

**DCD Markups for RAI 14.3-265 Supplement 1**

## 2.2.15 Instrumentation & Control Compliance With IEEE Std. 603

### Design Description

IEEE Std. 603 establishes the minimum functional and design requirements for the power, instrumentation, and control portions of safety systems. ESBWR divides safety systems into two parts: the safety-related distributed control and information system (Q-DCIS) platforms, and the associated functional systems that contain the sensors and actuators used by the Q-DCIS platforms.

In accordance with the software development process described in Section 3.2 and the defense-in-depth and diversity strategy described in Subsection 2.2.14, 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 2.2.10-1 shows 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.

Demonstration of compliance with IEEE Std. 603 means the Q-DCIS documentation include design bases that make appropriate reference to IEEE Std. 603 design criteria and that the resulting as-built equipment has been inspected, tested, or analyzed to show that the Q-DCIS will be capable of performing in accordance with the design bases. The choice of whether an inspection, test, or analysis is required to close a particular ITAAC is defined in the documentation associated with the {{Design Acceptance Criteria}} ITAAC closure report for the software projects in response to ITAAC defined in Section 3.2.

IEEE Std. 603 divides the Q-DCIS into three features: sense, command, and execute features. Sense features comprise sensors. Command features comprise the Q-DCIS platforms. Execute features comprise actuators. Each of these features is treated differently within Tier 1 because of influences outside of the scope of IEEE Std. 603.

As a result of these differences, Table 2.2.15-1 was developed to group the software projects with their associated functional system(s), if any, and to define how the various IEEE Std. 603 criteria will be demonstrated by an ITAAC for each software projects.

Table entries marked with an 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. Table entries marked with a 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, NBS, CMS-SPTM, NBS, and CRD. The report(s) may be referenced or attached to a software projects lifecycle phase summary baseline review record (BRR, reference Subsection 3.2) to close the Table 2.2.15-2 ITAAC.

Table headings contain the software projects or the functional system identifier and a parenthetical reference to the section or subsection where additional information about the software projects or functional system can be found. These parenthetical references are reverse references that point back to the originating system. The IEEE Std. 603 criteria apply only to those structures, systems, or components (SSC) directly associated with the performance of the safety-related function of the software projects. Complete lists of applicable SSC and functions are defined in the documentation associated with the {{Design Acceptance Criteria}} ITAAC closure report for each software projects in response to ITAAC defined in Section 3.2. These lists along with the information in the tables associated with a software projects or functional system in each column define the scope of the IEEE Std. 603 ITAAC.

The following paragraphs provide references to the tables associated with the software projects and their associated functional systems. For example, RPS refers to Subsection 2.2.7, which associates Tables 2.2.7-1, 2.2.7-2, and 2.2.7-3 with RPS.

Process sensors and actuators that provide sense and execute functions associated with the software projects in Table 2.2.15-1 are found in Tables 2.1.2-2, 2.2.2-6, 2.2.4-5, 2.4.1-2, 2.4.2-2, 2.15.1-1c, and 2.15.7-1, marked Yes in the Control Q-DCIS column.

Functional arrangement of the software projects platforms (except VBIF) are found in Tables 2.2.5-1, 2.2.7-1, 2.2.12-1, 2.2.13-1, and 2.2.14-1.

The independent control platform associated with the VBIF software projects are found in Table 2.15.1-1c.

Functions, initiators, and interfacing systems associated with the software projects (except for the functional system LD&IS) are found in Tables 2.2.5-2, 2.2.7-2, 2.2.13-2, and 2.2.14-2.

The isolation functions and monitored variables associated with the functional system LD&IS are found in Table 2.2.12-2.

Isolation valves associated with the functional system LD&IS are found in Table 2.15.1-1a, marked Yes in the Safety-Related column.

Isolation dampers associated with the functional system LD&IS are found in Tables 2.16.2-1, 2.16.2-3, 2.16.2-5, and 2.16.2-8.

Controls, interlocks, and bypasses associated with the software projects are found in Tables 2.2.5-3, 2.2.7-3, 2.2.12-4, 2.2.13-3, and 2.2.14-3.

The process radiation monitors associated with the functional system PRMS are found in Table 2.3.1-1, marked Yes in the Safety-Related column.

Refer to Sections 3.2, 3.3, 3.6, 3.7, and 3.8, as described, for ITAAC associated with the IEEE Std. 603 criteria that do not appear in Tables 2.2.15-1.

The design descriptions that demonstrate compliance with the IEEE Std. 603 standard are shown below:

- 1a. Criterion 4.1, Identification of design basis events: The software projects design bases list the applicable 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.

- 1b. Criterion 4.1, Identification of design basis events: The as-built software projects design bases reconcile any changes to the design bases events, applicable reactor modes of operation, initial conditions requiring protective action, and allowable limits of plant conditions for each such event.
- 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.
- 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.
- 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.
- 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.
- 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).
- 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).
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 8a. Criterion 5.1, Single-failure criterion: The software projects design bases show compliance with the single-failure criterion.
- 8b. Criterion 5.1, Single-failure criterion: The as-built software projects comply with the results of the FMEA.

- 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.
- 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.
- 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.
- 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.
- 10a1. Criteria 5.6 and 6.3, Independence: The software projects have four independent, redundant divisions.
- 10a2. Criteria 5.6 and 6.3, Independence: The software projects' interdivisional communication systems have optically isolated fiber optic communication pathways.
- 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.
- 10b1. Criteria 5.6 and 6.3, Independence: 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.
- 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.
- 11a. Criteria 5.7 and 6.5, Capability for Test & Calibration: The software projects have maintenance bypasses that allow test and their calibration of one out of four divisions while retaining capability to accomplish their safety-related functions.
- 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.
- 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.
- 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.

- 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.
- 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.
- 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.
- 14a. Criterion 5.11, Identification: The redundant portions of the software projects are distinctly identified.
- 14b. Criterion 5.11, Identification: The redundant portions of the as-built software projects are distinctly identified.
- 15a. Criterion 5.12, Auxiliary Features: Other auxiliary features cannot degrade the software projects' performance below an acceptable level.
- 15b. Criterion 5.12, Auxiliary Features: Other auxiliary features cannot degrade the as-built software projects' performance below an acceptable level.
- 16a. Criteria 6.1 and 7.1, Automatic Control: The software projects provide the means to automatically initiate and control the required safety-related functions.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 19a2. Criteria 6.6 and 7.4, Operating Bypasses: The software projects automatically remove activated operating bypass(es), if the plant conditions change so that an activated operating bypass is no longer permissible.

- 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.
- 19b2. Criteria 6.6 and 7.4, Operating Bypasses: The as-built software projects show that they automatically removes activated operating bypass(es), if the plant conditions change so that an activated operating bypass is no longer permissible.
- 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.
- 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.
- 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.
- 21a. Criterion 6.8, Setpoint: The software projects' setpoints for safety-related functions are determined by a defined setpoint methodology.
- 21b. Criterion 6.8, Setpoint: Any changes to the setpoints have been reconciled for as-built software projects.
- 22a. Criterion 8.1, Power source requirements: The software projects' electrical components receive power from their respective, divisional, safety-related power supplies.
- 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.
- 23a. Criterion 8.2, Non-electrical Power Sources: The software projects' actuators receive non-electric power from safety-related sources.
- 23b. Criterion 8.2, Non-electrical Power Sources: The as-built software projects' actuators receive non-electric power from safety-related sources.

### Inspections, Tests, Analyses and Acceptance Criteria

Table 2.2.15-2 defines the inspections, tests, and/or analyses, together with acceptance criteria for the software projects.

Subsections 2.1.2, 2.2.2, 2.2.4, 2.2.5, 2.2.7, 2.2.12, 2.2.13, 2.2.14, 2.3.1, 2.4.1, 2.4.2, 2.15.1, and 2.15.7, defines the inspections, tests, and/or analyses, together with associated acceptance criteria for the sensors, actuators, functional arrangement, functional performance, controls, interlocks, and bypasses associated with the software projects.

~~The design descriptions related to IEEE Std. 603 criteria are provided below. Safety-related Instrumentation and Control systems are designed to the following criteria from IEEE Std. 603 as listed in Table 2.2.15-1. An X in the table identifies the system for which an ITAAC applies. Refer to the Tier 1 Subsections cited in the table for additional design descriptions applicable to the listed systems. Note that only the safety-related portions of the listed systems are addressed.~~

- ~~(1) Criterion 5.1, Single Failure: The listed systems 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 design basis event requiring the safety-related functions, as identified in the applicable failure modes and effects analysis (FMEA).~~
- ~~(2) Criteria 5.2 and 7.3, Completion of Protective Actions: The listed systems 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.~~
- ~~(3) Criterion 5.4, Equipment Qualification: The listed systems 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.~~
- ~~(4) Criterion 5.5, System Integrity: The listed system's performance 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.~~
- ~~(5) Criteria 5.6 and 6.3, Independence: For the listed systems, physical, electrical, and communications independence between redundant portions of safety-related systems, between safety-related systems and the effects of a DBE, and between safety-related systems and nonsafety-related systems exist, as identified in the applicable FMEA.~~
- ~~(6) Criteria 5.7 and 6.5, Capability for Test & Calibration: The listed systems have the capability to have their equipment tested and calibrated while retaining their capability to accomplish their safety-related functions.~~
- ~~(7) Criterion 5.8, Information Displays: Information display systems 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.~~
- ~~(8) Criterion 5.9, Control of Access: The listed systems have features that permit administrative control of access to safety-related system equipment.~~
- ~~(9) Criterion 5.10, Repair: Safety-related systems 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 are distinctly identified for each redundant portion.~~
- ~~(11) Criterion 5.12, Auxiliary Features: Other auxiliary features cannot degrade the safety-related systems below an acceptable level.~~

- ~~(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.~~
- ~~(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.~~
- ~~(14) Criterion 5.15, Reliability: Analysis of the adequacy of the reliability of the safety-related system design is performed as part of the design reliability assurance program described in Section 3.6.~~
- ~~(15) Criteria 6.1 and 7.1, Automatic Control: The listed systems provide the means to automatically initiate and control the required safety-related functions.~~
- ~~(16) Criteria 6.2 and 7.2, Manual Control: The listed systems have features in the main control room to manually initiate and control the automatically initiated safety-related functions at the division level.~~
- ~~(17) Criterion 6.4, Derivation of System Inputs: 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.~~
- ~~(18) Criteria 6.6 and 7.4, Operating Bypasses: The listed systems 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.~~
- ~~(19) Criteria 6.7, 7.5, and 8.3, Maintenance Bypasses: The listed systems are capable of performing their safety-related functions, when one division is in maintenance bypass.~~
- ~~(20) Criterion 6.8, Setpoint: The listed system setpoints for safety-related functions are determined by a defined setpoint methodology.~~
- ~~(21) Criterion 8.1, Electrical Power Sources: The listed systems receive power from safety-related power supplies in the same division.~~
- ~~(22) Criterion 8.2, Non-electrical Power Sources: The listed systems receive non-electric power from safety-related sources.~~

#### ~~Inspections, Tests, Analysis and Acceptance Criteria~~

~~Table 2.2.15-2 provides a definition of the inspections, tests, and/or analyses, together with and acceptance criteria for the systems listed in Table 2.2.15-1.~~

**Table 2.2-15-1**  
**IEEE Std. 603 Criterion System Applicability Matrix <sup>(1)(2)</sup>**

Software projects	Table 2.2-15-2, Item No.	RTIF-NMS Platform																ICP		
		RTIF								NMS								VBIF	ATWS/SLC	
	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)	SSL/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 <sup>(1)(2)</sup>**

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<sup>(2)</sup>**

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)	GDGS (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 2.2.15-2ITAAC For IEEE Std. 603 Compliance Confirmation

<u>Design Commitment</u>	<u>Inspections, Tests, Analyses</u>	<u>Acceptance Criteria</u>
<p>1a. <u>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.</u></p>	<p><u>Inspection of the software projects design phase summary BRR will be performed for the identification of the design basis events.</u>            {{Design Acceptance Criteria}}</p>	<p><u>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}}</u></p>
<p>1b. <u>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.</u></p>	<p><u>Inspection of the as-built software projects of the installation phase summary BRR will be performed for the identification of the design basis events.</u></p>	<p><u>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.</u></p>

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

<u>Design Commitment</u>	<u>Inspections, Tests, Analyses</u>	<u>Acceptance Criteria</u>
<p>2a. <u>Criterion 4.4, Identification of variables monitored: The software projects design bases list:</u></p> <ul style="list-style-type: none"> <li>• <u>The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action</u></li> <li>• <u>The analytical limit associated with each variable</u></li> <li>• <u>The ranges (normal, abnormal, and accident conditions) associated with each variable</u></li> <li>• <u>The rates of change of these variables to be accommodated until proper completion of the protective action is ensured</u></li> </ul>	<p><u>Inspection of the software projects design phase summary BRR will be performed for identification of variables.</u></p> <p><u>}}Design Acceptance Criteria}}</u></p>	<p><u>Report(s) exist and conclude that the software projects design phase summary BRR identify:</u></p> <ul style="list-style-type: none"> <li>• <u>The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action</u></li> <li>• <u>The analytical limit associated with each variable</u></li> <li>• <u>The ranges (normal, abnormal, and accident conditions) associated with each variable</u></li> <li>• <u>The rates of change of these variables to be accommodated until proper completion of the protective action is ensured</u></li> </ul> <p><u>}}Design Acceptance Criteria}}</u></p>

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

<u>Design Commitment</u>	<u>Inspections, Tests, Analyses</u>	<u>Acceptance Criteria</u>
<p>2b. <u>Criterion 4.4, Identification of variables monitored: The as-built software projects design bases reconcile any changes to the list of:</u></p> <ul style="list-style-type: none"> <li>• <u>The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action</u></li> <li>• <u>The analytical limit associated with each variable</u></li> <li>• <u>The ranges (normal, abnormal, and accident conditions) associated with each variable</u></li> <li>• <u>The rates of change of these variables to be accommodated until proper completion of the protective action is ensured</u></li> </ul>	<p><u>Inspection of the software projects installation phase summary BRR will be performed for identification of variables.</u></p>	<p><u>Report(s) exist and conclude that the software projects installation phase summary BRR identify and comply with changes, deletions, and additions to:</u></p> <ul style="list-style-type: none"> <li>• <u>The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action</u></li> <li>• <u>The analytical limit associated with each variable</u></li> <li>• <u>The ranges (normal, abnormal, and accident conditions) associated with each variable</u></li> <li>• <u>The rates of change of these variables to be accommodated until proper completion of the protective action is ensured</u></li> </ul>

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

<u>Design Commitment</u>	<u>Inspections, Tests, Analyses</u>	<u>Acceptance Criteria</u>
<p>3a. <u>Criterion 4.5, Minimum criteria for manual initiation and control of protective actions subsequent to initiation: The software projects design bases list:</u></p> <ul style="list-style-type: none"> <li>• <u>The points in time and the plant conditions during which manual control is allowed.</u></li> <li>• <u>The justification for permitting initiation or control subsequent to initiation solely by manual means.</u></li> <li>• <u>The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations will be performed.</u></li> <li>• <u>The variables that will be displayed for the operator to use in taking manual action.</u></li> </ul>	<p><u>Inspection of the software projects design phase summary BRR will be performed for identification of the minimum criteria for manual initiation and control.</u>  <u>{{Design Acceptance Criteria}}</u></p>	<p><u>Report(s) exist and conclude that the software projects design phase summary BRR identify:</u></p> <ul style="list-style-type: none"> <li>• <u>The points in time and the plant conditions during which manual control is allowed.</u></li> <li>• <u>The justification for permitting initiation or control subsequent to initiation solely by manual means.</u></li> <li>• <u>The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations will be performed.</u></li> <li>• <u>The variables that will be displayed for the operator to use in taking manual action.</u></li> </ul> <p><u>{{Design Acceptance Criteria}}</u></p>

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

<u>Design Commitment</u>	<u>Inspections, Tests, Analyses</u>	<u>Acceptance Criteria</u>
<p>3b. <u>Criterion 4.5, Minimum criteria for manual initiation and control of protective actions subsequent to initiation: The as-built software projects design bases list:</u></p> <ul style="list-style-type: none"> <li>• <u>The points in time and the plant conditions during which manual control is allowed.</u></li> <li>• <u>The justification for permitting initiation or control subsequent to initiation solely by manual means.</u></li> <li>• <u>The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations will be performed.</u></li> <li>• <u>The variables that will be displayed for the operator to use in taking manual action.</u></li> </ul>	<p><u>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.</u></p>	<p><u>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:</u></p> <ul style="list-style-type: none"> <li>• <u>The points in time and the plant conditions during which manual control is allowed.</u></li> <li>• <u>The justification for permitting initiation or control subsequent to initiation solely by manual means.</u></li> <li>• <u>The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations will be performed.</u></li> <li>• <u>The variables that will be displayed for the operator to use in taking manual action.</u></li> </ul>

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

<u>Design Commitment</u>	<u>Inspections, Tests, Analyses</u>	<u>Acceptance Criteria</u>
<p>4a. <u>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).</u></p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>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).</u>                      {{Design Acceptance Criteria}}</p>
<p>4b. <u>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).</u></p>	<p><u>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.</u></p>	<p><u>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).</u></p>

Table 2.2.15-2  
ITAAC For IEEE Std. 603 Compliance Confirmation

<u>Design Commitment</u>	<u>Inspections, Tests, Analyses</u>	<u>Acceptance Criteria</u>
<p>5a. <u>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.</u></p>	<p><u>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.</u> <u>{{Design Acceptance Criteria}}</u></p>	<p><u>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.</u> <u>{{Design Acceptance Criteria}}</u></p>
<p>5b. <u>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.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

