U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

OFFICE OF NUCLEAR REACTOR REGULATION

7.1 INSTRUMENTATION AND CONTROLS - INTRODUCTION

REVIEW RESPONSIBILITIES

Primary - Instrumentation and Control Systems Branch (ICSB)

Secondary - None

I. AREAS OF REVIEW

The instrumentation and control systems important to safety fall into the following categories and are addressed in detail in subsequent sections of Chapter 7 or other sections of the safety analysis report (SAR).

Protection Systems are those instrumentation and control systems which initiate safety actions to mitigate the consequences of design basis events. The protection systems include the Reactor Trip System (RTS) discussed in Section 7.2 and the engineered safety features actuation system (ESFAS) discussed in Section 7.3 of the SAR.

Engineered Safety Features (ESF) Control Systems are those control systems which regulate the operation of ESF systems following their initiation by the protection system. The ESF control systems are discussed in Section 7.3 of the SAR.

Safe Shutdown Systems are those systems which must function to achieve and maintain a safe shutdown condition of the plant. The safe shutdown systems include those instrumentation and control systems which are used to maintain the reactor core in a subcritical condition and provide adequate core cooling to achieve and maintain both hot and cold shutdown conditions. Safe shutdown systems are discussed in Section 7.4 of the SAR.

Information Systems Important to Safety are those systems which provide information for the safe operation of the plant during normal operation, anticipated operational occurrences, and accidents. The information systems important to safety include those systems which provide information for manual initiation and control of safety systems, to indicate that plant safety functions are being accomplished, and to provide information from which appropriate actions can be

taken to mitigate the consequences of anticipated operational occurrences and accidents. During normal plant operation, the information systems important to safety provide information on the bypassed and inoperable status of safety systems. Information systems important to safety are discussed in Section 7.5 of the SAR.

Interlock Systems Important to Safety are those systems which operate to reduce the probability of occurrence of specific events or to maintain safety systems in a state to assure their availability in an accident. These systems differ from protection systems in that their safety action is taken prior to or to prevent accidents. Interlock systems important to safety are discussed in Section 7.6 of the SAR.

Control Systems are those systems used for normal operation that are not relied upon to perform safety functions following anticipated operational occurrences of accidents, but which control plant processes having a significant impact on plant safety. Control systems are discussed in Section 7.7 of the SAR.

Essential Auxiliary Supporting Systems are those systems that must function to assure the capability of the instrument and control systems important to safety to perform safety functions. Heating, ventilation and air conditioning systems, electrical power systems, and cooling water systems are typical examples of essential auxiliary supporting systems. Essential auxiliary supporting systems are discussed in other chapters of the SAR.

The instrumentation and control aspects of essential auxiliary supporting systems are addressed in the review of those SAR sections which discuss those systems. To the extent that the operation of essential auxiliary supporting systems are initiated by the protection system, this aspect is included in the review of the protection systems in Section 7.2 or 7.3 of the SAR.

All other instrumentation and control systems important to safety such as fire protection, fuel handling, radiation monitoring, and control of essential auxiliary supporting systems are addressed in the review of other SRP sections which discuss these systems.

The review of Section 7.1 of the SAR includes the tabulation of instrumentation and control systems important to safety and the acceptance criteria and guidelines applicable to each of these systems. The review also includes the identification of those instrumentation and control systems important to safety that are identical to those which have previously been reviewed by the staff and where the adequacy of these systems is based upon prior Commission approval. The bases for prior approval includes the staff's evaluation of applications for construction permits and operating licenses, preliminary and final design approvals for standardized plants, and topical reports.

II. ACCEPTANCE CRITERIA

The General Design Criteria (GDC), which are provided in the Commission regulations, establish minimum requirements for the design of nuclear power plants. IEEE Standard 279 "Criteria for Protection Systems for Nuclear Power Generating Stations," is also incorporated in 10 CFR Part 50, §50.55a(h) of the Commission's regulations. These criteria establish the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety. The structures, systems, and components important to safety are those that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public.

Regulatory guides amplify specific regulations, describe acceptable methods for meeting their requirements and provide guidance to applicants. Industry codes and standards set forth requirements and recommended practices applicable to instrumentation and control systems for nuclear power plants. These standards, as modified by the regulatory guides which endorse them, also provide acceptable methods for meeting the requirements of the regulations.

The acceptance criteria consist of the GDC and IEEE Std 279 which establish the Commission requirements for instrumentation and control systems important to safety. The regulatory guides and the endorsed industry codes and standards are the guidelines which are used as a basis for the evaluation of conformance to the requirements of the Commission's regulations. Table 7-1, "Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety" (Ref. 1), lists the acceptance criteria and guidelines applicable to instrumentation and control systems important to safety which are included in the evaluation of these systems as addressed in Chapter 7 of the SAR. TMI Action Plan requirements for instrumentation and control systems important to safety are identified in Table 7-2 (Ref. 2).

Other acceptance criteria which are applicable to instrumentation and control systems important to safety are not included when the evaluation of conformance to such criteria is addressed in the review of other SAR sections. For example, GDC 3 "Fire Protection," is not included in Table 7.1 since conformance to the requirements of GDC 3 is addressed in the review of Section 9.5.1 of the SAR.

Appendix A (Ref. 3) to this SRP section provides guidance on the applicability and review methods to be used in the evaluation of conformance to the acceptance criteria and guidelines for instrumentation and control systems important to safety. Appendix B (Ref. 4) to this SRP section provides guidance to be used in the evaluation of conformance to the requirements of IEEE Std 279.

