- Conformance: The ADS design complies with 10 CFR 50.34 (f) (2) (v) ([I.D.3).].

10 CFR 50.34(f)(2)(x)[II.D.1], Relief and Safety Valve Test Requirements:

- Conformance: The ADS design conforms to these requirements.

10 CFR 50.34(f)(2)(xi)[II.D.3], Direct Indication of Relief and Safety Valve Position in the Control Room:

- Conformance: The ADS design conforms to these requirements.

~~10 CFR 50.34 (f) (2) (xiv) (II.E.4.2), Containment Isolation Systems:~~

- ~~Conformance: The ADS design complies with 10 CFR 50.34 (f) (2) (xiv) (II.E.4.2).~~

10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: NBS provides the reactor water level measurement (temperature compensated) inputs to ADS. The reactor water level instrumentation errors due to non-condensable gases in instrument reference legs are addressed in Subsection 7.7.1.2.2.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instruments for Monitoring Plant Conditions Following Core Damage:

- Conformance: The ADS design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The ADS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)~~(1)(iv)~~(21), 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(b)~~(a)~~(1)~~(vi)~~, ITAAC in Design Certification Applications:

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

10 CFR 52.47(a)~~(1)(vii)~~(25), 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 ADS within the DCD conforms to this requirement.

10 CFR 52.47~~(b)~~(c)(2)~~(i)~~, Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.1.1.3.2 General Design Criteria

GDC 1, 2, 4, 13, 15, 19, 20, 21, 22, 23, ~~and~~ 24, 29, 30, 33, 35, and 37:

- Conformance: The ADS design complies with these GDCs.

7.3.1.1.3.3 Staff Requirements Memorandum

SRM on SECY 93-087, Item II.Q Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: Implementation of a Diverse I&C System, the DPS, is described in Section 7.8.

7.3.1.1.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Actuation Functions:

- Conformance: Components are tested periodically during refueling outages every two years. The ADS design conforms to RG 1.22 with the clarification that for the DPVs, periodic testing is interpreted to mean testing of the squib initiators in a laboratory after removal from the squib valves. ~~Refer also to Subsection 7.3.1.1.4.~~

  Because the DPVs are squib-actuated and cannot be closed once they are opened, there is no practicable system design to allow testing during reactor operation without creating an unacceptable breach of the RCPB. The SRVs are tested with the reactor at low power and at, or near, rated pressure. Both the squib wires and the SRV solenoids are continuously monitored for electrical continuity, as indicated in Subsection 7.3.1.1.4.

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

- Conformance: The ADS design conforms to RG 1.47. Automatic indication is provided in the MCR to inform the operator that the system is inoperable or a division is bypassed.

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

- Conformance: ~~The ADS design conforms to RG 1.53, IEEE Std. 603, Section 5.1, and IEEE Std. 379.~~ The ADS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The ADS design conforms to RG 1.62. Manual actuation of ADS requires the operator to actuate at least two dual action switches. This ensures that manual initiation of the ADS is a premeditated act.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The ADS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Instrument Setpoints for Safety-Related Systems:

- Conformance: The setpoints used to initiate the ADS are consistent with RG 1.105. Because the discrete setpoints in the ADS logic do not drift, most of the variation is expected to be in the process transmitters. Setpoints are continuously monitored and alarmed by the PCF. Reference 7.3-2 provides a detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEE Std. 338, as modified by ~~The ADS design conforms to the guidance of~~ RG 1.118. A full functional test of the ADS is not practical, because a LOCA results if the non-reclosable DPVs are opened. Acceptable reliability of equipment operation is

demonstrated by alternate test methods. System logic is periodically self-tested, and initiating circuits are continuously monitored. DPV valve initiators periodically are removed and test-fired in a laboratory. RPV level transmitters are located outside containment, so calibration verification can be performed during plant operation.

RG 1.151, Instrument Sensing Lines:

- Conformance: NBS provides the measurement inputs to ADS. The NBS instrument sensing lines conform to the guidelines of RG 1.151 and ISA-67.02.01. Flow restrictors are provided inside containment on instrument lines connected to the RCPB. Accessible manual isolation valves and self-actuating excess flow check valves are provided outside the drywell. The mechanical design guidelines as defined by ISA-67.02.01 and RG 1.151 are met as applicable for each installation.

RG 1.152, Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The ADS design conforms to ~~RG 1.153~~10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.168 as implemented on the SSLC/ESF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The ADS design conforms to RG 1.169 as implemented on the SSLC/ESF platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.170 as implemented on the SSLC/ESF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.171 as implemented on the SSLC/ESF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.172 as implemented on the SSLC/ESF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.173 as implemented on the SSLC/ESF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems:

- Conformance: The ADS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.3.1.1.3.5 Branch Technical Positions

~~BTP HICB-3, Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service:~~

- ~~Conformance: BTP HICB-3 is not applicable to the design because there is no reactor coolant pump.~~

~~BTP HICB-4, Guidance on Design Criteria for Auxiliary Feedwater Systems:~~

- ~~Conformance: BTP HICB-4 is not applicable to the ADS.~~

~~BTP HICB-6, Guidance on Design of I&C Provided to Accomplish Changeover from Injection to Recirculation Mode:~~

- ~~Conformance: There is no recirculation pump and no active ECCS pumps. Therefore, BTP HICB-6 is not applicable.~~

BTP HICB-8, Guidance on Application of RG 1.22:

- Conformance: BTP HICB-8 calls for the identification of the actuated equipment not tested during reactor operation, and for a discussion of how each conforms to the justification criteria of Paragraph D.4 of RG 1.22. The ADS design conforms to RG 1.22 with the clarification that for the DPVs, periodic testing is interpreted to mean testing of the squib initiators in a laboratory after removal from the squib valves.

  Because the DPVs are squib-actuated and cannot be closed once they are opened, there is no practicable system design to allow testing during reactor operation without creating an unacceptable breach of the RCPB. The SRVs are tested with the reactor at low power

and at, or near, rated pressure. Both the squib wires and the SRV solenoids are continuously monitored for electrical continuity, as indicated in Subsection 7.3.1.1.~~3~~4.

The SRVs and DPV initiators can be tested when the reactor is shut down.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The ADS design conforms to BTP HICB-11.

ADS logic is controlled by the SSLC/ESF system. SSLC/ESF logic controllers for the ADS use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices. The Q-DCIS provides the communication functions for SSLC/ESF. See Subsections 7.1.2, 7.1.3.2 and 7.1.3.3 for a description of the Q-DCIS communication system design.

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

- Conformance: The ADS design conforms to BTP HICB-12. See Reference 7.3-2.

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

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

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

- Conformance: The ADS design conforms to BTP HICB-14.

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

- Conformance: The level of detail provided for the ADS within the DCD conforms to BTP HICB-16.

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

- Conformance: The ADS design conforms to BTP HICB-17.

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

- ~~Conformance: The ADS design conforms to BTP HICB-18.~~

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

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

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

- Conformance: The ADS design conforms to BTP HICB-21.

7.3.1.1.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for 7.3 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v) ~~(~~[I.D.3~~)~~]~~, and 10 CFR 50.34(f)(2)(xiv)(II.E.4.2)~~ apply to the ADS. The ADS complies with the requirements as indicated above. TMI action plan requirements are addressed in Appendix 1A.

7.3.1.1.4 Testing and Inspection Requirements

The ADS trip logic units (TLUs) continuously self-test ~~(IEEE Std. 603, Sections 4.12, 5.7 and 6.5)~~, as shown in Table 7.3-1. A very low current is used to test the continuity of the SRV pilot solenoids and the bridge wires within the DPV squib valve actuating circuitry. The test current is continuously applied, and triggers an alarm if the circuit is interrupted. Testing of ADS equipment is conducted during refueling outages. Refer to Subsection 6.3.2.8.4 for a discussion of mechanical tests performed on the ADS. The same continuity test also is applied to the GDCS squib valves described in Subsection 7.3.1.2.

7.3.1.1.5 Instrumentation and Control Requirements

System status during normal plant operation and ADS performance monitoring ~~(IEEE Std. 603, Section 5.8)~~ in an accident relies on the following MCR indications (additional discussion on the ADS instrumentation is contained in Subsection 7.3.1.1.2):

- Status indication of the SRVs and DPVs;
- SRV discharge line temperature alarm;
- RPV pressure indication;
- Suppression pool high/low level alarm;
- GDCS pool low level alarm;
- Water level indication for the GDCS pools, suppression pool, and RPV; and
- Alarms for the following ADS parameters in the MCR:
  - Manual arming of ADS,
  - Manual actuation of ADS,

The GDCS has no equipment protective interlocks that could interrupt automatic system operation. To initiate the GDCS injection and equalization systems manually, a RPV low-pressure signal must be present. This prevents system initiation while the reactor is at operating pressure. The GDCS injection and equalizing functions are designed to operate from safety-related power. The system instrumentation is powered by divisionally separated safety-related power. The injection squib valve, and the equalizing squib valve logic and initiation circuitry is powered by divisionally separated, safety-related power (Refer to Section 8.3). The mechanical aspects of the GDCS are discussed in Subsection 6.3.2.

The two deluge system temperature switches and related contacts are safety-related only to prevent the inadvertent actuation of the deluge valves. No single failure within the deluge system control and monitoring equipment causes an inadvertent actuation of the deluge system ~~(IEEE Std. 603, Section 5.1)~~. This is to protect against inadvertently draining the GDCS pools, thereby preventing the injection and equalizing systems from performing their safety functions.

Table 7.1-1 identifies the GDCS and the associated codes and standards applied in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards. Any exceptions or clarifications are so noted.

7.3.1.2.3.1 Code of Federal Regulations

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

- Conformance: The GDCS design complies with these standards.

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

- Conformance: The GDCS design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the GDCS conforms to IEEE Std. 603 is discussed below.~~Safety-related systems 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 GDCS is divisionalized and designed with redundancy so failure of any instrument will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.~~
  - Section 4.2 (Safety-related Functions): See Subsection 7.3.1.2.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the GDCS system.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to GDCS.
  - Section 5.2 (Completion of Protective Actions): Completion of Protective Actions is not applicable beyond that discussed in subsection 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): See Subsection 7.3.1.2.4.
  - Section 6.2 and 7.2 (Manual Control): See Subsection 7.3.1.2.2.

- Section 6.4 (Derivation of System Inputs): The GDCS derives its sense and command features from direct measurements.
- Section 6.5 (Capability of Test and Calibration): See Subsection 7.3.1.2.4.
- Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the GDCS are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.
- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the GDCS are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the GDCS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the GDCS are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(1)(v)[II.K.3.13], HPCI and RCIC Initiation Levels,

- Conformance: The GDCS design conforms to these requirements.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design,

- Conformance: The GDCS design conforms to these requirements.

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

- Conformance: The GDCS design complies by providing automatic indication of bypassed and inoperable status ~~(IEEE Std. 603, Section 5.8)~~.

~~10 CFR 50.34(f)(2)(xiv)(II.E.4.2), Containment Isolation Systems:~~

- ~~Conformance: The GDCS design complies with this requirement.~~

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The GDCS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.63, Loss of All Alternating Current Power:

- Conformance: The GDCS conforms to these requirements.

10 CFR 52.47(a)~~(1)(iv)~~(21), 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)~~(b)(1)~~(vi)~~, ITAAC in Design Certification Applications:

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

10 CFR 52.47(a)~~(1)(vii)~~(25), 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 GDCS within the DCD conforms to this requirement.

10 CFR 52.47(c)~~(b)~~(2)~~(i)~~, Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.1.2.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, ~~and~~ 24, 29, 33, 35, and 37:

- Conformance: The GDCS design complies with these GDCs.

7.3.1.2.3.3 Staff Requirements Memorandum

SECY-93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems:

- Conformance: The GDCS design conforms to these criteria by providing diverse I&C, as described in Section 7.8.

7.3.1.2.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Function:

- Conformance: System logic is tested continually as described in Subsection 7.3.1.2.4. Components are tested periodically during refueling outages. The GDCS design complies with RG 1.22. In the GDCS, the squib valves are not actuated during reactor operation, because their actuation would adversely affect the operation of the plant by resulting in a reactor shutdown.

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

- Conformance: The GDCS design complies with RG 1.47. Automatic indication is provided in the MCR to inform the operator that the system is inoperable or a division is bypassed.

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

- Conformance: ~~The GDCS design complies with RG 1.53, IEEE Std. 603, Section 5.1, and IEEE Std. 379.~~ The GDCS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1;

additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The GDCS design complies with RG 1.62. Each division of the GDCS has a manual actuation switch in the MCR. Initiation of the system requires actuation of two switches to ensure that manual initiation is a premeditated act. There is an interlock between the manual initiation switches and a low reactor-pressure signal. This interlock prevents manual initiation of the system if the RPV is not depressurized.

RG 1.75, Physical Independence of Electric Systems:

- The GDCS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Instrument Setpoints for Safety-Related Systems:

- Conformance: The setpoints used to initiate GDCS are established consistent with RG 1.105. Reference 7.3-2 provides a detailed description of the GEH methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEE Std. 338, as modified by~~The GDCS design complies with the guidance of~~ RG 1.118.

RG 1.151, Instrument Sensing Lines:

- Conformance: NBS provides the measurement inputs to GDCS. The NBS instrument sensing lines conform to the guidelines of RG 1.151 and ISA-67.02.01. Flow restrictors are provided inside containment on instrument lines connected to the RCPB. Accessible manual isolation valves and self-actuating excess flow check valves are provided outside the drywell. The mechanical design guidelines as defined by ISA-67.02.01 and RG 1.151

are met as applicable for each installation.~~The GDCS design complies with the guidance of RG 1.151.~~

RG 1.152, Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.152.

RG 1.153, Criteria for Power, I&C Portions of Safety Systems:

- Conformance: The GDCS design complies with 10 CFR 50.55a(h)~~RG 1.153~~.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.168 as implemented on the SSLC/ESF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The GDCS design conforms to RG 1.169 as implemented on the SSLC/ESF platform..

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.170 as implemented on the SSLC/ESF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.171 as implemented on the SSLC/ESF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.172 as implemented on the SSLC/ESF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.173 as implemented on the SSLC/ESF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems:

- Conformance: The GDCS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.3.1.2.3.5 Branch Technical Positions

In accordance with the SRP for Section 7.3 and Table 7.1-1, the following BTPs are addressed for the GDCS:

BTP HICB-1, Guidance on Isolation of the Low Pressure Systems from the High Pressure Reactor Coolant System:

- Conformance: Because the portion of the GDCS downstream of the squib valves connected to the RPV has a design pressure equivalent to the reactor operating pressure, and the low pressure portion of the GDCS upstream of the squib valves is open to the GDCS pools, there is no need for over-pressure protection of the low pressure portion. A high-pressure interlock is provided to prevent inadvertent manual initiation of the GDCS.

~~BTP HICB-3, Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service:~~

- ~~Conformance: BTP HICB-3 is not applicable because the design has no reactor coolant pumps.~~

~~BTP HICB-4, Guidance on Design Criteria for Auxiliary Feedwater Systems:~~

- ~~Conformance: BTP HICB-4 is not applicable to the GDCS.~~

~~BTP HICB-6, Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode:~~

- ~~Conformance: There is no recirculation pump and no active ECCS pumps. Therefore, BTP HICB-6 is not applicable.~~

BTP HICB-8, Guidance on Application of RG 1.22:

- Conformance: BTP HICB-8 requires the identification of actuated equipment not tested during reactor operation and a discussion of how each conforms to the provision of Paragraph D.4 of RG 1.22. In the GDCS, the squib valves are not actuated during reactor operation, because their actuation would adversely affect the operation of the plant by resulting in a reactor shutdown.
  - Given the GDCS system requirements for zero RCPB leakage over the 60-year life of the plant, the only practical solution is for the system actuation valve to be non-reclosing with a metal diaphragm seal that is ruptured to initiate system flow.

– The GDCS is designed to provide adequate inventory make-up to the core in the event of a LOCA. The system has sufficient redundancy and reliability that core-cooling requirements are met in the event of a LOCA.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP -HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: SSLC/ESF logic controllers for the GDCS comply with BTP-HICB-11. SSLC/ESF logic controllers for the GDCS use safety-related fiber optic CIMs and ~~by using~~ fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

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

- Conformance: GDCS logic resides within the SSLC/ESF conforming to BTP HICB-12.

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

- ~~Conformance: BTP HICB-13 does not apply to the GDCS or to the SSLC/ESF neither of which uses the instruments.~~

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

- Conformance: The GDCS design conforms to BTP HICB-14.

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

- Conformance: The GDCS design conforms to BTP HICB-16

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

- Conformance: The GDCS design conforms to BTP HICB-17.

~~BTP HICB-18, Guidance on Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and control Systems:~~

- ~~Conformance: The GDCS design conforms to BTP HICB-18.~~

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

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

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

- Conformance: The GDCS design conforms to BTP HICB-21.

7.3.1.2.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for Section 7.3 and Table 7.1-1, 10 CFR 50.34(f)(2)(v)[I.D.3] ~~and 10CFR 50.34(f)(2)(xiv) [II.E.4.2]~~ (addressed above) apply to the GDCS. The GDCS design complies with these requirements. TMI action plan requirements are generically addressed in Appendix 1A.

7.3.1.2.4 Testing and Inspection Requirements

The GDCS TLUs are self-tested continually at preset intervals. The TLUs of each logic division, and the timers for the automatic logic, can be tested during plant operation ~~(IEEE Std. 603, Sections 5.7 and 6.5)~~. GDCS equipment inside containment is tested during refueling outages. Refer to Subsection 6.3.2.7.4 for a discussion of mechanical tests performed on the GDCS.

7.3.1.2.5 Instrumentation and Control Requirements

The performance and effectiveness of the GDCS in a postulated accident is verified by observing the following MCR indications ~~(IEEE Std. 603, Section 5.8)~~ (additional discussion on the GDCS instrumentation is contained in Subsection 7.3.1.2.2 and in Subsection 6.3.2.7.5):

- Status indication of locked-open maintenance valves;
- Status indication and alarm of the squib-actuated valves;
- Position indication of the GDCS check valves;
- Drywell and RPV pressure indication;
- Suppression pool high/low level alarm;
- GDCS pool high/low level alarm;
- Water level indication for the GDCS pools, suppression pool and RPV; and
- Squib valve open alarm.

The safety-related GDCS instrumentation is designed to operate in a drywell environment resulting from a LOCA. The thermocouples that initiate the deluge valves are qualified to operate in a severe accident environment. Safety-related instruments, located outside the drywell, are qualified for the environment in which they must perform their safety-related functions.

7.3.2 Passive Containment Cooling System

The Passive Containment Cooling System (PCCS) consists of condensers that are an integral part of the containment pressure boundary. The PCCS heat exchanger tubes are located in the

Manual control switches and associated logic are provided in the design of the LD&IS to give the operator the capability to perform manual control functions for initiation of isolation, logic reset, channel bypass and test functions ~~(IEEE Std. 603, Section 6.2 and 7.2)~~.

The instrumentation for the drywell Low Conductivity Waste (LCW) and High Conductivity Waste (HCW) sump levels is designed to meet the leakage rate requirements for identified and unidentified sources. The LD&IS includes isolation logic using high drywell pressure and low RPV water level for the isolation of the drain lines transferring waste from the sumps to the liquid radwaste system. Additional information on LD&IS operation is contained in Subsection 5.2.5.

Table 7.1-1 identifies the LD&IS function and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.3.3.3.1 Code of Federal Regulations

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

- Conformance: The LD&IS design complies with these standards.