<u>Design Commitment</u>	<u>Inspections, Tests, Analyses</u>	<u>Acceptance Criteria</u>
<p>6a. <u>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.</u></p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>
<p>6b. <u>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.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

<u>Design Commitment</u>	<u>Inspections, Tests, Analyses</u>	<u>Acceptance Criteria</u>
<p>7a. <u>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.</u></p>	<p><u>Inspection of the software projects design phase summary BRR will be performed of the applicable qualitative and quantitative reliability goals.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>
<p>7b. <u>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.</u></p>	<p><u>Inspection of the as-built software projects installation phase summary BRR will be performed of the applicable qualitative and quantitative reliability goals.</u></p>	<p><u>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.</u></p>

Table 2.2.15-2  
ITAAC For IEEE Std. 603 Compliance Confirmation

<u>Design Commitment</u>	<u>Inspections, Tests, Analyses</u>	<u>Acceptance Criteria</u>
<p>8a. <u>Criterion 5.1, Single-failure criterion: The software projects design bases show compliance with the single-failure criterion.</u></p>	<p><u>Inspection of the software projects' design phase summary BRR show that a Failures Mode and Effects Analysis (FMEA) have been completed.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>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:</u></p> <ul style="list-style-type: none"> <li><u>• Single detectable failures within safety-related systems concurrent with identifiable but non-detectable failures;</u></li> <li><u>• Failures caused by the single failure; and</u></li> <li><u>• Failures and spurious system actions that cause or are caused by the DBE requiring the safety-related functions.</u></li> </ul> <p>{{Design Acceptance Criteria}}</p>
<p>8b. <u>Criterion 5.1, Single-failure criterion: The as-built software projects comply with the results of the FMEA.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

<u>Design Commitment</u>	<u>Inspections, Tests, Analyses</u>	<u>Acceptance Criteria</u>
<p>9a1. <u>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.</u></p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>Report(s) exist and conclude that the software projects design phase summary BRR show “seal-in” features.</u>                      {{Design Acceptance Criteria}}</p>
<p>9a2. <u>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.</u></p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>Report(s) exist and conclude that the software projects design phase summary BRR show “manual reset” features.</u>                      {{Design Acceptance Criteria}}</p>
<p>9b1. <u>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.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>

**Table 2.2.15-2**  
**ITAAC For IEEE Std. 603 Compliance Confirmation**

<b><u>Design Commitment</u></b>	<b><u>Inspections, Tests, Analyses</u></b>	<b><u>Acceptance Criteria</u></b>
<p><u>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.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>
<p><u>10a1. Criteria 5.6 and 6.3, Independence: The software projects have four independent, redundant divisions.</u></p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>Report(s) exist and conclude that the software projects design phase summary BRR show that the software projects have four independent, redundant divisions.</u>                      {{Design Acceptance Criteria}}</p>
<p><u>10a2. Criteria 5.6 and 6.3, Independence: The software projects’ interdivisional communication systems have optically isolated fiber optic communication pathways.</u></p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

<u>Design Commitment</u>	<u>Inspections, Tests, Analyses</u>	<u>Acceptance Criteria</u>
<p><u>10a3. Criteria 5.6 and 6.3, Independence:</u>  <u>The software projects’ safety-related functions are performed independently of the existence and function of any nonsafety-related component, data, and communication channel.</u></p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>
<p><u>10b1. Criteria 5.6 and 6.3, Independence:</u>  <u>The as-built software projects have four independent, redundant divisions.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>
<p><u>10b2. Criteria 5.6 and 6.3, Independence:</u>  <u>The as-built software projects’ interdivisional communication systems have optically isolated fiber optic communication pathways.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>

**Table 2.2.15-2**  
**ITAAC For IEEE Std. 603 Compliance Confirmation**

<b><u>Design Commitment</u></b>	<b><u>Inspections, Tests, Analyses</u></b>	<b><u>Acceptance Criteria</u></b>
<p><u>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.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>
<p><u>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.</u></p>	<p><u>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.</u></p> <p align="center"><u>}}Design Acceptance Criteria}}</u></p>	<p><u>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.</u></p> <p align="center"><u>}}Design Acceptance Criteria}}</u></p>
<p><u>11b1. Criteria 5.7 and 6.5, Capability for Test &amp; Calibration: The as-built software projects' maintenance bypasses show that the divisions not in bypass status will accomplish their safety-related functions.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>

**Table 2.2.15-2**  
**ITAAC For IEEE Std. 603 Compliance Confirmation**

<b><u>Design Commitment</u></b>	<b><u>Inspections, Tests, Analyses</u></b>	<b><u>Acceptance Criteria</u></b>
<p><u>11b2. Criteria 5.7 and 6.5, Capability for Test &amp; 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.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>
<p><u>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.</u></p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>

Table 2.2.15-2ITAAC For IEEE Std. 603 Compliance Confirmation

<u>Design Commitment</u>	<u>Inspections, Tests, Analyses</u>	<u>Acceptance Criteria</u>
<u>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.</u>	<u>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.</u>	<u>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.</u>
<u>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.</u>	<u>Inspection of the software projects design phase summary BRR will be performed of the self-diagnostic features. {{Design Acceptance Criteria}}.</u>	<u>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}}.</u>
<u>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.</u>	<u>Inspection of the as-built software projects installation phase summary BRR will be performed of the self-diagnostic features.</u>	<u>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.</u>
<u>14a. Criterion 5.11, Identification: The redundant portions of the software projects are distinctly identified.</u>	<u>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}}.</u>	<u>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}}.</u>

**Table 2.2.15-2**  
**ITAAC For IEEE Std. 603 Compliance Confirmation**

<b><u>Design Commitment</u></b>	<b><u>Inspections, Tests, Analyses</u></b>	<b><u>Acceptance Criteria</u></b>
14b. <u>Criterion 5.11, Identification: The redundant portions of the as-built software projects are distinctly identified.</u>	<u>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.</u>	<u>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.</u>
15a. <u>Criterion 5.12, Auxiliary Features: Other auxiliary features cannot degrade the software projects' performance below an acceptable level.</u>	<u>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.</u> <u>{{Design Acceptance Criteria}}</u>	<u>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.</u> <u>{{Design Acceptance Criteria}}</u>
15b. <u>Criterion 5.12, Auxiliary Features: Other auxiliary features cannot degrade the as-built software projects' performance below an acceptable level.</u>	<u>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.</u>	<u>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.</u>
16a. <u>Criteria 6.1 and 7.1, Automatic Control: The software projects provides the means to automatically initiate and control the required safety-related functions.</u>	<u>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.</u> <u>{{Design Acceptance Criteria}}</u>	<u>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.</u> <u>{{Design Acceptance Criteria}}</u>

**Table 2.2.15-2**  
**ITAAC For IEEE Std. 603 Compliance Confirmation**

<b><u>Design Commitment</u></b>	<b><u>Inspections, Tests, Analyses</u></b>	<b><u>Acceptance Criteria</u></b>
<p><u>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.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>
<p><u>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.</u></p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>
<p><u>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.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>

Table 2.2.15-2ITAAC For IEEE Std. 603 Compliance Confirmation

<u>Design Commitment</u>	<u>Inspections, Tests, Analyses</u>	<u>Acceptance Criteria</u>
<u>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.</u>	<u>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.</u> <u>{{Design Acceptance Criteria}}</u>	<u>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.</u> <u>{{Design Acceptance Criteria}}</u>
<u>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.</u>	<u>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.</u>	<u>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.</u>
<u>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.</u>	<u>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.</u> <u>{{Design Acceptance Criteria}}</u>	<u>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.</u> <u>{{Design Acceptance Criteria}}</u>

**Table 2.2.15-2**  
**ITAAC For IEEE Std. 603 Compliance Confirmation**

<b><u>Design Commitment</u></b>	<b><u>Inspections, Tests, Analyses</u></b>	<b><u>Acceptance Criteria</u></b>
<p><u>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.</u></p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>
<p><u>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.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>
<p><u>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.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>

**Table 2.2.15-2**  
**ITAAC For IEEE Std. 603 Compliance Confirmation**

<b><u>Design Commitment</u></b>	<b><u>Inspections, Tests, Analyses</u></b>	<b><u>Acceptance Criteria</u></b>
<p>20a. <u>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.</u></p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>
<p>20b1. <u>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.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>
<p>20b2. <u>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.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>
<p>21a. <u>Criterion 6.8, Setpoint: The software projects', setpoints for safety-related functions are defined, determined and implemented based on a defined setpoint methodology.</u></p>	<p><u>Inspection of the software projects design phase summary BRR will be performed to verify that a defined setpoint methodology exists.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>Report(s) exist and conclude that the software projects design phase summary BRR show that a defined setpoint methodology exists.</u>                      {{Design Acceptance Criteria}}</p>

**Table 2.2.15-2**  
**ITAAC For IEEE Std. 603 Compliance Confirmation**

<b><u>Design Commitment</u></b>	<b><u>Inspections, Tests, Analyses</u></b>	<b><u>Acceptance Criteria</u></b>
<p><u>21b. Criterion 6.8, Setpoint: Any changes to the setpoints have been reconciled for the as-built software projects.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>
<p><u>22a. Criterion 8.1, Power source requirements: The software projects' electrical components receive power from their respective, divisional, safety-related power supplies.</u></p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>	<p><u>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.</u>                      {{Design Acceptance Criteria}}</p>
<p><u>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.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>

**Table 2.2.15-2**  
**ITAAC For IEEE Std. 603 Compliance Confirmation**

<u><b>Design Commitment</b></u>	<u><b>Inspections, Tests, Analyses</b></u>	<u><b>Acceptance Criteria</b></u>
<p><u>23a. Criterion 8.2, Non-electrical Power Sources: The software projects' actuators receive non-electric power from safety-related sources.</u></p>	<p><u>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.</u></p> <p><u>{{Design Acceptance Criteria}}</u></p>	<p><u>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.</u></p> <p><u>{{Design Acceptance Criteria}}</u></p>
<p><u>23b. Criterion 8.2, Non-electrical Power Sources: The as-built software projects' actuators receive non-electric power from safety-related sources.</u></p>	<p><u>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.</u></p>	<p><u>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.</u></p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
<p><del>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.</del></p>	<p><del>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}}</del></p>	<p><del>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}}</del></p>
<p><del>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.</del></p>	<p><del>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}}</del></p>	<p><del>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}}</del></p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
	<del>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.</del>	<del>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.</del>
<del>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.</del>	<del>See Section 3.8</del>	<del>See Section 3.8</del>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
<p><del>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.</del></p>	<p><del>See Section 3.8</del></p>	<p><del>See Section 3.8</del></p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
<p><del>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.</del></p>	<p><del>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}}</del></p> <p><del>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.</del></p>	<p><del>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}}</del></p> <p><del>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.</del></p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
	<p><del>e. 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.</del></p>	<p><del>e. 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.</del></p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
<p><del>6. Criteria 5.7 and 6.5, Capability for Test and Calibration:</del></p> <p><del>—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.</del></p>	<p><del>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}}</del></p> <p><del>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.</del></p> <p><del>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&amp;C systems' self-test features confirm computer system operation on system initiation.</del></p>	<p><del>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}}</del></p> <p><del>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.</del></p> <p><del>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&amp;C systems' self-test features confirm computer system operation on system initiation.</del></p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
<p><del>7. Criterion 5.8, Information Displays:</del>  <del>—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.</del></p>	<p><del>See Sections 3.3 and 3.7</del></p>	<p><del>See Section 3.3 and 3.7</del></p>
<p><del>8. Criterion 5.9, Control of Access:—</del>  <del>—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.</del></p>	<p><del>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}}</del></p>	<p><del>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}}</del></p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
<p><b>9. Criterion 5.10, Repair:</b></p> <p>— 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.</p>	<p>— 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.</p>	<p>— 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.</p>
<p><b>10. Criterion 5.11, Identification:</b></p> <p>— The listed safety related systems in Table 2.2.15-1 are distinctly identified for each redundant portion.</p>	<p>a. Inspection(s) will be performed of the “current revision” of the project design manual. {{Design Acceptance Criteria}}</p> <p>b. Inspection(s) will be performed of the as-installed safety related systems identification system.</p>	<p>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}}</p> <p>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.</p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
<p>11. Criterion 5.12, Auxiliary Features:  <del>—Other auxiliary features cannot degrade the safety-related systems listed in Table 2.2.15-1, below an acceptable level.</del></p>	<p><del>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.</del>  <del>{{Design Acceptance Criteria}}</del></p>	<p><del>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.</del> <del>{{Design Acceptance Criteria}}</del></p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
<p>12. Criterion 5.13, Multi-Unit Stations:</p> <p>— 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.</p>	<p>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:</p> <p>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.</p> <p>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.</p>	<p>— 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.</p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
<p><del>13. Criterion 5.14, Human Factors Considerations:</del></p> <p><del>—Human factors are incorporated in the design in accordance with the HFE design process described in Section 3.3.</del></p>	<p><del>See Section 3.3.</del></p>	<p><del>See Section 3.3.</del></p>
<p><del>14. Criterion 5.15, Reliability:</del></p> <p><del>—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.</del></p>	<p><del>See Section 3.6.</del></p>	<p><del>See Section 3.6.</del></p>
<p>15. Criteria 6.1 and 7.1, Automatic Control:</p> <p>—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.</p>	<p>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. <del>{{Design Acceptance Criteria}}</del></p> <p>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.</p>	<p>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. <del>{{Design Acceptance Criteria}}</del></p> <p>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.</p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
<p><del>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.</del></p>	<p><del>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}}</del></p> <p><del>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.</del></p>	<p><del>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}}</del></p> <p><del>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).</del></p>
<p><del>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.</del></p>	<p><del>Inspection(s) will be performed of the safety analyses and SLDs. {{Design Acceptance Criteria}}</del></p>	<p><del>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}}</del></p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
<p><del>18. Criteria 6.6 and 7.4, Operating Bypasses:</del></p> <p><del>—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.</del></p>	<p><del>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}}</del></p> <p><del>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.</del></p>	<p><del>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}}</del></p> <p><del>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.</del></p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
<p><del>19. Criteria 6.7, 7.5, and 8.3 Maintenance Bypasses:</del></p> <p><del>—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.</del></p>	<p><del>Inspection(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}}</del></p> <p><del>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.</del></p> <p><del>e. 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:</del></p>	<p><del>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}}</del></p> <p><del>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.</del></p> <p><del>e. 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.</del></p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
<p>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.</p>	<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>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}}</p> <p>b. Inspection(s) will be performed on the listed systems in table 2.2.15-1</p>	<p>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}}</p> <p>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.</p>

**Table 2.2.15-2**

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

<b>Design Commitment</b>	<b>Inspections, Tests, Analyses</b>	<b>Acceptance Criteria</b>
<p><del>2.2. Criterion 8.2, Non-electrical Power Sources:</del>  <del>—The listed systems in Table 2.2.15-1 receive non-electric power from safety-related sources.</del></p>	<p><del>a. Inspection(s) will be performed on the “current revision” of the P&amp;ID of the listed systems in Table 2.2.15-1. {{Design Acceptance Criteria}}</del></p> <p><del>b. Inspection(s) will be performed on the as-built mechanical installation of the listed systems in Table 2.2.15-1.</del></p>	<p><del>a. Inspection report(s) conclude(s) that the “current revision” of the P&amp;ID of the listed systems in Table 2.2.15-1 show non-electric power from safety-related sources. {{Design Acceptance Criteria}}</del></p> <p><del>b. Inspection report(s) conclude(s) that the listed systems in Table 2.2.15-1 receive non-electric power from safety-related sources.</del></p>

**Table 7.1-2**  
**I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference**

**Q-DCIS**

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

**Table 7.1-2**  
**I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference**

**Q-DCIS**

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

**Table 7.1-2**  
**I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference**

**Q-DCIS**

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

**Table 7.1-2**  
**I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference**

**Q-DCIS**

		<b>RTIF - NMS PLATFORM</b>							<b>SSLC/ESF PLATFORM</b>										<b>INDEPENDENT CONTROL PLATFORM</b>	
		<b>RTIF</b>					<b>NMS</b>													
<b>IEEE Std. 603 Section</b>	<b>Functions <sup>(1)</sup></b>	<b>RTIF</b>	<b>RPS</b>	<b>LD&amp;IS (MSIV Only) <sup>(6)</sup></b>	<b>CMS (includes SPTM) <sup>(6)</sup></b>	<b>NBS <sup>(6)</sup></b>	<b>CRD <sup>(6)</sup></b>	<b>NMS <sup>(3)</sup></b>	<b>SSLC/ESF <sup>(4)</sup></b>	<b>LD&amp;IS (Non-MSIV) <sup>(2)&amp;(6)</sup></b>	<b>PRMS</b>	<b>CMS <sup>(6)</sup></b>	<b>NBS (includes ADS) <sup>(6)</sup></b>	<b>GDCS</b>	<b>ICS</b>	<b>SLC <sup>(6)</sup></b>	<b>CBVS <sup>(7)</sup></b>	<b>CRD <sup>(6)</sup></b>	<b>VBIF</b>	<b>ATWS / SLC <sup>(5),(6)&amp;(7)</sup></b>
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 7.4.2.3.1	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:**