III. REVIEW PROCEDURES

The objectives of the review are to confirm that the instrumentation and control systems important to safety, addressed in Chapter 7 of the SAR, are identified with the appropriate acceptance criteria and guidelines applicable to each of these systems. This identification meets the applicable requirements of General Design Criterion 1, "Quality Standards and Records," of Appendix A of 10 CFR Part 50. General Design Criterion 1 requires that, "Structures, systems and components important to safety shall be designed, fabricated, erected and tested to quality standards commensurate with the importance of the safety function to be performed." Therefore, the review should confirm that the SAR includes (1) a discussion regarding the applicability of each criterion and guideline for each system important to safety, and (2) a statement that the criteria and guidelines are implemented (OL) or will be implemented (CP) in the design of instrumentation and control systems important to safety. If exceptions are taken to the guidelines, the review confirms that an acceptable basis has been provided for any exceptions.

The review of Section 7.1 of the SAR is performed as follows:

1. The categories of systems important to safety included in the areas of review for Chapter 7 of the SAR provided above should be used in assessing the completeness of the identification. The identification of instrumentation and control systems important to safety are reviewed to confirm that it is consistent with the design bases for safety systems as provided in other sections of the SAR, particularly in Chapters 5, 6, 8, 9, 10, and

15, and in subsequent sections of Chapter 7. The review of the systems identified is coordinated with the branches which have primary review responsibility for these systems.

2. The acceptance criteria applicable to each of the instrumentation and control systems important to safety are reviewed to confirm that the appropriate criteria have been identified for each system. Appendix A to this SRP section identifies the acceptance criteria applicable to the instrumentation and control systems important to safety and describes the method and scope of the review required to verify conformance.

3. The guidelines applicable to each of the instrumentation and control systems important to safety are reviewed to confirm that the appropriate guidelines have been identified for each system. Appendix A to this SRP section identifies the guidelines applicable to the instrumentation and control systems important to safety and describes the method and scope of the review required to verify conformance.

4. When the applicant takes exceptions to the guidelines applicable to instrumentation and control systems important to safety, the bases for such exception are reviewed to confirm that they are acceptable. The bases for the exceptions to the guidelines must demonstrate that a significant reduction in the margin of safety does not result and that the exceptions do not result in nonconformance to the requirements of the acceptance criteria.

5. The review includes those instrumentation and control systems important to safety that are identified as identical to systems that have been reviewed and approved by the staff. The evaluation of these systems in subsequent sections of Chapter 7 may be based upon prior staff approval. Where differences exist between prior approvals, they should be identified and the review should confirm that an adequate basis has been provided. The review should include an evaluation of differences to confirm that they are acceptable.

IV. EVALUATION FINDINGS

The review confirms that sufficient information has been provided and that the review supports conclusions of the following type to be included in the staff's safety evaluation report (SER).

> The applicant has identified the instrumentation and control systems important to safety and the acceptance criteria consisting of the General Design Criteria (GDC) and IEEE Std. 279, included in the Commission's regulations, which are applicable to those systems as identified in the Standard Review Plan (SRP). The applicant has also identified the guidelines consisting of the regulatory guides and the industry codes and standards which are applicable to the systems as identified in the SRP. (If exception to the guidelines has been taken by the applicant an evaluation of the exception or a reference to the section of the SER which addresses those exceptions should be provided.) We conclude that the implementation of the identified acceptance criteria and guidelines satisfies the requirements of GDC 1 with respect to the design, fabrication, erection, and testing to quality standards commensurate with the importance of the safety functions to be performed.

V. IMPLEMENTATION

The following is intended to provide guidance to applicants and licensees regarding the NRC staff's plans for using this SRP section.

Except in those cases in which the applicant proposes an acceptable alternative method for complying with specified portions of the Commission's regulations, the method described herein will be used by the staff in its evaluation of conformance with Commission regulations.

Implementation schedules for conformance to parts of the method discussed herein are contained in the referenced regulatory guides.

VI. REFERENCES

1. Standard Review Plan Section 7.1, Table 7-1, "Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety."

2. Standard Review Plan Section 7.1, Table 7-2, "TMI Action Plan Requirements for Instrumentation and Control Systems Important to Safety."

3. Standard Review Plan Section 7.1, Appendix A, "Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety."

4. Standard Review Plan Section 7.1, Appendix B, "Guidance for Evaluation of Conformance to IEEE Std 279."

5. Standard Review Plan, Appendix 7-A, "Branch Technical Position (ICSB)."

STANDARD REVIEW PLAN

TABLE 7-1

ACCEPTANCE CRITERIA AND GUIDELINES FOR

INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY

The matrix of Table 7-1 identifies the acceptance criteria (denoted by "A") and the guidelines (denoted by "G") and their applicability to the various sections of Chapter 7 of the SAR. These acceptance criteria include the applicable General Design Criteria and IEEE Standard 279 which establish the Commission requirements for the instrumentation and control systems important to safety. The guidelines for implementation of these requirements are provided in Regulatory Guides, the endorsed IEEE Standards and the Branch Technical Positions (BTP) of the Instrumentation and Control Systems Branch (ICSB). The BTPs listed in this table are contained in Appendix 7-A to Chapter 7 of the SRP. The guidelines are not mandatory and only set forth acceptable methods of implementing the acceptance criteria. The branch technical positions (Ref. 5) are used when a particular design problem has an identified and acceptable solution; they also are not mandatory. In all cases, the primary basis for acceptance of the design is conformance to the acceptance criteria.

Industry standards that are not endorsed by regulatory guides or incorporated in regulations or branch technical positions, or that have not been previously used and accepted in the licensing process, must be reviewed before they can be accepted as a sole basis for approval of a design. They are useful as guidance for identifying the subjects of importance to be considered in the review of the systems important to safety.

