U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

OFFICE OF NUCLEAR REACTOR REGULATION

Appendix 7.1-A

Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety

The acceptance criteria and guidelines for instrumentation and control (I&C) systems important to safety are divided into four categories: (1) regulations including ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," (paragraph 50.55a(h) of 10 CFR 50), (2) the General Design Criteria (GDC) of 10 CFR 50 Appendix A, (3) regulatory guides (including endorsed industry codes and standards), and (4) branch technical positions (BTPs). An "applicability" statement describes how each criterion and guideline applies to the review of I&C systems. Conformance to the requirements of GDC 1 is evaluated in the review of Section 7.1 of the safety analysis report (SAR). Conformance to the remaining requirements of the GDC applicable to I&C systems is evaluated on a system basis in the review of Sections 7.2 through 7.9 of the SAR. Likewise, the degree of conformance to the guidelines provided in the SRP, regulatory guides, and industry codes and standards is evaluated on a system basis in the review of Sections 7.2 through 7.9 of the SAR. Where exceptions are taken to the guidance provided by regulatory guides, and endorsed industry codes and standards, they should be evaluated as a part of the review of the applicability of these criteria. The evaluation findings should be provided as a part of the review of Section 7.1 of the SAR, or the exception should be noted and a reference provided to the section where it is addressed.

Three Mile Island (TMI) action plan requirements for I&C system systems important to safety are imposed by 10 CFR 50.34(f) for applications approved after February 16, 1982. For operating reactors that had approved construction permits prior to February 16, 1982, the TMI action plan requirements were imposed by Generic Letters that required conformance with NUREG-0718, "Licensing Requirements for Pending Applications for Construction Permits and Manufacturing License," NUREG-0737, "Clarification of TMI

Action Plan Requirements," NUREG-0737 Supplement 1, "Clarification of TMI Action Plan Requirements — Requirements for Emergency Response Capability," and NUREG-0694, "TMI-Related Requirements for New Operating Reactor Licenses." This appendix identifies both the CFR and TMI action plan reference numbers for the TMI action plan requirements relevant to Chapter 7 of the SAR. The action plan references are given in brackets following the reference to the equivalent requirement of 10 CFR 50.34(f). This appendix presents specific acceptance criteria for Three Mile Island (TMI) action plan items; however, important context information is found in the concepts contained in the referenced reports.

Acceptance criteria and guidelines are not included herein when the primary review responsibility for these aspects of I&C systems are reviewed in accordance with sections other than SRP Chapter 7.

1. Regulations — 10 CFR 50 and 10 CFR 52

a. 50.55a(a)(1) Quality Standards for Systems Important to Safety

"Structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed."

Applicability — All I&C systems

Review Methods — The licensee should commit to conformance with the regulatory guides and standards referenced in Sections 7.1 through 7.9 and Chapter 7 Appendix A. The design should conform with all regulatory guides and standards committed to by the applicant/licensee.

b. 50.55a(h) (ANSI/IEEE Std 279)

Applicability — The protection systems: reactor trip system (RTS), engineered safety features actuation system (ESFAS), and supporting data communication systems. One part of ANSI/IEEE Std 279, section 4.7.2, “Isolation Devices,” applies to all I&C systems. Section 4.13, “Indication of Bypasses,” also applies to information systems important to safety.

Review Methods — Appendix 7.1-B provides guidance for evaluating conformance to the requirements of ANSI/IEEE Std 279, including the applicable regulatory guides. NRC staff will use the criteria of Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," which endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," in the evaluation of the design, reliability, qualification and testability of the power instrumentation control portions of safety related systems. Appendix 7.1-C provides guidance for evaluating conformance to the guidance of Reg. Guide 1.153.

c. 50.34(f)(2)(v) [TMI Action Plan Item I.D.3] Bypass and Inoperable Status Indication

"Provide for automatic indication of the bypassed and operable status of safety systems."

Applicability — The protection systems, RTS, ESFAS, information systems important to safety, interlock systems, and supporting data communication systems.

Review Methods — Review of compliance with 10 CFR 50.34(f)(2)(v) should address the following characteristics described in ANSI/IEEE Std 279 and IEEE Std 603. SRP Appendix 7.1-B and Appendix 7.1-C discuss methods for review of these characteristics.

	Location of Review Guidance	
Topic	**Appendix 7.1-B Item**	**Appendix 7.1-C Item**
Auxiliary features	6	17
Indication of bypasses	14	13
Control and protection system interaction	8	24

The evaluation of conformance with this requirement should be addressed in the review of Sections 7.2, 7.3, and 7.6 of the SAR. Bypass and inoperable status indication is required only for selected information system and interlock functions, as discussed in SRP Sections 7.5 and 7.6.

d. 50.34(f)(2)(xii) [TMI Action Plan Item II.E.1.2] Auxiliary Feedwater System Automatic Initiation and Flow Indication

"Provide automatic and manual auxiliary feedwater (AFW) system initiation, and provide auxiliary feedwater system flow indication in the control room. (Applicable to PWRs only)."

Applicability — ESFAS and information systems important to safety in pressurized water reactors (PWRs).

Review Methods — AFW initiation and flow indication should conform with the requirements applicable to the ESFAS and instrumentation systems. NUREG-0737 provides additional guidance on conformance with this requirement. The evaluation of conformance with this requirements should be addressed in the review of Section 7.3 and 7.5 of the SAR.

e. 50.34(f)(2)(xvii) [TMI Action Plan Item II.F.1] Accident Monitoring Instrumentation

"Provide instrumentation to measure, record and readout in the control room: (A) containment pressure, (B) containment water level, (C) containment hydrogen concentration, (D) containment radiation intensity (high level), and (E) noble gas effluents at all potential, accident release points. Provide for continuous sampling of radioactive iodines and particulates in gaseous effluents from all potential accident release points, and for onsite capability to analyze and measure these samples."

Applicability — Information systems important to safety.

Review Methods — The accident monitoring instrumentation functions required by 10 CFR 50.34(f)(2)(xvii) should be included in the information systems important to safety and reviewed in accordance with the review guidance provided in SAR Section 7.5. The evaluation of conformance with this requirement should be addressed in the review of Section 7.5 of the SAR.

f. 50.34(f)(2)(xviii) [TMI Action Plan Item II.F.2] Instrumentation for the Detection of Inadequate Core Cooling

"Provide instruments that provide in the control room an unambiguous indication of inadequate core cooling, such as primary coolant saturation meters in PWRs, and a suitable combination of signals from indicators of coolant level in the reactor vessel and in-core thermocouples in PWRs and BWRs."