- <sup>(1)</sup> The IEEE Std. 603 criteria apply to the safety-related portions of the systems identified in this table.
- <sup>(2)</sup> 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.
- <sup>(3)</sup> NMS has Q and N parts. The Q parts are SRNM, LPRM, APRM, and OPRM. The N parts are AFIP and MRBM.
- <sup>(4)</sup> SSLC/ESF includes the RSS, MCRP, and safety-related VDUs.
- <sup>(5)</sup> Includes the NBS sensors associate with ATWS/SLC.
- <sup>(6)</sup> 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.
- <sup>(7)</sup> 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
<b>IEEE Std. 603 Section</b>	<b>Functions<sup>1</sup></b>	<b>Q-DCIS, N-DCIS</b>	<b>RPS, NMS<sup>2</sup>, SPTM<sup>3</sup>, MSIV (for LD&amp;IS)</b>	<b>SSLC/ESF ECCS<sup>4</sup> ,PCCS<sup>5</sup>, LD&amp;IS (except MSIV) CRHS, VBIF</b>	<b>Q and N-SS (that is, SLC, RSS, RWCU /SDC (N), ICS)</b>	<b>Q and N-IS (that is, Q IC-Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)</b>	<b>HP/LP-SI (N)</b>	<b>NBS (QN), RC&amp;IS (QN), FWCS (N), PAS (N), SB&amp;PC (N), NMS<sup>(2)</sup> (N) CIS (N)</b>	<b>ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)</b>
4	Safety System Designation	7.1.2.1 7.1.3.1.4 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		Instrumentation & Control Systems	Reactor Trip Systems	Engineered Safety Features	Safe Shutdown Systems	Information Systems	Interlock Systems	Control Systems	Diverse Instrumentation and Control Systems
<b>IEEE Std. 603 Section</b>	<b>Functions<sup>1</sup></b>	<b>Q-DCIS, N-DCIS</b>	<b>RPS, NMS<sup>2</sup>, SPTM<sup>3</sup>, MSIV (for LD&amp;IS)</b>	<b>SSLC/ESF ECCS<sup>4</sup>, PCCS<sup>5</sup>, LD&amp;IS (except MSIV) CRHS, VBIF</b>	<b>Q and N-SS (that is, SLC, RSS, RWCU /SDC (N), ICS)</b>	<b>Q and N-IS (that is, Q IC-Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)</b>	<b>HP/LP SI (N)</b>	<b>NBS (QN), RC&amp;IS (QN), FWCS (N), PAS (N), SB&amp;PC (N), NMS<sup>(2)</sup> (N) CIS (N)</b>	<b>ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)</b>
4.8	Adverse environmental conditions	7.1.2.1 7.1.3.1.4	-	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 7.1.3.1.4	-	-	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 <sup>1</sup>	Q-DCIS, N-DCIS	RPS, NMS <sup>2</sup> , SPTM <sup>3</sup> , MSIV (for LD&IS)	SSLC/ESF ECCS <sup>4</sup> PCCS <sup>5</sup> , 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 <sup>(2)</sup> (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 (GDOS) 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
<b>IEEE Std. 603 Section</b>	<b>Functions<sup>1</sup></b>	<b>Q-DCIS, N-DCIS</b>	<b>RPS, NMS<sup>2</sup>, SPTM<sup>3</sup>, MSIV (for LD&amp;IS)</b>	<b>SSLC/ESF ECCS<sup>4</sup> PCCS<sup>5</sup>, LD&amp;IS (except MSIV) CRHS, VBIF</b>	<b>Q and N-SS (that is, SLC, RSS, RWCU /SDC (N), ICS)</b>	<b>Q and N-IS (that is, Q IC-Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)</b>	<b>HP/LP SI (N)</b>	<b>NBS (QN), RC&amp;IS (QN), FWCS (N), PAS (N), SB&amp;PC (N), NMS<sup>(2)</sup> (N) CIS (N)</b>	<b>ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)</b>
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 <sup>1</sup>	Q-DCIS, N-DCIS	RPS, NMS <sup>2</sup> , SPTM <sup>3</sup> , MSIV (for LD&IS)	SSLC/ESF ECCS <sup>4</sup> PCCS <sup>5</sup> , 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 <sup>(2)</sup> (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 (GDGS) 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
<b>IEEE Std. 603 Section</b>	<b>Functions<sup>1</sup></b>	<b>Q-DCIS, N-DCIS</b>	<b>RPS, NMS<sup>2</sup>, SPTM<sup>3</sup>, MSIV (for LD&amp;IS)</b>	<b>SSLC/ESF ECCS<sup>4</sup> , PCCS<sup>5</sup>, LD&amp;IS (except MSIV) CRHS, VBIF</b>	<b>Q and N-SS (that is, SLC, RSS, RWCU /SDC (N), ICS)</b>	<b>Q and N-IS (that is, Q IC-Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)</b>	<b>HP/LP-SI (N)</b>	<b>NBS (QN), RC&amp;IS (QN), FWCS (N), PAS (N), SB&amp;PC (N), NMS<sup>(2)</sup> (N) CIS (N)</b>	<b>ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)</b>
6-7	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 <sup>1</sup>	Q-DCIS, N-DCIS	RPS, NMS <sup>2</sup> , SPTM <sup>3</sup> , MSIV (for LD&IS)	SSLC/ESF ECCS <sup>4</sup> PCCS <sup>5</sup> , 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 <sup>(2)</sup> (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 (GDGS) 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
<b>IEEE Std. 603 Section</b>	<b>Functions<sup>1</sup></b>	<b>Q-DCIS, N-DCIS</b>	<b>RPS, NMS<sup>2</sup>, SPTM<sup>3</sup>, MSIV (for LD&amp;IS)</b>	<b>SSLC/ESF ECCS<sup>4</sup> ,PCCS<sup>5</sup>, LD&amp;IS (except MSIV) CRHS, VBIF</b>	<b>Q and N-SS (that is, SLC, RSS, RWCU /SDC (N), ICS)</b>	<b>Q and N-IS (that is, Q IC-Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)</b>	<b>HP/LP-SI (N)</b>	<b>NBS (QN), RC&amp;IS (QN), FWCS (N), PAS (N), SB&amp;PC (N), NMS<sup>(2)</sup> (N) CIS (N)</b>	<b>ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)</b>
5-10-	Repair	7.1.6.6.1.11 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
<b>IEEE Std. 603 Section</b>	<b>Functions<sup>1</sup></b>	<b>Q-DCIS, N-DCIS</b>	<b>RPS, NMS<sup>2</sup>, SPTM<sup>3</sup>, MSIV (for LD&amp;IS)</b>	<b>SSLC/ESF ECCS<sup>4</sup> , PCCS<sup>5</sup>, LD&amp;IS (except MSIV) CRHS, VBIF</b>	<b>Q and N-SS (that is, SLC, RSS, RWCU /SDC (N), ICS)</b>	<b>Q and N-IS (that is, Q IC-Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)</b>	<b>HP/LP-SI (N)</b>	<b>NBS (QN), RC&amp;IS (QN), FWCS (N), PAS (N), SB&amp;PC (N), NMS<sup>(2)</sup> (N) CIS (N)</b>	<b>ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)</b>
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) 7.3.6.3.1 (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
<b>IEEE Std. 603 Section</b>	<b>Functions<sup>1</sup></b>	<b>Q-DCIS, N-DCIS</b>	<b>RPS, NMS<sup>2</sup>, SPTM<sup>3</sup>, MSIV (for LD&amp;IS)</b>	<b>SSLC/ESF ECCS<sup>4</sup> ,PCCS<sup>5</sup>, LD&amp;IS (except MSIV) CRHS, VBIF</b>	<b>Q and N-SS (that is, SLC, RSS, RWCU /SDC (N), ICS)</b>	<b>Q and N-IS (that is, Q IC-Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)</b>	<b>HP/LP SI (N)</b>	<b>NBS (QN), RC&amp;IS (QN), FWCS (N), PAS (N), SB&amp;PC (N), NMS<sup>(2)</sup> (N) CIS (N)</b>	<b>ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)</b>
6-5	Capability for testing and calibration	7.1.3.3 7.1.3.5 7.1.6.6.1.24	7.1.6.6.1.24 7.2.1.3.4 (RPS) 7.2.1.4.1	7.1.6.6.1.24 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)	7.1.6.6.1.24 7.4.1.3 (SLC) 7.4.3.4 (RWCU/SDC) 7.4.4.4 (ICS) 7.4.4.5	7.1.6.6.1.24 7.5.2.4 (CMS) 7.5.3.4 (PRMS)	-	7.1.6.6.1.24	-
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 <sup>1</sup>	Q-DCIS, N-DCIS	RPS, NMS <sup>2</sup> , SPTM <sup>3</sup> , MSIV (for LD&IS)	SSLC/ESF ECCS <sup>4</sup> PCCS <sup>5</sup> , 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 <sup>(2)</sup> (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
<b>IEEE Std. 603 Section</b>	<b>Functions<sup>1</sup></b>	<b>Q-DCIS, N-DCIS</b>	<b>RPS, NMS<sup>2</sup>, SPTM<sup>3</sup>, MSIV (for LD&amp;IS)</b>	<b>SSLC/ESF ECCS<sup>4</sup>, PCCS<sup>5</sup>, LD&amp;IS (except MSIV) CRHS, VBIF</b>	<b>Q and N-SS (that is, SLC, RSS, RWCU /SDC (N), ICS)</b>	<b>Q and N-IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)</b>	<b>HP/LP SI (N)</b>	<b>NBS (QN), RC&amp;IS (QN), FWCS (N), PAS (N), SB&amp;PC (N), NMS<sup>(2)</sup> (N) CIS (N)</b>	<b>ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), D* against CMF (N)</b>
7-3	Completion of protective action	- 7.1.6.6.1.3	-	7.3.1.2.1 (GDGS) 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 <sup>1</sup>	Q-DCIS, N-DCIS	RPS, NMS <sup>2</sup> , SPTM <sup>3</sup> , MSIV (for LD&IS)	SSLC/ESF ECCS <sup>4</sup> , PCCS <sup>5</sup> , 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 <sup>(2)</sup> (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, GDGS, 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

- Regulatory Guides (RGs) 1.22, 1.47, 1.53, 1.62, 1.75, 1.89, 1.97, 1.100, 1.105, 1.118, 1.151, 1.152, 1.153, 1.168, 1.169, 1.170, 1.171, 1.172, 1.173, 1.180, 1.204, and 1.209; and
- Branch Technical Positions (BTPs) HICB-1, 8, 9, 10, 11, 12, 14, 16, 17, 18, 19, and 21.

#### ***7.1.2.5 Q-DCIS Testing and Inspection Requirements Summary***

The Q-DCIS integrated hardware and software functions, including the network parameters and data status, are checked and tested together. The Analog-to-Digital (A/D) converters in the RMUs are the only components requiring periodic calibration checks. Some of the key diagnostics include:

- The central processing unit (CPU) status check,
- Parity checks, watchdog timer status,
- Voltage level in controllers,
- Data path integrity and data validation checks,
- Data cycling time, and
- Processor clock time.

#### ***7.1.2.6 Q-DCIS Operator Interface Requirements Summary***

The Q-DCIS VDUs support operator monitoring and manual control of the safety-related systems. The VDUs present process and diagnostic alarm information. When one of the two power supplies or communications paths within a division fails, the division and VDU operation continues automatically, without operator intervention. Failures in three divisions are required before there is a loss of a safety-related function.

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

- Q-DCIS MCR alarms for Division 1, 2, 3, and 4 trouble; and
- Q-DCIS MCR indications for Division 1, 2, 3, and 4 diagnostic displays.

#### ***7.1.2.7 Q-DCIS Boundary Summary***

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

#### ***7.1.2.8 Q-DCIS Major Systems Description Summary***

The Q-DCIS systems and components include equipment for the Reactor Trip System (RTS), and Engineered Safety Features Actuation System (ESFAS). The RTS includes the RPS function, the SRNM and PRNM functions of the NMS, and the SPTM function of the CMS. The

between the SSLC/ESF and N-DCIS is different from the gateway between the RTIF/NMS and the N-DCIS. The sending sources are different even though the receivers are the same.

Safety-related software is as simple as possible so that Q-DCIS components have neither interrupts from nonsafety-related devices nor do they respond to nonsafety-related component queries for information. The Q-DCIS components simply put information on the safety-related (Q-DCIS) networks in a known format so that other safety-related devices can retrieve what is needed for their function. Self-diagnostics information is also put on the DCIS networks. The safety-related fiber optic CIMs provide the safety-related isolation. The CIMs indiscriminately retrieve all of the divisional information from the safety-related (Q-DCIS) networks and send it one way to the N-DCIS (via fiber optic cable and a datalink or via a combination of fiber optic cable, datalinks and nonsafety-related gateways). Time tags are described below.

#### 7.1.3.3.3 Nonsafety-Related Gateways

The nonsafety-related gateways translate the information sent between the Q-DCIS (always through the required isolation, via datalinks and fiber optic cable) and the N-DCIS into a format that the other portion of the DCIS (either N-DCIS or Q-DCIS) can apply. The N-DCIS gateways package the safety-related information into the necessary message packets to support specific N-DCIS components for monitoring and alarm management purposes. The N-DCIS gateways also respond to interrupts and queries. Safety-related to nonsafety-related communication pathways that do not involve nonsafety-related gateways use safety-related fiber optic CIMs (which provide the safety-related isolation), datalinks, and fiber optic cable. Nonsafety-related gateways are not used when the N-DCIS (nonsafety-related receiver) is capable of receiving and extracting the data signal generated by the Q-DCIS (safety-related fiber optic CIM) without the need for data conversion. One example of datalink communication between the Q-DCIS and the N-DCIS without the use of a nonsafety-related gateway is the communication from the NMS to the MRBM and automated thermal limit monitor (ATLM). The nonsafety-related gateways, when necessary, handle the data translation/packaging interface, but do not serve to provide the required safety-related isolation for communications between the Q-DCIS and the N-DCIS. When nonsafety-related gateways are necessary they package the data for the various N-DCIS functions, respond to the N-DCIS requests for information and monitor communication link status. The safety-related isolation and separation (~~required by IEEE Std. 603, Sections 5.6 and 6.3~~) for communications between the Q-DCIS and the N-DCIS is always provided by the safety-related CIMs, as described above, regardless of whether a combination of datalinks and gateways is used or only a datalink is used.

#### 7.1.3.3.4 Communication from N-DCIS to Q-DCIS (DCIS Time tagging and NMS Calibration)

The safety-related systems are designed to not depend on nonsafety-related communication to function, therefore, loss of communication is never a safety issue. Specifically, no process feedback signals are sent from the N-DCIS to the Q-DCIS. The only signals sent from nonsafety-related components to safety-related components are those involved in time tagging and the transmission of data for calibration of the safety-related NMS, which is only possible under the specific circumstances described below.

cabinets. The RTIF, NMS, and SSLC/ESF cabinets are either centralized control processors or are various cabinets distributed throughout the division to perform the logic required by the safety-related systems.

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

There are at least two safety-related VDUs per division in the MCR. Divisions 1 and 2 have an additional VDU located on each RSS panel. The VDUs are used to monitor safety-related information from their connected division and are used to provide manual operator inputs to the safety-related (SSLC/ESF) logic. The VDUs provide access to a full range of plant parameters in accordance with the requirements of 10 CFR 50.34(f)(2)(iv), TMI Action Item I.D.2. The VDUs are also used for divisional self-diagnostics and divisional alarms.

The four VDU divisions allow checking of the operational availability of each sense and command feature input sensor for the RTIF, NMS, and SSLC/ESF systems. This is accomplished with a high degree of confidence by cross-checking between channels that bear a known relationship with each other ~~(IEEE Std. 603, Section 6.5.)~~.

#### 7.1.3.3.6 Two-out-of-four Voting Logic

The interconnections between Divisions 1, 2, 3, and 4 are used for two-out-of-four voting logic. The interconnections are provided between safety-related fiber optic CIMs through fiber optic cable; there are no electrical connections between divisions. Fail-safe systems like the RPS or the NMS interpret loss of interdivisional communication as a trip from that division. The trip counts toward the two-out-of-four voting logic initiations, unless the failed division is bypassed. Fail-as-is systems like the ECCS do not interpret loss of communications as a trip. The I&C design basis is N-2, therefore, safety-related systems are capable of performing all safety-related functions, with three out of four safety-related divisions available in the presence of a single failure.

The four redundant divisions of the Q-DCIS satisfy the single failure criterion of IEEE Std. 603, Section 5.1. They also satisfy the independence, testing, and repair requirements outlined in IEEE Std. 603, Section 5.6, 5.7, and 6.5. The safety-related fiber optic CIMs (transmitters/receivers), fiber optic cable, and network that are part of the Q-DCIS within and between the four redundant divisions satisfy the separation and independence requirements of divisional equipment. The cable routing separation meets the requirements of the SRP Subsection 9.5.1, "Fire Protection Programs".

### 7.1.3.3.7 Continuous Online Diagnostics and Redundant Power Supplies

The DCIS performs continuous online diagnostic functions that monitor transmission path quality and integrity as well as the integrity of most of the system components. Self-diagnostics extend down to the replaceable card or module level. Off-line tests with simulated input signals can also be used to verify the overall system integrity. Segments of Q-DCIS can be tested and calibrated while on-line when portions of safety-related logic are bypassed. These components and the dual redundant data communication pathways are repairable on-line if one pathway fails. Because of the redundant power supplies and communication pathways, almost all self-diagnostic alarms can be viewed in the MCR while a single failure and most multiple failures exist. The Q-DCIS failures are alarmed in the MCR (~~IEEE Std. 603, Section 5.7 and 6.5~~).