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

- Conformance: ~~Separation and isolation is preserved both mechanically and electrically in accordance with IEEE Std. 603, Section 5.6, and RG 1.75. The LD&IS consists of four redundantly designed divisions so failure of any instrument will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.~~ The LD&IS conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the LD&IS conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-Related Functions): See Subsection 7.3.3.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the LD&IS system.
  - Section 4.6 (Spatially Dependent Variables): See Subsection 5.2.5.2.1.
  - Section 5.2 (Completion of Protective Actions): See Subsection 7.3.3.3.
  - Section 5.7 (Capability for Test and Calibration): See Subsection 7.3.3.4 for LD&IS (MSIV), Subsection 7.3.5.4 for Non-MSIV, & 7.4.3.4 for RWCU/SDC.
  - Section 6.2 and 7.2 (Manual Control): See Subsections 7.3.3.3, 7.3.3.1 for LD&IS (MSIV), and 7.3.5.1 for non-MSIV.
  - Section 6.4 (Derivation of System Inputs): See Subsection 7.3.3.2 and Table 7.3-5.
  - Section 6.5 (Capability of Test and Calibration): See Subsections 7.3.3.4 for MSIV and 7.3.5.2.3, 7.3.5.2.4, & 7.3.5.4 for non-MSIV.

- Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the LD&IS are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.
- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the LD&IS (MSIV) are not applicable beyond that discussed in Subsection 7.1.6.6.1.23. See Subsections 7.3.5.2.3 & 7.3.5.2.4 for (non-MSIV).
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the LD&IS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the LD&IS are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The LD&IS design conforms to these requirements.

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

- Conformance: The LD&IS design complies by providing automatic indication of bypassed and inoperable status~~ (IEEE Std. 603, Section 5.8)~~.

10 CFR 50.34(f)(2)(xiv)~~(~~[II.E.4.2]~~)~~, TMI Action Plan Item IIE.4.2, Containment Isolation Systems:

- Conformance: The LD&IS design complies with this requirement.

10 CFR 50.34(f)(2)(xv)[II.E.4.4], Purge System Isolation Under Accident Conditions:

- Conformance: The LD&IS (non-MSIV) conforms to these requirements.

10 CFR 50.34(f)(2)(xxvi)[III.D.1.1], Leakage Control and Detection in Design Systems Outside Containment:

- Conformance: The LD&IS (non-MSIV) conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The LD&IS conforms to these requirements.

10 CFR 50.63, Loss of All Alternating Current Power:

- Conformance: The LD&IS conforms to these requirements.

10 CFR 52.47(a)~~(1)(iv)~~(21), Resolution of Unresolved and Generic Safety Issues:

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

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

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

10 CFR 52.47(a)~~(1)(vii)~~(25), 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 LD&IS in the DCD conforms to this requirement.

10 CFR 52.47~~(b)~~(c)(2)~~(i)~~, Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.3.3.2 General Design Criteria

GDC 1, 2, 4, 13, 15, 16, 19, 20, 21, 22, 23, ~~and~~ 24 29, and 30:

- Conformance: The LD&IS (non-MSIV) design complies with these GDCs.

GDC 1, 2, 4, 13, 15, 16, 19, 20, 21, 22, 23, 24, and 29:

- Conformance: The LD&IS (MSIV only) design complies with these GDCs.

7.3.3.3.3 Staff Requirements Memorandum

SRM on SECY 93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The LD&IS and ESF designs conform to item II.Q of SECY-93-087 (BTP HICB-19) by implementation of diverse I&C, described in Section 7.8.

7.3.3.3.4 Regulatory Guide

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

- Conformance: The LD&IS design conforms to RG 1.22.

RG 1.45, Reactor Coolant Pressure Boundary Leakage Detection Systems:

- Conformance: The LD&IS (non-MSIV) design conforms to RG 1.45.

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

- Conformance: The LD&IS design conforms to RG 1.47.

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

- Conformance: ~~The LD&IS design conforms to RG 1.53.~~The LD&IS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions.

Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The LD&IS design conforms to RG 1.62.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The LD&IS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The LD&IS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The LD&IS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Setpoints for Safety-Related Instrumentation:

- Conformance: The safety-related portions of the LD&IS design conform~~s~~ to RG 1.105. Reference 7.3-2 provides detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEE Std. 338, as modified by~~The LD&IS design conforms to~~ RG 1.118.

RG 1.151, Instrument Sensing Lines:

- Conformance: NBS provides the measurement inputs to LD&IS (non-MSIV). The NBS instrument sensing lines conform to the guidelines of RG 1.151 and ISA-67.02.01. Flow restrictors are provided inside containment on instrument lines connected to the RCPB. Accessible manual isolation valves and self-actuating excess flow check valves are provided outside the drywell. The mechanical design guidelines as defined by ISA-67.02.01 and RG 1.151 are met as applicable for each installation.

RG 1.152, Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS design conforms to RG 1.152.

RG 1.153, Power Instrumentation & Control Portions of Safety Systems:

- Conformance: The LD&IS design conforms to ~~RG 1.153~~10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS (MSIV Only) design conforms to RG 1.168 as implemented on the RTIF platform.

  The LD&IS (non-MSIV) design conforms to RG 1.168 as implemented on the SSLC/ESF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The LD&IS (MSIV Only) design conforms to RG 1.169 as implemented on the RTIF platform.

  The LD&IS (non-MSIV) design conforms to RG 1.169 as implemented on the SSLC/ESF platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS (MSIV Only) design conforms to RG 1.170 as implemented on the RTIF platform.

  The LD&IS (non-MSIV) design conforms to RG 1.170 as implemented on the SSLC/ESF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS (MSIV Only) design conforms to RG 1.171 as implemented on the RTIF platform.

  The LD&IS (non-MSIV) design conforms to RG 1.171 as implemented on the SSLC/ESF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS (MSIV Only) design conforms to RG 1.172 as implemented on the RTIF platform.

  The LD&IS (non-MSIV) design conforms to RG 1.172 as implemented on the SSLC/ESF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS (MSIV Only) design conforms to RG 1.173 as implemented on the RTIF platform.

  The LD&IS (non-MSIV) design conforms to RG 1.173 as implemented on the SSLC/ESF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems:

- Conformance: The LD&IS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The LD&IS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The LD&IS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.3.3.3.5 Branch Technical Positions

~~BTP HICB-3, Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service:~~

- ~~Conformance: BTP HICB-3 is not applicable to the design, which has no reactor coolant pump.~~

~~BTP HICB-4, Guidance on Design Criteria for Auxiliary Feedwater Systems:~~

- ~~Conformance: BTP HICB-4 is not applicable to the LD&IS.~~

~~BTP HICB-6, Guidance on Design of I&C Provided to Accomplish Changeover from Injection to Recirculation Mode:~~

- ~~Conformance: There is no recirculation pump and no active ECCS pumps. Therefore, BTP HICB-6 is not applicable.~~

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The LD&IS design complies with BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The LD&IS (MSIV only) design complies with BTP HICB-11. RTIF logic controllers for the LD&IS (non-MSIV) use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

  The LD&IS (non-MSIV) design complies with BTP HICB-11. SSLC/ESF logic controllers for the LD&IS (non-MSIV) use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

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

- Conformance: The LD&IS design complies with BTP HICB-12.

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

- ~~Conformance: This BTP does not apply to the LD&IS because this system does not use resistance temperature detector-type sensors.~~

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based I&C Systems:

- Conformance: The LD&IS design complies with BTP HICB-14.

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

- Conformance: The LD&IS design complies with BTP HICB-16.

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

- Conformance: The LD&IS design complies with BTP HICB-17.

~~BTP HICB-18, Guidance on the Use of PLC in Digital Computer-Based I&C Systems:~~

- ~~Conformance: The LD&IS design complies with BTP HICB-18.~~

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems:

- Conformance: The LD&IS design complies with BTP HICB-19. The implementation of an additional diverse instrumentation and control system is described in Section 7.8.

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

- Conformance: The LD&IS design complies with BTP HICB-21.

7.3.3.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for 7.3 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v)[I.D.3], and 10 CFR 50.34(f)(2)(xiv)[II.E.4.2] apply to the LD&IS. The LD&IS complies with these requirements as indicated above. TMI action plan requirements are addressed in Appendix 1A.

The CRHS isolation and EFU operation cannot be shut down automatically. EFU disengagement and de-energization of safety-related isolation dampers can be accomplished manually.

The CRHS isolation and EFU actuation are part of the SSLC/ESF system logic is illustrated in Figure 7.3-5. The required instrumentation for CRHS is described in Subsection 9.4.1.5. Alarms for CRHA/Control Room Habitability Area Heating, Ventilation, and Air Conditioning Subsystem conditions are discussed in Subsection 6.4.8.

7.3.4.3 Safety Evaluation

A safety evaluation of the CRHS is provided in Subsections 6.4.5 and 9.4.1.3.

Table 7.1-1 identifies the CRHS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.3.4.3.1 Code of Federal Regulations

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

- Conformance: The CRHS design complies with these standards.

10 C~~R~~FR 50.55a(h), Protection and Safety Systems compliance with ~~Criteria for Protection Systems for Nuclear Power Generating Stations (~~IEEE Std. 603~~)~~:

- Conformance: ~~Separation and isolation is preserved both mechanically and electrically in accordance with IEEE 603 and RG 1.75. The CRHS consists of four redundantly designed divisions so failure of any instrument will not interfere with system operation. Electrical separation is maintained between the redundant divisions.~~ The CRHS design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the CRHS conforms to IEEE Std. 603 is discussed below.

  – Section 4.2 (Safety-related Functions): See Subsection 6.4.1.1.

  – Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are discussed in Subsection 7.3.4.2.

  – Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to CRHS.

  – Section 5.2 (Completion of Protective Actions): Completion of Protective Actions are not applicable beyond that discussed in subsection 7.1.6.6.1.3.

  – Section 5.7 (Capability for Test and Calibration): Test and Calibrate features beyond that discussed in section 7.1.6.6.1.8 are not applicable.

  – Section 6.2 and 7.2 (Manual Control): See Subsection 7.3.4.2.

- Section 6.4 (Derivation of System Inputs): The CRHS derives its sense and command features from direct measurements as described in section 7.3.4.2.
- Section 6.5 (Capability of Test and Calibration): Capability for Test and Calibrate features beyond that discussed in section 7.1.6.6.1.21 is not applicable.
- Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the CRHS are discussed in subsection 7.3.4.2..
- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the CRHS are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the CRHS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the CRHS are discussed in subsection 7.3.4.2.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The CRHS design conforms to these requirements.

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

- Conformance: The CRHS design complies by providing automatic indication of bypassed and inoperable status.

~~10 CFR 50.34(f)(2)(xiv)(II.E.4.2), TMI Action Plan Item IIE.4.2 Containment Isolation Systems:~~

~~Conformance: The CRHS design complies with this requirement.~~

10 CFR 50.34(f)(2)(xxviii)[III.D.3.4], Control Room Habitability Problems Under Accident Conditions:

- Conformance: The CRHS design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The CHRS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.63, Loss of All Alternating Current Power:

- Conformance: The CRHS conforms to these requirements.

10 CFR 52.47(a)~~(1)(iv)~~(21), 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)~~(b)(1)~~(vi)~~, ITAAC in Design Certification Applications:

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

10 CFR 52.47(a)~~(1)(vii)~~(25), 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 CRHS in the DCD conforms to this requirement.

10 CFR 52.47~~(b)~~(c)(2)~~(i)~~, Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.4.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, ~~and~~ 24 and 29:

- Conformance: The CRHS design complies with these GDCs.

7.3.4.3.3 Staff Requirements Memorandum

SRM on SECY 93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The CRHS and ESF designs conform to these criteria, as described in Subsection 7.8.2.2.

7.3.4.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Actuation Function:

- Conformance: The CRHS design conforms to RG 1.22.

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

- Conformance: The CRHS design conforms to RG 1.47.

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

- Conformance: The CRHS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.~~The CRHS design conforms to RG 1.53.~~

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The CRHS design conforms to RG 1.62.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The CRHS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Setpoints for safety-related Instrumentation:

- Conformance: The CRHS design conforms to RG 1.105. Reference 7.3-2 provides detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: ~~The CRHS design conforms to~~Periodic testing of the protection systems is performed in accordance with IEE Std. 338, as modified by RG 1.118.

RG 1.152, Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.152.

RG 1.153, Power Instrumentation & Control Portions of Safety Systems:

- Conformance: The CRHS design conforms to 10 CFR 50.55a(h)~~RG 1.153~~.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.168 as implemented on the SSLC/ESF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The CRHS design conforms to RG 1.169 as implemented on the SSLC/ESF platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.170 as implemented on the SSLC/ESF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.171 as implemented on the SSLC/ESF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.172 as implemented on the SSLC/ESF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.173 as implemented on the SSLC/ESF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The CRHS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.3.4.3.5 Branch Technical Positions

~~BTP HICB-3, Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service:~~

- ~~Conformance: BTP HICB-3 is not applicable to the design, which has no reactor coolant pump.~~

~~BTP HICB-4, Guidance on Design Criteria for Auxiliary Feedwater Systems:~~

- ~~Conformance: BTP HICB-4 is not applicable to the CRHS.~~

~~BTP HICB-6, Guidance on Design of I&C Provided to Accomplish Changeover from Injection to Recirculation Mode:~~

- ~~Conformance: There is no recirculation pump and no active ECCS pumps. Therefore, BTP HICB-6 is not applicable.~~

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The CRHS design complies with BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The CRHS design complies with BTP HICB-11. SSLC/ESF logic controllers for the CRHS use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

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

- Conformance: The CRHS design complies with BTP HICB-12.

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

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

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based I&C Systems:

- Conformance: The CRHS design complies with BTP HICB-14.

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

- Conformance: The CRHS design complies with BTP HICB-16.

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

- Conformance: The CRHS design complies with BTP HICB-17.

~~BTP HICB-18, Guidance on the Use of PLCs in Digital Computer-Based I&C Systems:~~

- ~~Conformance: The CRHS design complies with BTP HICB-18.~~

BTPHICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems:

- Conformance: The CRHS design complies with BTP HICB-19. The implementation of an additional diverse instrumentation and control system is described in Section 7.8.

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

- Conformance: The CRHS design complies with BTP HICB-21.

7.3.4.3.6 Three Mile Island Action Plan Requirements

In accordance with Table 7.1-1, 10 CFR 50.34(f)(2)(v)~~ (~~[I.D.3~~)~~] ~~and 10 CFR 50.34(f)(2)(xiv) (II.E.4.2)~~ appl~~y~~ies to the CRHS. The CRHS complies with the regulatory requirements indicated above. TMI action plan requirements are addressed in Appendix 1A.

7.3.4.4 Testing and Inspection Requirements

Testing and inspections requirements are identified in Subsections 6.4.7 and 9.4.1.4.

7.3.4.5 Instrumentation and Control Requirements

The required instrumentation for the CRHS is described in Subsection 9.4.1.5 and alarms for abnormal CRHA/Control Room Habitability Area Heating, Ventilation, and Air Conditioning Subsystem conditions are addressed in Subsection 6.4.8.

7.3.5 Safety System Logic and Control/Engineered Safety Features

7.3.5.1 System Design Bases

The SSLC/ESF system performs the control logic processing of the plant sensor data and manual control switch signals activating the functions of the LD&IS (non-MSIV), ECCS and CRHS. The SSLC/ESF also performs control logic processing for the decay heat removal, - safe, stable shutdown, ~~function~~ and reactor pressure control functions of the ICS~~, and other safety-related functions~~. SSLC/ESF also provides safety-related display information in support of safety-related system performance and accident monitoring. Logic for detecting and signaling a control rod separation is also included in the SSLC/ESF system.

The SSLC/ESF:

- Monitors safety-related signals providing automatic control of the plant safety protection systems;
- Performs processing of plant sensor and equipment interlock signals according to the required trip and interlock logic, including time delays, of each safety-related interfacing plant system or system important to safe plant operation;

- Meets the performance requirements of each safety-related interfacing plant system or system important to safe plant operation, including transient response, delay time, and overall time to trip system actuators, or initiates necessary system operation;
- Monitors safety-related manual control switches used for system or component test, protection system manual initiation, and individual control of equipment actuators;
- Furnishes trip output signals to actuators driving safety-related system equipment (e.g. solenoids and squib explosive-actuated valves);
- Furnishes trip or initiation outputs signals to the logic of interfacing functions;
- Provides diagnostic facilities for detecting imminent failure of safety-related system components and provides an operator interface facilitating quick repair;
- Provides safety-related accident monitoring display information, alarm and status outputs to operator displays, annunciators, and the PCF; and
- Satisfies regulatory requirements for implementation of:
  - The single failure criterion,
  - Defense-in-depth protection,
  - 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 following functions:

- The non-MSIV isolation functions of the LD&IS;~~,~~
- ~~t~~The ADS functions of the NBS for SRV and DPV control;~~,~~
- ~~t~~The ECCS, and decay heat removal – safe, stable ~~functions of the GDCS and SLC system, the ECCS and~~ shutdown ~~cooling~~ and reactor pressure control functions of the ICS;~~, and~~
- ~~t~~The control room isolation function of the CRHS.~~ The SSLC/ESF architecture is presented Reference 7.3-1 and Reference 7.3-5.~~
- Logic for the detection of a CRD system control rod separation event and transmits the rod separation signal to the RC&IS (described in Subsections 4.6.1 and 7.7.2.2.7).

The SSLC/ESF system also provides safety-related display information for system performance monitoring and accident monitoring (described in Subsection 7.5.1).

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. The final trip signal (from two or more divisions) is then transmitted to the RMU function via the Q-DCIS network to initiate mechanical actuation devices.

There are two independent and redundant VLU functional trains (three for the DPV actuation logic) in each division of the SSLC/ESF equipment. The vote logic trip signals from each VLU functional train are transmitted to the RMU, where a two-out-of-two (or three-out-of-three) confirmation is performed. The redundant trains within a division are necessary to prevent single failures within a division from causing a squib initiator to fire; as a result each VLU logic train is required to operate to produce an output. Self-tests within the SSLC/ESF determine whether any one VLU function has failed, and such a failure is alarmed in the MCR.

associated VLU inputs in the four divisions. Interlocks are provided by a four-position joystick-type switch so only one division of sensors at a time can be placed in bypass. When such a bypass is made, all four divisions of two-out-of-four logic become two-out-of-three logic while the bypass is maintained. Bypass permits calibration and repair of sensors or the DTM function. Although all sensors for all systems are bypassed in one division, the remaining three divisions furnish sufficient redundant sensor data for safe operation. The logic is such that all four divisions still can perform two-out-of-four (two-out-of-three) trip decisions - even if sensors are bypassed. Bypass status is indicated to the operator until the bypass condition is removed. An interlock rejects simultaneous attempts to bypass more than one SSLC/ESF division. Any loss of communication caused by a bypass switch is interpreted as a "no bypass" signal.

7.3.5.2.4 Division-Out-of-Service Bypass

For a fail-safe design, a division-out-of-service bypass inhibits the trip output in a division from affecting the output load drivers/discrete outputs by maintaining that division's load drivers/discrete outputs in an energized state. Bypass status is indicated to the operator until the bypass condition is removed. Only one division can be bypassed at any one time. For the SSLC/ESF logic because the division-of-sensors bypass is implemented, and there are multiple trains of two-out-of-four VLU logic, no additional division trip logic bypass is implemented. Each of the VLU trip outputs is directly applied to one of the load drivers/discrete outputs in series. Each VLU trip is required to prevent inadvertent trip initiation of the squib valves. It is undesirable to perform the VLU logic bypass activities with the RMU electrically connected to the valve. The disable switch that bypasses the load driver/discrete output actuation for the squib initiators provides the effective bypass function required at the actuator level. (Refer to Figure 7.3-1a and Figure 7.3-1b.)

7.3.5.3 Safety Evaluation

The SSLC/ESF consists of a set of logic processing functions for the ESF systems and therefore is a safety-related system. The functions related to sensor signal processing and trip output are safety-related.

The four separated divisions of logic processing equipment provide the necessary degree of redundancy and independence to maintain safe operation despite the loss of portions of the processing capacity.

The SSLC/ESF system is designed so no single equipment failure causes inability to:

- Perform a reactor trip,
- ~~Establish containment isolation~~Perform safety-related decay heat removal and reactor pressure control, or
- Initiate the ESF.