Applicability — Information systems important to safety

Review Methods — Inadequate core cooling instrumentation functions should be included in the information systems important to safety and reviewed in accordance with the review guidance provided in SRP Section 7.5. Inadequate core cooling instrumentation should provide unambiguous indication of these conditions. It should provide the operator with sufficient information during accident situations to take planned manual actions, and to determine whether safety systems are operating properly. In addition, the instrumentation should also provide sufficient data for the operator to be able to evaluate the potential for core uncovery and gross breach of protective barriers, including the resultant release of radioactivity to the environment. NUREG-0737 provides additional guidance on conformance with this requirement. The evaluation of conformance with this requirement should be addressed in the review of Section 7.5 of the SAR.

g. 50.34(f)(2)(xiv) [TMI Action Plan Item II.E.4.2] Containment Isolation Systems

"Provide containment isolation systems that (A) ensure all non-essential systems are isolated automatically by the containment isolation system; (B) for each non-essential penetration (except instrument lines) have two isolation barriers in series; (C) do not result in reopening of the containment isolation valves on resetting of the isolation signal; (D) utilize a containment set point pressure for initiating containment isolation as low as is compatible with normal operation; and (E) include automatic closing on a high radiation signal for all systems that provide a path to the environs."

Applicability — ESFAS — note that item (B) is not included in the scope of HICB review.

Review Methods — The containment isolation functions of the ESFAS should be reviewed to confirm that the ESFAS automatically closes each isolation device on each nonessential penetration. Signal diversity should be provided for the containment isolation function. For plants with digital-computer based ESFAS, signal diversity can be confirmed by review of the licensee/applicant's defense-in-depth and diversity analysis.

Reopening of isolation valves should be performed on a valve-by-valve basis, or on a line-by-line basis, provided that electrical independence and the single-failure criterion for the ESFAS functions continue to be satisfied. Ganged reopening of containment isolation valves is not acceptable.

Draft Reg. Guide DG-1045 (the proposed revision 3 to Reg. Guide 1.105, "Instrument Setpoints for Safety Systems"), and BTP HICB-12 provide guidance on establishing and maintaining instrument setpoints. For isolation of nonessential containment penetrations, however, the trip setpoint should be established by adding measurement error terms to the highest pressure value expected during normal plant operations, rather than subtracting error terms from an accident analysis analytical limit. The setpoint should also be shown to be low enough to ensure protection system functions are actuated before analytical limits are reached. The pressure setpoint selected should be far enough above the maximum observed, or expected, pressure inside

containment during normal operation so that inadvertent containment isolation does not occur during normal operation from instrument drift or fluctuations due to the accuracy of the pressure sensor. The containment pressure history during normal operation should be used as a basis for arriving at an appropriate minimum pressure setpoint for initiating containment isolation. Applicants for new licenses should use pressure history data from similar plants that have operated for more than one year, if possible, to arrive at a minimum containment setpoint pressure.

Containment purge lines and other penetrations that provide a path to the environment should be isolated on a high radiation signal as one of the diverse isolation functions.

The review of these design provisions to address 10 CFR 50.34(f)(2)(xiv) should be addressed in the review of Section 7.3 of the SAR and should be coordinated with the Containment Systems and Severe Accident Branch (SCSB). NUREG-0737 provides additional guidance on conformance with these requirements.

h. 50.34(f)(2)(xix) [TMI Action Plan Item II.F.3] Instrument for Monitoring Plant Conditions Following Core Damage

"Provide instrumentation adequate for monitoring plant conditions following an accident that includes core damage."

Applicability — Information systems important to safety.

Review Methods — Instrumentation for monitoring plant conditions following core damage should be included in the information systems important to safety. There should be instrumentation of sufficient quantity, range, availability, and reliability to permit adequate monitoring of plant variables and systems during and after an accident. Sufficient information should be provided to the operator for (1) taking planned manual actions to shut the plant down safely; (2) determining whether the reactor trip, engineered safety feature systems, and manually initiated safety-related systems are performing their intended safety functions (i.e., reactivity control, core cooling, and maintaining reactor containment system (RCS) and containment integrity); and (3) determining the potential for causing a gross breach of the barriers to radioactivity release (i.e., fuel cladding). The evaluation of conformance with this requirement should be addressed in the review of Section 7.5 of the SAR.

i. 50.34(f)(2)(xx) [TMI Action Plan Item II.G.1] Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves

"Provide power supplies for pressurizer relief valves, block valves, and level indicators such that: (A) Level indicators are powered from vital buses, (B) motive and control power connections to the emergency power sources are through devices qualified in accordance with requirements applicable to systems important to safety, and (C) electric power is provided from emergency power sources. (Applicable to PWRs only)."

Applicability — Information systems important to safety in PWRs, and safe shutdown systems.

Review Methods — Pressurizer level indication, block valve position indication, and relief valve position indication should be supplied from a source of emergency power in the event of a loss of offsite power. The power supplies should conform with the guidance of NUREG-0737. The evaluation of conformance with this

requirement should be addressed in the review of Sections 7.4 and 7.5 of the SAR. The review of this requirement should be coordinated with the Electrical Engineering Branch (EELB).

j. 50.34(f)(2)(xxii) [TMI Action Plan Item II.K.2.9] Failure Mode and Effect Analysis of Integrated Control System

"Perform a failure modes and effects analysis of the integrated control system (ICS) to include consideration of failures and effects of input and output signals to the ICS. (Applicable to B&W-designed plants only)."

Applicability — Control systems in Babcock and Wilcox (B&W)-designed plants.

Review Methods — The recommendations of the generic failure modes and effects analysis described in BAW-1564, "Integrated Control System Reliability Analysis," should be incorporated into the design if this analysis applies to the plant. Otherwise a plant-specific failure mode and effect analysis should be conducted in accordance with NRC orders on B&W plants, and NUREG-0694. The evaluation of conformance with this requirement should be addressed in the review of Section 7.7 of the SAR.

k. 50.34(f)(2)(xxiii) [TMI Action Plan Item II.K.2.10] Anticipatory Trip on Loss of Main Feedwater or Turbine Trip

"Provide, as part of the reactor protection system, an anticipatory reactor trip that would be actuated on loss of main feedwater and on turbine trip. (Applicable to B&W-designed plants only)."

Applicability — RTS in B&W-designed plants.

Review Methods — The design should comply with the guidance of NUREG-0694 item II.K.1 and IEEE Std 279. Appendix 7.1-B item 6 and Appendix 7.1-C item 17 provide guidance on the review of auxiliary features such as anticipatory trips. The evaluation of conformance with this requirement should be addressed in the review of Section 7.2 of the SAR.

l. 50.34(f)(2)(xxiv) [TMI Action Plan Item II.K.3.23] Central Reactor Vessel Water Level Recording

"Provide the capability to record reactor vessel water level in one location on recorders that meet normal post-accident recording requirements. (Applicable to BWRs only)."