The Q-DCIS components and cabinets have redundant power supplies that are supplied by redundant uninterruptible power feeds within each division. These power feeds support the Q-DCIS operation for 72 hours with neither diesel-generator nor offsite power available. The loss of one power feed or power supply does not affect any safety-related system function (~~IEEE Std. 603, Section 8.1~~).

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

### 7.1.3.3.8 Acceptance Criteria, Guidance, and Conformance

The regulatory acceptance criteria and guidance applicable to each of the Q-DCIS systems identified in the “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants”, NUREG-0800 are stated in Table 7.1-1, “Regulatory Requirements Applicability Matrix”. Sections 7.2 through Section 7.8 contain regulatory conformance discussions for each specific system. The degree of applicability and conformance, along with any clarification or justification for exceptions, is presented in the safety evaluation sections for each specific system.

### 7.1.3.4 Q-DCIS Testing and Inspection Requirements

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

~~Both~~ The RTIF-NMS and SSLC/ESF platforms are readily accessible for testing purposes. Their continuous automatic online diagnostics detect data transmission errors and hardware failures at the replaceable card or module level. Online diagnostics for ~~NUMAC~~ RTIF-NMS and

~~TRICONSSLC/ESF~~ are qualified as safety-related in conjunction with functional software qualification (~~IEEE Std. 603, Section 5.7~~), and also meet the self-diagnostic characteristics for digital computer based protection systems recommended by IEEE Std. 7-4.3.2.

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

The ~~NUMACRTIF-NMS~~ hardware has ~~a~~ watchdog timers for various logic processors and logic functions that monitors the execution of the software. If the software stops executing (suspending the self-diagnostics), ~~the~~its watchdog timer resets the affected logic processor or logic function~~instrument~~. This results in a channel trip and alarm while the logic processor or logic function~~instrument~~ is resetting.

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

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

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

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

## Response Time Test

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

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

### 7.1.3.5 Q-DCIS Instrumentation and Control Requirements

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

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

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

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

## 7.2 REACTOR TRIP SYSTEM

The Reactor Trip System includes the Reactor Protection System (RPS), the Neutron Monitoring System (NMS), and the Suppression Pool Temperature Monitoring (SPTM) functions. These systems are discussed below in Subsections 7.2.1, 7.2.2 and 7.2.3, respectively.

### 7.2.1 Reactor Protection System

#### 7.2.1.1 System Bases

The RPS safety-related design bases (~~IEEE Std. 603, Sections 4.1, 4.2, and 4.3~~) are the following:

- To initiate an automatic safe shutdown of the reactor (also known as reactor trip) by means of rapid hydraulic insertion of all control rods (scram) when:
  - Anticipated operational occurrences (AOO) (transient) anomalous states occur, which potentially impair reactor safety; and
  - Errors in operation take place resulting in transients that potentially impair reactor safety.
- To initiate reactor power reduction and safe shutdown of the reactor by means of rapid hydraulic insertion of a predefined group of the control rods when necessary for rapid reactor power reduction. Several groups can be defined and scrambled in sequence. This feature is called Select Rod Insert (SRI) and is initiated by reliable signals from the Diverse Protection System (DPS).
- To provide timely protection against the onset and effects of conditions threatening the integrity of the reactor fuel barriers, the reactor coolant pressure boundary (RCPB), or containment vessel pressure boundary. This limits the uncontrolled release of radioactive materials from the fuel assembly or the RCPB. Also to provide such protection against conditions that threaten important plant equipment integrity.
- To initiate an automatic reactor trip whenever monitored process variables exceed or fall below their specified trip setpoints based on values determined by AOO, accident analyses, and instrument setpoint calculation methodology.
- To provide control switches for initiation of manual reactor scram by the plant operator when necessary.
- To provide reactor mode selection for enabling the appropriate instrument channel trip functions required in a particular mode of plant operation. Mode selection also provides for bypassing instrument channel trip functions that are not required and for establishing other necessary interlocks associated with the major plant operating modes.

- To provide selective automatic and manual operational trip bypasses, as necessary, to permit proper plant operations. These bypasses allow for protection requirements depending upon specific existing or subsequent reactor operating conditions.
- To provide seal-in of specific trip logic paths after trip conditions have been satisfied and to inhibit the trip reset, as necessary, to ensure subsequent required protective action sequences are completed.
- To provide manual reset capability permitting restoration of the RPS and other affected systems to their normal operational status following seal-in of any trip logic path or after a full reactor scram.
- To provide isolated outputs to other systems sharing instrument channel signals with the RPS, using trip signals generated by the RPS, or requiring other indications of specific RPS status for their inputs.
- To provide isolated outputs to appropriate warning, trip, or bypass alarm annunciators to operator displays (for example, flat panel or cathode ray tube [CRT] displays) and to the plant computer functions (PCF) of the Nonsafety-related Distributed Control and Information System (N-DCIS).
- To provide means for calibration and adjustment of trip function setpoints and to provide sufficient controls to permit surveillance and post-maintenance testing of RPS equipment.

The following bases ensure that the RPS is designed with sufficient reliability—~~(IEEE Std. 603, Section 5.1, 5.2, 5.6, 5.9, 5.12 and 6.2)~~:

- Single failures, bypasses, repairs, calibration, or adjustments do not impair the normal protective functions of the RPS and do not result in inadvertent reactor scram or insertion of control rods. The RPS is capable of accomplishing its protection functions in the presence of any single failure within the RPS (with any three of the four divisions of safety-related power available), any failures caused by a single failure, and any failure caused by any design basis event requiring RPS protective action.
- The RPS is designed to cause reactor scram even during system shutdown and loss of electrical power sources.
- The RPS fails into a safe state if conditions such as disconnection of the system (or portions of the system), loss of electrical power, or adverse environment are experienced.
- Loss of a single power source directly associated with RPS equipment and protection functions does not cause instrument channel trips, division trips, or scram solenoid de-energization resulting in full reactor scram or insertion of any control rod.
- Once initiated, RPS protective actions continue in their intended sequence until completion of hydraulic control rod insertion. The RPS trip is sealed-in and can only be reset manually. All manual resets are automatically inhibited for 10 seconds to allow sufficient time for scram completion.

out of service (with any three of the four divisions of safety-related AC power available). This is accomplished through the combination of fail-safe equipment design, redundant sensor division trip decision logic, and redundant two-out-of-four trip systems output scram logic. The dual two-out-of-four arrangement used in the RPS design ensures that the single-failure criterion is incorporated—~~(IEEE Std. 603, Section 5.1).~~

Equipment within the RPS is designed to fail into a trip-initiating state upon loss of power, loss or disconnection of any input signal, or loss of any internal or external device-to-device connection signal. The failure does not affect trip bypass logic signals or trip bypass permissive logic signals.

The design of the RPS includes two operator-controlled bypasses: the “division of sensors” and the “division of logic (division-out-of-service)” bypasses. These are independently controlled by separate fiber optic “joystick” switches allowing the operator to insert the bypass into only one division at a time. There is no combination of operator bypasses that can reduce the redundancy of the RPS system below the requirements of IEEE Std. 603 Sections 6.7 and 7.5. The system always is able to scram the reactor if any two like and un-bypassed parameters exceed their trip values. The required scram capability is maintained even if the RPS back panel chassis are keylock-disabled (not an operator function).

#### 7.2.1.2.4.1 Arrangement

The RPS-related equipment is divided into four redundant divisions of sensor (instrument) channels, trip logics, and trip actuators as well as two divisions of manual scram controls and scram logic circuitry. The sensor channels, divisions of trip logic, divisions of trip actuators, and associated portions of the divisions of scram logic circuitry together constitute the RPS automatic scram and air header dump (backup scram) initiation logic. The divisions of manual scram controls and associated portions of the divisions of scram logic circuitry together constitute the RPS manual scram and air header dump initiation logic.

The automatic and manual scram initiation logics are independent of each other and use diverse methods and equipment to initiate a reactor scram. A functional equipment arrangement is shown in Figure 7.2-1.

**Sensor Channels:** Equipment within a sensor channel consists of sensors (transducers or switches), a Digital Trip Module (DTM), and multiplexers. The sensors within each channel detect abnormal operating conditions and send analog (or discrete) output either directly to the RPS cabinets or to the Reactor Trip and Isolation Function (RTIF) Remote Multiplexer Units (RMUs) within the associated division of the Q-DCIS. The RMU within each division performs signal processing including analog to digital conversion, then sends the digital or digitized analog output values of the monitored variables to the DTM for trip determinations within the associated RPS sensor channel in the same division. The DTM in each sensor channel compares individual monitored variable values with trip setpoint values. For each variable the DTM sends a separate trip/no trip output signal to the functional Trip Logic Units (TLU) in the four divisions of trip logic. DTM signals sent from one division to other divisions are isolated optically using fiber-optic cables. The DTMs and TLUs are microprocessor-based modules of the RPS.

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

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

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

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

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

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

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

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

#### 7.2.1.2.4.2 Initiating Circuits

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

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

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

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

### 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

criteria 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.

### 7.2.1.3.6 Three Mile Island Action Plan Requirements

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

### 7.2.1.4 Testing and Inspection Requirements

#### 7.2.1.4.1 System Testing: Operational Verifiability

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

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

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

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

- MSIV limit switches, and
- TSV limit switches.

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

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

#### 7.2.1.4.2 Surveillance Testing and In-Service Testing

The RPS equipment testing includes:

- Preoperational, startup and refueling/outage inspection testing; and
- In-service and operational surveillance testing.

The RPS is designed to permit testing of an emergency reactor shutdown by methods simulating actual plant operation and duplicating, as closely as possible, the performance of protective actions even during reactor operation. These test methods support in-service verification of scram capability with high reliability. The RPS components and testing strategies are designed so that identifiable failures are detectable. Test methods are designed to facilitate recognition

and location of malfunctioning component to allow for the replacement, adjustment, or repair of the component.

In-service testing of the RPS is performed periodically to verify operability during normal plant operation and to ensure that each tested channel can perform its intended design function. The surveillance tests include: (a) instrument channel checks, (b) functional tests, (c) verification of proper sensor and channel calibration, (d) verification of applicable functions in the division of trip logic and division of actuators, and (e) response time tests.

### **7.2.1.5 Instrumentation and Control Requirements**

#### **7.2.1.5.1 Automatic Scram Variables**

Refer to Subsection 7.2.1.2.4.2 for discussions of the automatic scram initiating circuits and the systems that apply to them.

#### **7.2.1.5.2 Automatic and Manual Bypass of Selected Scram Functions**

##### **7.2.1.5.2.1 Operational Bypasses**

Manual or automatic bypass (take out of service) of certain scram functions permits the selection of suitable plant protection conditions during different conditions of reactor operation (~~IEEE Std. 603, Sections 6.6 and 7.4~~). These RPS operational bypasses inhibit actuation of those scram functions not required for a specific state of reactor operation.

The conditions of plant operation requiring automatic or manual bypass of certain reactor trip functions are described below.

- **Main steam TSV closure and steam governing TCV fast closure trip bypasses:** These permit continued reactor operation at low power levels when the TSVs or TCVs are closed. The main steam TSV closure and the steam governing TCV fast closure scram trip functions are automatically bypassed when the APRM simulated thermal power of the NMS is below 40% of the rated thermal power output.

The TSV closure and TCV fast closure trips are automatically bypassed if a sufficient number of the bypass valves are opened. This bypass occurs if a sufficient number of TBVs open to at least 10% within a preset time limit following the TCV fast closure or TSV closure signal to inhibit reactor trip. The NMS system provides the RPS with an analog simulated thermal power signal used to determine both the low power bypass and the required number of TBV needed to open for a post turbine trip or for full load rejection conditions. The low power bypass is automatically removed and both scram trip functions are enabled at reactor power levels above the bypass setpoint. The bypass permits the RPS to remain in its normal energized state under the specified conditions. This bypass condition is alarmed in the MCR.

- **CRD HCU accumulator charging header low-pressure bypass:** This bypass is allowed only when the Reactor Mode Switch is in either the Shutdown or Refuel position. If a

- NMS SRNM scram trip functions with Reactor Mode Switch in the Run position bypass: Whenever the Reactor Mode Switch is in the Run position, SRNM reactor scram trip functions are automatically bypassed. However, this bypass is not alarmed because it is the normal condition with the Reactor Mode Switch in the Run position. This bypass condition is indicated in the MCR. The SRNM rod block functions also are disabled when the Reactor Mode Switch is in the Run position.
- Non-coincident NMS scram trips in Run mode bypass: Whenever the Reactor Mode Switch is in the Run position, and the coincident/non-coincident NMS trip remains in the non-coincident position, the non-coincident NMS scram trip functions are automatically disabled (bypassed). This logic is an NMS function.

The non-coincident NMS trip function is required during initial fuel loading and subsequent refueling operations. During such operations the Reactor Mode Switch is in the Refuel position (or for certain testing conditions, in the Shutdown or Startup positions). A non-coincident NMS trip occurs in each division of trip logic when any single SRNM trip signal is present in the NMS if the coincident/non-coincident manual switch in the division is in the non-coincident position. This logic is an NMS function.

The non-coincident NMS trip function is automatically removed when the Reactor Mode Switch is in the Run position. If the coincident/non-coincident NMS trip selection switch is in the non-coincident position when the Reactor Mode Switch is in the Run position, there is an alarm in the MCR. When the reactor is in Shutdown, Refuel, or Startup mode, the non-coincident NMS trip can be bypassed manually by a separate “non-coincident trip disable” switch. These logics are NMS functions.

- RPV water level high trip bypass (indicated operational bypass): The RPV water level high trip function is automatically bypassed whenever the Reactor Mode Switch is in the Shutdown, Refuel, or Startup position. This bypass condition is alarmed in the MCR and is automatically removed if the Reactor Mode Switch is moved to the Run position.
- Condenser pressure high trip bypass (indicated operational bypass): The condenser pressure high trip function is automatically bypassed whenever the Reactor Mode Switch is in the Shutdown, Refuel, or Startup position. This bypass condition is alarmed in the MCR and is automatically removed if the Reactor Mode Switch is moved to the Run position.
- APRM, OPRM, and SRNM scram trips bypasses: These have manual bypass capabilities within the NMS, not the RPS.

#### 7.2.1.5.2.2 Maintenance Bypasses

Manual bypass capability is provided to allow certain portions of RPS-related equipment to be taken out of service for maintenance, repair, or replacement ~~(IEEE Std. 603, Sections 6.7 and 7.5)~~. Maintenance bypasses reduce the degree of redundancy of RPS channels but do not affect or eliminate any scram function. Protective functions are available while any RPS equipment is in maintenance bypass. Except where indicated otherwise, any maintenance bypass generates a status alarm at the MCR operator's console.

### 7.2.2.1.1 Startup Range Neutron Monitor Subsystem

#### 7.2.2.1.1.1 Trip Functions

The SRNM scram trip functions are discussed in Subsection 7.2.1.2.4.2, and rod block trip functions are discussed in Subsection 7.7.2.2. The SRNM channels also provide trip bypass.

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

- The trip signals provided in the SRNM design are shown in Table 7.2-3.
- SRNM trips are active only when the Reactor Mode Switch is not in the Run position. When the NMS coincident/non-coincident switch is in the non-coincident position any one of the SRNM can generate trips. When the Reactor Mode Switch is in the Run position, the NMS trip is in the coincident mode. For each division, the three SRNM scram trip signals are combined to form a divisional SRNM trip signal and then combined with the divisional APRM trip signal before being sent to the RPS.
- Trips dependent upon signal magnitude have setpoints adjustable in the instrument range.
- The period trip circuit compares the amplified and delayed neutron flux signal with its original signal and provides trips and/or alarms if the original signal exceeds the delayed one. The period alarm and scram setpoints are built-in through the period trip circuit or software algorithm.
- A short-period warning signal (Period Withdrawal Permissive) is provided to inhibit rod withdrawal to avoid an inadvertent scram due to excessive rod withdrawal.
- An SRNM interlock signal “ATWS Permissive” is established and sent to the Anticipated Transients Without Scram / Standby Liquid Control (ATWS/SLC) logic as a permissive signal to allow the initiation of liquid boron injection by the SLC system.
- The period trip is active except below a fixed power-level of approximately (1E-4%) of rated power. This approximately corresponds with the upper limit of the SRNM counting range.
- An instrument inoperative alarm is provided to signal that an SRNM channel is out of service.
- An SRNM channel is considered inoperative if any of the following conditions occur. Its Calibrate-Operate switch is not in the Operate mode, and
  - Any interlock in the channel is open,
  - The unit self-test function detects failures, or
  - The detector polarizing voltage falls below a preset level.

related power available). It also satisfies the IEEE Std. 603, Section 5.6 independence requirement.

#### 7.2.2.2.4.4 Signal Processing

Over the 10-decade power monitoring range two monitoring methods are used: (1) the counting method for the lower counting range (approximately  $1 \times 10^3$  neutrons/cm<sup>2</sup>/sec) to approximately  $1 \times 10^9$  neutrons/cm<sup>2</sup>/sec, and (2) the Campbelling technique Mean Square Voltage (MSV) for the higher range, from  $1 \times 10^8$  neutrons/cm<sup>2</sup>/sec to  $1 \times 10^{13}$  neutrons/cm<sup>2</sup>/sec of neutron flux.

In the counting range, after pre-amplification, the discrete pulses produced by the sensors are applied to a discriminator. The discriminator, together with other digital noise-limiter features, separates the neutron pulses from gamma radiation and other noise pulses. The neutron pulses are counted. The reactor thermal power is proportional to the count rate.