Physically separate divisions are established by their relationship with the RPV, which is spatially divided into four quadrants. The sensors, logic, and output actuators of the various systems are allocated to these divisions.

The digital devices in SSLC/ESF are, in general, microprocessor-based, software-controlled instruments.

Microprocessor-based logic in the SSLC/ESF activates the solenoid-controlled SRVs squib-actuated DPVs, GDCS injection and equalizing valves, ICS valves, and SLC squib valves.

A diverse I&C system is incorporated, featuring a totally independent set of selected reactor trip logic functions and ESF initiation logic functions addressing the requirements of the BTP HICB-19 position. This system is described in Section 7.8. The RPS logic is implemented using a diverse vendor furnished microprocessor-based platform. The SSLC/ESF system is designed to operate in a mild environment in clean areas within the CB and RB safety envelopes. Refer to Appendix 3H, Subsections 9.4.1 and 9.4.6 for specific environmental conditions.

Panel internal environments are maintained to ensure that reliability goals are achieved. Panel internal cooling is by natural convection. Fans are used to improve long-term reliability, but no credit is taken for forced-air cooling in the qualification of safety-related functions. Thermal design adequacy is considered during detail equipment design by analysis of heat loads (per circuit module, per bay, and per module).

Table 7.1-1 identifies the SSLC/ESF and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.3.5.3.1 Code of Federal Regulations

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

- Conformance: The SSLC/ESF design conforms to these standards.

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

- Conformance: ~~Safety-related systems are designed to conform to RG 1.153 and IEEE Std. 603 as discussed in Subsection 7.2.1.3.4.~~ The SSLC/ESF design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the SSLC/ESF design conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 7.3.5.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): See Subsections 7.3.5.2.2, 7.3.5.2.3 and 7.3.5.2.4.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to SSLC/ESF.
  - Section 5.2 (Completion of Protective Actions): See Subsections 7.3.5.2.2.
  - Section 5.7 (Capability for Test and Calibration): See Subsections 7.3.5.2.2 and 7.3.5.4.

- Section 6.2 and 7.2 (Manual Control): See Subsection 7.3.5.1.
- Section 6.4 (Derivation of System Inputs): The SSLC/ESF is a logic processing system only and its sensors are part of other systems.
- Section 6.5 (Capability of Test and Calibration): See Subsection 7.3.5.2.2 and 7.3.5.4.
- Section 6.6 and 7.4 (Operating Bypasses): See Subsection 7.3.5.2.2, 7.3.5.2.3 and 7.3.5.2.4.
- Section 6.7 and 7.5 (Maintenance Bypasses): See Subsection 7.3.5.2.2, 7.3.5.2.3 and 7.3.5.2.4.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the SSLC/ESF are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the SSLC/ESF are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(1)(v)[II.K.3.13], HPCI and RCIC Initiation Levels:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The SSLC/ESF design conforms to these requirements.

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

- Conformance: The SSLC/ESF complies by providing automatic indication of bypassed and inoperable status ~~(IEEE Std. 603, Sections 5.8, 6.2, and 7.2)~~.

10 CFR 50.34(f)(2)(viii)[II.B.3] Capability to Promptly Obtain and Analyze Samples from the Reactor Coolant System and Containment:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(x)[II.D.1], Relief and Safety Valve Test Requirements:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(xi)[II.D.3], Direct Indication of Relief and Safety Valve Position in the Control Room:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34 (f)(2)(xiv) [II.E.4.2], Containment Isolation Systems:

- Conformance: The SSLC/ESF logic controlling containment isolation functions conforms to these criteria.

10 CFR 50.34(f)(2)(xv)[II.E.4.4], Purge System Isolation Under Accident Conditions:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: NBS provides the reactor water level measurement (temperature compensated) inputs to SSLC/ESF. The reactor water level instrumentation errors due to non-condensable gases in instrument reference legs are addressed in Subsection 7.7.1.2.2.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)[II.K.1.22], Auxiliary Heat Removal Systems:

- Conformance: The SSLC/ESF conforms to these requirements.

10 CFR 50.34 (f)(2)(xxiii) [II.K.2.10], Anticipatory Reactor Trip:

- Conformance: The SSLC/ESF initiates the ICS in response to a Loss of All Feedwater Flow Event. This is an anticipatory trip actuated on ~~loss of power to two of the four main FW pumps~~a power generation bus loss event.

10 CFR 52.47(a)~~(1)(iv)~~(21), Resolution of Unresolved and Generic Safety Issues:

10 CFR 50.34(f)(2)(xxvi)[III.D.1.1], Leakage Control and Detection in Design Systems Outside Containment:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of In-plant Airborne Radioactivity:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(xxviii)[III.D.3.4] Control Room Habitability Problems Under Accident Conditions:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.44(c)(4), Combustible Gas Control For Nuclear Power Reactors, Monitoring:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The SSLC/ESF design conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.63, Loss of All Alternating Current Power:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 52.47(a)(21)~~(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)~~(b)(1)~~(vi)~~, ITAAC in Design Certification Applications:

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

10 CFR 52.47(a)~~(1)(vii)~~(25), 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 SSLC/ESF within the DCD conforms to this requirement.

10 CFR 52.47~~(b)~~(c)(2)~~(i)~~, Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.5.3.2 General Design Criteria

GDC 1, 2, 4, 13, 15, 16, 19, 20, 21, 22, 23, ~~and~~ 24, 29, 30, 33, 34, 35, 37, 41, 43, 63 and 64:

- Conformance: The SSLC/ESF design complies with these GDCs.

7.3.5.3.3 Staff Requirements Memorandum

SRM on SECY-93-087, Item II.Q Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The Reactor Trip (Protection) System and ESF designs conform to Item II.Q of SRM on SECY-93-087 (BTP HICB-19) in conjunction with the implementation of the DPS, described in Section 7.8.

SRM on SECY-93-087, Item II.T, Control Room Annunciator (Alarm) Reliability:

- Conformance: The SSLC/ESF VDU design meets the requirements of SECY-93-087, Item II.T for redundancy, independence, and separation in that the "alarm system" is considered redundant as follows:

- Alarm points are sent via dual networks to redundant message processors using dual power supplies. The processors are dedicated to alarm processing.
- The alarms are displayed on multiple independent VDUs (dual power supplies on each).
- The alarms are driven by redundant data links to the AMS (dual power). There are redundant alarm processors.
- There is one horn and one voice speaker. Test buttons are available to test the horn(s) and all the lights.
- There are no alarms requiring manually controlled actions for systems to accomplish their safety-related functions.

7.3.5.3.4 Regulatory Guides

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

- Conformance: The SSLC/ESF design complies with the guidance of RG 1.22.

RG 1.45, Reactor Coolant Pressure Boundary Leakage Detection Systems:

- Conformance: The SSLC/ESF design complies with the guidance of RG 1.45.

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

- Conformance: The SSLC/ESF provides bypass capability and status that complies with RG 1.47.

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

- Conformance: ~~The SSLC/ESF design complies with the guidance of RG 1.53, IEEE Std. 603, Section 5.1 and IEEE Std. 379.~~ The SSLC/ESF is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The SSLC/ESF design complies with the guidance of RG 1.62. Signals for manual initiation of protective actions are hardwired to the SSLC/ESF equipment.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The SSLC/ESF design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The SSLC/ESF design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The SSLC/ESF design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Instrument Setpoints for Safety-related Systems:

- Conformance: The SSLC/ESF design complies with RG 1.105. Reference 7.3-2 provides detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEE Std. 338, as modified by~~The SSLC/ESF design conforms to~~ RG 1.118~~ as amplified in IEEE Std. 338~~. Testing of the SSLC/ESF is performed in conjunction with the Q-DCIS.

RG 1.152, Criteria for Programmable Digital Computer System Software in safety-related Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF design conforms to the guidelines of RG 1.152. Additional discussion is provided in Subsection 7.2.1.3 describing RPS system compliance.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The SSLC/ESF design, in conjunction with the Q-DCIS, conforms to ~~RG 1.153~~10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used In Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF design complies with RG 1.168 as implemented on the SSLC/ESF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF design complies with RG 1.169 as implemented on the SSLC/ESF platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF design complies with RG 1.170 as implemented on the SSLC/ESF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF design complies with RG 1.171 as implemented on the SSLC/ESF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF design complies with RG 1.172 as implemented on the SSLC/ESF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF design complies with RG 1.173 as implemented on the SSLC/ESF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The SSLC/ESF design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The SSLC/ESF design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The SSLC/ESF design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.3.5.3.5 Branch Technical Positions

BTP HICB-1, Guidance on Isolation of the Low Pressure Systems from the High Pressure Reactor Coolant System:

- Conformance: The SSLC/ESF design complies with BTP HICB-1.

~~BTP HICB-3, Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service:~~

- ~~Conformance: BTP HICB-3 is not applicable because there is no reactor coolant pump.~~

~~BTP HICB-4, Guidance on Design Criteria for Auxiliary Feedwater Systems:~~

- ~~Conformance: BTP HICB-4 is not applicable to the SSLC/ESF.~~

~~BTP HICB-6, Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode:~~

- ~~Conformance: There is no recirculation pump and no active ECCS pumps. Therefore, BTP HICB-6 is not applicable.~~

BTP HICB-8, Guidance on Application of RG 1.22:

- Conformance: The SSLC/ESF is fully operational during reactor operation, and is tested in conjunction with the Q-DCIS. Therefore, the SSLC/ESF design complies with BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: SSLC/ESF logic controllers use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices. The Q-DCIS provides the communication functions for SSLC/ESF. See Subsection 7.1.2, 7.1.3.2 and 7.1.3.3 for descriptions of the Q-DCIS communication system design.

  Defined diverse and hardwired portions of RPS and SSLC/ESF may use coil-to-contact isolation of relays or contactors. This is acceptable according to BTP HICB-11 when the application is analyzed or tested in accordance with the guidelines of RG 1.75 and RG 1.153.

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

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

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

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

7.3.6.3.1 Code of Federal Regulations

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

- Conformance: The VB isolation function design complies with these standards.

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 VB isolation 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.~~The VB isolation function conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the VB isolation function conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-Related Function): See Subsection 7.3.6.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the VB isolation function.
  - Section 4.6 (Spatially Dependent Variables): See the Actuation Logic section of Subsection 7.3.6.2 & Subsection 6.2.1.1.5.5.1.
  - Section 5.2 (Completion of Protective Actions): Completion of protective actions is not applicable beyond that discussed in Subsection 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): See Subsection 7.6.3.4.
  - Section 6.2 and 7.2 (Manual Control): See Subsections 7.3.6.1 & 7.3.6.2.
  - Section 6.4 (Derivation of System Inputs): Derivation of system inputs for the VB isolation function are not applicable beyond that discussed in Subsection 7.1.6.6.1.20.
  - Section 6.5 (Capability of Test and Calibration): See Subsection 7.6.3.4.
  - Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the VB isolation function are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.
  - Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance Bypasses for the VB isolation function are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
  - Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the VB isolation function are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
  - Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the VB isolation function are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The VB isolation function design conforms to these requirements.

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

- Conformance: The VB isolation function design complies by providing automatic indication of bypassed and inoperable status (IEEE Std. 603, Section 5.8).

10 CFR 50.34(f)(2)(xiv)(II.E.4.2), Containment Isolation Systems:

Conformance: The VB isolation function design complies with this requirement.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The VB isolation function conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)(1)(iv)(21), 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)(b)(1)(vi), ITAAC in Design Certification Applications:

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

10 CFR 52.47(a)(1)(vii)(25), 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 design of the VB and VB isolation function within the DCD complies with this requirement.

10 CFR 52.47(b)(c)(2)(i), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety-related functions.

7.3.6.3.2 General Design Criteria

GDC 1, 2, 4, 13, 16, 19, 20, 21, 22, 23, and 24 and 29:

- Conformance: The VB isolation function design complies with these GDCs.

7.3.6.3.3 Staff Requirements Memorandum

SRM on SECY-93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems:

- Conformance: The VB isolation function design complies with these criteria through demonstration that no postulated common-mode failure of the control system could

disable the VB isolation function. The discrete logic and solid state controls used in this design are not subject to the vulnerabilities described by SECY-93-087, Item II.Q.

7.3.6.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Function:

- Conformance: The VB isolation function design conforms to RG 1.22. System logic and components are tested periodically during refueling outages.

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

- Conformance: The VB isolation function design conforms to RG 1.47. Automatic indication is provided in the MCR to inform the operator that the system is inoperable or a division is bypassed.

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

- Conformance: ~~The VB isolation function design conforms to RG 1.53, IEEE Std. 603, Section 5.1, and IEEE Std. 379.~~ The VB isolation function is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The VB isolation function design complies with RG 1.62. Each division has a manual actuation switch in the MCR. Initiation of the system requires actuation of two switches to ensure that manual initiation is a premeditated act.

RG 1.75, Physical Independence of Electric Systems:

- The VB isolation function design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Instrument Setpoints for Safety-Related Systems:

- Conformance: The setpoints established to control the VB isolation valve conform to RG 1.105. Reference 7.3-2 provides a detailed description of the GEH methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEE Std. 338, as modified by~~The VB isolation function design complies with the guidance of~~ RG 1.118.

RG 1.152, Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.152.

RG 1.153, Criteria for Power, I&C Portions of Safety Systems:

- Conformance: The VB isolation function design complies with IEEE Std. 603~~RG 1.153~~.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.168 as implemented on the independent control platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The VB isolation function design conforms to RG 1.169 as implemented on the independent control platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.170 as implemented on the independent control platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.171 as implemented on the independent control platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.172 as implemented on the independent control platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.173 as implemented on the independent control platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems:

- Conformance: The VB isolation function design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.3.6.3.5 Branch Technical Positions

In accordance with the SRP for Section 7.3 and Table 7.1-1, the following BTPs are addressed for the VB isolation function:

BTP HICB-8, Guidance on Application of RG 1.22:

- Conformance: The VB isolation function design conforms to BTP HICB 8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: Logic controllers for the VB isolation function use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

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

- Conformance: The setpoints established to control the VB isolation valve conform to this guide. Reference 7.3-2 provides a detailed description of the GEH methodology.

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

~~Conformance: This BTP does not apply to the VB isolation function because it does not use these instruments.~~

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

- Conformance: The VB isolation function design conforms to BTP HICB-14.

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

- Conformance: The level of detail in the VB isolation function description conforms to BTP HICB-16.

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

- Conformance: The VB isolation function design conforms to BTP HICB-17.

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

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

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

- Conformance: The VB isolation function design conforms to BTP HICB-19. The discrete logic and solid state controls used in this design are not subject to the vulnerabilities described by BTP HICB-19.

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

- Conformance: The VB isolation function design conforms to BTP HICB-21.

7.3.6.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for 7.3 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v)[I.D.3] and 10 CFR 50.34(f)(2)(xiv)[II.E.4.2] apply to the VB isolation function. The VB isolation function complies with the requirements as indicated above. TMI action plan requirements are addressed in Appendix 1A.

7.3.6.4 Testing and Inspection Requirements

The VB isolation function TLUs are self-tested continually at preset intervals and can be tested during plant operation~~ (IEEE Std. 603, Sections 5.7 and 6.5)~~. VB isolation function equipment

- Conformance: ~~The SLC system design conforms to IEEE Std. 603. Separation and isolation is maintained both mechanically and electrically in accordance with IEEE Std. 603Table 7.1-2 and Regulatory Guide (RG) 1.75. The SLC is designed so a single failure does not interfere with system operation. Electrical separation is maintained between safety-related divisions, and between safety-related and nonsafety-related portions.~~ The SLC system design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the SLC system design conforms to IEEE Std. 603 is discussed below.

  – Section 4.2 (Safety-related Functions): See Subsections 7.4.1.1 and 9.3.5.1.

  – Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are discussed in Subsection 9.3.5.2.

  – Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to SLC system design.

  – Section 5.2 (Completion of Protective Actions): Completion of Protective Actions are not applicable beyond that discussed in Subsection 7.1.6.6.1.3.

  – Section 5.7 (Capability for Test and Calibration): Test and Calibrate features are discussed in Subsections 7.4.1.4 and 9.3.5.4.

  – Section 6.2 and 7.2 (Manual Control): See Subsections 7.4.1.2.2, 7.4.1.3, 9.3.5.2 and 9.3.5.5.

  – Section 6.4 (Derivation of System Inputs): The SLC system derives its sense and command features from direct measurements as described in Subsections 7.4.1.2, 7.4.1.5 and 9.3.5.5.

  – Section 6.5 (Capability of Test and Calibration): Capability for Test and Calibrate features are discussed in Subsections 7.4.1.4 and 9.3.5.4.

  – Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the SLC system design beyond that discussed in Subsections 7.1.6.6.1.22 are not applicable.

  – Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the SLC system design beyond that discussed in Subsection 7.1.6.6.1.23 are not applicable.

  – Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the SLC system design are discussed in Subsections 7.4.1.2.1 and 9.3.5.2.

  – Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the SLC system design are discussed in Subsection 7.4.1.3.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The SLC design conforms to these requirements.

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

- Conformance: The SLC system design conforms to this requirement.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The SLC conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

~~10 CFR 50.62, Requirements for Reduction of Risk from ATWS Events for light-water Cooled Nuclear Power Plants:~~

- ~~Conformance: The SLC is automatically initiated, and is designed to perform its mitigation function reliably.~~

10 CFR 52.47(a)~~(1)(iv)~~(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: The SLC system design complies with this criterion. Reference Section 1.11 for resolution of unresolved and generic safety issues.

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

- Conformance: ITAAC are provided for I&C Equipment in Tier 1.

10 CFR 52.47(a)~~(1)(vii)~~(25), Interface Requirements:

- Conformance: There are no interface requirements for the SLC system.

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

- Conformance: The level of detail provided for the SLC system within the DCD conforms to this requirement.

10 CFR 52.47~~(b)~~(c)(2)~~(i)~~, Innovative Means of Accomplishing Safety Function:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.4.1.3.2 General Design Criteria.

In accordance with Table 7.1-1, the following General Design Criteria (GDC) are addressed for the SLC system:

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, ~~and~~ 24, 29, 35, and 37:

- Conformance: The SLC system design conforms to these GDC.

7.4.1.3.3 Staff Requirements Memorandum

SECY-93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems:

- Conformance: The SLC system design conforms to these criteria by providing diverse I&C, as described in Section 7.8.

7.4.1.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Actuation Functions:

- Conformance: The SLC system design conforms to RG 1.22.

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

- Conformance: The SLC system design conforms to RG 1.47.

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

- Conformance: The SLC is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

The SLC system design is a redundant backup to the reactor control and scram systems, and performs an ECCS function. The SLC system design has two redundant and parallel squib-type valves in each loop. Only one valve in each loop is required for the safety-related function of the SLC system. The SLC system instrumentation assuring operability of the system also is redundant.

~~RG 1.62, Manual Initiation of Protective Actions:~~

~~Conformance: The SLC system design conforms to RG 1.62. Dual (key-locked) control switches are provided, to actuate the SLC system.~~

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The SLC system design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Setpoints for Safety-Related Instrumentation:

- Conformance: The SLC system design conforms to RG 1.105, as described in Reference 7.4-2.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEE Std. 338, as modified by ~~The SLC system design conforms to~~ RG 1.118.

RG 1.151, Instrument Sensing Lines:

- Conformance: The SLC system design conforms to RG 1.151.

RG 1.152, Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: ~~Consistent with the discussion of other RGs and the General Design Criteria, the~~ The SLC system design conforms to ~~RG 1.153~~10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.168 as implemented on the SSLC/ESF platform. The SLC system design conforms to RG 1.168 as implemented on the independent control platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The SLC system design conforms to RG 1.169 as implemented on the SSLC/ESF platform. The SLC system design conforms to RG 1.169 as implemented on the independent control platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.170 as implemented on the SSLC/ESF platform. The SLC system design conforms to RG 1.170 as implemented on the independent control platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.171 as implemented on the SSLC/ESF platform. The SLC system design conforms to RG 1.171 as implemented on the independent control platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.172 as implemented on the SSLC/ESF platform. The SLC system design conforms to RG 1.172 as implemented on the independent control platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.173 as implemented on the SSLC/ESF platform. The SLC system design conforms to RG 1.173 as implemented on the independent control platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The SLC system design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.4.1.3.5 Branch Technical Positions

BTP HICB-8, Guidance on Application of Regulatory Guide 1.22:

- Conformance: The SLC system design conforms to BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The SLC system design conforms to BTP HICB-11. SSLC/ESF logic controllers for the SLC use safety-related fiber optic CIMs and fiber optic cables for

interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

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

- Conformance: The SLC system design conforms to BTP HICB-12.