Applicability — Information systems important to safety in BWRs.

Review Methods — The capability should be provided to record water level over the range from the top of the vessel dome to the lowest pressure tap. This range of water level indication should be available in one location on recorders that meet normal post-accident recording requirements. The evaluation of conformance with this requirement should be addressed in the review of Section 7.5 of the SAR.

m. 50.62 Requirements for Reduction of Risk from Anticipated Transients without Scram

"(1) Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to

perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system. (2) Each pressurized water reactor manufactured by Combustion Engineering or by Babcock and Wilcox must have a diverse scram system from the sensor output to interruption of power to the control rods. This scram system must be designed to perform its function in a reliable manner and be independent from the existing reactor trip system (from sensor output to interruption of power to the control rods). (3) Each boiling water reactor must have an alternate rod injection (ARI) system that is diverse (from the reactor trip system) from sensor output to the final actuation device. The ARI system must have redundant scram air header exhaust valves. The ARI must be designed to perform its function in a reliable manner and be independent (from the existing reactor trip system) from sensor output to the final actuation device. (4) Each boiling water reactor must have a standby liquid control system (SLCS). The SLCS and its injection location must be designed to perform its function in a reliable manner. The SLCS initiation must be automatic and must be designed to perform its function in a reliable manner for plants granted a construction permit after July 26, 1984, and for plants granted a construction permit prior to July 26, 1984, that have already been designed and built to include this feature. (5) Each boiling water reactor must have equipment to trip the reactor coolant recirculating pumps automatically under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner."

Applicability — Systems and equipment used for mitigating ATWS events pursuant to the requirements of 10 CFR 50.62 and supporting data communication systems.

Review Methods — Section 7.8 provides guidance for the evaluation of conformance to the requirements of 10 CFR 50.62.

n. 52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

"An application for design certification must contain proposed technical resolutions of those unresolved safety issues and medium- and high-priority generic safety issues that are identified in the version of NUREG-0933 current on the date six months prior to application and that are technically relevant to the design."

Applicability — All I&C systems that are part of applications for design certification under 10 CFR 52, Subpart B, or combined licenses under 10 CFR 52, Subpart C.

Review Methods — The design must address the unresolved and generic safety issues applicable to I&C systems as discussed above. As of April 1, 1997, these items are the following:

1. Task Action Plan Items

A-9	ATWS. Refer to Section 7.8.
A-24	Qualification of Class 1E safety equipment. Refer to SRP Chapter 3, Appendix 7.1-B item 5, and Appendix 7.1-C item 9.
A-47	Safety implications of control systems. Refer to resolution of Generic Letter 89-19.

2. Generic Issues

3	Setpoint drift in instrumentation. Refer to Draft Reg. Guide DG-1045 and BTP HICB-12.
45	Inoperability of instrumentation due to extreme cold weather. Refer to Reg. Guide 1.151, "Instrument Sensing Lines."
48	Limiting conditions for operation for Class 1E vital instrument buses in operating reactors. Refer to plant technical specification review in Chapter 16.
64	Identification of protection system instrument sensing lines. Refer to Appendix 7.1-B item 22, Appendix 7.1-C item 16, and Reg. Guide 1.151.
67.3.3	Improved accident monitoring. Refer to Reg. Guide 1.97 review in Section 7.5, BTP HICB-10 and 10 CFR 50.34 (f)(2)(xvii) and (xix) review.
75	Generic implications of ATWS events at Salem Nuclear Plant. Generic Letter 83-28. Refer to Appendix 7.1-B items 10 and 11 or Appendix 7.1-C items 12 and 27. Refer to Section 7.8 for review of ATWS mitigation systems.
120	On-line testability of protection systems. Refer to Appendix 7.1-B items 10 and 11 or Appendix 7.1-C items 12 and 27.
142	Leakage through electrical isolators in instrumentation circuits. Refer to Appendix 7.1-B items 3, 6, 7, and 8, or Appendix 7.1-C items 6, 10, 11, and 24.

3. Incorporation of Operating Experience

Bulletin 80-06	"ESF Reset Controls."
Bulletin 80-19	"Failures of Mercury-Wetted Matrix Relays in the RPS."
Bulletin 80-20	"Failures of Westinghouse Type W-2 Spring Return to Neutral Control Switches."
Bulletin 90-01 and Supplement 1 to Bulletin 90-01	"Loss of Fill-Oil in Transmitters Manufactured by Rosemount."
Generic Letter 83-28	"Required Actions Based on Generic Implications of Salem ATWS Events."
Generic Letter 85-06	"Quality Assurance Guidance for ATWS Equipment That is not Safety-Related."
Generic Letter 89-19	"Request for Action Related to Resolution of USI A-47."
Generic Letter 93-08	"Relocation of Technical Specification Tables of Instrument Response Time Limits."
Generic Letter 95-02	"Use of NUMARC/EPRI Report TR-102348, 'Guideline on Licensing Digital Upgrades,' in Determining Acceptability of Performing Analog-to-Digital Replacements Under 10 CFR 50.59."

Generic Letter 96-01 "Testing Of Safety-Related Logic Circuits."

The evaluation of conformance with this requirement for I&C systems should be addressed in the review of Section 7.1 through 7.9 of the SAR and the review of design certification documentation. The reviewer may document compliance with these requirements in Section 7 of the SER or may provide input to a separate SER section regarding resolution of generic issues.

o. 52.47(a)(1)(vi) ITAAC in Design Certification Applications

"An application for design certification must contain proposed tests, inspections, analyses, and acceptance criteria which are necessary and sufficient to provide reasonable assurance that, if the tests, inspections and analyses are performed and the acceptance criteria met, a plant which references the design is built and will operate in accordance with the design certification."

Applicability — All I&C systems that are part of applications for design certification under 10 CFR 52, Subpart B, or combined licenses under 10 CFR 52, Subpart C.

Review Methods — The ITAAC for I&C systems important to safety should be provided for each system in subsequent sections of Chapter 7 of the SAR. SECY-91-178, "Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) for Design Certifications and Combined Licenses," and Section 14.3 provide guidance on conformance to 10 CFR 52.47(a)(1)(vi). The evaluation of conformance with this requirement for I&C systems should be addressed by review of Section 7.1 through 7.9 of the SAR and the review of design certification documentation in conjunction with review of Section 14.3.5 of the SAR. Section 14.3 of the SRP describes the general acceptance criteria and review procedures for ITAAC. Section 14.3.5 describes the specific acceptance criteria and review procedures for I&C system ITAAC. The Staff review with respect to these requirements is documented in Section 14.3 of the SER.

p. 52.47(a)(1)(vii) Interface Requirements

"An application for design certification must contain the interface requirements to be met by those portions of the plant for which the application does not seek certification. These requirements must be sufficiently detailed to allow completion of the final safety analysis and design-specific probabilistic risk assessment required by paragraph (a)(1)(v) of this section."