In the MSV range, where it is difficult to distinguish among the individual pulses, a DC voltage signal proportional to the mean square value of the input signal is produced. The reactor power is proportional to this MSV. In the mid-range overlapping region, where both methods apply, the SRNM calculates a neutron flux value based on a weighted interpolation of the two flux values as calculated by each method. A continuous and smooth flux reading transfer is achieved in this manner. In addition, there is the calculation algorithm for the period-based trip circuitry generating a trip margin setpoint for the period trip protection function.

#### 7.2.2.2.4.5 Trip Functions

The SRNM scram trip functions are discussed in Subsection 7.2.2.1.1, and rod block trip functions are discussed in Subsection 7.7.2.2. The SRNM channels also provide trip bypass.

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

#### 7.2.2.2.4.6 Bypasses and Interlocks

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

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

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

#### 7.2.2.2.4.7 Redundancy and Diversity

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

#### 7.2.2.2.4.8 Environmental Considerations

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

The SRNM instruments are designed to operate under the expected environmental conditions. Environmental qualification is discussed in Section 3.11.

#### 7.2.2.2.5 Local Power Range Monitor

##### 7.2.2.2.5.1 General Description

The LPRM monitors local neutron flux in the power range. The LPRM provides input signals to the APRM (Subsection 7.2.2.2.6), the RC&IS (Subsection 7.7.2), and the PCF of the N-DCIS (Subsection 7.1.5).

##### 7.2.2.2.5.2 Uninterruptible Power Supply

Alternating current power for the LPRM circuitry is supplied by four pairs of redundant divisional 120 VAC UPS buses corresponding to the four safety-related divisions. The cabinets can perform their functions with either of their redundant power sources. Each division supplies power to one-fourth of the detectors. Each LPRM detector is provided with a DC power supply, housed in the designated divisional APRM instrument furnishing the detector polarizing potential.

### 7.3.1.1.2 System Description

The ADS is a subsystem of the NBS and comprises 10 SRVs, eight DPVs, and the associated I&C. The SRVs are nitrogen operated solenoid actuated relief valves. The DPVs are electrically operated squib valves. The SRVs and DPVs are divided into groups, and lift in sequence when required, and are described in detail in Subsection 5.2.2 and Subsection 6.3.2, respectively.

The NBS functional components (including the ADS) are shown on Figure 5.1-2. The mechanical aspects of the ADS functions within the ECCS are discussed in Subsection 6.3.3. Typical SRV and DPV logic and control are shown on Figures 7.3-1a and 7.3-1b, respectively.

### Automatic Operation

Actuation of ADS equipment is controlled automatically (~~IEEE Std. 603, Sections 6.1 and 7.1~~), without need for operator action. Capability for manual actuation also is provided (IEEE Std. 603, Sections 6.2 and 7.2).

Automatic actuation of the ADS occurs when the RPV water reaches Level 1, which is detected by four wide range RPV water level transmitters. These transmitters are separate from those used for Reactor Protection System (RPS) functions and different from the Diverse Protection System (DPS) wide range level transmitters.

When attainment of Level 1 is detected five SRVs (group 1) are opened to start RPV pressure reduction, followed by the remaining five SRVs (group 2) after a time delay. See Table 7.3-2 for the time delay parameters. The sequence continues with groups of DPVs, each opening after further successive time delays. See Table 7.3-3 for the DPV groups and time delay parameters. This sequential operation minimizes the water loss as a result of liquid swell in the RPV when its pressure is rapidly reduced. See Table 5.2-2 for the SRV and DPV settings and/or capacities.

Additionally, as discussed in Subsection 7.8.1.2, the DPS has the ability to open independently the same SRVs and DPVs using the same logic, but using diverse hardware/software equipment and reactor-level sensors separate from those used in the primary ECCS functions. For the ADS, the DPS can actuate a fourth, nonsafety-related solenoid on each of the SRVs, and a fourth squib initiator on each of the DPVs.

### Manual Operation

The safety-related Video Display Units (VDUs) in the MCR provide a display format allowing the operator to manually open each SRV and each DPV independently, using the primary Safety System Logic and Control/ESF (SSL/ESF) logic function (~~IEEE Std. 603, Sections 5.8, 6.2 and 7.2~~). Each nonsafety-related VDU in the MCR provides a display format allowing the operator to manually open each SRV independently, using the DPS logic function. Each display uses an “arm/fire” configuration requiring at least two deliberate operator actions. Operator use of the “arm” portion of the display triggers a plant alarm. The two manual opening schemes from SSL/ESF and from DPS are diverse.

Each safety-related VDU provides a display with an “arm/fire” switch (one per division) to manually initiate ADS as a system, rather than initiating each valve individually (IEEE Std. 603, Sections 5.8, 6.2 and 7.2). If the operator uses any two of the four “arm/fire” switches, the ADS

sequence seals in and starts the ADS valve opening sequence ~~(IEEE Std. 603, Section 5.2)~~. This requires at least four (two arm and two fire) deliberate operator actions.

### Actuation Logic

See Figure 7.3-1a for typical SRV actuation logic, and Figure 7.3-1b for typical GDCS and DPV actuation logic.

The ADS actuation logic is implemented in four SSLC/ESF divisions, each of which can make a Level 1 trip vote. Each of the divisional trip votes is shared with the other divisions. Normally, each of the four divisions makes a two-out-of-four trip decision from the four divisional votes; however, the entire SSLC/ESF system has a bypass control such that any single division of sensors can be removed from the two-out-of-four decision process, so that the remaining three divisions operate with a two-out-of-three trip decision. Only one division at a time can be bypassed, and used to facilitate either maintenance or calibration activities. Divisional bypasses are alarmed in the MCR.

Each division of the SSLC/ESF has two trains of two-out-of-four trip logic (except the DPV logic, which has three trains) to support the requirement that single divisional failures cannot result in inadvertently opening any ADS valve (SRV or DPV). (See Figures 7.3-1a, 7.3-1b). Each initiating logic has access to one channel of wide-range level sensing for the Level 1 trip decision. The four divisional water levels and their trip setpoints are continuously monitored for consistency by the N-DCIS plant computer functions (PCF). An inconsistency results in an alarm. The separate logic of each train issues the ECCS trip signal, if the RPV water drops below Level 1.

The ECCS trip signal actuates a timer (see Table 7.3-2). If the trip signal resets (as, for example, from an instrument column transient), the timer resets and restarts when the next ECCS trip signal is received. If the ECCS trip signal persists for 10 seconds, the logic seals in and issues an “initial start” signal ~~(IEEE Std. 603, Section 5.2)~~. The initial start signal also is transmitted to the SSLC/ESF (Subsection 7.3.5), ICS (Subsection 7.4.4), and GDCS (Subsection 7.3.1.2). The initial start signal specifically actuates five timers in each of the two two-out-of-four trip logic trains (per division) of ADS logic.

Divisional separation is maintained by using optical isolators and separate raceway, conduit, and penetration wiring to each SRV or DPV. Trip signals from any two divisions can open all of the ADS valves.

The actual firing circuit for the various squib initiators and SRV solenoids consists of the two load driver/discrete output circuits, followed by a continuity monitor and a disable switch all arranged in series, and located in the appropriate divisional Remote Multiplexing Units (RMUs) and DPS RMUs in the Reactor Building (RB). Because there is the division of sensors bypass, and there are multiple trains of two-out-of-four logic, no additional division of trip logic bypass is implemented in the SSLC/ESF logic. It is undesirable to perform this level of bypass activity with the RMU electrically connected to the valve. The disable switch described below provides the bypass function required. In addition to the usual RMU self-diagnostics, means are provided to indicate that each of the series load driver/discrete output circuits can be “closed” (the circuits can be exercised one at a time from the MCR) and to indicate that both have closed.

The disable switch (Figure 7.3-1b) that disables the firing circuit affects one valve and does not interact with the other valves allocated to that RMU. Operation of any disable switch triggers an MCR alarm indicating that the firing circuit is out of service. Although the load driver/discrete output checks can be done online (one at a time) without causing valve operation, opening the firing circuit with the disable switch allows the continuity monitor to be tested, and allows online surveillance and maintenance activities to be done, with the assurance that a valve is not opened inadvertently. The operation of a disable switch in any one division does not disable the SRV or DPV because it maintains the ability to be opened by its other divisional solenoid/squib initiator. Additionally it is not possible to lose single failure inadvertent actuation protection by any operator or disable switch action.

The ADS design parameters shown in Table 7.3-1 ensure that no single failure of an ADS division logic, SRV actuation pilot, or DPV igniter circuit can prevent successful system operation as long as any three of the four divisions of safety-related power are available. This satisfies the single failure criterion (~~IEEE Std. 603, Section 5.1~~).

Supporting systems for the ADS include the instrumentation, logic, control, and motive power sources. The instrumentation and logic power is supplied by the corresponding divisional safety-related power sources. The actual SRV solenoid and DPV squib initiator power also is supplied by the corresponding divisional safety-related power sources (See Subsection 8.3.1.1.3). The motive power for the electrically operated pneumatic pilot solenoid valves on the SRVs is from accumulators located near the SRVs, and supplied with nitrogen by the High Pressure Nitrogen Supply System (HPNSS).

#### 7.3.1.1.3 Safety Evaluation

Chapter 15 and Section 6.3 evaluate the individual and combined capabilities of the ECCS systems, including the ADS. For the entire range of reactor coolant system break sizes, the ECCS systems ensure that the reactor core always is submerged.

SSLC/ESF initiating instrumentation, including the ADS, responds to the potential inadequacy of core cooling regardless of the location of the breach in the reactor coolant pressure boundary (RCPB). Detection of RPV low water level, which is completely independent of breach location, is used to initiate the ADS.

The redundancy of the control and monitoring equipment for the ADS is consistent with the redundancy of the four divisions of ADS.

No single failure in the ADS initiation circuitry can prevent the ADS from depressurizing the RPV, or cause an inadvertent actuation of the ADS. This satisfies the single failure criterion of IEEE Std. 603, Section 5.1.

The ADS has no equipment protective interlocks that could interrupt automatic system operation.

The ADS instrumentation and logic, and the SRV and DPV initiation circuitry is powered by divisionally separated safety-related power sources.

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,

- Two-out-of-four ADS Level 1 signals,
- Automatic ADS initiation,
- Aborted ADS initiation,
- SRV solenoid loss of continuity,
- DPV squib firing circuit loss of continuity,
- Inconsistent wide range divisional RPV water level alarms,
- Any inconsistency in divisional input information from the four SSLC/ESF divisions to each Voter Logic Unit (VLU), as compared at the VLU, and
- Any single load driver/discrete output trip in the firing circuit of a DPV or SRV.

Safety-related ADS instrumentation located in the drywell is designed to operate in the environment resulting from a Loss of Coolant Accident (LOCA). Safety-related instruments located outside the containment also are qualified for the environment in which they must perform their safety function.

### 7.3.1.2 Gravity-Driven Cooling System

The basic components of the GDCS are within the containment. The GDCS pools, piping and valves are in the drywell. The suppression pool is on the outer periphery of the drywell within the containment envelope.

#### 7.3.1.2.1 System Design Bases

<p>The GDCS I&amp;C are designed to meet the following safety-related requirements (<del>IEEE Std. 603, Sections 4.1, 4.2, 4.5, 5.1, 5.8, 6.2, 7.2, and 7.3</del>) and 10 CFR 50.2, Design Bases:</p>
---

- Automatically initiate the GDCS to prevent fuel-cladding temperatures from reaching the limits of 10 CFR 50.46.
- Respond to a need for emergency core cooling following reactor depressurization, regardless of the physical location of the malfunction or break causing the need.
- Be completely automatic in operation. Manual initiation of GDCS is possible at any time, provided protective interlocks have been satisfied.
- Prevent the inadvertent actuation of the deluge valves thus preventing inadvertent draining of the GDCS pools.
- Prevent any single control logic and instrumentation failure from inadvertently opening a GDCS injection valve or equalizing valve.
- Display GDCS valve positions and GDCS pool levels on a mimic of the system in the MCR.

two of the four switches, the GDCS sequence seals in and starts the GDCS valve sequencing (~~IEEE Std. 603, Section 5.2~~). This manual actuation also is interlocked with RPV pressure. This requires four deliberate (two-arm and two-fire) operator actions. For all of the manual initiations, operator use of the “arm” portion of the display triggers a plant alarm.

The safety-related VDUs in the MCR provide a display format allowing the operator to manually open each GDCS injection valve independently, using the primary SSLC/ESF logic function (~~IEEE Std. 603, Sections 5.8, 6.2 and 7.2~~). Likewise, each nonsafety-related VDU in the MCR provides a display format allowing the operator to individually open each GDCS injection valve independently, using the DPS logic function. Each display uses an “arm/fire” configuration (interlocked with a low reactor pressure signal) requiring at least two deliberate operator actions. Operator use of the “arm” portion of the display triggers a plant alarm. The two manual opening schemes from the SSLC/ESF (primary) and the DPS (backup) are diverse.

In addition the safety-related VDUs in the MCR provide a display format allowing the operator manually to open each GDCS equalizing valve independently, using the primary SSLC/ESF logic function (~~IEEE Std. 603, Sections 5.8, 6.2 and 7.2~~). Likewise, each nonsafety-related VDU in the MCR provides a display format allowing the operator to individually open each GDCS equalizing valve independently, using the DPS logic function. Each display uses an “arm/fire” configuration requiring at least two deliberate operator actions (interlocked with a low reactor pressure signal). Operator use of the “arm” portion of the display triggers a plant alarm. The two manual opening schemes from the SSLC/ESF (primary) and the DPS (backup) are diverse.

### Actuation Logic

The logic elements providing controls for the actuation of the GDCS injection and equalizing squib valves are contained in the SSLC/ESF portion of the Q-DCIS, outside the drywell containment. RPV level transmitters used to initiate GDCS are part of the NBS, and are located on racks outside the drywell.

The SSLC/ESF logic sends an initial start signal to the GDCS logic that automatically initiates the GDCS following reactor depressurization under LOCA conditions.

Each of the two trains per division is presented with the initial start signal from the same SSLC/ESF logic initiating the ADS. The SSLC/ESF logic adds a time delay (Table 7.3-4) to the initial start signal, and then operates all of the GDCS injection valves. Once the initial start signal is given to both ADS and GDCS (starting the various timers), the sequence is sealed in and cannot be aborted by the plant operator.

The GDCS injection and equalizing valve logic includes the SSLC/ESF “division of sensors” bypass switch, two-out-of-four trip decisions, and single-failure proof actuation logic - with any three of the four divisions of safety-related power available. The valve logic also is single-failure proof against inadvertent actuation, meaning each division of logic has three load drivers each of which must operate for the associated squib valves to fire.

The wide range level sensors that are used for the ADS logic and fuel zone range RPV water level are also used for the GDCS equalizing valve logic; these are diverse from the sensors used for RPS functions and from those used by the DPS. Both sets of transmitters belong to the NBS.

The generation of the initial start signal for the GDCS is described above (Automatic Operation). The logic for all squib initiators is similar. The signals are acquired per division by RMUs of the same division. The data are sent via fiber optic cables to the SSLC/ESF cabinets located in the corresponding divisional I&C equipment rooms in the Control Building (CB). Each division's logic compares the measured parameters to setpoints. If there is a discrepancy in outputs a sensor trip signal is sent both to its own division and to each of the other divisions by appropriately isolated fiber optic cables.

Each division has access to all four divisional sensor trip signals, and performs a redundant two-out-of-four vote on the four sensor trip signals. (The vote is two-out-of-three if one division is bypassed, because no more than one division can be bypassed at any one time.)

Each division therefore has two separate trip logics that can independently perform a two-out-of-four vote on the sensor trips. The effect is that any two divisions sensing the appropriate trip conditions results in all divisions providing a trip signal.

The existence of the multiple logic trips per division is necessitated by the requirement that no injection or equalizing squib valve inadvertently be fired as the result of a single failure ~~(IEEE Std. 603, Section 5.1)~~.

For the eight GDCS injection squib valves logic, each of the two (per division) initial start signals actuates an adjustable timer with a preset time delay (as specified in Table 7.3-4). After the time delay, each of the two timers outputs a trip signal to the GDCS squib load drivers/discrete outputs. There are eight injection squib valves, each with three divisional squib initiators, and one DPS squib initiator.

Within the RMU, for each squib initiator, there is a series circuit of divisional power, three load drivers/discrete outputs in series, a current monitor, and a normally closed disable switch. Each of the two timers must transmit a trip signal to the corresponding series load driver/discrete output. The effect is that both two-out-of-four trip voters, both timers, and all of the load drivers/discrete outputs must operate to fire the squib initiator, making the design single failure proof against inadvertent actuation. Because each GDCS injection squib valve always has three squib initiators, powered by three different divisions, the design is also single-failure proof if required to operate all eight valves, and even will initiate with the loss of two divisions of power.

The current monitor continuously verifies squib electrical continuity, and the disable switch is used when performing maintenance or surveillance testing, or testing the current monitor. If the disable switch opens the circuit, an alarm signal is sent to the MCR, indicating that the squib initiator (not the valve) is inoperable.

For diversity, the DPS also is able to fire its squib electrical initiator on each of the eight GDCS injection squib valves, using single-failure proof logic (both to operate and to avoid inadvertent operation). This is accomplished using a completely separate squib initiator connected to the DPS system (see Figures 7.3-1b 1 and 7.3-1c). The DPS system uses diverse (from the SSLC/ESF) sensors, hardware, and software to operate the GDCS injection valves. Figure 7.3-2 shows the initiation logic of a typical equalizing squib valve.

Within the RMU, for each squib initiator, there is a series circuit of divisional power, three load drivers/discrete outputs in series, a current monitor, and a normally closed disable switch. To

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)(H.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.