ACCEPTANCE CRITERIA FOR INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY - TABLE 7-1

CRITERIA	TITLE	APPLICABILITY							REMARKS
		7.1	7.2	7.3	7.4	7.5	7.6	7.7	
1. 10 CFR Part 50									
a. § 50.55a(h)	Criteria for Protection Systems for Nuclear Power Generating Stations (IEEE Std 279)		A	A	*	*	*		
2. General Design Criteria (GDC), Appendix A to 10 CFR Part 50									
a. GDC 1	Quality Standards and Records	A							
b. GDC 2	Design Bases for Protection Against Natural Phenomena		A	A	A	A	A		
c. GDC 4	Environmental and Missile Design Bases		A	A	A	A	A		
d. GDC 13	Instrumentation and Control		A	A	A	A	A	A	
e. GDC 19	Control Room		A	A	A	A	A	A	
f. GDC 20	Protection System Functions		A	A					

*Although not required by the Commission Regulations, the criteria of IEEE Std 279 address considerations such as design bases, redundancy, independence, single failures, qualification, bypasses, status indication and testing that are used as guidance, where appropriate, for systems addressed in these sections of the SRP.

TABLE 7-1 (CONTINUED)

CRITERIA	TITLE	APPLICABILITY						REMARKS
		7.1	7.2	7.3	7.4	7.5	7.6	7.7	
g. GDC 21	Protection Systems Reliability and Testability		A	A					
h. GDC 22	Protection System Independence		A	A					
i. GDC 23	Protection System Failure Modes		A	A					
j. GDC 24	Separation of Protection and Control Systems		A	A					
k. GDC 25	Protection System Requirements for Reactivity Control Malfunctions		A						
l. GDC 29	Protection Against Anticipated Operational Occurrences		A	A					
3. Regulatory Guides (RG)									
a. RG 1.22	Periodic Testing of Protection System Actuation Functions		G	G	G	G	G		
b. RG 1.47	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems		G	G	G	G	G		
c. RG 1.53	Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems		G	G	G	G	G		See IEEE Std 379 (ANSI N41.2)

TABLE 7-1 (CONTINUED)

CRITERIA	TITLE	APPLICABILITY						REMARKS
		7.1	7.2	7.3	7.4	7.5	7.6	7.7	
d. RG 1.62	Manual Initiation of Protection Actions		G	G	G		G		
e. RG 1.75	Physical Independence of Electric Systems		G	G	G	G	G		See IEEE Std 384 (ANSI N41.14)
f. RG 1.97	Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident					G			See ANSI/ANS 4.5
g. RG 1.105	Instrument Spans and Setpoints		G	G	G	G	G		
h. RG 1.118	Periodic Testing of Electric Power and Protection Systems		G	G	G	G	G		See IEEE Std 338
i. RG 1.151	Instrument Sensing Lines					G		G	See ANSI/ISA-S67.02
4. Branch Technical Positions (BTP) ICSB									
a. BTP ICSB 3	Isolation of Low Pressure Systems from the High Pressure Reactor Coolant System						G		
b. BTP ICSB 4	Requirements on Motor-Operated Valves in the ECCS Accumulator Lines						G		
c. BTP ICSB 12	Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service		G	G					

TABLE 7-1 (CONTINUED)

CRITERIA	TITLE	APPLICABILITY							REMARKS
		7.1	7.2	7.3	7.4	7.5	7.6	7.7	
d. BTP ICSB 13	Design Criteria for Auxiliary Feedwater Systems			G					
e. BTP ICSB 14	Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors		G					G	
f. BTP ICSB 16	Control Element Assembly (CEA) Interlocks in Combustion Engineering Reactors		G						
g. BTP ICSB 20	Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode			G					
h. BTP ICSB 21	Guidance for Application of Reg. Guide 1.47		G	G	G	G	G		
i. BTP ICSB 22	Guidance for Application of Reg. Guide 1.22		G	G	G	G	G		
j. BTP ICSB 26	Requirements for Reactor Protection System Anticipatory Trips		G						

STANDARD REVIEW PLAN

TABLE 7-2

TMI ACTION PLAN REQUIREMENTS FOR

INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY

The matrix of Table 7-2 identifies the TMI action plan requirements and their applicability (denoted by "A") to the various sections of Chapter 7 of the SAR. Further clarification of the action plan requirements are provided in the referenced NUREGs.

IMI ACTION PLAN REQUIREMENTS FOR INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY - TABLE 7-2

ITEM	TITLE	APPLICABILITY 7.1	7.2	7.3	7.4	7.5	7.6	7.7	NUREGs*
II.D.3	Relief and safety valve position indication					A			0718, 0737, 0694
II.E.1.2	Auxiliary feedwater system automatic initiation and flow indication			A					0718, 0737, 0694
II.E.4.2	Containment Isolation Dependability Positions (4), (6) & (7)			A					
II.F.1	Accident monitoring instrumentation Positions (4), (5), and (6)					A			0718, 0737, 0694
II.F.3	Instrumentation for monitoring accident conditions (RG 1.97, Rev. 2)					A			0718
II.K.1	IE Bulletins								
.21	Safety-grade anticipatory trip								Superceded by II.K.2.10
.23	RV level indication					A			0694
II.K.2	Orders on B&W plants								
.8	Auxiliary feedwater system upgrading								Superceded by II.E.1.2
.9	FMEA on the ICS							A	0718, 0737, 0694
.10	Safety-grade anticipatory trip		A						0718, 0737, 0694
II.K.3	Final recommendations, B&O Task Force								
.1	Auto PORV isolation						A		0737
.9	PID controller							A	0737, 0694
.10	Proposed anticipatory trip modification		A						0737, 0694
.12	Anticipatory reactor trip		A						0737, 0694
.13	HPCI and RCIC initiation levels			A					0718, 0737
.15	Isolation of HPCI and RCIC			A					0737
.18	ADS actuation			A					0718, 0737
.21	Restart of LPCS and LCPI			A					0718, 0737
.22	RCIC automatic switchover			A					0737
.23	Central water level recording					A			0718

*NUREG-0718, "Licensing Requirements for Pending Applications for Construction Permits and Manufacturing License," NUREG-0737, "Clarification of TMI Action Plan Requirements," and NUREG-0694, "TMI-Related Requirements for New Operating Licenses."