Applicability — All I&C systems that are part of applications for design certification under 10 CFR 52, Subpart B, or combined licenses under 10 CFR 52, Subpart C.

Review Methods — The evaluation of conformance with this requirement for I&C systems should be addressed by review of Section 7.1 through 7.9 of the SAR and the review of design certification documentation in conjunction with review of Section 14.3.5 of the SAR. SRP Section 1.8 describes the review methods for interface requirements.

q. 52.47(a)(2) Level of Detail

"The application must contain a level of design information sufficient to enable the Commission to judge the applicant/licensee's proposed means of assuring that construction conforms to the design and to reach a final

conclusion on all safety questions associated with the design before the certification is granted. The information submitted for a design certification must include performance requirements and design information sufficiently detailed to permit the preparation of acceptance and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant/licensee. The Commission will require, prior to design certification, that information normally contained in certain procurement specifications and construction and installation specifications be completed and available for audit if such information is necessary for the Commission to make its safety determination."

Applicability — All I&C safety systems that are part of applications for design certification under 10 CFR 52, Subpart B, or combined licenses under 10 CFR 52, Subpart C.

Review Methods — Sufficient information for an NRC safety determination should be provided for each I&C system. BTP HICB-16 provides additional guidance for evaluating the sufficiency of the information about I&C system in design certification applications made under 10 CFR 52, Subpart B.

r. 52.47(b)(2)(i) Innovative Means of Accomplishing Safety Functions

"Certification of a standard design which differs significantly from the light water reactor designs described in paragraph (b)(1) of this section or utilizes simplified, inherent, passive, or other innovative means to accomplish its safety functions will be granted only if (A) (1) The performance of each safety feature of the design has been demonstrated through either analysis, appropriate test programs, experience, or a combination thereof; (2) Interdependent effects among the safety features of the design have been found acceptable by analysis, appropriate test programs, experience, or a combination thereof; (3) Sufficient data exist on the safety features of the design to assess the analytical tools used for safety analyses over a sufficient range of normal operating conditions, transient conditions, and specified accident sequences, including equilibrium core conditions; and (4) The scope of the design is complete except for site-specific elements such as the service water intake structure and the ultimate heat sink; or (B) There has been acceptable testing of an appropriately sited, full-size, prototype of the design over a sufficient range of normal operating conditions, transient conditions, and specified accident sequences, including equilibrium core conditions. If the criterion in paragraph (b)(2)(i)(A)(4) of this section is not met, the testing of the prototype must demonstrate that the non-certified portion of the plant cannot significantly affect the safe operation of the plant."

Applicability — The protection systems, RTS and ESFAS in applications for design certification under 10 CFR 52, Subpart B, or combined licenses under 10 CFR 52, Subpart C.

Review Methods — The reviewer should identify technologies that have not previously been accepted by the Staff and establish a basis for acceptance prior to proceeding with the review.

s. 52.79(c) ITAAC in Combined License Applications

"The application for a combined license must include the proposed inspections, tests and analyses, including those applicable to emergency planning, which the licensee shall perform and the acceptance criteria therefore which are necessary and sufficient to provide reasonable assurance that, if the inspections, tests and analyses are performed and the acceptance criteria met, the facility has been constructed and will operate in conformity with the combined license, the provisions of the Atomic Energy Act, and the NRC's

regulations. Where the application references a certified standard design, the inspections, tests, analyses and acceptance criteria contained in the certified design must apply to those portions of the facility design which are covered by the design certification."

Applicability — All I&C systems that are part of applications for combined licenses under 10 CFR 52, Subpart C.

Review Methods — The ITAAC for I&C systems important to safety should be provided for each system in subsequent sections of Chapter 7 of the SAR. SECY-91-178 and SRP Section 14.3 provide guidance on conformance to 10 CFR 52.47(c). The evaluation of conformance with this requirement for I&C systems should be addressed by review of Section 7.1 through 7.9 of the SAR and the review of combined license documentation in conjunction with review of Section 14.3.5 of the SAR. Section 14.3 of the SRP describes the general acceptance criteria and review procedures for ITAAC. Section 14.3.5 describes the specific acceptance criteria and review procedures for I&C system ITAAC. The Staff review with respect to these requirements is documented in Section 14.3 of the SER.

2. 10 CFR 50 Appendix A, General Design Criteria

a. Criterion 1 — Quality Standards and Records

"Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit."

Applicability — All I&C systems and components important to safety.

Review Methods — Regulatory guides and endorsed codes and standards applicable to I&C systems important to safety are identified in Section 4 of this appendix. These guidelines provide the information needed to determine their applicability. The review of Section 7.1 of the SAR should confirm that the appropriate regulatory guides and endorsed standards are identified as applicable for each instrument and control system important to safety.

The evaluation of the quality assurance program and appropriate records are addressed in the review of Section 17 of the SAR.

b. Criterion 2 — Design Bases for Protection Against Natural Phenomena

"Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect: (1) appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy,

quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena, and (3) the importance of the safety functions to be performed."

Applicability — All instrumentation and control safety systems and supporting data communication systems.

Review Methods — The design bases for protection against natural phenomena for I&C systems important to safety should be provided for the I&C system. The design bases should identify those systems and components which should be qualified to survive the effects of earthquakes and other natural phenomena. The review should confirm that the I&C systems important to safety are qualified for protection against natural phenomena consistent with the analysis of these events as provided in Chapter 3 of the SAR, and that they are located and housed in structures consistent with these requirements.

The evaluation of the adequacy of qualification programs to demonstrate the capability of I&C systems to withstand the effects of natural phenomena is addressed in the review of Section 3.10 of the SAR.

The instrumentation systems needed for severe accidents must be designed so there is reasonable assurance that they will operate in the severe-accident environment for which they are intended, and over the time span for which they are needed. They need not be subject to additional environmental or seismic qualification testing or analysis.

The review of conformance with GDC 2 should be coordinated with the Plant Systems Branch (SPLB) and the Mechanical Engineering Branch (EMEB).

c. Criterion 4 — Environmental and Missile Design Bases

"Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures, systems, and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids that may result from equipment failures and from events and conditions outside the nuclear power unit."

Applicability — All I&C safety systems and supporting data communication systems.