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

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

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

- Conformance: The SLC system design conforms to BTP HICB-14.

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

- Conformance: The level of detail provided for the SLC system conforms to BTP HICB-16.

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

- Conformance: The SLC system design conforms to BTP HICB-17.

~~BTP HICB-18, Guidance on Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and control Systems:~~

~~Conformance: The SLC system design conforms to BTP HICB-18.~~

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

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

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

- Conformance: The SLC system design conforms to BTP HICB-21.

7.4.1.4 Testing and Inspection Requirements

Testing and inspection requirements are described further in Subsection 9.3.5.4. An initial SLC system performance verification test is conducted as part of the startup test program. This test is intended to demonstrate that the SLC system performance is in accordance with design requirements.

A full test of this system is not possible during plant operation. Other than the two squib valves in each loop, there are no active components in this system, that are required to actuate for

7.4.2.2 System Description

7.4.2.2.1 General

The RSS has two redundant and independent panels. All parameters displayed and/or controlled from Division 1 and Division 2 in the MCR also are displayed and/or can be controlled from any of the two RSS panels ~~(IEEE Std. 603, Section 5.8)~~. Each panel contains:

- Division 1 Manual Scram Switch,
- Division 2 Manual Scram Switch,
- Division 1 Manual Main Steam Isolation Valve (MSIV) Isolation Switch,
- Division 2 Manual MSIV Isolation Switch,
- Division 1 Safety-related Video Display Unit (VDU),
- Division 2 Safety-related VDU,
- Nonsafety-related VDU, and
- Nonsafety-related Communications Equipment.

All data from the Q-DCIS and N-DCIS networks are available for display on the RSS panels. Because the VDUs on the RSS panels are connected to Q-DCIS or N-DCIS through the same networks serving corresponding VDUs at the MCR, all Division 1 and 2 safety-related and nonsafety-related display/control functions at the MCR also are available at the RSS panels. A simplified RSS panel schematic is provided in Figure 7.4-1. A simplified network functional ~~block~~ diagram of the Q-DCIS and N-DCIS is included as ~~part of~~ Figure 7.1-1.~~, and a functional network diagram appears as Figure 7.1-2.~~ This~~ese~~ diagram~~s~~ indicates the relationships of safety-related ~~or~~ and nonsafety-related systems with their peers, and with plant data acquisition systems. Section 7.1 contains a description of these relationships. The software for the RSS safety-related VDUs is developed as part of the SSLC/ESF platform hardware/software development process. The software for the RSS nonsafety-related VDUs is developed as part of the nonsafety-related network segment hardware/software development processes.

The two RSS panels are located in different rooms inside the Reactor Building (RB). Each RSS Panel room has a sliding fire door with a minimum fire rating of three hours. The RSS panel room environment typically is similar to the MCR environment. Access to and use of the RSS panels is administratively controlled. This satisfies the control access requirement of IEEE Std. 603, Section 5.9.

The RSS provides sufficient redundancy in its control and monitoring capability, to accommodate a single failure in the interfacing systems, a single failure in the RSS controls and the event that caused the MCR evacuation. The RSS is designed such that any failure within it does not degrade the capability of interfacing safety-related systems. The RSS satisfies the single-failure criterion and independence requirements of IEEE Std. 603, Sections 5.1, 5.6, and 6.3.

any other safety or nonsafety-related system) is outside the MCR, ICS operation is not affected by an event necessitating MCR evacuation, and continued operation of the isolation condensers is assured. If the event necessitating MCR evacuation results in a loss of the reactor pressure regulator, but does not cause main steam line isolation, the ICS initiates on high pressure. With the ICS in operation, the isolation condensers provide initial decay heat removal, and further reactor cooldown is achieved from the RSS panels using the RWCU/SDC.

7.4.2.3 Safety Evaluation

The RSS is classified as a safety-related system that can control safety-related systems or equipment.

The RSS provides instrumentation and controls (I&C) outside the MCR to allow prompt hot shutdown of the reactor after a scram and to maintain safe conditions during hot shutdown. It also provides capability for subsequent cold shutdown of the reactor through the use of suitable operating procedures.

Table 7.1-1 identifies the RSS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.4.2.3.1 Code of Federal Regulations

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

- Conformance: The RSS design conforms to these requirements.

10 CFR 50.55a(h), Protection and Safety Systems Compliance with ~~Criteria for Protection Systems for Nuclear Power Generating Stations (~~IEEE Std. 603~~)~~:

- Conformance: The RSS design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the RSS design conforms to IEEE Std. 603 is discussed below.~~Separation and isolation is preserved both mechanically and electrically in accordance with IEEE 603, Section 5.6 and 6.3, and RG 1.75.~~

  – Section 4.2 (Safety-Related Function): See Subsections 7.4.2.1 and 7.4.2.2.2.

  – Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the RSS design.

  – Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to RSS design.

  – Section 5.2 (Completion of Protective Actions): Completion of Protective Actions is not applicable beyond that discussed in section 7.1.6.6.1.3.

  – Section 5.7 (Capability for Test and Calibration): See Subsections 7.4.2.4.

  – Section 6.2 and 7.2 (Manual Control): See Subsections 7.2.1.5.5 & 7.4.2.2.3.

- Section 6.4 (Derivation of System Inputs): Derivation of System Inputs is not applicable for the RSS.
- Section 6.5 (Capability of Test and Calibration): Testing sense and command sensors is not applicable to RSS.
- Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the RSS are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.
- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the RSS are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the RSS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the RSS are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

~~With regard to IEEE 603, Section 5.1, an event is assumed to have occurred causing the evacuation of the MCR. The RSS is designed to accommodate a single failure in the interfacing systems or RSS controls for these scenarios (IEEE Std. 603, Section 5.1). The effects of such failures are analyzed below.~~

~~The loss of one complete RWCU/SDC, RCCW or plant service water loop could extend the time needed for the reactor to reach cold shutdown conditions. However, the ultimate ability of the RSS to facilitate such conditions is not impaired. Each RWCU/SDC loop provides 50% capacity for residual heat removal, and each RCCW and plant service water train provides approximately 50% capacity for shutdown cooling. The RWCU/SDC, RCCW, and plant service water systems, in conjunction with the ICS, can bring the plant to cold shutdown within 36 hours assuming the most restrictive single active failure.~~

~~In the event that one CRD train fails or is out of service for maintenance, the remaining pump can provide sufficient makeup to maintain RPV water level during reactor cooldown.~~

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The RSS design conforms to these requirements.

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

- Conformance: The RSS design conforms to these requirements by providing automatic indication of bypassed and inoperable status.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The RSS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)~~(1)(iv)~~(21), 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(b)~~(a)~~(1)~~(vi)~~, ITAAC in Design Certification Applications:

- Conformance: ITAAC for the RSS are identified in Tier 1.

10 CFR 52.47(a)~~(1)(vii)~~(25), Interface Requirements:

- Conformance: There are no interface requirements for RSS.

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

- Conformance: The level of detail provided for the RSS within the DCD conforms to this requirement.

10 CFR 52.47~~(b)~~(c)(2)~~(i)~~, Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.4.2.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23,~~and~~ 24, and 29:

- Conformance: The RSS design conforms to these GDC.

7.4.2.3.3 Staff Requirements Memorandum

SRM on SECY-93-087, Item II.T, Control Room Annunciator (Alarm) Reliability:

- Conformance: The AMS meets the requirements of SECY-93-087, Item II.T for redundancy, independence, and separation in that the "alarm system" is considered redundant as follows:
  - Alarm points are sent via dual networks to redundant message processors using dual power supplies. The processors are dedicated to alarm processing.
  - The alarms are displayed on multiple independent Video Display Units (VDUs) (dual power supplies on each).
  - The alarms are driven by redundant datalinks to the AMS (dual power). There are redundant alarm processors.
  - There is one horn and one voice speaker. Test buttons are available to test the horn and all the lights.
  - There are no alarms requiring manually controlled actions for safety systems to accomplish their safety-related functions.

~~7.4.2.3.3~~ 7.4.2.3.4 Regulatory Guides

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

- Conformance: The RSS design conforms to RG 1.22.

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

- Conformance: The RSS system design conforms to RG 1.47.

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

- Conformance: The RSS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.~~The RSS design conforms to RG 1.53, IEEE Std. 603, Section 5.1, and IEEE Std. 379.~~

In addition, separation and isolation is preserved both mechanically and electrically in accordance with IEEE 603, Sections 5.6 and 6.3, and RG 1.75.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The RSS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The RSS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The RSS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEE Std. 338, as modified by ~~The RSS design conforms to~~ RG 1.118.

RG 1.153, Power Instrumentation & Control Portions of Safety Systems:

- Conformance: The RSS design conforms to 10 CFR 50.55a(h)~~RG 1.153~~.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems:

- Conformance: The RSS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The RSS design conforms to RG 1.204.

RG 1.209, Guidelines For Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The RSS Safety-Related system design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

~~7.4.2.3.4~~ 7.4.2.3.5 Branch Technical Positions

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The RSS design complies with BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The RSS design conforms to BTP HICB-11. Logic controllers for the RSS use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

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

- Conformance: The RSS design conforms to BTP HICB-12.

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

- Conformance: The RSS design conforms to BTP HICB-14.

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

- Conformance: The level of detail provided for RSS conforms to BTP HICB-16.

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

- Conformance: The RSS design conforms to BTP HICB-17.

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

~~Conformance: The RSS design conforms to BTP HICB-18.~~

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

- Conformance: The RSS design conforms to BTP HICB-21.

~~7.4.2.3.5~~ 7.4.2.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for 7.4 and with Table 7.1-1, there are no Three Mile Island (TMI) action plan requirements applicable for the RSS. TMI action plan requirements are generically addressed in Table 1A-1 of Appendix 1A.

From the foregoing analyses, it is concluded that the RSS meets its design bases.

7.4.2.4 Testing and Inspection Requirements

The capability to safely shut down the reactor from outside the MCR is confirmed during the Initial Plant Test Program (Refer to Section 14.2). Testing to confirm the functionality of each RSS control circuit is performed during each refueling outage.

Minimum Requirements to Place and Maintain Plant in MODE 3 from Location Outside MCR

On the basis of Sections 15.5.6.2 and 15.5.6.3 which provide the assumptions and results of safe shutdown fire analysis, only a manual scram of the plant from the MCR is required to reach and maintain Mode 3 (hot shutdown). If the operator is not able to initiate manual scram from the MCR due to spread of the fire, manual scram can be initiated from either of the RSS panels. Therefore, the operability of Division 1& 2 Manual Scram Switches at either of the two RSS panels is the minimum requirement to achieve and maintain Mode 3 from a location outside MCR.

7.4.2.5 Instrumentation and Control Requirements

The parameters displayed and/or controlled from Division 1 and Division 2 in the MCR also are displayed and/or can be controlled from either of the RSS panels.

7.4.3 Reactor Water Cleanup/Shutdown Cooling System

7.4.3.1 System Design Bases

The RWCU/SDC system design bases are described further in Subsections 5.4.8.1 and 5.4.8.2. Figure 5.1-4 shows the basic configuration of the RWCU/SDC system.

The RWCU/SDC system is one of the dual redundant Plant Investment Protection (PIP) systems whose instrumentation belongs to the N-DCIS. The RWCU/SDC system functions are not

Temperature elements are provided in the RPV bottom drain, the regenerative heat exchanger supply inlet and outlet, the non-regenerative heat exchanger outlet, the demineralizer influent (located at the pump suction), and the inlet and outlet of the regenerative heat exchanger return.

Temperature elements located in the NBS and a reactor cooldown controller with temperature feedback are used to provide the necessary signals to control pump speed during cooldown to maintain the required cooldown rate.

Density compensated system mass flow is measured in the process lines (by mid-vessel nozzles with venturi-type flow elements in each line) from the reactor bottom, located inside the containment. Flow elements also are provided in the Seismic Category I RWCU/SDC return lines to the feedwater lines and in the overboarding lines. The flow transmitters for all of these flow elements are arranged in a two-out-of-four logic configuration used to detect high RWCU/SDC differential mass flow due to a break outside the containment and to close the inboard and outboard containment isolation valves of the affected RWCU/SDC train. The containment isolation function on detection of RWCU/SDC high differential mass flow (due to a break outside the containment) is part of the LD&IS described in Subsection 7.3.3. See Figures 7.4-2a through 7.4-2e for the logic for detection of a RWCU/SDC pipe break outside containment.

Flow orifices are used for flow monitoring of demineralizer inlet flow and to open the demineralizer bypass control valve if the flow exceeds the demineralizer capacity.

7.4.3.3 Safety Evaluation

The RWCU/SDC system functions are nonsafety-related, with the exception of containment isolation functions and providing instruments to detect high differential mass flow following a RWCU/SDC break outside the containment. Refer to Subsection 6.2.4 for the containment isolation functions, and Subsection 7.3.3 for the containment isolation and leak detection functions performed by the LD&IS.

Table 7.1-1 identifies the RWCU/SDC system and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.4.3.3.1 Code of Federal Regulations

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

- Conformance: The RWCU/SDC system design conforms to these requirements.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The RWCU/SDC design conforms to these requirements.

10 CFR 50.55a(h), Protection and Safety System Compliance with IEEE 603:

- Conformance: The ~~RWCU/SDC system is nonsafety-related, 10CFR 50.55a(h) and IEEE Std. 603 are not applicable to this system~~safety-related requirements are addressed in Subsection 7.3.3, LD&IS.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The RWCU/SDC conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants:

- Conformance: The RWCU/SDC conforms to these requirements.

10 CFR 52.47(a)~~(1)(iv)~~(21), Resolution of Unresolved and Generic Safety Issues:

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

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

- Conformance: ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)~~(1)(vii)~~(25), Interface Requirements:

- Conformance: There are no interface requirements for the RWCU/SDC system.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the RWCU/SDC within the DCD documents conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The RWCU/SDC design does not use innovative means for accomplishing safety functions.

7.4.3.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, ~~and~~ 24, 33, and 38:

- Conformance: The RWCU/SDC system is nonsafety-related, but is designed to conform to these GDC.

7.4.3.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The RWCU/SDC design conforms to RG 1.97, which endorses IEEE 497.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.151, Instrument Sensing Lines:

- Conformance: RG 1.151 is applicable to safety-related sensing lines. However, sections of endorsed standard ANSI/ISA-S67.02.01 on design practices for tubing, vents, and drains also apply to nonsafety-related instrumentation.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The RWCU/SDC system design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The safety-related requirements are addressed in Subsection 7.3.3, LD&IS.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RWCU/SDC design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The RWCU/SDC design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RWCU/SDC design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RWCU/SDC design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RWCU/SDC design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The RWCU/SDC design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems:

- Conformance: The RWCU/SDC system design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

~~RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:~~

- ~~Conformance: The RWCU/SDC system design conforms to RG 1.204.~~

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The RWCU/SDC system design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.4.3.3.4 Branch Technical Positions

BTP HICB-1, Guidance on Isolation of the Low Pressure Systems from the High Pressure Reactor Coolant System:

- Conformance: The RWCU/SDC design conforms to BTP HICB-1.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

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

- Conformance: The level of detail provided for the RWCU/SDC system design conforms to BTP HICB-16.

7.4.3.4 Testing and Inspection Requirements

The RWCU/SDC system instruments are calibrated and tested during the preoperational testing program to confirm the instrumentation is correctly installed and functions as designed. In addition, calibration and surveillance testing of the containment isolation devices is performed at regular intervals ~~(IEEE Std. 603, Section 5.7 and 6.5)~~. To the maximum extent possible, instrumentation requiring regular calibration, testing, and maintenance is mounted on accessible panels or racks located outside high radiation areas.

function of the CRD system operating in conjunction with safety relief valves and the suppression pool cooling systems.

The DPS discussed in Section 7.8 provides diverse nonsafety-related signals for ICS initiation and opening of equalizing valves between the equipment storage pool and the IC/PCC expansion pools.

Table 7.1-1 identifies the ICS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.4.4.3.1 Code of Federal Regulations

10 CFR 50.55a(h), ~~Criteria for Protection Systems for Nuclear Power Generating Stations (~~Protection and Safety Systems Compliance with IEEE Std. 603~~)~~:

- Conformance: ~~Separation and isolation is preserved both mechanically and electrically, in accordance with IEEE Std. 603, Section 5.6 and 6.3,~~Table 7.1-2 ~~and RG 1.75. The ICS is divisionalized and redundantly designed so failure of any instrument does not interfere with the system operation. Electrical separation is maintained between the redundant divisions.~~ The ICS design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the ICS conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 5.4.6.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are discussed in Subsections 5.4.6.2.3 and 7.4.4.3.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to ICS.
  - Section 5.2 (Completion of Protective Actions): Completion of Protective Actions are not applicable beyond that discussed in Subsection 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): Test and Calibrate features are discussed in Subsection 5.4.6.4.
  - Section 6.2 and 7.2 (Manual Control): See Subsections 5.4.6.2.2 and 5.4.6.2.3.
  - Section 6.4 (Derivation of System Inputs): The ICS derives its sense and command features from direct measurements as described in Subsections 5.4.6.5, 7.4.4.3 and 7.8.
  - Section 6.5 (Capability of Test and Calibration): Capability for Test and Calibrate features beyond that discussed in are discussed in Subsection 5.4.6.4.
  - Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the SLC beyond that discussed in Subsections 7.1.6.6.1.22 are not applicable.

- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the SLC beyond that discussed in Subsection 7.1.6.6.1.23 are not applicable.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the ICS beyond that discussed in Subsection 7.1.6.6.1.26 are not applicable.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the beyond that discussed in Subsection 7.1.6.6.1.27 are not applicable.

10 CFR 50.34(f)(1)(v)[II.K.3.13], HPCI and RCIC Initiation Levels,

- Conformance: The ICS design conforms to these requirements.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design,

- Conformance: The ICS design conforms to these requirements.

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

- Conformance: The ICS design conforms to this requirement because it is an ECCS.

10 CFR 50.34(f)(2)[II.K.1.22], Auxiliary Heat Removal Systems:

- Conformance: The ICS conforms to these requirements.

10 CFR 50.34(f)(2)(xxiii)[II.K.2.10], Anticipatory Reactor Trip:

- Conformance: The ICS will initiate in response to a Loss of All Feedwater Flow Event. This is an anticipatory trip actuated on ~~loss of power to two of the four main feedwater pumps~~a power generation buss loss event.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The ICS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants:

- Conformance: The ICS conforms to these requirements.

10 CFR 50.63, Loss of All Alternating Current Power:

- Conformance: The ICS conforms to these requirements.

10 CFR 52.47(a)~~(1)(iv)~~(21), 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)~~(b)(1)~~(vi)~~, ITAAC in Design Certification Applications:

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

10 CFR 52.47(a)~~(1)(vii)~~(25), Interface Requirements:

- Conformance: There are no interface requirements for ICS.

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

- Conformance: The level of detail provided for the ICS within the DCD conforms to this BTP.

10 CFR 52.47~~(b)~~(c)(2)~~(i)~~, Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.4.4.3.2 General Design Criteria

In accordance with the SRP for Section 7.4 and Table 7.1-1, the following GDC are addressed for the ICS:

GDC 1, 2, 4, 13, 19 , 20, 21, 22, 23, ~~and,~~ 24, 29, 33, 34, 35, 37, and 44:

- Conformance: The ICS design conforms to these GDC.