APPENDIX A

STANDARD REVIEW PLAN SECTION 7.1

ACCEPTANCE CRITERIA AND GUIDELINES FOR INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY

The acceptance criteria and guidelines for instrumentation and control systems important to safety are divided into two categories: (1) Regulations including the General Design Criteria and IEEE 279 (paragraph 50.55a(h) of 10 CFR Part 50) and (2) Regulatory Guides (including endorsed industry codes and standards) and Branch Technical Positions. For each criterion and guideline, a statement is provided on its applicability to the review of instrumentation and control systems. Conformance to the requirements of GDC 1 is evaluated in the review of Section 7.1 of the SAR. Conformance to the requirement of the remainder of the GDC applicable to instrumentation and control systems is evaluated on a system basis in the review of the system as described in SAR Sections 7.2 through 7.7. Likewise, the degree of conformance to the guidelines provided in regulatory guides and industry codes and standards is evaluated on a system basis in the review of Sections 7.2 through 7.7 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.

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

1. Regulations (General Design Criteria and IEEE Std 279)

   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 instrumentation and control systems and components important to safety.

Review Methods: Regulatory guides and endorsed codes and standards applicable to instrumentation and control systems important to safety are identified in Section 2 of this Appendix. These guidelines provide the information required 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 therefore 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 systems and components important to safety.

Review Methods: The design bases for protection against natural phenomena for instrumentation and control systems important to safety should be provided for each system in the subsequent sections of Chapter 7 of the SAR. The design bases should identify those systems and components which are qualified to survive the effects of earthquakes and other natural phenomena. The review should confirm that the instrument and control 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 consistant with these requirements.

The evaluation of the adequacy of qualification programs to demonstrate the capability of instrumentation and control systems to withstand the effects of natural phenomena is addressed in the review of Section 3.10 of the SAR.

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 instrumentation and control systems and components important to safety.

Review Methods: The environmental and missile design bases for instrumentation and control 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 which are qualified to accommodate the effects of environmental conditions and protected for dynamic effects of missiles, pipe whipping, and discharging fluids. If systems or components are qualified to survive the environmental effects of postulated accidents for only finite periods of time, the bases for limited operability should be provided. The review should confirm that the instrument and control systems important to safety are qualified to be compatible with the environmental effects of accidents consistent with the analysis of these events as provided in Chapter 15 and with the effects of missiles as provided in Chapter 3 of the SAR.

The evaluation of the adequacy of qualification programs to demonstrate the capability of instrumentation and control systems to accommodate the environmental effects of postulated accidents and missiles is addressed in the review of Section 3.11 of the SAR.

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 instrumentation and control systems.

Review Methods: Regulatory Guide (RG) 1.97 provides guidance on conformance to GDC 13 for information systems important to safety. RG 1.151 provides guidance on conformance to GDC 13 for instrument sensing line as related to providing protection due to extreme cold weather. The evaluation of conformance to this aspect of GDC 13 is addressed in the

review of Section 7.5 of the SAR. The evaluation of control systems to maintain system variables within prescribed operating ranges is addressed in the review of Section 7.7 of the SAR.

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: The control room and instrumentation and control systems important to safety.

Review Methods: RG 1.97 provides guidance on conformance to GDC 19 for information systems provided in the control room from which actions can be taken to operate the unit safely. The evaluation of conformance to this aspect of GDC 19 is addressed in the review of Section 7.5 of the SAR. The evaluation of plant control systems used during normal operation is addressed in the review of Section 7.7 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.

Guidance does not exist to specifically define indication and controls features which should be provided at appropriate locations outside the control room. Guidelines for the review of remote shutdown capabilities are provided in SRP Section 7.4. The evaluation of conformance to this aspect of GDC 19 is addressed in the review of Section 7.4 of the SAR.

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 accept-

able 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: reactor trip system (RTS), engineered safety features actuation system (ESFAS).

Review Method: Chapter 15 of the SAR provides the bases for protective system functions for anticipated operational occurrences and accidents. The evaluation of conformance to GDC 20 is 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 inservice 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 and ESFAS.

Review Methods: See RGs 1.22, 1.47, 1.53, 1.118 and IEEE Stds 338 and 379 below. The evaluation of conformance to GDC 21 is 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 and ESFAS.

Review Methods: See RG 1.75 and IEEE Std 384 below. The evaluation of conformance to GDC 22 is addressed in the review of Sections 7.2 and 7.3 of the SAR.

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 and ESFAS.

Review Methods: RG 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants," states that an analysis should be performed to demonstrate conformance to the requirements of the GDC. Conformance to the requirements of GDC 23 is 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: The protection systems: RTS and ESFAS.

Review Methods: Requirements related to control and protection system interaction are given in Section 4.7 of IEEE Std 279. Conformance to the requirements of GDC 24 is addressed in the review of Sections 7.2 and 7.3 of the SAR.

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 and reactivity control system interlocks identified in Chapter 15, if required, to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems.