Review Methods — The environmental and missile design bases for I&C systems important to safety should be provided for each system in subsequent sections of Chapter 7 of the SAR. The design bases should identify those systems and components that are qualified to accommodate the effects of environmental conditions and protected from dynamic effects of missiles, pipe whipping, and discharging fluids. If systems or components are qualified to survive the environmental effects of postulated accidents for limited periods of time, the bases for limited operability should be provided. Review of equipment qualification for environmental conditions should be conducted in accordance with the guidance provided in Appendix 7.1-B item 5 and Appendix 7.1-C item 9.

The instrumentation systems needed for severe accidents must be designed so there is reasonable assurance that they will operate in the severe-accident environment for which they are intended and over the time span for which they are needed. They need not be subject to additional environmental qualification requirements.

The review of this requirement should be coordinated with EELB.

d. Criterion 13 — Instrumentation and Control

"Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges."

Applicability — All I&C systems and supporting data communication systems.

Review Methods — Review of compliance with GDC 13 should include consideration of the following topics.

- Instrumentation to monitor plant variables and systems — See SRP Sections 7.5 and 7.7.
- Instrumentation to monitor the status of protection systems — See Appendix 7.1-B items 10, 13, 18, and 20, or Appendix 7.1-C items 13 and 27.
- Instrumentation and controls for manual initiation of safety functions — See Appendix 7.1-B items 18 and 20 or Appendix 7.1-C items 13, 18, and 23.
- Instrumentation and controls to support diverse actuation of safety functions — See Section 7.8.
- Instrumentation and controls to regulate ESF systems — See Section 7.3.
- Interlocks to maintain variables and systems within safe states — See Section 7.6.
- Instrumentation and controls to maintain variables and systems within normal operational limits — See Section 7.7.
- Protection of instrument sensing lines from environmental extremes — See Reg. Guide 1.151.
- Setpoints for instrumentation system alarms and control system actions — See BTP HICB-12.
- Data communication systems that support plant instrumentation and controls — See Section 7.9.

Instrumentation and control systems should support conformance to the regulatory requirements applicable to the process systems which they control. Requirements to be noted in this regard include the following General Design Criteria.

General Design Criterion	Lead Reviewer	Location of Review Guidance
GDC 10 Reactor Design	Reactor Systems Branch (SRXB)	SRP Chapter 4
GDC 12 Suppression of Reactor Power Oscillations	SRXB	SRP Section 4.3
GDC 15 Reactor Coolant System Design	SRXB	SRP Section 5.4
GDC 16 Containment Design	Containment and Severe Accident Branch (SCSB)	SRP Section 6.2
GDC 28 Reactivity Limits	SRXB	SRP Section 4.3
GDC 33 Reactor Coolant Makeup	SRXB	SRP Chapter 9
GDC 34 Residual Heat Removal	SRXB	SRP Sections 5.4.6 and 5.4.7
GDC 35 Emergency Core Cooling	SRXB	SRP Section 6.3
GDC 38 Containment Heat Removal	SCSB	SRP Section 6.2.2
GDC 41 Containment Atmosphere Cleanup	Plant Systems Branch (SPLB)	SRP Section 6.5
GDC 44 Cooling Water	SPLB	SRP Chapter 9

Depending upon the applicant/licensee instrumentation and control system architecture, review of instrumentation and controls for these functions may be an HICB primary review responsibility as part of the review of SAR Chapter 7, or a secondary responsibility supporting other branches' review of other SAR sections. The review methods described in this Appendix should be used as appropriate. The review guidance of Appendix 7.1-B or Appendix 7.1-C should also be applied to I&C systems required for operation of engineered safety feature systems or their essential auxiliary systems.

e. Criterion 19 — Control Room

"A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident.

"Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures."

Applicability — All I&C systems and supporting data communication systems.

Review Methods — The evaluation of the instrumentation and controls available to operate the nuclear power unit under normal and accident conditions is addressed in the review of Sections 7.3, 7.5, and Section 7.7 of the SAR. The evaluation of reactor trip functions, interlock functions, and diverse I&C functions that support safe operation are addressed in the review of Sections 7.2, 7.6, and 7.8 of the SAR. The evaluation of safe shutdown and remote shutdown capabilities are addressed in the review of Section 7.4 of the SAR.

The adequacy of the human factor aspects of the control room design is addressed in the review of Chapter 18 of the SAR. The evaluation of the habitability aspects of GDC 19 with respect to radiation protection is addressed in the review of Section 6.4 of the SAR.

Guidelines for the review of safe shutdown capabilities, including remote shutdown capabilities, are provided in SRP Section 7.4.

f. Criterion 20 — Protection System Functions

"The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences, and (2) to sense accident conditions and to initiate the operation of systems and components important to safety."

Applicability — The protection systems, RTS and ESFAS.

Review Methods — Review of compliance with GDC 20 should address the following characteristics described in ANSI/IEEE Std 279 and IEEE Std 603. SRP Appendix 7.1-B and Appendix 7.1-C discuss methods for review of these characteristics.

	Location of Review Guidance	
Topic	**Appendix 7.1-B Item**	**Appendix 7.1-C Item**
Design basis requirements	1	4
General function requirements	2	5 and 22
System integrity	6	10
Setpoints	1	30

The evaluation of conformance with this requirement should be addressed in the review of Sections 7.2 and 7.3 of the SAR.

g. Criterion 21 — Protection System Reliability and Testability

"The protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function, and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred."

Applicability — The protection systems, RTS, ESFAS, and supporting data communication systems.

Review Methods — Review of compliance with GDC 21 should address the following characteristics described in ANSI/IEEE Std 279 and IEEE Std 603. SRP Appendix 7.1-B and Appendix 7.1-C discuss methods for review of these characteristics.

Topic	**Location of Review Guidance**	
	Appendix 7.1-B Item	**Appendix 7.1-C Item**
Design basis reliability requirements and reliability determination methods	1	4
Single-failure criterion	3	6
Completion of protective action once initiated	17	7 and 25
Quality	4	8
System integrity	6	10
Physical, electrical, and communications independence	7 and 8	11 and 24
Capability for test and calibration	10 and 11	12 and 27
Indication of bypass	14	13
Control of access to safety system equipment	15 and 19	14
Repair and troubleshooting provisions	21	15
Identification of protection system equipment	22	16
Auxiliary features	6	17
Multi-unit stations	6	18
Human factors considerations	20	19
Reliability	2	20

Topic	Location of Review Guidance	
	Appendix 7.1-B Item	Appendix 7.1-C Item
Manual controls	18	23
Derivation of system inputs	9	26
Operating bypasses	13	28
Maintenance bypasses	12	29
Multiple setpoints	16	30
Power sources	6	31

The evaluation of conformance with this requirement should be addressed in the review of Sections 7.2 and 7.3 of the SAR.

h. Criterion 22 — Protection System Independence

"The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."