7.4.4.3.3 Staff Requirements Memorandum

SECY-93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems:

- Conformance: The ICS design conforms to these criteria by providing diverse I&C, as described in Section 7.8.

7.4.4.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Actuation Functions:

- Conformance: The ICS system design conforms to RG 1.22.

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

- Conformance: The ICS design conforms to RG 1.47.

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

- Conformance: The ICS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.~~The ICS design conforms to RG 1.53.~~

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The ICS design conforms to RG 1.62.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The ICS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Instrument Setpoints for Safety-Related Systems:

- Conformance: The setpoints used to initiate ICS automatic operation or isolation are established consistent with this guide. Reference 7.4-2 provides a detailed description of the GEH methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEE Std. 338, as modified by ~~The ICS design conforms to~~ RG 1.118.

RG 1.151 - Instrument Sensing Lines:

- Conformance: The ICS design conforms with RG 1.151.

RG 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The ICS design conforms to ~~RG 1.153~~10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.168 as implemented on the SSLC/ESF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.169 as implemented on the SSLC/ESF platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.170 as implemented on the SSLC/ESF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.171 as implemented on the SSLC/ESF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.172 as implemented on the SSLC/ESF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.173 as implemented on the SSLC/ESF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems:

- Conformance: The ICS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.4.4.3.5 Branch Technical Positions

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The ICS design conforms to BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The ICS design conforms to BTP HICB-11. SSLC/ESF logic controllers for ICS use safety-related fiber optic communication interface modules and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

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

- Conformance: The ICS logic resides within the SSLC/ESF so that the design conforms to BTP HICB-12.

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

- ~~Conformance: BTP HICB-13 does not apply to ICS because this system does not use resistance temperature detector-type sensors.~~

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based I&C Systems:

- Conformance: The ICS design conforms to BTP HICB-14.

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

- Conformance: The level of detail provided in the ICS description conforms to BTP HICB-16.

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

- Conformance: The ICS design conforms to BTP HICB-17.

~~BTP HICB-18, Guidance on the Use of Programmable Logic Controllers in Digital Computer Based I&C Systems:~~

- ~~Conformance: The ICS design conforms to BTP HICB-18.~~

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

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

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

- Conformance: The ICS design conforms to BTP HICB-21.

7.4.4.4 Testing and Inspection Requirements

Refer to Subsection 5.4.6.4. ~~(IEEE Std. 603, Sections 5.7 and 6.5).~~

7.4.4.5 Instrumentation and Control Requirements

Refer to Subsection 5.4.6.5. ~~(IEEE Std. 603, Sections 4.4, 4.5, 5.7, and 6.5).~~

The ICS indications reported in the MCR ~~(IEEE Std. 603, Section 5.8)~~ are:

- Radiation level in each IC pool compartment airspace,
- Mass flow rate in condensate return line,
- Mass flow rate in steam supply line,
- Temperatures of steam and condensate return lines,
- Temperatures of IC top and bottom vent lines, and
- Valve positions.

The following manual controls are provided by the ICS ~~(IEEE Std. 603, Sections 6.2 and 7.2)~~ to:

- Open/close condensate return valves,
- Close condensate return isolation valves,
- Close steam supply isolation valves,
- Open/close all bottom vent valves,
- Open/close all top vent valves, and
- Open/close purge line valve.

7.4.5 COL Information

None.

7.4.6 References

7.4-1 (Deleted)

7.5 SAFETY-RELATED AND NONSAFETY-RELATED INFORMATION SYSTEMS

This section discusses instrumentation associated with:

- Post Accident Monitoring (PAM),
- Containment Monitoring System (CMS),
- Process Radiation Monitoring System (PRMS),
- Area Radiation Monitoring System (ARMS), and
- Pool Monitoring ~~Subsystems~~Instrumentation.

The safety-related portions of the PAM Instrumentation, CMS, PRMS, and Pool Monitoring Instrumentation~~Subsystems~~ are part of a group of ~~systems~~ instruments/equipment collectively called the Safety-Related Distributed Control and Information System (Q-DCIS). A simplified network functional ~~block~~ diagram of the ~~Q-~~DCIS is included as ~~part of~~ Figure 7.1-1 ~~and a functional network diagram appears as Figure 7.1-2~~ (not all systems are shown on these figures.)

This~~ese~~ diagram~~s~~ schematically indicates the relationships of a safety-related system with its safety-related peers and with nonsafety-related plant data systems called the Nonsafety-Related Distributed Control and Information System (N-DCIS). Section 7.1 contains a description of these relationships.

The nonsafety-related portions of the PAM instrumentation, CMS, PRMS, and the ARMS are part of the N-DCIS.

7.5.1 Post Accident Monitoring Instrumentation

7.5.1.1 System Design Bases

The PAM instrumentation safety-related design bases are to:

- Provide instrumentation to monitor variables and systems over their anticipated ranges for accident conditions as appropriate to ensure adequate safety.
- Provide the appropriate Main Control Room (MCR) instrumentation and displays to provide the information from which actions can be taken to maintain a safe plant condition under accident conditions, including Loss-of-Coolant Accidents (LOCAs).
- Provide equipment (including the necessary instrumentation) at appropriate locations outside the MCR with the capability for prompt hot shutdown of the reactor, and
- Provide the means for monitoring the reactor containment atmosphere spaces containing components that recirculate LOCA fluids, effluent discharge paths, and the plant environs for radioactivity that may be released as a result of accidents.

7.5.1.2 System Descriptions

The safety-related portions of the PAM systems are those systems that provide information for the safe operation of the plant during normal operation, Anticipated Operational Occurrences (AOOs) and accidents, to help ensure performance of manual safety-related functions. The safety-related information systems:

- Include those systems that provide information for manual initiation and control of safety-related systems,
- Indicate that safety-related plant functions are being accomplished, and
- Provide information, from which appropriate actions can be taken to mitigate the consequences of accidents.

The nonsafety-related portions of the PAM systems include the Safety Parameter Display System (SPDS), information systems associated with the emergency response facilities and the Emergency Response Data System (ERDS), none of which perform safety-related functions.

7.5.1.3 Safety Evaluation

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

7.5.1.3.1 Code of Federal Regulations

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

- Conformance: The PAM instrumentation design complies with these standards.

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

- Conformance: ~~The PAM safety-related instrumentation design complies with these requirements. Q-DCIS interdivisional and cross-platform signal transmission is performed via fiber optic cables.~~ The PAM instrumentation design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the PAM conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 7.5.1.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the PAM instrumentation design.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to PAM instrumentation design.

- Section 5.2 (Completion of Protective Actions): The Post Accident Monitoring system does not provide any trip or isolation functions.
- Section 5.7 (Capability for Test and Calibration): Test and Calibration requirements are not applicable beyond that discussed in Subsection 7.1.6.6.1.8.
- Section 6.2 and 7.2 (Manual Control): Manual Control is not applicable beyond that discussed in Subsection 7.1.6.6.1.18.
- Section 6.4 (Derivation of System Inputs): Derivation of System Inputs for PAM instrumentation is not applicable beyond that discussed in Subsection 7.1.6.6.1.20.
- Section 6.5 (Capability of Test and Calibration): Test and Calibration requirements for PAM instrumentation design is not applicable beyond that discussed in Subsection7.1.6.6.1.21.
- Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the PAM instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.
- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for PAM instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for PAM instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for PAM instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The PAM design conforms to these requirements.

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

- Conformance: The PAM instrumentation design conforms to the Bypass and Inoperable Status Indication (BISI) requirements of 10 CFR 50.34(f)(2)(v)(I.D.3). ~~The systems providing inputs to the PAM instrumentation to which these requirements apply are defined in Table 7.1-1.~~ General conformance is discussed in Subsection 7.1.6.1, and specific conformance is discussed in the system specific sections.

10 CFR 50.34(f)(2)(xvii) [II.F.1], Accident Monitoring Instrumentation:

- Conformance: The PAM instrumentation design complies with these requirements.

10 CFR 50.34(f)(2)(xviii) [II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: The PAM instrumentation design complies with this requirement. The direct water-level instrument system provides for the detection of conditions indicative of

inadequate core cooling (Refer to Table 1A-1 of Appendix 1A, Three Mile Island [TMI] Action Plan Items).

10 CFR 50.34(f)(2)(xix) [II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The PAM instrumentation design conforms to this requirement. The PAM instrumentation design conforms to RG 1.97.

10 CFR 50.34(f)(2)(xxiv) [II.K.3.23], Recording of Reactor Vessel Water Level:

- Conformance: The PAM instrumentation design conforms to this requirement. (Refer to Table 1.A-1 of Appendix 1A TMI Action Plan Items).

10 CFR 50.34(f)(2)(xxvi)[III.D.1.1], Leakage Control and Detection in Design Systems Outside Containment:

- Conformance: The PAM design conforms to these requirements.

10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of In-plant Airborne Radioactivity:

- Conformance: The PAM design conforms to these requirements.

10 CFR 52.47(a)~~(1)(iv)~~(21), 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)~~(b)(1)~~(vi)~~, Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) in Design Certification Applications:

- Conformance: ITAAC are provided for the Instrumentation and Control (I&C) systems and equipment in Tier 1.

10 CFR 52.47(a)~~(1) (vii)~~(25), 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 PAM instrumentation within the DCD conforms to this requirement.

10 CFR 52.47~~(b)~~(c)(2)~~(i)~~, Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.5.1.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 24, 63, and 64:

- Conformance: The PAM instrumentation design conforms to these GDC.

7.5.1.3.3 Staff Requirements Memorandum

Item II.T of SECY 93-087, Control Room Annunciator (Alarm) Reliability:

- Conformance: The alarm management system (AMS) design conforms to the Control Room Annunciator (Alarm) Reliability requirements of SECY 93-087, Item II.T. The systems to which this requirement applies are defined in Table 7.1-1. General conformance is discussed in Subsection 7.1.6.3, and specific conformance is discussed in the system specific sections.

7.5.1.3.4 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The PAM instrumentation design conforms to RG 1.97, which endorses (with certain exceptions specified in Section C of the RG) IEEE Std. 497 that establishes flexible, performance-based criteria for the selection, performance, design, qualification, display, and quality assurance of accident monitoring variables. IEEE Std. 497 identifies five types of variables for accident monitoring and the criteria for the selection of each type of variable.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The PAM design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The PAM design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The PAM instrumentation design conforms to IEEE Std. 603.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAM design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The PAM design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAM design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAM design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAM design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAM design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The PAM instrumentation design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

~~RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:~~

- ~~Conformance: The PAM instrumentation design conforms to RG 1.204.~~

~~RG 1.97 - Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:~~

- ~~Conformance: The PAM instrumentation design conforms to RG 1.97, which endorses (with certain exceptions specified in Section C of the RG) IEEE Std. 497 that establishes flexible, performance-based criteria for the selection, performance, design, qualification, display, and quality assurance of accident monitoring variables. IEEE Std. 497 identifies five types of variables for accident monitoring and the criteria for the selection of each type of variable.~~

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

Variable Types and Selection Criteria

The five variable types (A, B, C, D, E) and their selection criteria are defined in Section 4 and Table 1 of IEEE Std. 497. Table 1 summarizes the selection criteria for each variable type and the source documents such as plant accident analysis licensing basis, Emergency Procedure

7.5.2.3 Safety Evaluation

The CMS design, including the sensors and the instrumentation channels, is engineered into both safety-related and nonsafety-related subsystems. Safety-related systems are environmentally and seismically qualified for continuous monitoring during reactor operation, as well as abnormal and accident plant conditions. The system design conforms to the System Design Bases.

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

7.5.2.3.1 Code of Federal Regulations

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

- Conformance: The CMS design complies with these standards.

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

- Conformance: The CMS design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the CMS design conforms to IEEE Std. 603 is discussed below.~~Separation and isolation is preserved both mechanically and electrically in accordance with IEEE Std. 603, Section 5.6 and RG 1.75. The CMS safety-related subsystems are divisionalized and are designed with redundancy so that failure of any instrument does not interfere with the system operation. Electrical separation is maintained between the redundant divisions.~~
  - Section 4.2 (Safety-related Functions): See Subsection 7.5.2.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the CMS system.
  - Section 4.6 (Spatially Dependent Variables): See Subsection 7.5.2.2.
  - Section 5.2 (Completion of Protective Actions): Completion of Protective Actions are not applicable beyond that discussed in subsection 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): See Subsections 7.5.2.1.
  - Section 6.2 and 7.2 (Manual Control): See Subsection 7.5.2.1 and 7.5.2.2.
  - Section 6.4 (Derivation of System Inputs): The CMS derives its sense and command features from direct measurements, See Subsections 7.5.2.2.
  - Section 6.5 (Capability of Test and Calibration): See Subsection 7.5.2.4.
  - Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the CMS are not applicable.

- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the CMS are not applicable.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the CMS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the CMS are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The CMS design conforms to these requirements.

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

- Conformance: The CMS design complies by being able to provide automatic indication of bypassed and inoperable status.

10 CFR 50.34(f)(2)(viii)[II.B.3], Compatibility to Promptly Obtain and Analyze Containment Atmosphere Samples:

- Conformance: The CMS design complies with this requirement.

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:

- Conformance: The CMS design complies with these requirements.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The CMS design complies with these requirements.

10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of In-plant Airborne Radioactivity:

- Conformance: The CMS design complies with this requirement.

~~10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:~~

- ~~Conformance: The CMS design complies with this requirement.~~

~~10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:~~

- ~~Conformance: The CMS design complies with this requirement.~~

10 CFR 50.44(c)(4), Combustible Gas Control For Nuclear Power Reactors, Monitoring:

- Conformance: The CMS design complies with this requirement.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The CMS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)~~(1)(iv)~~(21), 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(b)~~(a)~~(1)~~(vi)~~, ITAAC in Design Certification Applications:

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

10 CFR 52.47(a)(25)~~(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 CMS within the DCD conforms to this requirement.

10 CFR 52.47~~(b)~~(c)(2)~~(i)~~, Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.5.2.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, ~~and~~ 24, 29, 41, 43, and 64:

- Conformance: The CMS design complies with these GDC.

7.5.2.3.3 Staff Requirements Memorandum

SRM on SECY 93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The CMS design conforms to item II.Q of SECY-93-087 (BTP HICB-19) by implementation of diverse I&C, described in Section 7.8.

~~SRM on SECY-93-087, Item II.T, Control Room Annunciator (Alarm) Reliability:~~

- ~~Conformance: The CMS AMS meets the requirements of SECY-93-087, Item II.T for redundancy, independence, and separation in that the "alarm system" is considered redundant as follows:~~
  - ~~Alarm points are sent via dual networks to redundant message processors using dual power supplies. The processors are dedicated to alarm processing.~~
  - ~~The alarms are displayed on multiple independent Video Display Units (VDUs) (dual power supplies on each).~~

- ~~The alarms are driven by redundant datalinks to the AMS (dual power). There are redundant alarm processors.~~
- ~~There is one horn and one voice speaker. Test buttons are available to test the horn and all the lights.~~
- ~~There are no alarms requiring manually controlled actions for safety systems to accomplish their safety-related functions.~~

7.5.2.3.4 Regulatory Guides

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

- Conformance: The CMS design conforms to RG 1.22.

RG 1.45, Reactor Coolant Pressure Boundary Leakage Detection Systems:

- The CMS design complies with RG 1.45.

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

- Conformance: The CMS design conforms to RG 1.47.

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

- Conformance: The CMS is organized into four physically and electrically-isolated divisions that use the principle of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single-failure criterion.~~The CMS design conforms to RG 1.53.~~

RG 1.75, Physical Independence of Electrical Systems:

- Conformance: The CMS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The CMS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, ~~–~~Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The CMS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Setpoints for Safety-Related Instrumentation:

- Conformance: The safety-related portions of the CMS design conform~~s~~ to RG 1.105. Reference 7.5-2 provides a detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEE Std. 338, as modified by ~~The CMS design conforms to~~ RG 1.118.

RG 1.151, Instrument Sensing Lines

- Conformance: The CMS design conforms to RG 1.151.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The CMS design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The CMS design conforms to ~~RG 1.153~~10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits For Digital Computer Software Used In Safety Systems:

- Conformance: The CMS design conforms to RG 1.168 as implemented on the SSLC/ESF platform.

RG 1.169, Configuration Management Plans For Digital Computer Software Used In Safety Systems:

- Conformance: The CMS design conforms to RG 1.169 as implemented on the SSLC/ESF platform.

RG 1.170, Software Test Documentation For Digital Computer Software Used In Safety Systems:

- Conformance: The CMS design conforms to RG 1.170 as implemented on the SSLC/ESF platform.

RG 1.171, Software Unit Testing For Digital Computer Software Used In Safety Systems:

- Conformance: The CMS design conforms to RG 1.171 as implemented on the SSLC/ESF platform.

RG 1.172, Software Requirements Specifications For Digital Computer Software Used In Safety Systems:

- Conformance: The CMS design conforms to RG 1.172 as implemented on the SSLC/ESF platform.

RG 1.173, Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems:.

- Conformance: The CMS design conforms to RG 1.173 as implemented on the SSLC/ESF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The CMS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The CMS design conforms to RG 1.204.RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control System in Nuclear Power Plants.

- Conformance: The CMS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.5.2.3.5 Branch Technical Positions

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The CMS design complies with BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The CMS design conforms to BTP HICB-11. SSLC/ESF logic controllers for the CMS use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

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

- Conformance: The CMS design conforms to BTP HICB-12.

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

- ~~Conformance: BTP HICB-13 does not apply to the CMS design because this system does not use resistance temperature detector-type sensors.~~

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

- Conformance: The CMS design conforms to BTP HICB-14.

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

- Conformance: The level of detail provided for the CMS design conforms to BTP HICB-16.

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

- Conformance: The CMS design conforms to BTP HICB-17.

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

- ~~Conformance: The CMS design conforms to BTP HICB-18.~~

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

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

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

- Conformance: The CMS design complies with BTP HICB-21.

Subsection 7.3.5.3.5 provides a discussion of BTP HICB-14, BTP HICB-17, ~~BTP HICB-18,~~ and BTP HICB-21 in conjunction with the SSLC/ESF system.

7.5.2.3.6 Three Mile Island Action Plan Requirements

In accordance with SRP 7.5, and with Table 7.1-1, 10 CFR 50.34(f)(2)(v) [I.D.3], 10 CFR 50.34(f)(2)(xvii)[II.F.1], 10 CFR 50.34(f)(2)(viii)[II.B.3], and 10 CFR 50.34 (f)(2)(xix)[II.F.3] apply to the CMS. In addition, 10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], also applies. The CMS complies with these requirements, as indicated above. TMI action plan requirements are addressed generically in Appendix 1A.

7.5.2.4 Testing and Inspection Requirements

In-service and Surveillance Testing: In-service testing is performed periodically on each CMS subsystem to verify operability and to ensure its readiness status for post accident monitoring ~~(IEEE Std. 603, Section 6.5)~~. Surveillance testing includes instrument channel checks of the radiation and gas monitors, functional tests to verify equipment operability, sensor calibration and response tests, and leakage tests of the gas sampling lines.

- Radwaste Building Stack.

~~Plant Stack.~~

The PRMS alerts operators when radiation levels exceed preset limits and initiates automatically the required protection action to isolate, contain or redirect radioactivity releases from the environs. See Subsection 11.5.1.1.2 for process and effluent paths and/or areas with the potential for excessive radiation levels.

The system is configured as shown in Figure 11.5-1 and Table 11.5-3.

7.5.3.1 Design Bases

The design bases are provided in Section 11.5.

7.5.3.2 System Description

The system description is provided in Section 11.5.

7.5.3.3 Safety Evaluation

The safety-related PRMS, including the sensors and the instrumentation channels, is environmentally and seismically qualified for continuous monitoring during reactor operation as well as abnormal and accident plant conditions.

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

7.5.3.3.1 Code of Federal Regulations

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

- Conformance: The PRMS design complies with these standards.

