C.I.7. Instrumentation and Controls

Nuclear power plant instrumentation senses various plant parameters and transmits appropriate signals to the control systems during normal operation, and to the reactor trip and engineered-safety-feature systems during abnormal and accident conditions. The information provided in this chapter should emphasize those instruments and associated equipment which constitute the protection and safety systems. 10 CFR 50.55a(h) requires protection systems to meet the requirements of IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," which provides criteria for applying IEEE Std 603 to computer systems, was endorsed by Regulatory Guide 1.152, Rev.2. Other IEEE Standards referenced in this document should be the revision endorsed by the current revision of a regulatory guide unless a specific revision in the document is provided. The analysis of control systems and instrumentation should be provided, particularly considerations of control system-induced transients which, if not terminated in a timely manner, could result in fuel damage, and subsequent fission product release to the environment and the public.

Information for post-accident monitoring should also be provided to guide the plant operators to take necessary manual actions for public safety.

Regardless of the type of application, the fundamental purpose is to demonstrate that the facility and equipment, the operating procedures, the processes to be performed, and other technical requirements provide reasonable assurance that the applicant/licensee will comply with the regulations of 10 CFR Chapter I, and that public health and safety will be protected.

The application should describe the applicable life-cycle development activities. The application should describe the system requirements and demonstrate how the final system meets these requirements. Non-digital-computer-based systems implementation may focus on component and system requirements, design outputs, and validation (e.g., type test). Computer-based systems should focus on demonstrating the disciplined and high quality implementation of the life-cycle activities.

Appendix C.I.7-A provides guidance on submittals related to digital instrumentation and control system applications. Appendix C.I.7-B provides guidance on submittals related to conformance with IEEE Std 603. Appendix C.I.7-C provides guidance on submittals related to conformance with IEEE Std 7-4.3.2. The information described in Appendices C.I.7-A, C.I.7-B, and C.I.7-C may be submitted in topical reports.

C.I.7.1 *Introduction*

C.I.7.1.1 Identification of Safety-Related Systems

The application document should list all instrumentation, control, and supporting systems that are safety related, including alarm, communication, and display instrumentation. The document should distinguish between those systems designed and built by the nuclear steam system supplier and those designed or built by others. Systems that are identical to those of a nuclear power plant of similar design that has recently received a COL license should be identified. Systems that are different should also be identified and the differences and their effects on safety-related systems should be discussed.

C.I.7.1.2 Identification of Safety Criteria

The application document should provide a regulatory requirements applicability matrix that lists all design bases, criteria, regulatory guides, standards, and other documents that will be implemented in the design of the systems listed in Section C.I.7.1.1. The specific information identified in SRP Chapter 7, Appendix 7.1-A, "Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety," should be included in this section of the SAR.

The Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety are divided into four categories: (1) regulations in 10 CFR 50.55a(h) including guidance in IEEE Std 603, (2) the General Design Criteria (GDC) of Appendix A to 10 CFR Part 50, (3) regulatory guides (including endorsed industry codes and standards), and (4) SRP Chapter 7, branch technical positions (10 CFR 50.34(h), conformance with the SRP).

The applicant should describe the technical design bases for all protection system functions, including the reactor trip function, engineered safety features, emergency power, interlocks, bypasses, and equipment protection. Diversity requirements also should be stated.

C.I.7.2 *Reactor Trip System*

C.I.7.2.1 Description

C.I.7.2.1.1 *System Description*

The applicant should provide a description of the reactor trip system that includes initiating circuits, logic, bypasses, interlocks, redundancy, diversity, defense-in-depth design features, and actuated devices. Any supporting systems should be identified and described. Those parts of the reactor trip system that are not required for safety also should be identified.

C.I.7.2.1.2 *Design Basis Information*

The application document for a reactor trip system should address all topics listed in Appendix C.I.7-B, "Conformance with IEEE Std 603." Major design considerations that should be emphasized are:

- single-failure criterion
- quality of components and modules
- independence
- defense-in-depth and diversity
- system testing and inoperable surveillance
- use of digital systems (guidance provided in SRP Chapter 7, Appendix 7.0-A)
- setpoint determination
- equipment qualification

The applicant should provide preliminary logic diagrams, piping and instrumentation diagrams, and location layout drawings of all reactor trip systems and supporting systems in the SAR.

C.I.7.2.2 Analysis

The applicant should provide analyses, including a failure mode and effects analysis, to demonstrate how the requirements of the General Design Criteria and IEEE Std 603/IEEE Std 7-4.3.2 are satisfied and the extent to which applicable regulatory guides, and other appropriate criteria and standards are satisfied. In addition to postulated accidents and failures, these analyses should include, but not be limited to, considerations of instrumentation installed to prevent or mitigate the consequences of:

- spurious control rod withdrawals
- loss of plant instrument air systems
- loss of cooling water to vital equipment
- plant load rejection
- turbine trip

The analyses also should discuss the need for and method of changing to more restrictive trip setpoints during abnormal operating conditions such as operation with fewer than all reactor coolant loops operating. Reference may be made to other sections of the SAR for supporting systems.