Applicability — The protection systems — RTS, ESFAS, and supporting data communication systems.

Review Methods — Review of compliance with GDC 22 should address the following characteristics described in ANSI/IEEE Std 279 and IEEE Std 603. SRP Appendix 7.1-B and Appendix 7.1-C discuss methods for review of these characteristics.

Topic	Location of Review Guidance	
	Appendix 7.1-B Item	Appendix 7.1-C Item
Design basis reliability requirements	1	4
Single-failure criterion	3	6
Quality	4	8
Equipment qualification	5	9
System integrity	6	10
Physical, electrical, and communications independence	7 and 8	11 and 24
Manual controls	18	23

Topic	Location of Review Guidance	
	Appendix 7.1-B Item	Appendix 7.1-C Item
Setpoints	1	30
Power sources	6	31

i. Criterion 23 — Protection System Failure Modes

"The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire pressure, steam, water, and radiation) are experienced."

Applicability — The protection systems, RTS, ESFAS, and supporting data communication systems.

Review Methods — Review of compliance with GDC 23 is accomplished as part of the review of system integrity requirements discussed in ANSI/IEEE Std 279 and IEEE Std 603. SRP Appendix 7.1-B and Appendix 7.1-C discuss methods for review of these characteristics. Appendix 7.1-B item 7 and Appendix 7.1-C item 10 provide review guidance that encompass the review with respect to compliance with GDC 23. The evaluation of conformance with this requirement should be addressed in the review of Sections 7.2 and 7.3 of the SAR.

j. Criterion 24 — Separation of Protection and Control Systems

"The protection system shall be separated from control systems to the extent that failure of any single control system component, or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

Applicability — All I&C systems.

Review Methods — Review of compliance with GDC 24 should address the following characteristics described in ANSI/IEEE Std 279 and IEEE Std 603. SRP Appendix 7.1-B and Appendix 7.1-C discuss methods for review of these characteristics.

Topic	Location of Review Guidance	
	Appendix 7.1-B Item	Appendix 7.1-C Item
Single-failure criterion	3	6
Independence	7	11

Topic	Location of Review Guidance	
	Appendix 7.1-B Item	**Appendix 7.1-C Item**
Control–protection interaction	8	24
Auxiliary features	6	17
Power sources	6	31

Separation of protection and control systems should be considered in the review of all sections of Chapter 7 of the SAR to confirm that all interfaces between control systems and protection systems have been properly identified and addressed.

k. Criterion 25 — Protection System Requirements for Reactivity Control Malfunctions

"The protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods."

Applicability — The reactor trip system. Also reactivity control system interlocks identified in Chapter 15 as required to ensure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems.

Review Methods — Confirmation that the protection system is designed for an appropriate spectrum of reactivity control system malfunctions is addressed in the review of protection system design basis requirements as discussed in ANSI/IEEE Std 279 and IEEE Std 603. Appendix 7.1-B item 1 and Appendix 7.1-C item 4 provide review guidance for this topic. The evaluation of conformance with this requirement should be addressed in the review of Section 7.2 of the SAR.

l. Criterion 29 — Protection Against Anticipated Operational Occurrences

"The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences."

Applicability — The protection systems, reactivity control functions of control systems, and supporting data communication systems.

Review Methods — Evaluation with respect to the requirements of GDC 29 is based upon conformance of the protection system and reactivity control systems to the applicable GDCs discussed in Sections a through k above. Probabilistic reliability assessments may be performed by the NRC staff to provide a basis for development of deterministic criteria for specific systems. The review of these systems will address conformance to the deterministic criteria so established. Conformance of the reactivity control systems to GDC 29 is addressed in the review of Section 7.2 of the SAR.

3. Staff Requirements Memoranda

Note: This section quotes positions that are extracted from Staff Requirements Memoranda (SRM) and the associated SECY memoranda. Specific positions are not necessarily separated from explanatory material in these documents. The quotes given here do not include the explanatory material provided in the SECY or SRM. The quotes may also combine material from the SRM and SECY to fully represent the NRC position.

a. Item II.Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control systems" of Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs"

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.

2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the SAR using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.

Applicability — RTS, ESFAS, diverse instrumentation and control systems, control systems, and supporting data communication systems in plants utilizing digital computer-based RTS or ESFAS.

Review Methods — BTP HICB-19 provides guidance for the evaluation of compliance with this requirement. SRP Sections 7.7 and 7.8 provide guidance for the review of control system and diverse instrumentation and control system features that are credited as non-safety diverse means of protecting against common-mode failure within the safety systems.

b. Item II.T, "Control Room Annunciator (Alarm) Reliability," of Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs"

The annunciator system is considered to consist of sets of alarms (which may be displayed on tiles, video display units (VDUs), or other devices) and sound equipment; logic and processing support; and functions to enable operators to silence, acknowledge, reset, and test alarms.

The main control room (MCR) shall contain compact, redundant operator workstations with multiple display and control devices that provide organized, hierarchical access to alarms, displays, and controls. Each workstation shall have the full capability to perform MCR functions as well as support division of tasks between two operators.

The display and control features shall be designed to satisfy existing regulations, for example: separation and independence requirements for Class 1E circuits (IEEE Std 384, "Criteria for Separation of Class 1E Equipment and Circuits"); criteria for protection systems (ANSI/IEEE Std 279); and requirements for manual initiation of protective actions at the systems level (Reg. Guide 1.62, "Manual Initiation of Protection Action"). The designer shall use existing defensive measures (e.g., segmentation, fault tolerance, signal validation, self-testing, error checking, and supervisory watchdog programs), as appropriate, to ensure that alarm, display, and control functions provided by the redundant workstations meet these standards.

Alarms that are provided for manually controlled actions for which no automatic control is provided, and that are required for the safety systems to accomplish their safety functions, shall meet the applicable requirements for Class 1E equipment and circuits.

Applicability — Information systems important to safety and supporting data communication systems in advanced light water reactors.

Review Methods — Section 7.5 describes methods for review of annunciator systems in ALWRs.

4. Regulatory Guides (including endorsed industry codes and standards) and Branch Technical Positions

a. Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions"

Applicability — RTS, ESFAS, diverse instrumentation and control systems, and supporting data communication systems.

Review Methods — Reg. Guide 1.22 provides bases for evaluating conformance to GDC 21 and ANSI/IEEE Std 279, Sections 4.10 through 4.13. BTP HICB-8 describes the Staff position on the scope of periodic testing in protection systems. BTP HICB-17 provides additional guidance on acceptable periodic testing provisions for digital computer-based systems.

b. Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"

Applicability — RTS, ESFAS, information systems important to safety, safety interlock systems, and supporting data communication systems.