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) [H.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

Isolation Condenser/Passive Containment Cooling (IC/PCC) pool outside the containment. Containment (drywell) pressure above the suppression pool (wetwell) pressure, similar to the situation during a loss of reactor coolant into the drywell, forces flow through the PCCS condensers. Condensate from the PCCS drains to the GDCS pools. As the flow passes through the PCCS condensers, heat is rejected to the IC/PCC pool, thereby cooling the containment atmosphere. This action occurs automatically, without the need for actuation of components. The PCCS does not have instrumentation, control logic, or power-actuated valves, and does not need or use electrical power for its operation in the first 72 hours after a LOCA. For long-term effectiveness of the PCCS, the vent fans are manually initiated by operator action. Other information on the PCCS is given in Subsection 6.2.2 and leak rates are discussed in Subsection 16B.3.3.

### 7.3.3 Leak Detection and Isolation System

The primary function of the Leak Detection and Isolation System (LD&IS) is to detect and monitor leakage from the RCPB and to initiate the appropriate safety action to isolate the source of the leak. The system is designed to automatically initiate the isolation of certain designated process lines penetrating the containment, to prevent release of radioactive material from the RCPB. The initiation of the isolation functions closes the appropriate containment isolation valves. The LD&IS functions are performed in two separate safety-related platforms. The Main Steam Isolation Valve (MSIV) isolation logic functions are performed in the Reactor Trip and Isolation Function (RTIF) platform, while all other containment isolation logic functions are performed in the SSLC/ESF platform. The non-safety monitoring functions of LD&IS are performed in the N-DCIS.

#### 7.3.3.1 System Design Bases

The following safety-related system design criteria are applicable to the design of the LD&IS (IEEE Std. 603, Sections 5.1, 5.2, 5.6, 5.7, 5.9, 6.1, and 6.8).

- The LD&IS is engineered as a safety-related system, Seismic Category 1, and conforms to the regulatory requirements, guidelines, and industry standards listed in Table 7.1-1 for this system.
- The MSIV function of LD&IS logic design is fail-safe, such that loss of electrical power to the logic of one LD&IS division initiates a channel trip. The containment isolation function of LD&IS logic design is fail as-is such that loss of power to the logic of one division does not result in a trip.
- Isolation is initiated with precision and reliability once leakage has been detected from the RCPB.
- Once isolation is initiated, the action continues to completion. Deliberate operator action is required to reopen the isolation valves.
- The LD&IS design meets the single failure criterion because no single failure within the system, with any three of the four divisions of safety-related power available, initiates inadvertent isolation or prevents isolation when required.

- Drywell sumps liquid drain lines,
- Containment purge and vent lines,
- RB area air supply and exhaust ducts,
- Feedwater lines, and
- Fission products sampling lines.

The nonsafety-related detected and monitored sources or indications of leakage are:

- Condensate flow from the upper and lower drywell air coolers,
- Leakage to the drywell from valves equipped with leak-off lines between the two valve stem packings,
- Fission product leakages into the drywell detected by the Process Radiation Monitoring System (PRMS),
- RPV head flange pressure seal leakage,
- Drywell floor drain and drywell equipment drain sump level change,
- Drywell temperature,
- SRV discharge line temperature,
- RB equipment and floor drain sump pump activity,
- Equipment areas differential temperature, and
- RCCWS intersystem leakage radiation.

Drywell sump levels and flow rates are used to quantify identified and unidentified leakages.

The LD&IS control functions initiating automatic isolation functions are classified safety-related, and these functions use redundant divisional channels satisfying both the mechanical and electrical separation criteria as well as the single failure criterion ~~(IEEE Std. 603, Sections 5.1 and 5.6)~~. This system operates continuously during normal reactor operation, and during plant abnormal and accident conditions.

The system design is configured as shown in Figure 7.3-3. The LD&IS interfacing sensor parameters are listed in Table 7.3-5. A detailed description of detection methods, monitored plant parameters, and the monitoring instrumentation is included in Subsection 5.2.5.

### ***7.3.3.3 Safety Evaluation***

The LD&IS control and isolation functions, including the sensors and channel instrumentation, are a safety-related system, and qualified environmentally and seismically for continuous operation during plant normal, abnormal, and accident conditions. The system design conforms to the design bases described in Subsection 7.3.3.1. The LD&IS system design uses

measurements and redundant instrument channels to detect and monitor reactor coolant leakage in (and external to) the containment, and to detect and isolate the source of the leak, thereby preventing radioactive releases to the environs. The isolation logic uses four redundant divisional channels to monitor a leakage parameter and uses the two-out-of-four coincidence voting logic technique for initiation of the isolation function. This design technique improves system availability to perform safety-related functions, satisfies the single failure criterion, and permits channel bypass for maintenance and repair during normal plant operation. Loss of one channel due to failure or power loss does not cause inadvertent isolation.

The four redundant divisions of the MSIV isolation function of the LD&IS comprise a fail-safe design. The isolation logic is energized under normal conditions and de-energized to initiate the isolation function on indication of abnormal leakage. The four redundant divisions of the containment isolation and feedwater isolation functions of the LD&IS use fail as-is designs and energized-to-trip logic.

The signals used to isolate the feedwater lines by closing the feedwater isolation valves (FWIVs) are:

- Feedwater lines differential pressure high coincident with high drywell pressure,
- High drywell water level coincident with high drywell pressure,
- RPV water Level 0.5 with time delay, and
- RPV water Level 8.

The signals provided to stop the feedwater pumps by opening the feedwater pump ASD controller power circuit breakers are:

- Feedwater lines differential pressure high coincident with high drywell pressure,
- High drywell water level coincident with high drywell pressure,
- RPV water Level 0.5 with time delay, and
- RPV water Level 9.

<p>The LD&amp;IS logic is designed to seal-in the isolation signal once the trip has been initiated (<del>IEEE Std. 603, Section 5.2</del>). The isolation signal overrides any control action to trigger the opening of isolation valves. Reset of the isolation logic is required before any isolation valve can be opened manually. Manual valve override capability is provided for valves that are required to operate following a design basis event on a valve-by-valve or line-by-line basis. The valve override requires at least two deliberate operator actions and is under administrative controls. The override status is alarmed in the MCR.</p>	
---	--

The system logic design incorporates provisions to permit bypass of a single division of sensors at one time for repair and maintenance without affecting system capability to perform its safety-related functions. With one division of sensors in the bypass mode, no other division of sensors simultaneously can be bypassed.

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) ~~(H)(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.

### 7.3.3.4 *Testing and Inspection Requirements*

#### 7.3.3.4.1 **In-service & Surveillance Tests**

In-service testing of the leak detection and monitoring channels is performed periodically to verify operability during normal plant operation and to assure that each tested channel can perform its intended design function. The surveillance tests include instrument channel checks, functional tests, verification of proper sensor and channel calibration, and response time tests.

The LD&IS instrument channels use conventional sensors for leak detection and monitoring, and require no special or unique testing methods.

The setpoint verifications, trip logic tests, and channel integrity tests for the safety-related functions of LD&IS are processed and tested by the RTIF and SSLC/ESF platforms.

#### 7.3.3.4.2 **Main Steam Isolation Valve Closure Tests**

The LD&IS design provides manual capability and incorporates logic provisions to test closure of each of the MSIVs during normal reactor operation ~~(IEEE Std. 603, Sections 5.7 and 6.5)~~. To verify MSIV closure capability, each MSIV is tested periodically for partial closure while in service without causing a plant outage ~~(IEEE Std. 603, Section 6.5)~~.

#### 7.3.3.4.3 **Testing and Maintenance in the Bypass Mode**

Testing, calibration, and maintenance are performed on the equipment in accordance with established procedures when the channel is either out of service or deliberately has been bypassed.

#### 7.3.3.5 *Instrumentation and Controls Requirements*

The LD&IS is designed to detect and monitor leakage from the RCPB, using a diversity of parameters and redundant instrument channels. The monitored leakage parameters are provided continuously to the RTIF and SSLC/ESF for processing and initiation of trips required for the isolation functions.

The LD&IS instrumentation requirements for each specific monitoring and isolation function are described in detail in Subsection 5.2.5. The plant parameters monitored for leakage detection, isolation, and alarms are summarized in Tables 5.2-6 and 5.2-7. The containment isolation functions accomplished by valves and control signals required for the isolation of process lines penetrating the containment are summarized in Tables 6.2-15 through 6.2-42.

### 7.3.4 **Control Room Habitability System**

The Control Room Habitability System (CRHS) is an SSLC/ESF system that provides a safe environment within the MCR, allowing the operator(s) to:

- Control the nuclear reactor and its auxiliary systems during normal conditions,

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

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

#### **7.3.5.4 Testing and Inspection Requirements**

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

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

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

In-service testing of the SSLC/ESF is performed periodically to verify operability during normal plant operation and to assure that each tested channel can perform its intended design function. The surveillance tests include, as required, instrument channel checks, functional tests, verification of proper sensor and channel calibration, verification of applicable logic functions in the VLU trains, and response time tests.

All test features adhere to the single failure criterion so that:

- No single failure in the test circuitry incapacitates an SSLC/ESF safety function, and
- No single failure in the test circuitry causes an inadvertent scram, MSIV closure, other PCV isolation, or actuation of any ESF system.

### 7.3.5.5 Instrumentation and Controls Requirements

The SSLC/ESF equipment uses microprocessor-based programmable logic and control instruments, with standardized interchangeable modules. Discrete solid-state logic also is used when applicable.

Control programs for each microprocessor-controlled instrument are in the form of software residing in non-volatile memory. The storage medium is in general Programmable Read-Only Memory (PROM). Programs are under the control of a real-time operating system residing in non-volatile memory. The equipment is qualified with a verification and validation program conforming to applicable codes and standards.

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

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

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

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

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

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

#### 7.3.6.1 System Design Bases

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

- Automatically isolates an excessively leaking VB using a VB isolation valve.
- The VB and VB isolation valve are qualified for a harsh environment inside the drywell.
- Manual opening and closing of a VB isolation valve is provided for in the design.
- No single control logic and instrumentation failure opens/closes more than one VB isolation valve.
- VB and VB isolation valve positions are displayed in the MCR.
- The safety-related function is met with one VB/VB isolation valve path isolated together with any active identifiable single failure.
- Divisional instruments performing VB isolation valve logic are powered by the associated safety-related divisional power supplies.
- Containment system VB isolation function logic controllers are independent ~~(IEEE Std. 603, Section 5.6).~~

### 7.3.6.2 System Description

The wetwell-to-drywell VB isolation function comprises independent logic controllers, three sets of VBs, and three sets of VB isolation valves, ~~and independent logic controllers~~. A more detailed description is given in Subsection 6.2.1.1.2.

- Automatic Operation
  - Closure of the VB isolation valve is performed automatically, without need for operator action, once excessive bypass leakage through a VB is detected.
  - Automatic actuation logic is performed by a control system with components similar to those used in the ATWS/SLC control system. These components are an independent Q-DCIS subsystem.
  - Each VB/VB isolation valve pair has dedicated sensors and logic. Each VB isolation valve operates independently of the other VB isolation valves according to input received from its sensors. Logic is processed for each individual isolation valve; failure of the logic for one isolation valve does not affect the logic for any other isolation valve.
- Manual Operation
  - Manual controls are available to the operator in the MCR to:
    - Open each VB isolation valve, and
    - Close each VB isolation valve.

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)(H.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

- ~~□ 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

~~inside containment~~ is tested during [reactor operation to support VBIV stroke testing as specified in Table 3.9-8 and Subsection 6.2.1.1.5](#)~~refueling outages~~. Refer to Subsection 6.2.1.1.5 for a discussion of mechanical tests performed on the VB isolation functions.

### 7.3.6.5 Instrumentation and Control Requirements

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

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

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

### 7.3.7 COL Information

None

### 7.3.8 References

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

## 7.4 SAFETY-RELATED SAFE SHUTDOWN AND NONSAFETY-RELATED COLD SHUTDOWN SYSTEMS

In accordance with the Standard Review Plan, this section describes "...those instrumentation and control (I&C) systems used to achieve and maintain a safe shutdown condition of the plant." However, some I&C systems performing cold shutdown functions are not safety-related. This is justified by the existence of safety-related systems (Isolation Condenser System [ICS], Gravity-Driven Cooling System [GDCS], Standby Liquid Control [SLC] system, and Passive Containment Cooling System [PCCS]) that use natural circulation in the performance of their shutdown functions. Additionally, some safety-related criteria, such as provision of redundant trains and protection against single failures, are implemented in the design of the nonsafety-related systems. Consequently, safety-related and nonsafety-related systems performing safe shutdown or cold shutdown functions, respectively, are addressed in this section.

### 7.4.1 Standby Liquid Control System

#### 7.4.1.1 System Design Bases

The SLC system design bases are presented within Subsection 9.3.5 (~~IEEE Std. 603, Sections 4.1, 4.2, 4.5, 4.8, and 4.10~~).

The I&C for the SLC support the passive system capability requirements to perform the following.

- Provide a diverse, backup means to shut down the reactor from full power to a subcritical condition, using soluble boron injection, and maintain the reactor subcritical while it is brought to a cold shutdown condition. SLC system logic provides manual initiation capability in the Main Control Room (MCR), to satisfy the diverse shutdown requirements, and is independent of normal reactivity control provisions.
- Provide system actuation upon receipt of manual and automatic initiation signals in response to either Anticipated Transients Without Scram (ATWS) events, or design basis events (DBE) requiring Emergency Core Cooling System (ECCS) operation.

Four divisions of safety-related sense and command logic are used for automatic SLC initiation and for automatic SLC accumulator isolation. Redundant SLC accumulator level and pressure instrumentation is provided to monitor system performance and to ensure reliable logic processing. Valve position indication and continuity monitoring of the SLC squib injection valves are provided to ensure availability.

Safety-related SLC system components are designed for the environmental conditions applicable to their location. Safety-related SLC system components are also designed to preclude adverse interaction from nonsafety-related portions of the system.

The SLC design bases are discussed further within Subsection 9.3.5, and Figure 9.3-1 shows the basic configuration. DBE mitigation crediting the SLC system is discussed in Chapter 15, "Safety Analyses." (~~IEEE Std. 603, Sections 4.1, 4.2, 4.5, 4.8, and 4.10~~).

The SLC system initiation function is part of a group of systems 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.~~ ~~Th~~[ese](#) diagrams ~~indicates~~ the relationships of the SLC system with its safety-related peers, and with nonsafety-related plant data systems collectively called the Nonsafety-Related distributed Control and Information System (N-DCIS). Section 7.1 contains a description of these relationships.

#### 7.4.1.2 System Description

A detailed system description is given in Subsection 9.3.5.2. The I&C of the SLC system are described below. The safety-related SLC system provides diverse backup capability for reactor shutdown, which is independent of the Reactor Protection System (RPS). For the reactor shutdown function, the SLC system is manually initiated from the MCR by using dual, key-locked control switches. Parameters such as neutron flux, reactor vessel pressure and level, and control rod position are available to the operator in the MCR to assess the need for manual SLC initiation. Additionally, accumulator pressure and solution level, as well as squib injection valve and shut-off valve status indication, are provided in the MCR to monitor the operating and performance status of the SLC system. ~~(IEEE Std. 603, Section 4.5)~~

The SLC system is initiated automatically as part of the ECCS, to mitigate Loss-of-Coolant-Accident (LOCA) events. The SLC system receives an actuation command 50 seconds after a confirmed LOCA. The SLC actuation sequence corresponds to the first Depressurization Valve (DPV) actuation (as described in the Automatic Depressurization System [ADS] logic discussion in Subsection 7.3.1.1). The SLC system also receives a diverse ECCS initiation signal from the Diverse Protection System (DPS).

The SLC system also starts automatically on an ATWS mitigation signal persisting for 180 seconds. The ATWS mitigation (ATWS/SLC) logic performs the diverse emergency shutdown function (in compliance with the requirements of 10 CFR 50.62). ATWS/SLC logic is described in Section 7.8.1, Diverse I&C Systems, and is depicted on Figure 7.8-3, ATWS Mitigation Logic (SLC System Initiation, Feedwater Runback).

The ATWS/SLC logic uses sensors, hardware, and software platforms diverse from the Safety System Logic and Control/Engineered Safety Features (SSL/ESF), RPS, and DPS hardware/software platforms.

To avoid reducing boron concentration during SLC operation, the SLC system logic transmits an isolation signal to the Reactor Water Clean-Up/Shutdown Cooling System (RWCUS/SDC) via the Leak Detection and Isolation System (LD&IS).

To avoid the injection of nitrogen into the Reactor Pressure Vessel (RPV) System, four divisional, safety-related level sensors per SLC accumulator are used to provide automatic isolation of series accumulator shut-off valves on (a voted two-out-of-four) low accumulator level. The SLC system processors of the ATWS/SLC mitigation logic platform perform the shut-off valve isolation logic.

Accumulator temperature, solution level, and accumulator pressure are indicated locally inside the accumulator room.

Boron injection and shut-off valve position status are provided in the MCR.

#### 7.4.1.2.1 Power Sources

Power for the safety functions of the SLC system is derived from safety-related 120 VAC Uninterruptible Power Supplies (UPS) (see Subsection 8.3.1.1.3). Divisional assignments are made to ensure the availability of each SLC system loop, assuming one safety-related division of power is not in service in addition to a single active failure. Additionally, a squib initiator in each loop is activated by the DPS as part of the diversity and defense-in-depth strategy (described in Subsection 7.8.1.2). To avoid adverse interaction, electrical isolation is maintained between the safety-related divisions, and between the safety-related divisions and the DPS ~~(IEEE Std. 603, Sections 5.12, 8.1, and 8.2).~~

#### 7.4.1.2.2 Control Functions

There are four control functions for the SLC system.