Review Methods: Chapter 15 of the SAR provides the bases for the protection system and reactivity control system interlocks. Section 7.7 should provide an evaluation of failures in the reactivity control systems. The evaluation of conformance to the requirement of GDC 25 is addressed in the review of the reactor trip system in Section 7.2, and in the review of reactivity control system interlocks in Section 7.7 of the SAR. See BTP ICSB 14.

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 and reactivity control systems.

Review Methods: Conformance to requirements of GDC 29 is concluded based upon conformance of the protection system and reactivity control systems to the above applicable GDCs. Probabilistic reliability assessments may be performed by the Commission to provide a basis for development of deterministic criteria for specific systems. However, 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.

m. IEEE-279, Criteria for Protection Systems for Nuclear Power Generating Stations (10 CFR Part 50, § 50.55a(h)).

Applicability: The protection systems: RTS and ESFAS.

Review Methods: Appendix B to SRP Section 7.1 provides guidance for the evaluation of conformance to the requirements of IEEE Std 279, including the applicable regulatory guides as noted in Item 2 below.

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

a. RG 1.22, "Periodic Testing of Protection System Functions."

Applicability: The protection systems: RTS and ESFAS.

Review Methods: Provides bases for evaluating conformance to GDC 21 and IEEE Std 279, Sections 4.10 through 4.13.

b. RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System."

Applicability: All instrumentation and control systems which perform a safety function.

Review Methods: Provides a bases for evaluating conformance to GDC 21 and IEEE Std 279, Section 3.14 for protection systems. Provides a bases for evaluating the adequacy of bypass and inoperable status indication for instrumentation and control systems important to safety as addressed in the review of Section 7.5 of the SAR.

c. RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems." (Endorses IEEE Std 379, "Guide for the Application of the Single Failure Criterion to Nuclear Power Generating Station Protection System.")

Applicability: The protection systems: RTS and ESFAS.

Review Methods: Provides a bases for evaluating conformance to GDC 21 and IEEE Std 279, Section 4.2.

d. RG 1.62, "Manual Initiation of Protection Action."

Applicability: The protection systems: RTS and ESFAS.

Review Methods: Provides a basis for evaluating conformance to IEEE Std 279, Section 4.17.

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

Applicability: All instrumentation and control systems important to safety.

Review Methods: Provides a basis for evaluating conformance to GDC 21 and IEEE Std 279, Section 4.6 for protection systems. Provides a basis for evaluating the adequacy of instrumentation and control systems important to safety which incorporate redundant or diverse features to satisfy the single failure criterion. The ICSB evaluation is limited to the review of components and electrical wiring internals to 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. RG 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: Provides a basis for evaluating conformance to GDC 13. The ICSB 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.

g. RG 1.105, "Instrument Spans and Setpoints."

Applicability: The instrumentation and control systems important to safety.

Review Methods: Provides a basis for evaluating conformance to GDC 13 and IEEE Std 279, Section 3.

h. RG 1.118, "Periodic Testing of Electric Power and Protection Systems." (Endorses IEEE Std 338, "Criteria for Periodic Testing of Nuclear Power Generating Station Protection Systems.")

Applicability: The protection system: RTS and ESFAS.

Review Methods: Provides a basis for evaluating conformance to GDC 21 and IEEE Std 279, Section 4.16. The ICSB evaluation is limited to the review of testing of protection systems. The evaluation of testing of electric power systems is addressed in the review of Chapter 8 of the SAR.

i. RG 1.51, "Instrument Sensing Lines." (Enclosures ANSI/ISA-S67.02," Nuclear Safety Related Instrument Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants.")

Applicability: Safety related instrument sensing lines.

Review Methods: Provides a basis for evaluating conformance to GDC 13. The ICSB evaluation should be based on meeting the guidance provided in Regulatory Position 5 of the guide.

j. Branch Technical Positions (BTPs).

Applicability: As noted in the BTPs in Appendix 7-A of the SRP.

Review Methods: The BTPs provide bases for evaluating specific problem areas as identified in the BTPs.

APPENDIX A

STANDARD REVIEW PLAN SECTION 7.1

ACCEPTANCE CRITERIA AND GUIDELINES FOR INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY

The acceptance criteria and guidelines for instrumentation and control systems important to safety are divided into two categories: (1) Regulations including the General Design Criteria and IEEE 279 (paragraph 50.55a(h) of 10 CFR Part 50) and (2) Regulatory Guides (including endorsed industry codes and standards) and Branch Technical Positions. For each criterion and guideline, a statement is provided on its applicability to the review of instrumentation and control systems. Conformance to the requirements of GDC 1 is evaluated in the review of Section 7.1 of the SAR. Conformance to the requirement of the remainder of the GDC applicable to instrumentation and control systems is evaluated on a system basis in the review of the system as described in SAR Sections 7.2 through 7.7. Likewise, the degree of conformance to the guidelines provided in regulatory guides and industry codes and standards is evaluated on a system basis in the review of Sections 7.2 through 7.7 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.

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

1. Regulations (General Design Criteria and IEEE Std 279)

   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 instrumentation and control systems and components important to safety.

Review Methods: Regulatory guides and endorsed codes and standards applicable to instrumentation and control systems important to safety are identified in Section 2 of this Appendix. These guidelines provide the information required 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 therefore 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 systems and components important to safety.

Review Methods: The design bases for protection against natural phenomena for instrumentation and control systems important to safety should be provided for each system in the subsequent sections of Chapter 7 of the SAR. The design bases should identify those systems and components which are qualified to survive the effects of earthquakes and other natural phenomena. The review should confirm that the instrument and control 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 consistant with these requirements.

The evaluation of the adequacy of qualification programs to demonstrate the capability of instrumentation and control systems to withstand the effects of natural phenomena is addressed in the review of Section 3.10 of the SAR.