Review Methods — Reg. Guide 1.47 provides bases for evaluating conformance to GDC 21 and ANSI/IEEE Std 279, Sections 4.13 and 4.20 for protection systems. The regulatory guide also provides bases for evaluating the adequacy of bypass and inoperable status indication for I&C systems important to safety as addressed in the review of Section 7.5 of the SAR.

c. *Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems,"* (Endorses ANSI/IEEE Std 379, Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems")

Applicability — All I&C safety systems and supporting data communication systems.

Review Methods — Reg. Guide 1.53 provides a basis for evaluating conformance to GDC 21 and ANSI/IEEE Std 279, Section 4.2.

d. *Regulatory Guide 1.62, "Manual Initiation of Protection Action"*

Applicability — RTS, ESFAS, and diverse instrumentation and control systems.

Review Methods — Reg. Guide 1.62 provides a basis for evaluating conformance to ANSI/IEEE Std 279, Section 4.17. Reg. Guide 1.62 also provides guidance that should be considered in the review of manual initiation of ATWS mitigation and diverse actuation system functions.

e. *Regulatory Guide 1.75, "Physical Independence of Electrical Systems,"* (Endorses IEEE Std 384, "Criteria for Separation of Class 1E Equipment and Circuits")

Applicability — All I&C systems.

Review Methods — Reg. Guide 1.75 provides a basis for evaluating conformance to GDC 21 and ANSI/IEEE Std 279, Sections 4.6 and 4.22 for protection systems and for evaluating the adequacy of I&C systems important to safety that incorporate redundant or diverse features to satisfy the single-failure criterion. The HICB evaluation is limited to the review of components and electrical wiring inside racks, panels, and control boards for systems important to safety. The evaluation of the physical separation of electrical cables is addressed in the review of Chapter 8 of the SAR.

f. *Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident"*

Applicability — Information systems important to safety.

Review Methods — Reg. Guide 1.97 provides a basis for evaluating conformance to GDC 13. The HICB evaluation is limited to the review of instrumentation for monitoring plant conditions. The evaluation of instrumentation for monitoring environs conditions and radiation monitoring systems are addressed in the review of other sections of the SAR. Section 7.5 and BTP HICB-10 describe the review of post-accident monitoring systems.

g. *Draft Regulatory Guide DG-1045, proposed revision 3 to Reg. Guide 1.105, "Instrument Setpoints for Safety Systems,"* (Endorses ISA-S67.04, "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants")

Applicability — All I&C systems.

Review Methods — Draft Reg. Guide DG-1045 provides a basis for evaluating conformance to GDC 13 and ANSI/IEEE Std 279, Section 3. BTP HICB-12 provides guidance for establishing and maintaining instrument set points.

Draft Reg. Guide DG-1045 and ISA-S67.04 are specifically directed at establishing setpoints for trip functions. Nevertheless, their guidance is equally relevant to accounting for measurement uncertainties when determining the indicated plant conditions at which emergency procedures will require operator action, determining the setpoint for interlock functions, and determining setpoints for control functions provided to maintain plant variables and systems within prescribed operating ranges. Therefore, the guidance of Draft Reg. Guide DG-1045 is useful in reviewing all I&C systems important to safety even if no automatic trip functions are involved.

h. *Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems,"* (Endorses IEEE Std 338, Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems")

Applicability — All I&C safety systems, diverse instrumentation and control systems, and supporting data communication systems.

Review Methods — Reg. Guide 1.118 provides a basis for evaluating conformance to GDC 21 and ANSI/IEEE Std 279, Section 4.10. The HICB evaluation is limited to the review of testing of protection systems. The evaluation of testing of electric power systems is addressed by others in the review of Chapter 8 of the SAR. BTP HICB-17 discusses periodic test provisions in digital computer-based systems.

i. *Regulatory Guide 1.151, "Instrument Sensing Lines,"* (Endorses ANSI/ISA-S67.02, "Nuclear Safety-Related Instrument Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants")

Applicability — I&C sensing lines and sensing line environmental control systems.

Review Methods — Reg. Guide 1.151 provides a basis for evaluating conformance to GDC 13. Environmental control systems for all I&C systems are addressed in the review of Section 7.7 of the SAR.

j. *Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,"* (Endorses IEEE Std 7-4.3.2,"IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations")

Applicability — All instrumentation and control safety systems and supporting data communication systems.

Review Methods — Reg. Guide 1.152 provides a basis for evaluating conformance of computers with GDC 21. Appendix 7.1-C provides review guidance for the evaluation of conformance to the guidance of Reg. Guide 1.152 in conjunction with Reg. Guide 1.153.

k. *Regulatory Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems,"* (Endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"*)*

Applicability — All instrumentation and control safety systems and supporting data communication systems.

Review Methods — Reg. Guide 1.153 provides an acceptable method of addressing the requirements of ANSI/IEEE Std 279. Appendix C to Section 7.1 provides guidance for the evaluation of conformance to the guidance of Reg. Guide 1.153 as supplemented by Reg. Guide 1.152.

l. *Regulatory Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,"* (Endorses ANSI/IEEE Std 1012, "IEEE Standard for Software Verification and Validation Plans," and IEEE Std 1028, "IEEE Standard for Software Reviews and Audits")

Applicability — All I&C systems and components important to safety.

Review Methods — Reg. Guide 1.168 provides a basis for evaluating conformance with 10 CFR 50.55a(a)(1), 50.55a(h), GDC 1 and Criteria I, II, III, XI, and XVIII of 10 CFR 50 Appendix B for computer-based systems. It endorses, with comments, ANSI/IEEE Std 1012 for planning the verification and validation of safety system software. It also endorses, with comments, IEEE Std 1028 as providing acceptable approaches for carrying out software reviews, inspections, walkthroughs, and audits.

BTP HICB-14 describes the review of planning, and implementation of verification, validation, and audits of digital computer software.

m. *Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,"* (Endorses IEEE Std 828, "IEEE Standard for Software Configuration Management Plans," and ANSI/IEEE Std 1042, "IEEE Guide to Software Configuration Management")

Applicability — All I&C systems and components important to safety.

Review Methods — Reg. Guide 1.169 provides a basis for evaluating conformance with 10 CFR 50.55a(a)(1), 50.55a(h), GDC 1 and Criterion III of 10 CFR 50 Appendix B for computer-based systems. It endorses, with comments, IEEE Std 828 for planning the configuration management of safety system software. It also endorses, with comments, ANSI/IEEE Std 1042 as acceptable guidance for carrying out configuration management plans produced under the auspices of IEEE Std 828.