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

- Conformance: The PRMS design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the SLC conforms to IEEE Std. 603 is discussed below.~~Separation and isolation is preserved both mechanically and electrically in accordance with IEEE Std. 603, Section 5.6, and RG 1.75. The PRMS safety-related subsystems are divisionalized and are designed with redundancy so failure of any instrument does not interfere with system operation. Electrical separation is maintained between the redundant divisions.~~
  - Section 4.2 (Safety-related Functions): See Subsection 11.5.1.1.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the PRMS system.

- Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to PRMS.
- Section 5.2 (Completion of Protective Actions): Completion of Protective Actions are not applicable beyond that discussed in subsection 7.1.6.6.1.3.
- Section 5.7 (Capability for Test and Calibration): See Subsections 11.5.6.1, 11.5.6.2, and 11.5.6.3.
- Section 6.2 and 7.2 (Manual Control): See Subsection 7.5.3.3.3.
- Section 6.4 (Derivation of System Inputs): The PRMS derives its sense and command features from direct measurements.
- Section 6.5 (Capability of Test and Calibration): See Subsection 11.5.6.1, 11.5.6.2, and 11.5.6.3.
- Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the PRMS are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.
- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the PRMS are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the PRMS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the PRMS are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design,

- Conformance: The PRMS design conforms to these requirements.

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

- Conformance: The PRMS design complies by being able to provide automatic indication of bypassed and inoperable status.

~~10 CFR 50.34(f)(2)(viii)[II.B.3], Compatibility to Promptly Obtain and Analyze Containment Atmosphere Samples:~~

- ~~Conformance: The PRMS design complies with this requirement.~~

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:

- Conformance: The PRMS design complies with this requirement.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The PRMS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of In-plant Airborne Radioactivity:

- Conformance: The PRMS design complies with this requirement.

~~10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:~~

~~Conformance: The PRMS design complies with this requirement.~~

10 CFR 50.34(f)(2)(xxviii)[III.D.3.4] Control Room Habitability Problems Under Accident Conditions:

- Conformance: The PRMS design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The PRMS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)~~(1)(iv)~~(21), 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(b)~~(a)~~(1)~~(vi)~~, ITAAC in Design Certification Applications:

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

10 CFR 52.47(a)(25)~~(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 PRMS within the DCD documents conforms to this requirement.

10 CFR 52.47~~(b)~~(c)(2)~~(i)~~, Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.5.3.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, 29, and 64:

- Conformance: The PRMS design complies with these GDC.

7.5.3.3.3 Staff Requirements Memorandum

SRM on SECY 93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The PRMS design conforms to item II.Q of SECY-93-087 (BTP HICB-19).

~~SRM on SECY-93-087, Item II.T, Control Room Annunciator (Alarm) Reliability:~~

- ~~Conformance: The PRMS AMS design meets the requirements of SECY-93-087, Item II.T for redundancy, independence, and separation in that the "alarm system" is considered redundant as follows:~~
  - ~~Alarm points are sent via dual networks to redundant message processors using dual power supplies. The processors are dedicated to alarm processing.~~
  - ~~The alarms are displayed on multiple independent VDUs (dual power supplies on each).~~
  - ~~The alarms are driven by redundant data links to the AMS (dual power). There are redundant alarm processors.~~
  - ~~There is one horn and one voice speaker. Test buttons are available to test the horn(s) and all the lights.~~
  - ~~There are no alarms requiring manually controlled actions for systems to accomplish their safety-related functions.~~

7.5.3.3.4 Regulatory Guides

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

- Conformance: The PRMS design conforms to RG 1.22.

RG 1.45, Reactor Coolant Pressure Boundary Leakage Detection Systems:

- Conformance: The PRMS design complies with RG 1.45.

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

- Conformance: The PRMS design conforms to RG 1.47.

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

- Conformance: The PRMS is organized into four physically and electrically-isolated divisions that use the principle of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single-failure criterion.~~The PRMS design conforms to RG 1.53.~~

RG 1.75, Physical Independence of Electrical Systems:

- Conformance: The PRMS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The PRMS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The PRMS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Setpoints for Safety-Related Instrumentation:

- Conformance: The safety-related portions of the PRMS design conform~~s~~ to RG 1.105. Reference 7.5-2 provides a detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEE Std. 338, as modified by ~~The PRMS design conforms to~~ RG 1.118.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The PRMS design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The PRMS design conforms to 10 CFR 50.55a(h)~~RG 1.153~~.

RG 1.168, Verification, Validation, Reviews, and Audits For Digital Computer Software Used In Safety Systems:

- Conformance: The PRMS design conforms to RG 1.168 as implemented on the SSLC/ESF platform..

RG 1.169, Configuration Management Plans For Digital Computer Software Used In Safety Systems:

- Conformance: The PRMS design conforms to RG 1.169 as implemented on the SSLC/ESF platform..

RG 1.170, Software Test Documentation For Digital Computer Software Used In Safety Systems:

- Conformance: The PRMS design conforms to RG 1.170 as implemented on the SSLC/ESF platform..

RG 1.171, Software Unit Testing For Digital Computer Software Used In Safety Systems:

- Conformance: The PRMS design conforms to RG 1.171 as implemented on the SSLC/ESF platform..

RG 1.172, Software Requirements Specifications For Digital Computer Software Used In Safety Systems:

- Conformance: The PRMS design conforms to RG 1.172 as implemented on the SSLC/ESF platform..

RG 1.173, Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems:

- Conformance: The PRMS design conforms to RG 1.173 as implemented on the SSLC/ESF platform..

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The PRMS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The PRMS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The PRMS design conforms to RG 1.209See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.5.3.3.5 Branch Technical Positions

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The PRMS design complies with BTP HICB-8.

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The PRMS design conforms to BTP HICB-11. SSLC/ESF logic controllers for the PRMS use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

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

- Conformance: The PRMS design conforms to BTP HICB-12.

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

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

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

- Conformance: The PRMS design conforms to BTP HICB-14.

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

- Conformance: The level of detail provided for the PRMS design conforms to BTP HICB-16.

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

- Conformance: The PRMS design conforms to BTP HICB-17.

~~BTP HICB-18 - Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems:~~

- ~~Conformance: The PRMS design conforms to BTP HICB-18.~~

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems:

- Conformance: The PRMS design complies with BTP HICB-19.

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

- Conformance: The PRMS design complies with BTP HICB-21.

BTP HICB-14, BTP HICB-17, BTP HICB-18, and BTP HICB-21 are addressed in conjunction with the SSLC/ESF in Subsection 7.3.5.3.5.

7.5.3.3.6 Three Mile Island Action Plan Requirements

In accordance with SRP 7.5 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v)[I.D.3], ~~10 CFR 50.34(f)(2)(viii)[II.B.3],~~ 10 CFR 50.34(f)(2)(xvii) [II.F.1], 10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], and 10 CFR 50.34 (f)(2)(xix)[II.F.3] apply to the PRMS. The PRMS complies with these

- Conformance: The ARMS design complies with these standards.

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

- ~~Conformance: Because the ARMS is a nonsafety-related system, this regulation is not applicable.~~

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design,

- Conformance: The ARMS design conforms to these requirements.

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:

- Conformance: The ARMS design complies with this requirement.

10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: ARMS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of In-plant Airborne Radioactivity:

- Conformance: The ARMS design complies with this requirement.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The ARMS design complies with this requirement.

10 CFR 50.34(f)(2)(xxiv)[II.K.3.23] Capability to Record Reactor Vessel Water Level in One Location on Recorders that Meet Normal Post-Accident Recording Requirements:

- Conformance: The ARMS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxvi)[III.D.1.1], Leakage Control and Detection in Design Systems Outside Containment:

- Conformance: The ARMS conforms to these requirements.

10 CFR 52.47(a)~~(1)(iv)~~(21), 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)~~(b)(1)~~(vi)~~, ITAAC in Design Certification Applications:

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

10 CFR 52.47(a)~~(1)(vii)~~(25), Interface Requirements:

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

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the ARMS within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The ARMS design does not use innovative means for accomplishing safety functions.

7.5.4.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 24, 63, and 64:

- Conformance: The ARMS design complies with these GDC.

7.5.4.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, ~~–~~Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.~~The ARMS area radiation level instrumentation conforms to RG 1.97.~~

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The ARMS design conforms to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ARMS design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The ARMS design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ARMS design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ARMS design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ARMS design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The ARMS design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The ARMS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

~~RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:~~

- ~~Conformance: The ARMS design conforms to RG 1.204.~~

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.5.4.3.4 Branch Technical Positions

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.~~The ARMS design conforms to BTP HICB-10.~~

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

- Conformance: The level of detail provided for the ARMS complies with BTP HICB-16.

7.5.4.3.5 Three Mile Island Action Plan Requirements

In accordance with SRP 7.5 and with Table 7.1-1, 10 CFR 50.34(f)(2)(xvii)[II.F.1], 10 CFR 50.34(f)(2)(xix)[II.F.3], and 10 CFR 50.34(f)(2)(xxvii)[III.D.3.3] apply to the ARMS.

The ARMS design complies with these requirements, as indicated above. TMI action plan requirements are addressed generically in Appendix 1A.

7.5.4.4 Testing and Inspection Requirements

ARMS channels are tested and calibrated using the plant operating and maintenance procedures. Each Signal Conditioning Unit (SCU) is equipped with an internal self-diagnostic feature to detect and locate instrument failures. The SCU is also equipped with internal software to facilitate electronic calibration. Each SCU is provided with a means for adjustment of electronic calibration and trip setting. These adjustments do not require equipment removal from its associated panel. The SCU is also provided with a means for generating internal signals that can be used both to check the calibration of the electronic circuits that process the Radiation Detector Assembly's signal and to verify trip setpoints.

The SCU is provided with a means for administrative control of all adjustments and setpoints.

7.5.4.5 Instrumentation and Control Requirements

Every ARM channel consists of a gamma sensitive detector and a digital area radiation processor. All channels are provided with local visual and audible alarms and local readouts. Where appropriate, additional readouts and alarms are provided by local auxiliary units.

7.5.5 Pool Monitoring ~~Subsystems~~Instrumentation

General Functional Requirements Conformance

Suppression Pool

The safety-related requirement of the Suppression Pool Temperature Monitoring (SPTM) function is to protect the suppression pool temperature from exceeding established limits. The SPTM, which is a Containment Monitoring (CMS) function, continuously monitors pool temperatures and provides visual indications and alarms to the MCR panels for automatic suppression pool cooling during reactor operation and accident conditions as discussed and evaluated in Subsection 7.2.3.

The CMS provides temperature and level instruments for monitoring suppression pool water temperature and water level, respectively. The CMS instruments provide functions necessary to maintain suppression water temperature and level required for safety-related Emergency Core Cooling System (ECCS) functions described in Subsection 7.3.1.2. For this reason, they are classified as safety-related. The CMS also includes nonsafety-related temperature sensors for the DPS diverse scram function described in Subsection 7.8.1.2.1.

The suppression pool-cooling mode of the Fuel and Auxiliary Pools Cooling System (FAPCS) is automatically initiated by a high pool-temperature signal provided that either FAPCS Train A or Train B is in standby mode. The water level instrument generates a low water level signal when the suppression pool level decreases to a low level setpoint. This signal trips the FAPCS pump when it operates with suction from the suppression pool.

Gravity-Driven Cooling System Pools

The Gravity-Driven Cooling System (GDCS) provides the GDCS pools ~~are provided~~ with safety-related instruments that monitor water level. Each instrument generates high or low water level signals when the water level reading increases above or decreases below its setpoint. Each high and low-level signal initiates an alarm in the MCR. Additionally, a low-level trips the FAPCS system pump operating in the GDCS pool-cooling mode. The high-level setpoint is established to avoid overflow of GDCS pool water. The low water level setpoint is established to prevent inadvertent draining of the pool water below the minimum safe level.

The instruments provide necessary information to the operator for maintaining GDCS water level required for the safety-related ECCS function as discussed and evaluated in Subsection 7.3.1.2. ~~For this reason, they are classified as safety-related.~~The GDCS also provides nonsafety-related instrumentation for the DPS diverse emergency core cooling function described in Subsection 7.8.1.2.2.

IC/PCC Expansion Pools

The FAPCS provides the Isolation Condenser / Passive Containment Cooling System (IC/PCCS) expansion pools ~~are pro~~component~~vided~~ with safety-related instruments that monitor water level. Each instrument generates high or low water-level signals when the water level reading increases above or decreases below its setpoint. Each high or low level signal initiates an alarm in the MCR. Additionally, a low level signal trips the IC/PCCS pool cooling and cleanup system. The high water-level setpoint is established to avoid overflow of IC/PCCS expansion pool water. The low water-level setpoint is established to prevent inadvertent draining of the IC/PCCS expansion pool water below the minimum safe level.

The instruments provide necessary information to the operator for refilling the IC/PCCS pools following an accident. ~~For this reason, each is classified as a safety-related component.~~ Safety-related water level sensors are included to allow ICS to automatically open the equalizing valves between the equipment storage pool and the IC/PCC expansion pools when a low water level is detected in either of the IC/PCC expansion pools to provide makeup water to support design basis events, as discussed and evaluated in Subsection 7.4.4. The FAPCS also includes nonsafety-related IC/PCCS expansion pool level sensors for use by DPS as described in Subsection 7.8.1.2.5.

Spent Fuel Pool

The FAPCS provides the Spent Fuel pool ~~is provided~~ with safety-related instruments that monitor water level. Each instrument generates a high and low water level signal when the water level reading increases above or decreases below its setpoint. Anti-siphoning holes are provided in all submerged portions of FAPCS discharge lines at the elevation of normal water level to prevent significant draining of the pool in the event of a pipe break. These level instruments are safety-related to ensure proper level is maintained.

The skimmer surge tanks are used for receiving overflow water from the spent fuel pool, and as a pump suction source during the spent fuel pool-cooling mode of operation. These tanks are provided with instruments that monitor their water level. The instruments generate high-high, high, low, or low-low water level signals when the water level reading increases above or

decreases below its setpoint. The high and low level signals are used for the opening and closing of the Condensate Storage and Transfer System valve for make up water to skimmer surge tanks. The high-high and low-low signals initiate high and low water level alarms in the MCR. Additionally, the low level signal is used for tripping the FAPCS pump operating in the spent fuel pool-cooling mode. The high level setpoint is established to avoid overflow of skimmer surge tank water. The low water level setpoint is established to prevent inadvertent draining of the tank water below the minimum safe level.

The level instruments for the spent fuel pool are classified as safety-related components because they provide necessary information to the operator for performing the safety-related function of refilling the spent fuel pool following an accident.

7.5.5.1 System Design Bases

See Subsection 9.1.3.1.

7.5.5.2 System Description

See Subsection 9.1.3.2.

7.5.5.3 Safety Evaluation

This subsection addresses Pool Monitoring Instrumentations conformance to regulatory requirements, guidelines, and industry standards.

~~See Subsection 9.1.3.3.~~

7.5.5.3.1 Code of Federal Regulations

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

- Conformance: The safety-related Pool Monitoring instrumentation design complies with these standards.

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

- Conformance: The safety-related Pool Monitoring instrumentation design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the Pool Monitoring conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): Safety-related functions of the Pool Monitoring instrumentation are described in Subsection 7.5.5. The design bases for the instrumentation is included with the system that uses the signal from the sensor as shown below.
    - GDCS pools (Subsection 7.3.1.2.1),
    - IC/PCCS Expansion Pools (Subsection 5.4.6.1), and

- Spent Fuel Pool (Subsection 7.5.1.1).

– Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the Pool Monitoring instrumentation design.

– Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to Pool Monitoring instrumentation design.

– Section 5.2 (Completion of Protective Actions): The Pool Monitoring instrumentation does not provide any trip or isolation functions.

– Section 5.7 (Capability for Test and Calibration): See Subsection 9.1.3.4.

– Section 6.2 and 7.2 (Manual Control): Manual Control is not applicable beyond that discussed in Subsection 7.1.6.6.1.18.

– Section 6.4 (Derivation of System Inputs): Derivation of System Inputs for Pool Monitoring instrumentation is not applicable beyond that discussed in Subsection 7.1.6.6.1.20.

– Section 6.5 (Capability of Test and Calibration): See Subsection 9.1.3.4.

– Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the Pool Monitoring instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.

– Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for Pool Monitoring instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.

– Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for Pool Monitoring instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.

– Section 8.3 (Maintenance Bypasses): Maintenance bypasses for Pool Monitoring instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The Pool Monitoring instrumentation design conforms to these standards.

10 CFR 50.34(f)(2)(xvii) [II.F.1], Accident Monitoring Instrumentation:

- Conformance: The Pool Monitoring instrumentation design complies with these requirements.

10 CFR 50.34(f)(2)(xviii) [II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: The Pool Monitoring instrumentation design complies with this requirement. The direct water-level instrument system provides for the detection of conditions indicative of inadequate core cooling (Refer to Table 1A-1 of Appendix 1A, Three Mile Island [TMI] Action Plan Items).

10 CFR 50.34(f)(2)(xix) [II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The Pool Monitoring instrumentation design conforms to this requirement. The Pool Monitoring instrumentation design conforms to RG 1.97.

10 CFR 50.34(f)(2)(xxiv) [II.K.3.23], Recording of Reactor Vessel Water Level:

- Conformance: The Pool Monitoring instrumentation design conforms to this requirement. (Refer to Table 1.A-1 of Appendix 1A TMI Action Plan Items).

10 CFR 52.47(a)(21), 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(b)(1), Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) in Design Certification Applications:

- Conformance: ITAAC are provided for the Instrumentation and Control (I&C) systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

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

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the Pool Monitoring instrumentation within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.5.5.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 24, 34, 35, 38, and 63:

- Conformance: The Pool Monitoring instrumentation design conforms to these GDC.

7.5.5.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The Pool Monitoring instrumentation design conforms to RG 1.97, which endorses (with certain exceptions specified in Section C of the RG) IEEE Std. 497 that establishes flexible, performance-based criteria for the selection, performance, design, qualification, display, and quality assurance of accident monitoring variables. IEEE Std. 497 identifies five types of variables for accident monitoring and the criteria for the selection of each type of variable.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The Pool Monitoring instrumentation design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The Pool Monitoring instrumentation design, in conjunction with the Q-DCIS, conforms to IEEE Std. 603.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The Pool Monitoring instrumentation design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.5.5.3.4 Branch Technical Positions

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The Pool Monitoring instrumentation design conforms to RG 1.97 Revision 4, IEEE Standard 497-2002 (with clarifications and exceptions stated in RG 1.97 Revision 4), and RG 1.100.

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

- Conformance: The level of detail provided for the Pool Monitoring instrumentation design conforms to BTP HICB-16.

passing through the check valves. A safety relief valve is provided upstream of the testable check valves to protect against over-pressurization of the pipe by leakage through the check valves. The relief valve discharge line is monitored to detect any leakage through the check valves. ~~The MOVs block any leakage passing through the check valves and protect low pressure FAPCS piping by the HP/LP interlock system~~

The FAPCS HP/LP interlock logic ~~system~~ prevents the opening of the isolation valves on the LPCI discharge line. The interlock logic ~~system~~ vprohibits the LPCI line isolation valves from being opened whenever the reactor pressure is greater than the reactor pressure permissive setpoint for the interlock logic, thereby precluding over-pressurization of~~protecting~~ the low pressure FAPCS piping ~~from over-pressurization~~ during reactor power operation. The interlock logic ~~system is designed to~~ permits LPCI mode initiation when the reactor pressure is below its reactor pressure permissive setpoint allowing the operator to manually open either isolation valve. The interlock logic ~~system~~ operates automatically, and its status is provided to the reactor operator in the MCR.

~~The LPCI line provides a path to bring in fire water/suppression pool water for reactor shutdown cooling 72 hours after a Design Basis Event (DBE), if the normal shut-down cooling system is not available. Therefore the HP/LP interlock system is nonsafety-related within the scope of Regulatory Treatment of Non-Safety Systems (RTNSS).~~

~~Table 7.1-1 identifies the HP/LP interlock~~ systems ~~and the associated codes and standards applied, in accordance with NUREG-0800.~~ This subsection addresses conformance of the nonsafety-related HP/LP interlock logic ~~system~~ to regulatory requirements, guidelines, and industry standards.