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 instrumentation and control systems and components important to safety.

Review Methods: The environmental and missile design bases for instrumentation and control 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 which are qualified to accommodate the effects of environmental conditions and protected for dynamic effects of missiles, pipe whipping, and discharging fluids. If systems or components are qualified to survive the environmental effects of postulated accidents for only finite periods of time, the bases for limited operability should be provided. The review should confirm that the instrument and control systems important to safety are qualified to be compatible with the environmental effects of accidents consistent with the analysis of these events as provided in Chapter 15 and with the effects of missiles as provided in Chapter 3 of the SAR.

The evaluation of the adequacy of qualification programs to demonstrate the capability of instrumentation and control systems to accommodate the environmental effects of postulated accidents and missiles is addressed in the review of Section 3.11 of the SAR.

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 instrumentation and control systems.

Review Methods: Regulatory Guide (RG) 1.97 provides guidance on conformance to GDC 13 for information systems important to safety. The evaluation of conformance to this aspect of GDC 13 is addressed in the review of Section 7.5 of the SAR. The evaluation of control systems to maintain system variables within prescribed operating ranges is addressed in the review of Section 7.7 of the SAR.

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: The control room and instrumentation and control systems important to safety.

Review Methods: RG 1.97 provides guidance on conformance to GDC 19 for information systems provided in the control room from which actions can be taken to operate the unit safely. The evaluation of conformance to this aspect of GDC 19 is addressed in the review of Section 7.5 of the SAR. The evaluation of plant control systems used during normal operation is addressed in the review of Section 7.7 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.

Guidance does not exist to specifically define indication and controls features which should be provided at appropriate locations outside the control room. Guidelines for the review of remote shutdown capabilities are provided in SRP Section 7.4. The evaluation of conformance to this aspect of GDC 19 is addressed in the review of Section 7.4 of the SAR.

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: reactor trip system (RTS), engineered safety features actuation system (ESFAS).

Review Method: Chapter 15 of the SAR provides the bases for protective system functions for anticipated operational occurrences and accidents. The evaluation of conformance to GDC 20 is 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 inservice 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 and ESFAS.

Review Methods: See RGs 1.22, 1.47, 1.53, 1.118 and IEEE Stds 338 and 379 below. The evaluation of conformance to GDC 21 is 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 and ESFAS.

Review Methods: See RG 1.75 and IEEE Std 384 below. The evaluation of conformance to GDC 22 is addressed in the review of Sections 7.2 and 7.3 of the SAR.

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 and ESFAS.

Review Methods: RG 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants," states that an analysis should be performed to demonstrate conformance to the requirements of the GDC. Conformance to the requirements of GDC 23 is 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: The protection systems: RTS and ESFAS.

Review Methods: Requirements related to control and protection system interaction are given in Section 4.7 of IEEE Std 279. Conformance to the requirements of GDC 24 is addressed in the review of Sections 7.2 and 7.3 of the SAR.

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 and reactivity control system interlocks identified in Chapter 15, if required, to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems.

Review Methods: Chapter 15 of the SAR provides the bases for the protection system and reactivity control system interlocks. Section 7.7 should provide an evaluation of failures in the reactivity control systems. The evaluation of conformance to the requirement of GDC 25 is addressed in the review of the reactor trip system in Section 7.2, and in the review of reactivity control system interlocks in Section 7.7 of the SAR. See BTP ICSB 14.

1. 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 and reactivity control systems.

Review Methods: Conformance to requirements of GDC 29 is concluded based upon conformance of the protection system and reactivity control systems to the above applicable GDCs. Probabilistic reliability assessments may be performed by the Commission to provide a basis for development of deterministic criteria for specific systems. However, 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.

m. IEEE-279, Criteria for Protection Systems for Nuclear Power Generating Stations (10 CFR Part 50, § 50.55a(h)).

Applicability: The protection systems: RTS and ESFAS.

Review Methods: Appendix B to SRP Section 7.1 provides guidance for the evaluation of conformance to the requirements of IEEE Std 279, including the applicable regulatory guides as noted in Item 2 below.

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

a. RG 1.22, "Periodic Testing of Protection System Functions."

Applicability: The protection systems: RTS and ESFAS.

Review Methods: Provides bases for evaluating conformance to GDC 21 and IEEE Std 279, Sections 4.10 through 4.13.

b. RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System."

Applicability: All instrumentation and control systems which perform a safety function.

Review Methods: Provides a bases for evaluating conformance to GDC 21 and IEEE Std 279, Section 3.14 for protection systems. Provides a bases for evaluating the adequacy of bypass and inoperable status indication for instrumentation and control systems important to safety as addressed in the review of Section 7.5 of the SAR.

c. RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems." (Endorses IEEE Std 379, "Guide for the Application of the Single Failure Criterion to Nuclear Power Generating Station Protection System.")

Applicability: The protection systems: RTS and ESFAS.

Review Methods: Provides a bases for evaluating conformance to GDC 21 and IEEE Std 279, Section 4.2.

d. RG 1.62, "Manual Initiation of Protection Action."

Applicability: The protection systems: RTS and ESFAS.

Review Methods: Provides a basis for evaluating conformance to IEEE Std 279, Section 4.17.

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

Applicability: All instrumentation and control systems important to safety.

Review Methods: Provides a basis for evaluating conformance to GDC 21 and IEEE Std 279, Section 4.6 for protection systems. Provides a basis for evaluating the adequacy of instrumentation and control systems important to safety which incorporate redundant or diverse features to satisfy the single failure criterion. The ICSB evaluation is limited to the review of components and electrical wiring internals to 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. RG 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: Provides a basis for evaluating conformance to GDC 13. The ICSB 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.

g. RG 1.105, "Instrument Spans and Setpoints."