- The firing signals to the squib initiators originate from SSLC/ESF for the ECCS injection function, from ATWS/SLC for the ATWS mitigation function, and from manual control switches in the MCR. Successful firing of either or both squib valves in each SLC system loop assures completion of the SLC system operation. ~~(IEEE Std. 603, Section 5.2).~~
- An open signal is provided to the normally open accumulator shut-off valves to support the ECCS injection function. Control logic also is provided for automatic closure of the shut-off valves. Shut-off valve isolation occurs automatically on a two-out-of-four low-level logic, using the safety-related accumulator level instrumentation. Closure signals to the redundant, fail-as-is shut-off valves ensure that at least one valve closes, to prevent nitrogen entry into the RPV.
- Control logic also is provided for manual venting of the accumulators. This function is not safety-related. Serial solenoid valves in each vent line may be actuated by respective manual switches in the MCR.
- Automatic nitrogen makeup to the accumulators is provided to accommodate slow long-term leakage from the system. This makeup function only is required to maintain accumulator pressure. It is not required to assure full solution injection and therefore, is not safety-related.

#### 7.4.1.3 Safety Evaluation

The safety evaluation for the mechanical aspects of the SLC system is presented in Subsection 9.3.5.3 ~~(IEEE Std. 603, Section 4.8)~~. The SLC I&C are capable of performing their intended safety-related functions based on the following design features. The safety-related SLC I&C are designed to operate under the environmental conditions anticipated at their equipment

locations ~~(IEEE Std. 603, Section 5.4)~~. Inter-division communication (and communication with nonsafety-related interfaces) occurs through qualified isolation devices ~~(IEEE Std. 603, Section 5.6)~~. Isolated ECCS initiation signals, as well as isolated ATWS mitigation signals from the DPS, are transmitted to the SLC squib injection valves to provide defense against a common mode software failure of the SSLC/ESF logic platform (discussed in Section 7.8).

The only automatic actuation logic originating from within the SLC system logic processors transmits the low accumulator-level isolation signals for the accumulator shut-off valves, and the RWCU/SDC isolation signal via the LD&IS on SLC system injection. The SLC logic processors are separate components of the diverse ATWS/SLC mitigation logic platform.

Redundant divisions of voting logic enable the SLC system to perform its safety-related function with one division removed from service coincident with a single failure ~~(IEEE Std. 603, Section 5.1)~~. Division of sensors bypass capability allows a safety-related SLC sensor to be removed from service, while maintaining a high level of reliability ~~(IEEE Std. 603, Section 5.7, 6.5, and 6.7)~~. Alarmed indication of the bypass condition provides off-normal condition status monitoring ~~(IEEE Std. 603, Section 5.8)~~. With an SLC accumulator-level sensor removed from service, the shut-off valve voting logic changes from two-out-of-four to two-out-of-three. Redundant signals are used to confirm the demand for squib injection valve operation. Three load drivers in series are provided to avoid spurious operation of the squib valves. Alarmed, disable switches are provided to allow removal of a squib valve initiator and associated control circuit from service, and to protect against spurious operation while performing maintenance. Continuity monitoring of the squib injection valve circuitry is provided to confirm availability automatically. Position indication for the SLC system valves also is provided to determine system configuration.

Manual SLC system initiation requires operation of dual control switches, with each switch requiring two distinct operator actions. The manual SLC system switches are protected by key-locks to minimize the likelihood of inadvertent operation.

In addition to squib injection valve continuity monitoring, status indication of squib injection and accumulator shut-off valves, accumulator level and pressure indication, and alarms are provided to allow monitoring of SLC accumulator standby status.

The SLC system also conforms to the applicable general requirements for safety-related systems presented in Chapter 3.

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

#### 7.4.1.3.1 Code of Federal Regulations

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

- Conformance: The SLC system design conforms to these standards.

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

injection to occur. Only one squib valve actuation in each loop is required for injection to occur. If one of the valves in each loop actuates with the system in its normal operating configuration, and critical system parameters (accumulator level and pressure) are within their normal ranges, injection would occur. Testing of the squib injection and accumulator shut-off valve logic is performed periodically to verify operability.

Routine testing, monitoring of critical system parameters, and surveillances ensure operability with an acceptably low probability of demand failure ~~(IEEE Std. 603, Section 5.7)~~.

#### **7.4.1.5 Instrumentation and Control Requirements**

Status indications of full-open or full-closed valve positions are provided for the key valves in the SLC system, such as the squib injection valves and the accumulator shut-off valves. An open indication for these valves is required to ensure SLC system operation ~~(IEEE Std. 603, Section 5.8)~~.

Pressure-level and solution-level alarms and indications for each accumulator ~~(IEEE Std. 603, Section 5.8)~~ are provided in the MCR to:

- Ensure operability of the system;
- Warn the operator of an out-of-tolerance level or pressure condition; and
- Provide verification of proper system operation after initiation.

The measurements are redundant to minimize vulnerability to instrument or indicator failure. The level instrumentation for each accumulator is quadruple redundant to support the two-out-of-four initiation logic for closure of the shut-off valve. The pressure indications and alarms are dual redundant and the signals from both channels are needed before adding nitrogen to an accumulator. These instruments also provide local level and pressure indication.

Local indication and MCR alarms are provided for the nitrogen gas and neutron poison solution makeup. The low-level alarms are set to provide adequate time for recharging the manually operated nitrogen and sodium pentaborate solution supply systems.

### **7.4.2 Remote Shutdown System**

#### **7.4.2.1 System Design Bases**

The safety-related Remote Shutdown System (RSS) is used to provide operators with the means to safely shut down the reactor from a place outside the MCR if it becomes uninhabitable. The RSS provides remote control of the systems needed to bring the reactor to a hot shutdown after a scram. The RSS also provides the subsequent capability to bring the plant to (and maintain) a cold shutdown condition.

### 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.~~ [These diagrams indicate 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.

#### 7.4.2.2.2 Operating Conditions

The following conditions are assumed coincident with the event necessitating evacuation of the MCR and transfer of operation to the RSS panel ~~(IEEE Std. 603, Sections 4.1, 4.2, and 4.5).~~

- The plant is operating under normal conditions and at less than or equal to rated power. No Anticipated Operational Occurrence (AOO), seismic event, or other abnormal plant condition except for loss of off-site power is assumed.
- The RSS panel is powered from buses supplied by uninterruptible safety-related and nonsafety-related 120 VAC systems.
- The reactor operator can either manually scram the reactor before leaving the MCR, or use the manual scram switches on the RSS panel.
- Plant personnel have evacuated the MCR.
- The reactor operator can isolate the main steam lines by closing the manual Main Steam Isolation Valve (MSIV) isolation switches from the RSS.
- The reactor feedwater system, which is normally available, is conservatively assumed to be inoperable.
- The initiating event is assumed not to cause failure of the Alternating Current (AC) control power supplies to the RSS panel, or failure of the power feeds to equipment functionally controlled from the RSS panel. This assumption is justified because the power feeds to the RSS do not pass through the MCR.

#### 7.4.2.2.3 System Operation

When evacuation of the MCR is necessary, the reactor is manually scrammed. If there has been no loss of off-site power, the turbine bypass valves automatically control reactor pressure, and the reactor feedwater system automatically maintains RPV water level. With these functions operable (and they should remain operable through the MCR evacuation), reactor cooldown is achieved through the normal heat sinks. This cooldown process can be supplemented from the RSS panel using the RWCU/SDC system. The RWCU/SDC system provides the capability to bring the reactor from a high-pressure condition to cold shutdown. Control of both RWCU/SDC trains is provided on the RSS panel. The Reactor Component Cooling Water System (RCCWS) is aligned to provide cooling water to the RWCU/SDC non-regenerative heat exchangers, and the Plant Service Water System (PSWS) is aligned to cool the RCCW heat exchangers. Control of two RCCW trains and two PSWS trains is provided on the RSS panel.

However, if the reactor feedwater system is not available due to loss of off-site power, as postulated in the first bullet of Subsection 7.4.2.2.2 Operating Conditions, control of the Control Rod Drive (CRD) system from the RSS may be utilized. Control of the high-pressure makeup injection capability of the CRD system ensures that the RPV water level remains above the ADS trip setpoint and above the elevation of the RWCU/SDC mid-vessel suction line nozzle. If main steam line isolation automatically occurs, or is manually initiated from the RSS, the ICS automatically controls reactor pressure. Because the logic processing equipment for the ICS (or

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.

#### 7.4.3.5 Instrumentation and Control Requirements

Operation of the RWCU/SDC system is from the MCR. The main I&C available to the MCR operator includes:

- Manual and automatic flow controllers for system, demineralizer, and overboarding flow;
- Flow indications for system, demineralizer, and overboarding flow;
- Position indications for containment isolation valves, flow control valves, and motor-operated valves;
- Temperature indication for demineralizer influent water;
- Conductivity recorders for demineralizer influent and effluent;
- Temperature of the system supply water (from the RPV bottom head);
- Temperature of the system return (to feedwater line) water;
- Temperatures of the non-regenerative and regenerative heat exchanger water (reactor coolant sides);
- Process alarms (for example, high water temperatures, high overboarding line pressure, low system flow, high system flow, high conductivity, etc.); and
- Pressure indication for the overboarding line.

### 7.4.4 Isolation Condenser System

#### 7.4.4.1 System Design Bases

Refer to Subsection 5.4.6.1 for the design bases of the ICS (~~IEEE Std. 603, Sections 4.1 and 4.2~~). Figure 5.1-3 shows the basic configuration of the ICS.

The ICS is one of the ESF systems whose I&C belong to a group of systems collectively called the 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~~. ~~Th~~ese diagrams indicates the relationships of the ICS with its safety-related peers, and with nonsafety-related plant data systems collectively called the N-DCIS. Section 7.1 contains a description of these relationships.

#### 7.4.4.2 System Description

Refer to Subsection 5.4.6.2 for the ICS system description.

#### 7.4.4.3 Safety Evaluation

Conformance of ICS equipment to the requirements of IEEE Std. 603 (other than I&C) is addressed in Subsections 5.4.6.2 and 5.4.6.3. The paragraph on “Isolation Condenser Operation”

- 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)

continuously displayed. The channels are equipped with upscale alarms to indicate high radiation and an alarm to indicate channel malfunction.

- MCR alarms are provided for indications of high radiation dose rates, inoperative radiation monitors, high oxygen concentration levels, high hydrogen concentration levels, and abnormal samples for each subsystem.
- Each gas sampling rack is provided with its own gas calibration sources of known concentration levels to calibrate periodically the oxygen and hydrogen analyzers and the sensors.
- The lower drywell water level is monitored to indicate any increases in water level that may occur in the lower drywell following a LOCA condition.
- The upper drywell water level is also monitored and compared with the RPV nozzle elevations.
- The drywell and wetwell pressure instrumentation is located throughout the containment and provides safety-related and nonsafety-related functions for both normal and post-accident monitoring, including drywell pressure inputs for reactor scram protection monitoring. In addition, pressure signals are provided to the Diverse Protection System (DPS) for diverse scram protection monitoring.

MCR alarms and indication are provided for suppression pool temperature monitoring as discussed in Subsection 7.2.3.

### 7.5.2.2 System Description

<p>The CMS is a divisionalized and segregated (safety/nonsafety-related) monitoring system (<del>IEEE Std. 603, Section 5-6</del>), and is configured as shown in Figure 7.5-1. The specific system features are as follows.</p>	
--	--

- Radiation monitoring and gas H<sub>2</sub>/O<sub>2</sub> sampling are provided for the drywell and for the airspace above the suppression pool.
- Each radiation monitoring channel uses one gamma-sensitive ion chamber and one digital log radiation monitor. Four channels are provided, two for the drywell and two for the suppression pool (wetwell) airspace.
- During normal plant operation, both the radiation monitoring and gas sampling subsystems are operating. For post-accident monitoring, the gas sampling subsystem is automatically activated by the LOCA signal to alternate its sampling between the drywell and the wetwell. The area of sampling can be selected manually or sequentially controlled.
- Heat tracing is provided on the gas sampling lines for control of moisture and condensation.

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.

- 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;~~

### 7.7.2.2.7.3 Establishment of RRPS

The RRPS is normally established before plant startup and stored in the memory of the N-DCIS equipment and the RC&IS. The N-DCIS and RC&IS allow modifications to be made to the RRPS through operator actions. The N-DCIS provides compliance verification of the proposed changes to the RRPS with the ganged withdrawal sequence requirements.

The RC&IS provides the capability for an operator to request a download of the RRPS from the N-DCIS. The new RRPS data are loaded into the RAPI. Download of the new RRPS data can only be completed when the RC&IS is in manual rod movement mode and when a permissive switch located at the RAPI-A panel is activated. The RC&IS provides feedback signals to the N-DCIS to confirm a successful download of the RRPS data.

Rod withdrawal block signals are generated whenever selected single or ganged rod movements differ from those allowed by the RRPS. The RC&IS can either be in the automatic or semi-automatic rod movement mode. The RC&IS provides for activation of an alarm at the operator's panel for an RRPS violation.

### 7.7.2.2.7.4 Rod Block Function

The rod block logic of the RC&IS, upon receipt of input signals from other systems and internal RC&IS subsystems, inhibits movement of control rods. In most cases, only a rod withdrawal block is activated. However, the RWM can also activate a rod insertion block for enforcement of the GWSR.

Rod block signals to the RC&IS from safety-related systems are appropriately isolated. This provides required isolation between safety-related and nonsafety-related systems while preventing electrical failures from propagating into the safety-related systems ~~(IEEE Std. 603, Subsection 5.6.3)~~.

The presence of any rod block signal, in either channel or both channels of the RC&IS logic, causes automatic changeover from automatic mode to manual mode. The automatic rod movement mode can be restored by taking the appropriate action to clear the rod block and by using the RC&IS mode switch to restore the automatic rod movement mode.

If either channel or both channels of the RC&IS logic receives a signal from any of the following type of conditions, a rod block is initiated. These conditions are:

- Rod separation detection (rod withdrawal block only for those selected rod(s) for which the separation condition is detected and for which the rods are not in the Inoperable Bypass condition, applicable when the RPS Reactor Mode Switch is in the Startup or Run position);
- Reactor Mode Switch in Shutdown position (rod withdrawal block for all control rods, applicable when the RPS Reactor Mode Switch is in the Shutdown position);
- SRNM withdrawal block (rod withdrawal block for all control rods, not applicable when the RPS Reactor Mode Switch is in the Run position);
- APRM withdrawal block (rod withdrawal block for all control rods);

- Latched full-in and full-in position reed switches (discrete signal; these two reed switches are wired in parallel);
- Buffer contact reed switch (discrete signal); and
- Scram timing position reed switches (discrete signals) at the following positions:
  - 0% insertion,
  - 10% insertion,
  - 40% insertion,
  - 60% insertion, and
  - 100% insertion.

The induction motor controllers provide the proper 3-phase power to the FMCRD motor, the directly associated MBB, and the holding brakes of the CRD system to accomplish the RC&IS rod movement functions.

The RC&IS does not directly interface with any other basic plant instrumentation. The other inputs to the RC&IS are by hardwired signal interfaces, data communication links with other systems, or from the RC&IS dedicated operator interface.

### 7.7.3 Feedwater Control System

The FWCS accomplishes both RPV water level control and FW temperature control. RPV water level control is accomplished by manipulating the speed of the FW pumps. FW temperature control is accomplished by manipulating the heating steam flow to the seventh stage FW heaters or directing a portion of the FW flow around the high-pressure FW heaters. The two functions are performed by two sets of triple redundant fault tolerant digital controllers (FTDCs) located in separate cabinets. Each set of FTDCs is dedicated to perform one function. The ESBWR HP FW Heater Temperature Control Diagram is provided in Figure 7.7-7.

#### 7.7.3.1 System Design Bases

##### 7.7.3.1.1 Safety-Related Design Bases

The FWCS is not a safety-related system and is not required for safe shutdown of the plant. Therefore, the FWCS has no safety-related design basis. In the power operation mode, only one of the triple redundant controllers can be removed from service. Refer to Subsection 7.3.3 (the LD&IS) for FW line isolation protections.

##### 7.7.3.1.2 Power Generation (Nonsafety) Design Bases

The FWCS is designed so that the functional capabilities of safety-related systems are not inhibited (~~IEEE Std. 603, Subsection 5.6.3~~). The FWCS regulates the flow of FW into the RPV to maintain predetermined water level limits during transients and normal plant operating modes; additionally the FWCS controls FW temperature to allow reactor power control without moving

## 7.7.4 Plant Automation System

### 7.7.4.1 System Design Bases

#### 7.7.4.1.1 Safety Design Bases

The PAS has no safety-related design basis, but is designed so that the functional capabilities of safety-related systems are not hindered. Abnormal events requiring control rod scrams are sensed and controlled by the safety-related RPS, which is fully independent of the PAS. Discussions of the RPS are provided in Subsection 7.2.1.

The PAS provides the capability for supervisory control of the entire plant. It does this by supplying setpoint commands to independent nonsafety-related automatic control systems as changing load demands and plant conditions dictate.

#### 7.7.4.1.2 Power Generation (Non-Safety) Design Bases

The power generation basis of this system is to provide supervisory control that regulates reactivity during criticality control, provides heatup and pressurization control, regulates reactor power, controls turbine/generator output, controls secondary nonsafety-related systems, and provides reactor startup / shutdown controls.