7.6.1.3.1 Code of Federal Regulations

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

- Conformance: The HP/LP interlock logic ~~system~~ is nonsafety-related. ~~The testable check valves and upstream MOVs provide pressure boundary integrity for the RWCU/SDC system. The actuators for the testable check valves, the solenoids, electrical modules and cables are nonsafety-related and these fall under RTNSS. The quality assurance requirements are similar to those for the safety-related components.~~

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

- Conformance: The HP/LP interlock logic ~~system~~ is nonsafety-related. 10 CFR 50.55a(h) and IEEE Std. 603 are not applicable. ~~to this system, however each of the parallel air operated testable check valves and each of the parallel MOVs is powered either from the PIP A or PIP B buses. Similarly, interlock logic is implemented in the PIP A N-DCIS or PIP B N-DCIS providing separation and isolation, both mechanically and electrically.~~

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

- Conformance: The HP/LP interlock logic ~~system~~ does not have a bypass feature.

~~Pressure transmitters and trip actuators for initiating a reactor scram, and pressure transmitters and trip actuators for bypassing the main steam line isolation valve (MSIV) closure scram are discussed in Subsection 7.2.1. High pressure and low pressure (HP/LP) interlocks are discussed in Subsection 7.6.1.1.~~

~~Pressure transmitters that are used for pressure recording are discussed in Subsection 7.2.1.2.~~

Safety Relief Valve Leak Detection

Thermocouples are located in the discharge pipes of ten Safety Relief Valves (SRVs) (Reference Subsection 5.2.5). The temperature signals are recorded, and temperatures indicative of a leaking SRV are alarmed in the MCR.

Main Steam Flow Rate

Differential pressure transmitters are used to infer main steam flow rate. Pressure taps from the throat of the RPV steam outlet nozzles, in conjunction with the RPV dome pressure taps, measure differential pressure. The square root of differential pressure is proportional to the main steam flow rate.~~ Safety-related transmitters provide input to the Leak Detection and Isolation System (LD&IS) logic.~~ Outputs from nonsafety-related transmitters are used for feedwater (FW) control.

7.7.1.3 Safety Evaluation

Section 7.7 addresses only the nonsafety-related portion of the NBS instruments.~~The safety-related reactor water level and dome pressure instruments are designed to withstand the loads and environmental conditions under which they must function. Sufficient separate sensors and indicators are provided so that a single failure cannot result in the loss of level indication. The combined range of the wide range and fuel zone water level instrumentation ensures that adequate level information is available over the entire range of postulated design basis accident conditions (IEEE Std. 603, Sections 4.8 and 5.1).~~

~~Table 7.1-1 identifies the safety-related NBS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.~~

The nonsafety-related instruments discussed in this subsection are designed to operate under normal and peak operating conditions of system pressure and at ambient pressures and temperatures. Any mechanical interface between nonsafety-related instruments and safety-related instrument piping or the RCPB is classified as safety-related to avoid compromise of the safety-related sensing capability and/or the RCPB. If a line break occurs in a nonsafety-related portion of a sensing line, the excess flow check valve closes to stop the flow of reactor coolant. If there is a single failure of the excess flow check valve, a restriction orifice limits the flow of coolant to within acceptable bounds.

7.7.1.3.1 Code of Federal Regulations

~~10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate Core Cooling Instrumentation:~~

~~Conformance: Reactor water level instrumentation errors due to non-condensable gases in instrument reference legs are addressed in Subsection 7.7.1.2.2.~~

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

- Conformance: The NBS conforms to these criteria, as shown by the following commitments to applicable Regulatory Guides (RG) and standards.

~~10 CFR 50.55a(h), Criteria for Protection Systems for Nuclear Power Generating Stations (IEEE Std. 603):~~

~~Conformance: Safety-related portions of the NBS are designed to conform to IEEE Std. 603, as discussed in Subsection 7.2.1.3.4.~~

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The NBS design conforms to these requirements.

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

~~Conformance: The NBS design of bypass and inoperable status indication conforms to this requirement.~~

10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: Reactor water level instrumentation errors due to non-condensable gases in instrument reference legs are addressed in Subsection 7.7.1.2.2.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)~~(1)(iv)~~(21), 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)~~(b)(1)~~(vi)~~, ITAAC in Design Certification Applications:

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

10 CFR 52.47(a)~~(1)(vii)~~(25), 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 NBS within the DCD conforms to this regulation.

10 CFR 52.47~~(b)~~(c)(2)~~(i)~~, Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.7.1.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, and 24:

- Conformance: The NBS design complies with these GDC.

~~7.7.1.3.3 Staff Requirements Memorandum~~

~~Staff Requirements Memorandum (SRM) on SECY-93-087 II.Q, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:~~

- ~~Conformance: In addition to the features already incorporated in the design to provide defense-in-depth against common mode failures that address this SRM, the NBS ADS function and other ESF designs conform to Item II.Q of SECY-93-087, NRC Branch Technical Position (BTP) HICB-19 through the implementation of an additional Diverse Instrumentation and Control System described in Section 7.8.~~

~~7.7.1.3.4~~ 7.7.1.3.3 Regulatory Guides

~~RG 1.75, Physical Independence of Electric Systems:~~

- ~~Conformance: The NBS system design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.~~

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification). ~~The safety-related portions of the NBS design conform to RG 1.89.~~

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

~~RG 1.105, Instrument Setpoints for safety-related Systems:~~

- ~~Conformance: The safety-related portions of the NBS design comply with RG 1.105. Reference 7.7-3 provides a detailed description of the GEH setpoint methodology.~~

RGs 1.151, Instrument Sensing Lines:

- Conformance: The instrument sensing lines for the NBS instrumentation conform to the guidelines of RG 1.151 and ISA-67.02.01. Flow restrictors are provided inside containment on instrument lines connected to the RCPB. Accessible manual isolation valves and self-actuating excess flow check valves are provided outside the drywell. The mechanical design guidelines as defined by ISA-67.02.01 and RG 1.151 are met as applicable for each installation.

~~RG 1.152, Computer Software Used in Safety-related Systems:~~

~~Conformance: The safety-related portions of the NBS design conform to RG 1.152.~~

~~RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:~~

~~Conformance: The safety-related portions of the NBS design comply with RG 1.153.~~

~~RG 1.168, Verification, Validation, Reviews, and Audits For Digital Computer Software Used In Safety Systems:~~

~~Conformance: The safety-related portions of the NBS design conform to RG 1.168.~~

~~RG 1.169, Configuration Management Plans For Digital Computer Software Used In Safety Systems:~~

~~Conformance: The safety-related portions of the NBS design conform to RG 1.169.~~

~~RG 1.170, Software Test Documentation For Digital Computer Software Used In Safety Systems:~~

~~Conformance: The safety-related portions of the NBS design conform to RG 1.170.~~

~~RG 1.171, Software Unit Testing For Digital Computer Software Used In Safety Systems:~~

~~Conformance: The safety-related portions of the NBS design conform to RG 1.171.~~

~~RG 1.172, Software Requirements Specifications For Digital Computer Software Used In Safety Systems:~~

~~Conformance: The safety-related portions of the NBS design conform to RG 1.172.~~

~~RG 1.173, Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems:~~

~~Conformance: The safety-related portions of the NBS design conform to RG 1.173.~~

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems.

- Conformance: The NBS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The NBS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification). ~~The safety-related portions of the NBS design conform to RG 1.209.~~

~~7.7.1.3.5~~ 7.7.1.3.4 Branch Technical Positions

~~BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:~~

- ~~Conformance: The NBS design complies with BTP HICB-11.~~

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

- ~~Conformance: The safety-related portions of the NBS design comply with BTP HICB-12. Reference 7.7-3 provides a detailed description of the GEH setpoint methodology.~~

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

- Conformance: The level of detail provided for this system complies with BTP HICB-16.

BTP HICB-14, 17, 18, 19, and 21 are discussed in association with the Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) in Subsection 7.3.5.3.

7.7.1.4 Testing and Inspection Requirements

Calibration and testing of the various instruments are performed during preoperational testing to confirm that the instrumentation is installed correctly and performs as intended.

Pressure, differential pressure, water level, and flow instruments are located outside the drywell so that calibration and test signals can be applied during reactor operation. Temperature elements located inside the drywell can be tested and calibrated from junction boxes located outside the drywell ~~(IEEE Std. 603, Section 5.7)~~.

7.7.1.5 Instrumentation and Control Requirements

The information available to the reactor operator from the NBS instrumentation is discussed in Section 7.1. ~~this subsection (IEEE Std. 603, Section 5.8) consists of:~~

- ~~RPV water level indicated in the MCR on displays associated with the different water level ranges;~~
- ~~The reactor pressure indicated in the MCR and at four local instrument racks in the Reactor Building (RB);~~
- ~~The discharge line temperatures of the SRVs viewed on safety-related video display units (VDUs) in the MCR. Any temperature exceeding the trip setting is alarmed to indicate leakage of a SRV seat;~~

adjusted, if needed, as a result of plant startup testing results. It is anticipated that none or very few of the RC&IS setpoints (besides the continual ATLM rod block setpoint updates) require adjustment as a result of startup testing results.

7.7.2.2.7.11 Environmental Considerations

The RC&IS is not required for safety-related purposes, nor is it required to operate after a design basis accident. This system is required to operate in the normal plant environmental conditions at the locations of the RC&IS equipment, in the back-panel area of the MCR and in applicable areas of the RB.

7.7.2.3 Safety Evaluation

The circuitry described for the RC&IS is completely independent of the circuitry controlling the scram valves. This separation of the scram and normal rod control functions prevents failures in the RC&IS circuitry from affecting the scram circuitry. The scram circuitry is discussed in Subsection 7.2.1. Because the RC&IS directly controls movement of each control rod as an individual unit, a failure that results in inadvertent movement of a control rod affects only one control rod. The malfunctioning of any single control rod does not impair the effectiveness of a reactor scram. Therefore, no single failure in the RC&IS prevents a reactor scram. Repair, adjustment, or maintenance of the RC&IS components does not affect the scram circuitry.

Chapter 15 examines the various failure mode considerations for this system. The expected and abnormal transients and accident events analyzed in subsections 15.2.3.1, 15.2.3.2, 15.3.1, 15.3.7, 15.3.8, and 15.3.9 envelope the failure modes associated with RC&IS ~~components~~ digital controls.

Table 7.1-1 identifies the RC&IS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.7.2.3.1 Code of Federal Regulations

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

- Conformance: The RC&IS design conforms to these requirements.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The RC&IS design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The RC&IS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for reduction of risk from Anticipated Transients Without Scram (ATWS) events for light-water-cooled nuclear power plants:

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

10 CFR 52.47(a)~~(1)(iv)~~(21), Resolution of Unresolved and Generic Safety Issues:

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

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

- Conformance: ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)~~(1)(vii)~~(25), Interface Requirements:

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

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the RC&IS within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The RC&IS design does not use innovative means for accomplishing safety functions.

7.7.2.3.2 General Design Criteria

GDC 1, 2, 4, 12, 13, 19, 24, 25, 26, 27, 28 and 29:

- Conformance: The RC&IS complies with these GDC.

7.7.2.3.3 Staff Requirements Memorandum

SRM on SECY 93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The portions of RC&IS that provide interface support for DPS conform to item II.Q of SECY-93-087.

~~7.7.2.3.3~~ 7.7.2.3.4 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The RC&IS design conforms to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RC&IS design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The RC&IS design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RC&IS design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RC&IS design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RC&IS design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The RC&IS design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems:

- Conformance: The RC&IS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

~~RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:~~

- ~~Conformance: The RC&IS design conforms to RG 1.204.~~

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

~~7.7.2.3.4~~ 7.7.2.3.5 Branch Technical Positions

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

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

- Conformance: The level of detail provided for the RC&IS design conforms to BTP HICB-16.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems:

- Conformance: The portions of RC&IS that provide interface support for DPS conform to BTP HICB-19.

7.7.2.4 Testing and Inspection Requirements

The RC&IS equipment is designed with consideration for online testing capabilities. The system can be maintained on line while repairs or replacement of hardware take place without causing any abnormal upset condition. The single-channel bypass capabilities support having continued RC&IS operation while repair or maintenance work is being performed on the dual-channel portion of the RC&IS equipment.

7.7.2.5 Instrumentation and Control Requirements

The CRD system is the RC&IS main direct interface to gather control rod position information and FMCRD status information and execute control rod movement commands. The FMCRD-related instrumentation that provides direct input to the RC&IS is addressed as part of the CRD system in Subsection 4.6.1. The primary output of the RC&IS to accomplish the RC&IS related rod movement functions is the 3-phase AC power to the FMCRD motors, associated AC power to the MBBs, and the holding brakes of the CRD system.

The RC&IS modules that interface with FMCRD instrumentation include the appropriate signal conditioning and conversion components (for example, RDC, discrete contact closure or reed switch input circuitry, and excitation power sources/supplies) for acquisition of:

- Resolver A and B position feedback signals (continuous signals);
- Coupling check (overtravel-out) position reed switch (discrete signal);

- The FW temperature controller is unable to decrease FW temperature if the reactor thermal power is greater than 100%. The validated reactor thermal power signal is provided by the NMS.
- Individual temperature control valves are "locked up" if they are not at their demanded position within a prespecified time or one-way "locked up" if there is an ATLM one-way block (to prevent FW temperature from additional decrease [increase], the steam heating valves are blocked from further closing [opening] the bypass valves are blocked from further opening [closing]).
- The heating valves to the seventh FW heater and the high pressure FW heater bypass valves are not open simultaneously.

7.7.3.3 Safety Evaluation

The FWCS is a power generation system that maintains proper RPV water level and FW temperature. Its level control range is from high water level (Level 8) to low water level (Level 3) and its nominal FW temperature control range at 100% rated power is from 188°C (370°F) to 215.6°C (420°F). FW temperature can be increased up to 252.2°C (486°F) which reduces the rated reactor power by approximately 15%. The RPV water level rising to Level 8 or falling to Level 3 results in the shutdown of the reactor by the RPS. If the RPV water level rises too high (Level 8), the main turbine trips, the ASD feed pump ~~ASD~~ flow demand is reduced to zero, and the safety-related FW isolation valves are closed by LD&IS. Continued rising water level to Level 9 results in a trip of all ASD feed pumps by the DPS and the ASD controller power supply being interrupted by LD&IS . If the reactor thermal power versus FW temperature combination is outside of the area allowed by the reactor power versus FW temperature map, the RC&IS initiates a control rod withdrawal block and FW temperature control valve one-way block. If the reactor thermal power versus FW temperature combination further departs from the area allowed by the reactor power versus FW temperature map (high reactor thermal power, high feedwater temperature or low feedwater temperature), the RPS initiates reactor shutdown. The RPS uses eight safety-related measurements of FW temperature (two per division) and implements a reactor scram using two-out-of-four logic based on a validated reactor thermal power. Refer to Subsection 7.2.1 for the RPS description.

The FWCS initiates a runback of FW pump FW demand to zero and closes the LFCV and RWCU/SDC OBCV when it receives an ATWS trip signal from the ATWS/SLC Logic. Refer to Subsection 7.8.1.1.

A combined FW temperature change and FW flow/reactor water level change caused by controller failure is precluded by implementing the two control schemes in physically different cabinets and logic processors.

A loss of FW heating that results in a significant decrease in FW temperature is independently detected by the ATLMs and by the DPS, either of which will mitigate the event by initiating SCRRI and SRI functions. These interlocks mitigate the effects of a reactor power increase due to reduced FW temperature. Although no credit is taken for the function in a safety analysis, the FW temperature control system also mitigates inadvertent FW temperature changes in either direction by manipulating its control valves to maintain the setpoint temperature. The

temperature difference between FW lines A and B is monitored and alarmed if it exceeds the allowable value.

A total failure of the triple redundant FW temperature control system such that the outputs all fail downscale (or upscale), and the heating steam valves close (or open), or the bypass valves close (or open) is highly unlikely. No single failure or operator error of the FW temperature control system results in more than a 55.6°C (100°F) decrease in the final FW temperature. The design meets the requirements for the condensate and FW system specification in Subsection 10.4.7.1.

Chapter 15 examines the various failure mode considerations for this system. The expected and abnormal transients and accident events analyzed in Subsections 15.2.4.2, 15.3.1, and 15.3.2 envelope the failure modes associated with the FWCS digital controls.

Table 7.1-1 identifies the FWCS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.7.3.3.1 Code of Federal Regulations

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

- Conformance: The FWCS design conforms to these requirements.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The FWCS design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The FWCS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

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

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

10 CFR 52.47(a)~~(1)(iv)~~(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Unresolved and generic safety issues are discussed in Section 1.11.

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

- Conformance: ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)~~(1)(vii)~~(25), Interface Requirements:

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

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the FWCS within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The FWCS design does not use innovative means for accomplishing safety functions.

7.7.3.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, and 24:

- Conformance: The FWCS design complies with these GDC.

7.7.3.3.3 Staff Requirements Memorandum

SRM on SECY 93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The portions of FWCS that provide interface support for DPS conform to item II.Q of SECY-93-087.

~~7.7.3.3.3~~ 7.7.3.3.4 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.151, Instrument Sensing Lines:

- Conformance: The FWCS receives signals from sensors on vessel instrument lines in the NBS. Refer to Subsection 7.7.1.3 for a discussion of the guidance of RG 1.151 in relation to the NBS.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The FWCS design conforms to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The FWCS design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The FWCS design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The FWCS design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The FWCS design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The FWCS design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The FWCS design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The FWCS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

~~RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:~~

- ~~Conformance: The FWCS design conforms to RG 1.204.~~

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

~~7.7.3.3.4~~ 7.7.3.3.5 Branch Technical Positions

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 conforms to BTP HICB-16.

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

- Conformance: The portions of FWCS that provide interface support for DPS conform to BTP HICB-19.

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.

- Conformance: The PAS design conforms to these requirements.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The PAS design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The PAS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)~~(1)(iv)~~(21), Resolution of Unresolved and Generic Safety Issues:

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

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

- Conformance: ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)~~(1)(vii)~~(25), Interface Requirements:

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

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the PAS within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The PAS design does not use innovative means for accomplishing safety functions.

7.7.4.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, and 24:

- Conformance: The PAS design complies with these GDC.

7.7.4.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The PAS design conforms to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAS design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The PAS design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAS design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAS design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAS design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAS design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems:

- Conformance: The PAS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

~~RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:~~

- ~~Conformance: The PAS design conforms to RG 1.204.~~

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.7.4.3.4 Branch Technical Positions

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

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

- Conformance: The level of detail provided for the PAS conforms to BTP HICB-16.

7.7.4.4 Testing and Inspection Requirements

The FTDC input and output communication interfaces function continuously during normal power operation. Abnormal functioning of these components can be detected during operation. In addition, the FTDC is equipped with self-test and on-line diagnostic capabilities for identifying and isolating failures of input/output signals, buses, power supplies, processors, and inter-processor communications. These on-line tests and diagnostics can be performed without interrupting the normal control operation of the PAS.

7.7.4.5 Instrumentation and Control Requirements

The instrumentation required for the system can be categorized as (1) MCR instrumentation, needed for the man-machine interface, (2) hardware and software instrumentation for input/output interfaces and controller functions, and (3) direct non multiplexed sensor inputs needed by the system. The PAS hardware comprises triple redundant master controllers and duplicate system controllers. PAS software is required for controller functions and input/output interfaces.

7.7.5 Steam Bypass and Pressure Control System

7.7.5.1 System Design Bases

7.7.5.1.1 Safety Design Bases

The SB&PC System does not perform or ensure any safety-related function, is classified as a nonsafety-related system, and has no safety-related design basis. In the Power Operation Mode, only one of the three triple redundant FTDCs can be removed from service.