Applicability: The instrumentation and control systems important to safety.

Review Methods: Provides a basis for evaluating conformance to GDC 13 and IEEE Std 279, Section 3.

h. RG 1.118, "Periodic Testing of Electric Power and Protection Systems." (Endorses IEEE Std 338, "Criteria for Periodic Testing of Nuclear Power Generating Station Protection Systems.")

Applicability: The protection system: RTS and ESFAS.

Review Methods: Provides a basis for evaluating conformance to GDC 21 and IEEE Std 279, Section 4.16. The ICSB evaluation is limited to the review of testing of protection systems. The evaluation of testing of electric power systems is addressed in the review of Chapter 8 of the SAR.

i. Branch Technical Positions (BTPs).

Applicability: As noted in the BTPs in Appendix 7-A of the SRP.

Review Methods: The BTPs provide bases for evaluating specific problem areas as identified in the BTPs.

APPENDIX B

STANDARD REVIEW PLAN SECTION 7.1

GUIDANCE FOR EVALUATION OF CONFORMANCE TO IEEE STD 279

10 CFR Part 50, § 50.55a(h) of the Commission Regulations requires protection systems to meet the requirements of IEEE Std 279. The Scope of IEEE Std 279 indicates that protection systems include those systems that actuate reactor trip and that in the event of a serious reactor accident, actuate engineered safeguards features. This appendix discusses the requirements of IEEE Std 279, Sections 3 and 4, as they are used in the review of the RTS and ESFAS to determine that these systems meet Commission Regulations, although not required by Commission Regulations, the criteria of IEEE Std 279 address considerations such as design bases, redundancy, independence, single failures, qualification, bypasses, status indication, and testing that are used as guidance, where appropriate, for instrumentation and control systems not a part of the protection system but having a high degree of importance to safety.

1. Section 3, Design Bases - This section requires that a specific protection system design basis be provided. Section 3(1) requires the identification of conditions which require protective action. This information should be consistent with the analysis provided in Chapter 15 of the SAR.

   Section 3(2) requires the identification of variables that are monitored in order to provide protective action. The tables in Sections 7.2 and 7.3 of the SAR should provide this information.

   Section 3(3) requires the identification of the minimum number and location of sensors for those variables in 3(2) that have a spatial dependence. The applicant's analysis should demonstrate that the number and location of sensors are adequate.

   Sections 3(4), 3(5), and 3(6) require the identification of operational limits, the margin between operational limits and the level for the onset of unsafe conditions (setpoint), and limits which require protective action (safety limit - i.e., value assumed in the safety analysis) for each variable. The applicant's analysis should confirm that there is adequate margin between operating limits and setpoints such that there is a low probability for inadvertent actuation of the system. The applicant's analysis should confirm that there is adequate margin between set points and safety limits such that the system initiates protective actions before safety limits are exceeded.

   Section 3(7) requires that the range of transient and steady-state conditions of both the energy supply and the environment during normal, abnormal, and accident conditions for which the system must perform be identified. This information is used in subsequent evaluations.

   Section 3(8) requires that the malfunctions, accidents, or other unusual events which could physically damage protective system components or could cause environmental changes leading to functional degradation of system performance, and for which provisions must be incorporated to

retain necessary protective action be identified. This information is used in subsequent evaluations.

Section 3(9) requires that the performance requirements including system response times, system accuracies, ranges, and rates of change of sensed variables to be accommodated until conclusion of the protective action be identified. The applicant's analysis, including the applicable portion provided in Chapter 15, should confirm that the system performance requirements are adequate to assure completion of protective actions. Regulatory Guide (RG) 1.105, "Instrument Spans and Set Points," provides guidance for evaluating Sections 3(5) and 3(9).

2. Section 4.1, General Functional Requirements - This section requires that the protection system shall, with precision and reliability, automatically initiate protective action for the range of conditions and performance enumerated in Sections 3(7) through 3(9). The applicant's analysis should confirm that the protection system has been qualified to demonstrate that the performance requirements are met. The evaluation of the precision of the protection system is addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis. The evaluation of reliability of the protection system is addressed to the extent that conservatively rated high quality components are used. Automatic initiation is required for all protective functions. Manual initiation is also a requirement (see Section 4.17 and RG 1.62).

3. Section 4.2, Single Failure Criterion - This section requires that any single failure within the protection system shall not prevent proper protective action at the system level when required. The applicant's analysis should confirm that the requirements of the single failure criterion are satisfied. Guidance in the application of the single failure criterion is provided in IEEE Std 379 as supplemented by RG 1.53. Components and systems not qualified for seismic events or accident environments and nonsafety-grade components and systems are assumed to fail to function if failure adversely affects protection system performance. These components and systems are assumed to function if functioning adversely affects protection system performance. All failures in the protection system that can be predicted as a result of an event for which the protection system is designed to provide a protective function are assumed to occur if the failure adversely affects the protection system performance. In general, the lack of equipment qualification may serve as a bases to assume failures. After assuming the failures of nonsafety-grade, nonqualified equipment and those failures caused by a specific event, a random single failure is arbitrarily assumed. With these failures assumed, the protection system must be capable of performing the protective functions required to mitigate the consequences of the specific event.

4. Section 4.3, Quality of Components and Modules - The applicant should confirm that quality assurance provisions of Appendix B to 10 CFR Part 50 are applicable to the protection system. The evaluation of the adequacy of the quality assurance program is addressed in the review of Chapter 17 of the SAR.