BTP HICB-14 describes the review of configuration management for digital computer software.

n. *Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,"* (Endorses IEEE Std 829, "IEEE Standard for Software Test Documentation")

Applicability — All I&C systems and components important to safety.

Review Methods — Reg. Guide 1.170 provides a basis for evaluating conformance with 10 CFR 50.55a(h), GDC 1, GDC 21, and Criteria I, III, IV, VI, XI, and XVII of 10 CFR 50 Appendix B for computer-based

systems. It endorses, with comments, IEEE Std 829 as providing acceptable approaches for documenting software testing.

BTP HICB-14 describes the review of testing of digital computer software.

o. Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," (Endorses ANSI/IEEE Std 1008, "IEEE Standard for Software Unit Testing")

Applicability — All I&C systems and components important to safety.

Review Methods — Reg. Guide 1.171 provides a basis for evaluating conformance with 10 CFR 50.55a(h), GDC 1, GDC 21 and Criteria I, II, III, V, VI, XI, and XVII of 10 CFR 50 Appendix B for computer-based systems. It endorses, with comments, ANSI/IEEE Std 1008 as providing acceptable approaches to unit testing of software.

BTP HICB-14 describes the review of testing of digital computer software.

p. Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," (Endorses IEEE Std 830, "IEEE Recommended Practice for Software Requirements Specifications")

Applicability — All I&C systems and components important to safety.

Review Methods — Reg. Guide 1.172 provides a basis for evaluating conformance with 10 CFR 50.55a(h), GDC 1 and Criterion III of 10 CFR 50 Appendix B for computer-based systems. It endorses, with comments, IEEE Std 830 as describing an acceptable approach to the development of software requirements specifications.

BTP HICB-14 describes the review of software requirements specifications.

q. Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," (Endorses IEEE Std 1074, "IEEE Standard for Developing Software Life Cycle Processes")

Applicability — All I&C systems and components important to safety.

Review Methods — Reg. Guide 1.173 provides a basis for evaluating conformance with 10 CFR 50.55a(h), GDC 1 and Criteria I, II, III, VI, XV, and XVII of 10 CFR 50 Appendix B for computer-based systems. It endorses, with comments, IEEE Std 1074 as providing acceptable approaches to defining software development processes.

BTP HICB-14 describes the review of software development plans and software project management plans which should outline the licensee/applicant’s software life cycle. BTP HICB-14 also describes the review of each activity group described in IEEE Std 1074.

5. Branch Technical Positions

Applicability — As noted in Table 7-1.

Review Methods — The BTPs provide bases for evaluating specific review areas.

References

ANS Std 4.5. "Criteria for Accident Monitoring Functions in Light Water Cooled Reactors."

ANSI/IEEE Std 1008-1987. "IEEE Standard for Software Unit Testing."

ANSI/IEEE Std 1012-1986. "IEEE Standard for Software Verification and Validation Plans."

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

ANSI/IEEE Std 379-1988. "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

ANSI/IEEE Std 829-1983. "IEEE Standard for Software Test Documentation."

BAW-1564. "Integrated Control System Reliability Analysis." Babcock and Wilcox, August 17, 1979.

Bulletin 80-06. "ESF Reset Controls." March 13, 1980.

Bulletin 80-19. Rev. 1 " Failures of Mercury-Wetted Matrix Relays in the RPS," August 15, 1980.

Bulletin 80-20. " Failures of Westinghouse Type W-2 Spring Return to Neutral Control Switches." July, 1980.

Bulletin 90-01. "Loss of Fill-Oil in Transmitters Manufactured by Rosemount." March 9, 1990.

Bulletin 90-01 Supplement. "Loss of Fill-Oil in Transmitters Manufactured by Rosemount." December 22, 1992.

Draft Regulatory Guide DG-1045. Proposed Revision 3 to Regulatory Guide 1.105, "Instrument Setpoints for Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

EPRI Topical Report TR-102348. "Guideline on Licensing Digital Upgrades." Electric Power Research Institute.

Generic Letter 83-28. " Required Actions Based on Generic Implications of Salem ATWS Events." July 8, 1993.

Generic Letter 85-06. "Quality Assurance Guidance For ATWS Equipment That Is Not Safety-Related." April 16, 1985.

Generic Letter 89-19. "Request for Action Related to Resolution of USI A-47." September 20, 1989.

Generic Letter 93-08. "Relocation of Technical Specification Tables of Instrument Response Time Limits." December 29, 1993.

Generic Letter 95-02. "Use of NUMARC/EPRI Report TR-102348 in Determining Acceptability of Performing Analog-to-Digital Replacements Under 10 CFR 50.59." April 26, 1995.

Generic Letter 96-01. "Testing of Safety-Related Logic Circuits." January 10, 1996.

IEEE Std 1028-1988. "IEEE Standard for Software Reviews and Audits."

IEEE Std 1042-1987. "IEEE Guide to Software Configuration Management."

IEEE Std 1074-1995. "IEEE Standard for Developing Software Life Cycle Processes."

IEEE Std 338-1987. "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."

IEEE Std 384-1992. "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits."

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

IEEE Std 7-4.3.2-1993. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

IEEE Std 828-1990. "IEEE Standard for Software Configuration Management Plans."

IEEE Std 830-1993. "IEEE Recommended Practice for Software Requirements Specifications."

ISA-S67.04-1994. "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants."

NUREG-0694. "TMI-Related Requirements for New Operating Reactor Licenses." 1980.

NUREG-0718. "Licensing Requirements for Pending Applications for Construction Permits and Manufacturing License." 1981.

NUREG-0737. "Clarification of TMI Action Plan Requirements." 1982.

NUREG-0737 Supplement 1. "Clarification of TMI Action Plan Requirements — Requirements for Emergency Response Capability." January 1983.

Regulatory Guide 1.118. "Periodic Testing of Electric Power and Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1995.

Regulatory Guide 1.151. "Instrument Sensing Lines." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1983.

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, January 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.168. "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.169. "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.170. "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.171. "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.172. "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.173. "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

Regulatory Guide 1.22. "Periodic Testing of Protection System Actuation Functions." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1972.

Regulatory Guide 1.47. "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.53. "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.62. "Manual Initiation of Protection Action." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.70. "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants." Office of Standards Development, U.S. Nuclear Regulatory Commission, November 1978.

Regulatory Guide 1.75. "Physical Independence of Electrical Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1978.

Regulatory Guide 1.97. "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident." Revision 3, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, May 1983.

SECY 91-178. "Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) for Design Certifications and Combined Licenses." June 12, 1991.