### 7.7.4.2 System Description

The primary purposes of the PAS are reactivity control, heatup and pressurization control, reactor power control, generator power control (MWe control), and plant shutdown control. The PAS consists of triple redundant process controllers. The functions of the PAS are accomplished by suitable algorithms for different phases of reactor operation which include approach to criticality, heatup, reactor power increase, automatic load following, reactor power decrease, and shutdown. The N-DCIS accepts one-way communication from the Q-DCIS so that the safety-related information can be monitored, archived, and alarmed seamlessly with the N-DCIS data (IEEE Std. 603, Subsection 5.6.3).

Through the N-DCIS, the PAS receives input from the following major safety-related systems: NMS (Subsection 7.2.2) and the RPS (Subsection 7.2.1). Through the N-DCIS, the PAS receives input from the following major nonsafety-related systems: the RC&IS (Subsection 7.7.2), SB&PC System (Subsection 7.7.5), FWCS (Subsection 7.7.3), RWCU/SDC (Subsection 7.4.3), and the Turbine Generator Control System (TGCS) (Subsection 10.2.2). The output demand request signals from the PAS are sent to the RC&IS to position the control rods, to the SB&CS for pressure setpoints, and to the TGCS for load following operation. A simplified functional block diagram of the PAS is provided in Figure 7.7-4.

The PAS interfaces with the operator's control console to perform its designed functions. From the operator's control console for automatic plant startup, power operation, and shutdown functions, the operator uses the PAS to issue supervisory control commands to nonsafety-related systems. The operator also uses the PAS to adjust setpoints of lower level controllers to support automation of the normal plant startup, shutdown, and power range operations. In the automatic mode, the PAS also issues command signals to the turbine master controller, which contains

### 7.7.5.1.2 Power Generation (Non-safety) Design Bases

The SB&PC System is designed so that the functional capabilities of safety-related systems are not inhibited ~~(IEEE Std. 603, Subsection 5.6.3)~~. The SB&PC System is required for the power generation cycle because it controls reactor pressure during plant startup, power generation, and shutdown modes of operation.

The design objective is to enable a fast and stable response to system pressure disturbances, and to pressure setpoint changes over the operating range. This is done using Turbine Control Valves (TCVs) through the TGCS and Turbine Bypass Valves (TBVs) for controlling reactor pressure. In addition, the design objective of the SB&PC System is to discharge reactor steam directly to the main condenser in order to regulate reactor pressure whenever the turbine cannot use all of the steam generated by the reactor.

### 7.7.5.2 System Description

#### 7.7.5.2.1 General Description

The purpose of the SB&PC System is to control reactor pressure during plant startup, power generation, and shutdown modes of operation. The SB&PC System is implemented on triple redundant FTDCs. Power supplies and input/output signals are redundant. The controller is designed for a MTTF of no less than 1000 years. Control of reactor pressure is accomplished through control of the TCVs through the TGCS and TBVs, so that susceptibility to reactor trip, turbine-generator trip, main steam isolation, and safety relief valve opening is minimized. Triple redundant FTDCs using feedback signals from RPV dome pressure sensors generate command signals for the TBVs and pressure regulation demand signals used by the TGCS to generate demand signals for the TCVs. For normal operation, the TCVs regulate reactor pressure. However, whenever the total steam flow demand from the SB&PC System exceeds the effective TCV steam flow demand, the SB&PC System sends the excess steam flow directly to the main condenser through the TBVs.

The ability of the plant to load follow the grid system demands is accomplished by the aid of control rod actions. In response to the resulting steam production demand changes, the SB&PC System adjusts the demand signals sent to the TGCS so that the TGCS adjusts the TCVs to accept the control steam output change, thereby controlling pressure.

Controls and valves are designed so that steam flow is shut off when control system electrical power or hydraulic system pressure is lost.

Refer to Figure 7.7-5, SB&PC System Simplified Functional Block Diagram, and Figure 7.7-6, SB&PC System FTDC Block Diagram for an overview of SB&PC System functions and interfaces. Additional information is provided in Table 7.7-1, "Major Plant Automation System Interfaces".

#### 7.7.5.2.2 Normal Plant Operation

At steady-state plant operation, the SB&PC System maintains RPV pressure at a set value, to ensure optimum plant performance. During normal operational plant maneuvers (pressure

- 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.

the design description defines the important design feature/performance that merits Tier 1 treatment whereas the acceptance criterion defines a measurement standard for determining if the as-built facility is in compliance with the Tier 1 design description commitment. NRC guidance in NUREG-0800, Section 14.3, states the following regarding acceptance criteria:

In general, the acceptance criteria should be objective and unambiguous. In some cases, the acceptance criteria may be more general because the detailed supporting information in Tier 2 does not lend itself to concise verification. For example, the acceptance criteria for the design integrity of piping and structures may be that a report “exists” that concludes the design commitments are met. In these cases, Tier 2 provides the detailed supporting information on multiple interdependent parameters that should be provided in order to demonstrate that a satisfactory report exists.

Numeric performance values for SSCs are specified as ITAAC acceptance criteria when values consistent with the design commitments are possible, or when failure to meet the stated acceptance criterion would clearly indicate a failure to properly implement the design or meet the safety analysis.

Where appropriate, Tier 2 has identified detailed criteria applicable to the same design feature or function that is the subject of more general acceptance criteria in the ITAAC table.

For numerical acceptance criteria, ranges and/or tolerances are generally included. This is necessary and acceptable because:

- Specification of a single-value acceptance criterion is impractical because minute/trivial deviations would represent noncompliance;
- Tolerances recognize that legitimate site variations can occur in complex construction projects; and
- Minor variations in plant parameters within the tolerance bounds have no effect on plant safety.

The Acceptance Criteria column specifies that a report documents the successful completion of the ITAAC verification. This is generally intended to represent the front material (e.g., a form) that would be included in an ITAAC closure package to summarize completion of the ITAAC. All supporting information would be referenced in such a report and be included in the closure package or the location specified in the report. The “report” may be a simple form that consolidates all of the necessary information related to the verification package for supporting successful completion of the ITAAC.

#### [14.3.2.3 Safety-Related System Compliance with 10CFR 50.55a\(h\), IEEE Std. 603 Criteria](#)

[IEEE Std. 603 establishes the minimum functional and design requirements for the power, instrumentation, and control portions of safety systems. ESBWR divides safety systems into two parts: the Q-DCIS platforms, and the associated functional systems that contain the sensors and actuators used by the Q-DCIS platforms.](#)

[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 shows 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.

Demonstration of compliance with IEEE Std. 603 means the Q-DCIS documentation include design bases that make appropriate reference to IEEE Std. 603 design criteria and that the resulting as-built equipment has been inspected, tested, or analyzed to show that the Q-DCIS will be capable of performing in accordance with the design bases. The choice of whether an inspection, test, or analysis is required to close a particular ITAAC is defined in the documentation associated with the {{Design Acceptance Criteria}} ITAAC closure report for the software project.

IEEE Std. 603 divides the Q-DCIS into three features: sense, command, and execute features. Sense features comprise sensors. Command features comprise the Q-DCIS platforms. Execute features comprise actuators. Each of these features is treated differently within Tier 1 because of influences outside of the scope of IEEE Std. 603. As a result of these differences, Table 14.3-3 was developed to group the software projects with their associated functional system(s), if any.

As a result of these differences, Table 14.3-3 was developed to group the software projects with their associated functional system(s), if any, and to define how the various IEEE Std. 603 criteria will be demonstrated by an ITAAC for each software project.

Table entries marked with an 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. Table entries marked with a 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 for the RTIF software project will demonstrate compliance to IEEE Std. 603 criterion 5.1 for RPS, LD&IS, CMS-SPTM, MSIV, NBS, and CRD. The report(s) may be referenced or attached to a software project baseline review record (BRR, reference Subsection 3.2) to close the Table 2.2.15-2 ITAAC.

Table headings contain the software project or the functional system identifier and a parenthetical reference to the section or subsection where additional information about the software project or functional system can be found. These parenthetical references are reverse references that point back to the originating system. The IEEE Std. 603 criteria apply only to those structures, systems, or components (SSC) directly associated with the performance of the safety-related function of the software project. Complete lists of applicable SSC and functions are defined in the documentation associated with the {{Design Acceptance Criteria}} ITAAC closure report for each software project in response to ITAAC defined in Subsection 14.3.3.2. These lists along with the information in the tables associated with a software project or functional system in each column define the scope of the IEEE Std. 603 ITAAC.

Refer to DCD Tier 1, Sections 3.2, 3.3, 3.6, 3.7, and 3.8, as described, for ITAAC associated with the IEEE Std. 603 criteria that do not appear in Table 14.3-3.

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 software project 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 consideration of the effects that the associated sensors and actuators have on the performance of the safety-related function.

IEEE Std. 603, Criteria 4.2, 4.3, 4.10, 4.11, and 4.12, are not included in Tier 1 as ITAAC because NUREG 0800, Section 14.3.5, and RG 1.206, Section C.III-A, do not raise these criteria to the level required for inclusion into Tier 1 as ITAAC.

IEEE Std. 603, Criterion 5.3, Quality, requires that the Q-DCIS be of a quality that is 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. The QA for SSCs is addressed by a QA program and is not the subject of Tier 1 ITAAC.

Refer to DCD Tier 1, Section 3.2, for the ITAAC associated with the software plans that control the additional IEEE Std. 7-4.3.2 criteria related to the following hardware and software quality assurance requirements summarized from Section 7.1.6.6.1.4:

- a. 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).
- b. 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).
- c. 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).
- d. 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).
- e. 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).
- f. 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).

IEEE Std. 603, Criterion 5.4, Equipment Qualification, requires that the software project be 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. Refer to DCD Tier 1, Section 3.8, for the ITAAC associated with the environmental and seismic qualification process that demonstrates equipment qualification. Refer to DCD Tier 1, Section 3.2, for the ITAAC associated with the software plans that control the additional IEEE Std. 7-4.3.2 criteria related to the following hardware and software qualification requirements summarized from Section 7.1.6.6.1.5:

- a. IEEE Std. 7-4.3.2, Criterion 5.4.1, The software project 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 (STP).

- b. 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. 603, Criterion 5.5, System Integrity, requires that the software project'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. Refer to DCD Tier 1, Section 3.8, for the ITAAC associated with the environmental and seismic qualification process that demonstrates system integrity. Refer to DCD Tier 1, Section 3.2, for the ITAAC associated with the software plans that control the additional IEEE Std. 7-4.3.2 criteria related to the following hardware and software system integrity requirements summarized from Section 7.1.6.6.1.6:

- a. 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.
- b. 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.
- c. 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.

IEEE Std. 603, Criterion 5.8, Information Displays requires that information displays for the software project 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. Refer to DCD Tier 1, Section 3.3, for the ITAAC associated with the HFE process and refer to DCD Tier 1, Section 3.7, for the ITAAC associated with the post-accident monitoring design process.

IEEE Std. 7-4.3.2, Criterion 5.11, Identification requires that firmware and software be identified and retrievable using software maintenance tools. Refer to DCD Tier 1, Section 3.2, for the ITAAC associated with the software plans that control the identification and retrieval of software identification using software maintenance tools.

Criterion 5.13, Multi-Unit Stations: The multi-unit station criteria do not apply to the standard single unit plant design submitted for NRC certification.

Criterion 5.14, Human Factors Considerations: Human factors are incorporated in the design in accordance with the HFE design process described in DCD Tier 1, Section 3.3.

Criterion 5.15, Reliability: Analyses of the adequacy of the reliability of the software project design, including its software, are performed as part of the design reliability assurance program described in DCD Tier 1, Section 3.6.

[The remaining IEEE Std. 603 criteria not listed above appear as ITAAC in DCD Tier 1, Section 2.2.15, and are discussed in Subsection 7.1.6.6.1.](#)

### 14.3.3 Tier 1, Section 3 - Non-System Based Material

Tier 1 design descriptions and their associated ITAAC for design and construction activities that are applicable to more than one system are included in this section. Design related processes have been included in Tier 1 for:

Aspects of the ESBWR design likely to undergo rapid, beneficial technological developments in the lifetime of the design certification. Certifying the design processes associated with these areas of the design rather than specific design details permits future license applicants referencing the ESBWR design certification to take advantage of the best technology available at the time of a site-specific application and facility construction. Examples include design of programmable, microprocessor-based instrumentation and control systems.

- Aspects of the design that depend upon characteristics of as procured, as-installed systems, structures and components. These characteristics are not available at the time of certification, and therefore, cannot be used to develop and certify design details. Examples include design of piping systems that depend upon detailed routing and equipment information and equipment qualification.
- Thus, the material in Section 3 may be included because, in selected areas of the design, Tier 2 may not contain sufficient design detail. These ITAAC may represent what is commonly referred to as Design Acceptance Criteria. For these Design Acceptance Criteria, the Tier 1 ITAAC, combined with design information and appropriate design methodologies, codes, and standards provided in Tier 2, provide sufficient detail to provide an adequate basis for the NRC to make a final safety determination regarding the design, subject only to satisfactory design implementation and verification of the Design Acceptance Criteria ITAAC following completion of the Design Acceptance Criteria ITAAC. Design Acceptance Criteria also have confirmation ITAAC which ensure that the as-built plant conforms to the design Design Acceptance Criteria ITAAC.

Entries in this section of Tier 1 have the same structure as the system material discussed in Subsection 14.3.2; i.e., design description text and figures and a table of ITAAC entries. The objective of this Tier 1 material is to address selected design and construction activities, which are applicable to more than one system and cannot conveniently be covered in the system-by-system information presented in Tier 1, Section 2. Where appropriate, Tier 1 specifies that these non-system based ITAAC may be closed on a system-by-system basis for purposes of system turnover. However, the final ITAAC closure package must include verification that all of the systems were completed for that particular ITAAC.

The following summarizes the scope and bases for the Tier 1, Section 3 entries. For each, the design description text defines the applicability of the entry.

#### *14.3.3.1 Design of Piping Systems and Components*

The piping design section of Tier 1 defines the processes by which ESBWR piping is designed and evaluated. The material applies to piping systems that are classified as safety-related. In general, these piping systems are designated as Seismic Category I and are further classified as

**Table 14.3-3**  
**IEEE Std. 603 Criterion System Applicability Matrix**

Referencing Platform (1)(2)	RTIF-NMS Platform								SSLC/ESF Platform										ICP	
	RTIF							NMS											VBIF	ATWS/SLC
Table 2.2.15-2, Item No.	IEEE Std. 603 Criterion	RTIF (7.1.2, 14.3.3.2)	RPS (7.2.1)	LD&IS MSIV (7.3.3) [Note (4)]	CMS-SPTM (7.2.3)	NBS (7.2.1)	CRD (7.2.1)	NMS (7.2.2, 14.3.3.2)	SSLC/ESF (7.1.2, 14.3.3.2)	LD&IS non-MSIV (7.3.3) [Note (3)]	PRMS (7.5.3)	CMS non-SPTM (7.5.2) [Note (4)]	NBS (7.3.1)/ADS (N/A)	GDCS (7.3.1)	ICS (7.4.4)	SLC (7.4.1)	CBVS (7.3.4) [Note (5)]	CRD (7.7.2.2.2)	VB Isolation Function (7.3.6, 14.3.3.2)	ATWS/SLC (7.8.1, 14.3.3.2)
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 14.3-3**  
**IEEE Std. 603 Criterion System Applicability Matrix**

Table 2.2-15-2, Item No.	IEEE Std. 603 Criterion	RTIF-NMS Platform								SSLC/ESF Platform								ICP		
		RTIF							NMS									VBIF	ATWS/SLC	
		<a href="#">RTIF (7.1.2, 14.3.3.2)</a>	<a href="#">RPS (7.2.1)</a>	<a href="#">LD&amp;IS MSIV (7.3.3) [Note (4)]</a>	<a href="#">CMS-SPTM (7.2.3)</a>	<a href="#">NBS (7.2.1)</a>	<a href="#">CRD (7.2.1)</a>	<a href="#">NMS (7.2.2, 14.3.3.2)</a>	<a href="#">SSLC/ESF (7.1.2, 14.3.3.2)</a>	<a href="#">LD&amp;IS non-MSIV (7.3.3) [Note (3)]</a>	<a href="#">PRMS (7.5.3)</a>	<a href="#">CMS non-SPTM (7.5.2) [Note (4)]</a>	<a href="#">NBS (7.3.1)/ADS (N/A)</a>	<a href="#">GDSCS (7.3.1)</a>	<a href="#">ICS (7.4.4)</a>	<a href="#">SLC (7.4.1)</a>	<a href="#">CBVS (7.3.4) [Note (5)]</a>	<a href="#">CRD (7.7.2.2.2)</a>	<a href="#">VB Isolation Function (7.3.6, 14.3.3.2)</a>	<a href="#">ATWS/SLC (7.8.1, 14.3.3.2)</a>
<a href="#">18</a>	<a href="#">6.2 and 7.2</a>	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	R	R	
<a href="#">18</a>	<a href="#">6.4</a>	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	R	R	
<a href="#">19</a>	<a href="#">6.6 and 7.4</a>	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	R	R	
<a href="#">20</a>	<a href="#">6.7, 7.5, and 8.3</a>	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	R	R	
<a href="#">21</a>	<a href="#">6.8</a>	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	R	R	
<a href="#">22</a>	<a href="#">8.1</a>	R	C	C	C	C	C	R	R	C	C	C	C	C	C	C	C	R	R	
<a href="#">23</a>	<a href="#">8.2</a>	R	C	C	C	C	C	R	R	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