5. Section 4.4, Equipment Qualification - The applicant should confirm that the protection system equipment is designed to meet the functional performance requirements over the range of normal environmental conditions for the area in which it is located. The applicant should confirm that a single failure within the environmental control system for any area in which protection system equipment is located will not result in conditions which could result in damage to the protection system equipment nor prevent the balance of the protection system not within the area from accomplishing its safety function. In this regard, the loss of an environmental control system is treated as a single failure which should not prevent the protection system from accomplishing its safety functions. In that loss of environmental control systems do not usually result in prompt changes in environmental conditions, the design bases may rely upon monitoring environmental conditions in areas and taking appropriate action to assure that extremes in environmental conditions are maintained within nondamage limits until the environmental control systems are returned to normal operation. If such bases are used, the applicant should confirm that there is independence between environmental control systems and sensing systems which would indicate the failure or malfunctioning of environmental control systems.

   The evaluation of conformance to the requirements of GDC 2 and 4 satisfies the requirements for equipment qualification to harsh environments and seismic events. Guidance for the review of this aspect of equipment qualification is given in Appendix A to SRP Section 7.1.

6. Section 4.5, Channel Integrity - Information provided in Sections 3(7) and 3(8) is reviewed to confirm that the design includes the qualification of equipment for the conditions identified in the design bases. Consequential failures are not an acceptable base for satisfying this requirement. The review should confirm that tests have been conducted on protection system equipment components and the system racks and panels as a whole to demonstrate the functional performance requirements of the protection system over the range of transient and steady-state conditions of both the energy supply and the environment. Where tests have not been conducted, the applicant should confirm that the protection system components are conservatively designed to operate over the range of service conditions.

7. Section 4.6, Channel Independence - Guidance for evaluation of channel independence is provided in IEEE Std 384 as supplemented by RG 1.75. The applicant should confirm that the protection system design precludes the use of components that are common to redundant channels, such as actuation, reset, mode, and test switches; common sensing lines; or any other features which could compromise the independence of redundant channels. Electrical independence shall include the utilization of separate power sources. Physical independence is attained by physical separation and physical barriers.

8. Section 4.7, Control and Protection System Interaction - Control and protection system interaction involves more than examining the electrical isolation and interconnection. The functional performance of control systems must be such that a control system cannot prevent proper action of a protection system. This section of IEEE Std 279, with regard to isolation devices and multiple failures resulting from a credible single event, is explained by example in the document. The applicant's analysis

should confirm that the requirements for control and protection system interaction are satisfied. See Section 4.2 above.

9. Section 4.8, Derivation of System Inputs - This requirement is self-explanatory. A protection system that requires loss of flow protection would normally derive its signal from flow sensors. A design might use an indirect parameter such as a pressure signal or pump speed. However, the applicant should verify that any indirect parameter would be valid for all events.

   Even a directly measured variable should be reviewed and its response to postulated events compared with the credit taken for the parameter in the events for which it provides protection.

10. Section 4.9, Capability for Sensor Checks - The most common method used to verify the availability of the input sensors is by cross checking between redundant channels that have readout available. When only two channels of readout are provided; the applicant should state the basis used to ensure that an operator will not take incorrect action when the two channel readouts differ. The applicant should state the method to be used for checking the operational availability of nonindicating sensors.

11. Section 4.10, Capability for Test and Calibration - Guidance on periodic testing of the protection system is provided in RG 1.22 and in IEEE Std 338 as supplemented by RG 1.118. The extent of test and calibration capability provided bears heavily on whether the design meets the single failure criterion. Any failure that is not detectable must be considered concurrently with any random postulated, detectable, single failure. Periodic testing should duplicate, as closely as practical, the overall performance required of the protection system. The test should confirm operability of both the automatic and manual circuitry. The capability should be provided to permit testing during power operation. When this capability can only be achieved by overlapping tests, the test scheme must be such that the tests do, in fact, overlap from one test segment to another. Test procedures that require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment are not acceptable test procedures for use during power operation. Periodic tests conducted during power operation should use only permanently installed test equipment.

12. Section 4.11, Channel Bypass and Removal from Operations - In general, it is an operational rather than a safety problem if testing causes the initiation of a protective action.

13. Section 4.12, Operating Bypass - The requirement for automatic removal of operational bypasses means that the reactor operator shall have no role in such removal. The operator may be required to take action to prevent the unnecessary initiation of a protective action, and this is acceptable.

14. Section 4.13, Indication of Bypass - Guidance on bypasses and inoperable status indication is provided in RG 1.47 and BTP ICSB 21.

15. Section 4.14, Access to Means for Bypassing - In practice, administrative control is used as the basis for assuring that access to the means for bypassing is limited to qualified plant personnel and that permission of the control room operator is obtained to gain access.

16. Section 4.15, Multiple Setpoints - The staff interpretation of "positive means" is that automatic action is provided to ensure that the more restrictive setpoint is used when required.

17. Section 4.16, Completion of a Protective Action Once it is Initiated - Self-explanatory.

18. Section 4.17, Manual Initiation - Guidance on manual initiation of protective action is provided in RG 1.62.

19. Section 4.18, Access to Setpoint Adjustments, Calibrations, and Test Points - See procedure above for Section 4.14.

20. Section 4.19, Identification of Protective Actions - The method of identification of status at the channel level may be accomplished by lights, indicators, and annunciators.

21. Section 4.20, Information Read-out - The method used to establish adequacy of information readout would include a review of the protection system inputs to annunciators and event recorders.

22. Section 4.21, System Repair - Self-explanatory.

23. Section 4.22, Identification - Guidance on identification is provided in IEEE Std 384 as supplemented by RG 1.75. The preferred identification method is color coding of components, cables, and cabinets.