Table 7.1-1 identifies the nonsafety-related SB&PC System and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.7.5.3.1 Code of Federal Regulations

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

- Conformance: The SB&PC design conforms to these requirements.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The SB&PC design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)~~(1)(iv)~~(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: The SB&PC System is nonsafety-related and conforms in that there are no unresolved issues for the SB&PC System. Resolution of unresolved and generic safety issues is discussed in Section 1.11.

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

- Conformance: Inspection, test, analyses, and acceptance criteria of the SB&PC System FTDC are identified in Tier 1.

10 CFR 52.47(a)~~(1)(vii)~~(25), Interface Requirements:

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

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the SB&PC within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The SB&PC design does not use innovative means for accomplishing safety functions.

7.7.5.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, and 24:

- Conformance: The SB&PC System design conforms to these GDC.

7.7.5.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.151, Instrument Sensing Lines:

- Conformance: RG 1.151 is not applicable to the SB&PC System. The SB&PC System receives RPV dome pressure signals from sensors in the NBS (refer to Subsection 7.7.1.3). The SB&PC System also receives condenser absolute pressure signals from sensors in the Main Condenser and Auxiliaries System.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The SB&PC design conforms to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SB&PC design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The SB&PC design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SB&PC design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SB&PC design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SB&PC design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The SB&PC design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interface in Safety-related Instrumentation and Control Systems:~~.~~

- Conformance: ~~The SB&PC System design conforms to RG 1.180.~~See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

~~RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:~~

- ~~Conformance: The SB&PC System design conforms to RG 1.204.~~

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.7.5.3.4 Branch Technical Positions

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

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

- Conformance: The level of detail provided in this subsection conforms to BTP HICB-16.

7.7.5.4 Testing and Inspection Requirements

The FTDC input and output communication interfaces function continuously during normal power operation. Abnormal operation of these components is detected during operation. The FTDC is equipped with on-line diagnostic capabilities to identify and isolate failure of I/O signals, buses, power supplies, processors, and inter-processor communications. On-line diagnostics are performed without interrupting the normal control operation of the SB&PC System.

The SB&PC System components and critical components of interfacing systems are tested to ensure the specified performance requirements are satisfied. Preoperational testing of the

7.7.6.2.2.2 Classification

The MRBM is nonsafety-related. Its activating interface is through the RC&IS, which is also a nonsafety-related system.

7.7.6.2.2.3 Power Supply

The power supply for the MRBM is from the non-divisional, nonsafety-related 120 VAC UPS buses in two different load groups.

7.7.6.2.2.4 Environmental Considerations

The MRBM is located in the MCR. It is physically and electrically isolated from the safety-related NMS subsystems. All interfaces with the safety-related NMS subsystems are through fiber optic isolators.

7.7.6.3 Safety Evaluation

Table 7.1-1 identifies the nonsafety-related control systems and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.7.6.3.1 Code of Federal Regulations

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

- Conformance: The AFIP and MRBM subsystem designs conform to these requirements.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The AFIP and MRBM designs conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)~~(1)(iv)~~(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Unresolved and generic safety issues are discussed in Section 1.11.

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

- Conformance: ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)~~(1)(vii)~~(25), Interface Requirements:

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

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the AFIP and MRBM within the DCD conforms to this BTP.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The AFIP and MRBM designs do not use innovative means for accomplishing safety functions.

7.7.6.3.2 General Design Criteria

GDC 1, 2, 4, 12, 13, 19, 24, 25, 26, 27, ~~and~~ 28 and 29:

- Conformance: The AFIP and MRBM subsystem designs comply with these GDC.

7.7.6.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The AFIP and MRBM subsystem designs conform to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The AFIP and MRBM designs conform to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The AFIP and MRBM designs conform to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The AFIP and MRBM designs conform to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The AFIP and MRBM designs conform to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The AFIP and MRBM designs conform to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The AFIP and MRBM designs conform to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems:

- Conformance: The AFIP and MRBM subsystem designs conform to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

~~RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:~~

- ~~Conformance: The AFIP and MRBM subsystem designs conform to RG 1.204.~~

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.7.6.3.4 Branch Technical Positions

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

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

- Conformance: The level of detail provided in this subsection conforms to BTP HICB-16.

The MRBM instrument is provided with necessary operator interface functions meeting NMS man-machine interface requirements.

The MRBM includes basic logic such as continuous LPRM data collection, MRBM rod block algorithm calculation, MRBM setpoint comparison, and communication protocol with the N-DCIS. The MRBM subsystem is located within the nonsafety-related equipment rooms of the CB having acceptable environmental conditions and physical and electrical separation from the safety-related NMS instruments..

7.7.7 Containment Inerting System

7.7.7.1 System Design Bases

The CIS design bases are discussed in Subsection 6.2.5.2.1.

7.7.7.2 System Description

The CIS system description is discussed in Subsection 6.2.5.2.

7.7.7.3 Safety Evaluation

The CIS safety evaluation is discussed in Subsection 6.2.5.2.3.

Table 7.1-1 identifies the CIS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.7.7.3.1 Code of Federal Regulations

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

- Conformance: The CIS design conforms to these requirements.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The CIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xv)[II.E.4.4], Purge System Isolation Under Accident Conditions:

- Conformance: The CIS conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The CIS conforms to these standards. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)~~(1)(iv)~~(21), 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)~~(b)(1)~~(vi)~~, ITAAC in Design Certification Applications:

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

10 CFR 52.47(a)~~(1)(vii)~~(25), Interface Requirements:

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

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the CIS within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The CIS design does not use innovative means for accomplishing safety functions.

7.7.7.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, ~~and~~ 24, 41, 42, and 43:

- Conformance: The CIS design conforms to these GDC. I&C are provided to operate the system and monitor process variables during startup, normal, and abnormal reactor operation. The CIS is operable from the MCR.

7.7.7.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97 - Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.151, Instrument Sensing Lines:

- Conformance:~~"~~ The CIS instrument lines penetrating containment comply with the guidance of RG 1.151. Sensing lines are Seismic Category I Quality Group B and are provided with redundant isolation valves that can be isolated locally or remote manually from the MCR.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The CIS design conforms to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CIS design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The CIS design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CIS design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CIS design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CIS design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The CIS design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems:

- Conformance: The CIS system design conforms to RG 1.180.

~~RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:~~

- ~~Conformance: The CIS system design conforms to RG 1.204.~~

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.7.7.3.4 Branch Technical Positions

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

~~Only~~ BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52, is applicable to the nonsafety-related CIS. The level of detail provided in this subsection conforms to BTP HICB-16.

7.7.7.4 Testing and Inspection Requirements

The CIS testing and inspection requirements are discussed in Subsection 9.4.9.

7.7.7.5 Instrumentation and Control Requirements

7.7.7.5.1 Logic and Interlocks

The CIS operation is manually or automatically activated from the MCR by aligning corresponding valves through remote manual control switches. During the inerting mode, a temperature controller accomplishes automatic control of the steam supply once the steam-heated nitrogen vaporizer has been activated. A temperature sensor at the outlet of the steam-heated vaporizer provides input to the temperature controller that then regulates the amount of steam. Low nitrogen temperature in the steam vaporizer outlet causes an alarm and a low-low temperature condition shuts off the main inerting line. The auxiliary steam supply is manually terminated. When the required inert containment pressure is reached, the CIS drywell pressure switch provides a signal to isolate the nitrogen supply shutoff valve.

Upon completion of the initial inerting, the CIS is manually or automatically aligned to its make-up mode. Make-up nitrogen is obtained by the automatic modulation of a pressure control valve on the nitrogen supply. The opening and closing of the pressure control valve is driven by the pressure controller in response to change of containment pressure. Make-up nitrogen supply is vaporized and heated up to an appropriate temperature by an electric heater that is manually loaded to its power source. Once activated, it continues to operate in automatic on-off mode until manually disconnected. Temperature sensors provide switching signals to start/stop the heater. When the required temperature is reached, the heater automatically cuts off electrical power to the heater elements.

The de-inerting process is manually or automatically activated, by aligning the CIS with the RB Heating, Ventilation and Air Conditioning (HVAC) to replace gases in the containment with breathable air.

During containment isolation events, the CIS containment isolation valves automatically close upon receipt of the isolation signal from LD&IS. Details of the isolation logic are discussed in Subsection 7.3.3.

The CIS can provide continued nitrogen makeup during isolation events. This is accomplished by overriding, with controlled bypass switches, the isolation signal to the makeup isolation valves.

A simplified system diagram is shown in Figure 6.2-29.

Table 7.8-1 provides a summary of the functions, initiators, and interfacing systems used by the diverse I&C systems for ATWS mitigation or for mitigation of design basis events described in Chapter 15. Table 7.8-2 provides a list of the controls, interlocks, and bypasses used by the diverse I&C systems for ATWS mitigation or for mitigation of design basis events described in Chapter 15. Tables 7.8-3 and 7.8-4 describe additional diverse instrumentation and control features used to ensure that releases during a common mode protection system failure coincident with the design basis events discussed in the Safety Analysis of Chapter 15 do not exceed the radiation guidelines from 10 CFR 52.47(a)(2)(iv).

Mitigation of common mode failures is provided by:

- Manual scram and Main Steam Isolation Valve (MSIV) isolation by the operator in the Main Control Room (MCR) in response to diverse parameter indications;
- Availability of diverse manual initiation of the passive ECCS functions including Gravity-Driven Cooling System (GDCS) squib valve initiation, Safety Relief Valve (SRV) initiation, Depressurization Valve (DPV) initiation, Isolation Condenser System (ICS) initiation, and SLC System squib valve initiation. Manual initiation functions are available in the safety-related systems and in the DPS;
- Core makeup water capability from the Condensate and Feedwater System (C&FS), CRD System, and Fuel and Auxiliary Pools Cooling System (FAPCS) in the Low Pressure Coolant Injection (LPCI) mode;
- Long-term shutdown capability in the two redundant Remote Shutdown System (RSS) panels which are equipped with Division 1 and 2 controls for manual scram and MSIV closure, Division 1 and 2 safety-related Video Display Units (VDUs), and ~~a~~ nonsafety-related ~~VDU~~ displays and controls to allow monitoring and control of all plant systems. Local displays of process variables in the RSS system are continuously powered and are available for monitoring at any time;
- Diverse scram~~reactor trip initiation logic~~, which is different from the safety-related RPS, using separate and independent hardware with diverse software;
- Diverse ESF initiation logic, which is different from the SSLC/ESF, using separate and independent hardware with diverse software;
- ATWS mitigation using liquid boron injection for emergency plant shutdown through the SLC system;
- ATWS mitigation using alternate rod insertion (ARI) to hydraulically scram the plant using the three sets of air header dump valves of the CRD system;
- Selected Control Rod Run-in (SCRRI) command to the Rod Control and Information System (RC&IS);
- Select Rod Insert (SRI) to hydraulically insert selected control rods with every SCRRI action; and

- Identical modules that provide simple, readily verifiable functions such as setpoint comparison and two-out-of-four logic; and
- Standard protocols for multiplexing and other data transmission functions that are verified to industry standards and are qualified to safety-related standards.

7.8.3 Safety Evaluation

The DPS is designed as a highly reliable nonsafety-related system that meets the probabilistic risk assessment (PRA) requirements to minimize failures on demand and to minimize inadvertent operation. The DPS components are designed to ensure that reliability goals and system design requirements are met. The sensors and actuation devices that interface directly with safety-related structures, systems, and components (SSC) are qualified to meet the Seismic Category I classification~~ (IEEE Std. 603, Section 5.4)~~.

Consistent with the guidance in IEEE Std. 603, Section 5.6 and IEEE Std. 384, the nonsafety-related DPS is designed to avoid adverse interaction with the protection systems with which it interfaces. Because the DPS logic does not communicate with the RPS logic, credible DPS failure modes do not prevent the RPS from performing a reactor scram~~trip~~. The DPS cannot cause the RPS to initiate a reactor scram ~~trip~~ prematurely. Credible DPS failure modes cannot prevent the SSLC/ESF actuation system from initiating ECCS functions and/or performing fission product barrier isolation functions. Additionally, credible DPS failure modes cannot result in premature operation of these protection systems.

The ATWS/SLC logic is designed to mitigate a failure of the normal reactor trip system to function and is diverse from and independent of the RPS. The ATWS/SLC logic platform is designed as a safety-related system with four independent divisions powered from divisionally separated safety-related power sources. Each redundant division of ATWS/SLC logic, which uses two-out-of-four voting logic, is capable of performing ATWS mitigation during reactor operation.

A quality assurance program that meets or exceeds the guidance contained in NRC Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," is applied to all diverse I&C systems and components described in this section. Software used in diverse instrumentation and control systems is designed and developed in accordance with the requirements of Reference 7.8-3.

The guidance contained in the SRM on SECY 93-087 Item II.Q, SRP BTP HICB-19, and Generic Letter 85-06 is applicable to the DPS and to all portions of the systems shown in Figure 7.8-1 and identified in Table 3.2-1 that are required to perform sense and actuate functions in support of the diverse instrumentation and control functions described in this Section.

Table 7.1-1 identifies the diverse I&C and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.8.3.1 Code of Federal Regulations

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

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

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

- Conformance: The safety-related portions of the diverse I&C conform to IEEE Std. 603. Conformance information is found in Subsections 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the diverse I&C conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 7.8.1.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are for the Diverse I&C system are described in Tables 7.8-1 and 7.8-2.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to the Diverse I&C system beyond that discussed in Subsection 7.1.6.6.1.1.
  - Section 5.2 (Completion of Protective Actions): Completion of Protective Actions is not applicable to the Diverse I&C system beyond that discussed in Subsection 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): Capability for Test and Calibration is not applicable to the Diverse I&C system beyond that discussed in Subsection 7.1.6.6.1.8.
  - Section 6.2 and 7.2 (Manual Control): Manual Control is not applicable to the Diverse I&C system beyond that discussed in Subsection 7.1.6.6.1.18.
  - Section 6.4 (Derivation of System Inputs): Derivation of System Inputs is not applicable to the Diverse I&C system beyond that discussed in Subsection 7.1.6.6.1.20.
  - Section 6.5 (Capability of Test and Calibration): Capability for Test and Calibration is not applicable to the Diverse I&C system beyond that discussed in Subsection 7.1.6.6.1.8.
  - Section 6.6 and 7.4 (Operating Bypasses): Operating Bypasses are for the Diverse I&C system are described in Table 7.8-2.
  - Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the Diverse I&C system are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
  - Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the Diverse I&C system are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.

– Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the Diverse I&C system power sources are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

~~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)(iii) [I.D.1], Human Factors Principles for Control Room Design:

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

10 CFR 50.34(f)(2)(iv) [I.D.2], Minimum Set of Parameters on a Safety Display Console Defining the Safety Status of the Plant:

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

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

- Conformance: The ~~diverse I&C systems~~safety-related ATWS mitigation logic conform to these requirements by providing automatic indication of bypassed and inoperable status.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

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)~~(21), 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)~~(b)(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)~~(25), 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.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The diverse I&C systems design does not use innovative means for accomplishing safety functions.

7.8.3.2 General Design Criteria

General Design Criteria (GDC) 1, 2, 4, 13, 19, and 24:

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

General Design Criteria (GDC) 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, and 29:

- Conformance: The safety-related ATWS mitigation logic 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:

- Conformance The safety-related ATWS mitigation logic is organized into four physically and electrically isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single-failure criterion.~~conforms to the guidance in RG 1.53~~. This RG is not applicable to the nonsafety-related DPS.

RG 1.62, Manual Initiation of Protection Actions:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in RG 1.62. This RG is not applicable to the nonsafety-related DPS.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in RG 1.75. This RG is not applicable to the nonsafety-related DPS.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: ~~The safety-related ATWS mitigation logic conforms to the guidance in RG 1.89. This RG is not applicable to the nonsafety-related DPS~~.See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97-Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: ~~The safety-related ATWS mitigation logic conforms to RG 1.100. This RG is not applicable to the nonsafety-related DPS.~~See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Instrument Setpoints for Safety Systems:

- Conformance: The safety-related ATWS mitigation logic setpoints are consistent with this guide. The guidance in RG 1.105 is also applied to any portions of the nonsafety-related DPS used for maintaining ~~design limits described in~~automatic initiation function required by the Technical Specifications. Reference 7.8-4 provides a detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in RG 1.118. This RG is not applicable to the nonsafety-related DPS.

RG 1.151, Instrument Sensing Lines:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in RG 1.151. Sections of endorsed standard ANSI/ISA-S67.02.01 on design practices for tubing, vents, and drains also apply to sensing lines that support DPS.

RG 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants:

- Conformance: The ~~safety-related ATWS mitigation logic~~diverse I&C conforms to the guidance in RG 1.152. ~~This RG is not applicable to the nonsafety-related DPS.~~

RG 1.153, Criteria for Power Instrumentation and Control Portions of Safety Systems:

- Conformance: The safety-related ATWS mitigation logic conforms to ~~the guidance in RG 1.153~~10 CFR 50.55a(h). This RG is not applicable to the nonsafety-related DPS.

RG 1.168, Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ~~safety-related ATWS mitigation logic~~diverse I&C conforms to the guidance in RG 1.168. ~~This RG is not applicable to the nonsafety-related DPS.~~

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ~~safety-related ATWS mitigation logic~~diverse I&C conforms to the guidance in RG 1.169. ~~This RG is not applicable to the nonsafety-related DPS.~~

RG 1.170, Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The ~~safety-related ATWS mitigation logic~~diverse I&C conforms to the guidance in RG 1.170. ~~This RG is not applicable to the nonsafety-related DPS.~~

RG 1.171, Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The ~~safety-related ATWS mitigation logic~~diverse I&C conforms to the guidance in RG 1.171. ~~This RG is not applicable to the nonsafety-related DPS.~~

RG 1.172, Software Requirements Specifications for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The ~~safety-related ATWS mitigation logic~~diverse I&C conforms to the guidance in RG 1.172. ~~This RG is not applicable to the nonsafety-related DPS.~~

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The ~~safety-related ATWS mitigation logic~~diverse I&C conforms to the guidance in RG 1.173. ~~This RG is not applicable to the nonsafety-related DPS.~~

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: ~~The safety-related ATWS mitigation logic conforms to the guidance in RG 1.180. This RG is not applicable to the nonsafety-related DPS.~~See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The ~~diverse I&C design~~safety-related ATWS mitigation logic conforms to the guidance provided in RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: ~~The safety-related ATWS mitigation logic conforms to the guidance in RG 1.209. This RG is not applicable to the nonsafety-related DPS.~~See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.8.3.5 Branch Technical Position

BTP HICB-8, Guidance on Application of RG 1.22:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in HICB-8. This BTP is not applicable to the nonsafety-related DPS.

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Application and Qualification of Isolation Devices:

- Conformance: The safety-related ATWS mitigation logic~~diverse I&C design~~ conforms to BTP HICB-11. BTP HICB-11 is not applicable to the nonsafety-related DPS because all interfacing isolation devices are part of the safety-related systems.

BTP HICB-12, Establishing and Maintaining Instrument Setpoints:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in HICB-12. This BTP is not applicable to the nonsafety-related DPS.

BTP HICB-14, Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in HICB-14. This BTP is not applicable to the nonsafety-related DPS.

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

- Conformance: The level of detail for the diverse I&C systems conform to BTP HICB-16.

BTP HICB-17, Self-Test and Surveillance Test for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in HICB-17. This BTP is not applicable to the nonsafety-related DPS.

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

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in HICB-18. This BTP is not applicable to the nonsafety-related DPS.

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

- Conformance: Reference 7.8-1 details the echelons of defense used in the design that conforms to BTP HICB-19. This document also discusses the basis for selection of the DPS functions used as backups for the RPS and SSLC/ESF. A failure modes and effects analysis based on the Guidance in NUREG/CR-6303 (Reference 7.8-2) is performed to ensure the radiation guidelines from ~~10 CFR 100~~ 10 CFR 52.47(a)(2)(iv) are not exceeded in the event of a common mode failure of the RPS or SSLC/ESF software platform during the design basis events discussed in the Safety Analyses.

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