C.I.7.3 *Engineered-Safety-Feature Systems*

C.I.7.3.1 Description

C.I.7.3.1.1 *System Description*

The applicant should provide a description of the instrumentation and controls associated with the engineered safety features (ESF), including initiating circuits, logic, bypasses, interlocks, sequencing, redundancy, diversity, defense-in-depth design features, and actuated devices. Any supporting systems should be identified and described. Those parts of the ESF system not required for safety also should be identified.

C.I.7.3.1.2 *Design Basis Information*

The application document for engineered safety features systems should address all topics listed in Appendix C.I.7-B, "Conformance with IEEE Std 603." Major design considerations that should be emphasized are:

- single-failure criterion
- quality of components and modules
- independence
- defense-in-depth and diversity
- system testing and inoperable surveillance
- use of digital systems (guidance provided in SRP Chapter 7, Appendix 7.0-A)
- setpoint determination
- ESF control systems
- equipment qualification

The applicant should provide logic diagrams, piping and instrumentation diagrams, and location layout drawings of all engineered safety features systems and supporting systems in the SAR.

C.I.7.3.2 Analysis

The applicant should provide analyses, including a failure mode and effects analysis, to demonstrate how the requirements of the General Design Criteria and IEEE Std 603/IEEE Std 7-4.3.2 are satisfied and the extent to which applicable regulatory guides and other appropriate criteria and standards are satisfied. In addition to postulated accidents and failures, these analyses should include considerations of (1) loss of plant instrument air systems and (2) loss of cooling water to vital equipment. The method for periodic testing of engineered-safety-feature instrumentation and control equipment and the effects on system integrity during testing also should be described.

C.I.7.4 *Systems Required for Safe Shutdown*

C.I.7.4.1 Description

The applicant should provide a description of the systems that are needed for safe shutdown of the plant, including initiating circuits, logic, bypasses, interlocks, redundancy, diversity, defense-in-depth design features, and actuated devices. Any supporting systems also should be identified and described.

The application document for shutdown safety systems should address all topics listed in Appendix C.I.7-B, "Evaluation of Conformance with IEEE Std 603." Major design consideration that should be emphasized are:

- I&C systems required for safety shutdown
- single-failure criterion
- quality of components and modules
- independence
- periodic testing
- use of digital systems (Guidance provided in SRP Chapter 7, Appendix 7.0-A)
- remote shutdown capability: Describe the provisions taken in accordance with General Design Criterion 19 to provide the required equipment outside the control room to achieve and maintain hot and cold shutdown conditions. The design of remote shutdown stations should provide appropriate displays so that the operator can monitor the status of the shutdown. Access to remote shutdown stations should be under strict administrative controls.

The applicant should provide logic diagrams, piping and instrumentation diagrams, and location layout drawings of all safe shutdown systems and supporting systems in the SAR.

C.I.7.4.2 Analysis

The applicant should provide analyses that demonstrate how the requirements of the General Design Criteria, IEEE Std 603/IEEE Std 7-4.3.2, applicable regulatory guides, and other appropriate criteria and standards are satisfied. These analyses should include considerations of instrumentation installed to permit a safe shutdown in the event of:

- loss of plant instrument air systems
- loss of cooling water to vital equipment
- plant load rejection
- turbine trip

C.I.7.5 *Information System Important to Safety*

C.I.7.5.1 Description

The application document should include a description of the instrumentation system functions that provide information to enable the operator to perform required safety functions. These system functions are:

- post-accident monitoring (PAM) systems (RG 1.97)
- bypassed and inoperable status indication for safety system (RG 1.47)
- plant annunciators (alarms) (use of digital systems; see SRP Appendix 7.0-A)
- safety parameter displays
- information systems associated with the emergency response facilities and nuclear data link

C.I.7.5.2 Analysis

The applicant should provide an analysis to demonstrate that the operator has sufficient information to perform required manual safety functions (e.g., safe control rod patterns, manual engineered-safety-feature operations, possible unanticipated post-accident operations, and monitoring the status of safety equipment) and sufficient time to make reasoned judgments and take action where operator action is essential for maintaining the plant in a safe condition. The applicant should identify appropriate safety criteria in the FSAR and demonstrate compliance with these criteria in the FSAR.

Information should be provided to identify the information readouts and indications provided to the operator for monitoring conditions in the reactor, the reactor coolant system, and in the containment and safety-related process systems, including engineered safety features. The information available to the operator should include all operating conditions of the plant, including anticipated operational occurrences, and accident and post-accident conditions (including information from instrumentation that follows the course of accidents). The information should include the design criteria, the type of information to be displayed, number of channels provided, their range, accuracy, and location, and a discussion of the adequacy of the design.

C.I.7.6 *Interlock Systems Important to Safety*

This section should contain information describing all other instrumentation systems required for safety that are not addressed in the sections describing the reactor trip system, engineered safety features systems, safe shutdown systems, information system, or any of their supporting systems. These other systems include interlock systems to prevent over-pressurization of low-pressure systems when these systems are connected to high-pressure systems, interlocks to prevent over-pressurizing the primary coolant system during low-temperature operations, interlocks to isolate safety systems from non-safety systems, and interlocks to preclude inadvertent inter-ties between redundant or diverse safety systems for the purposes of testing or maintenance.

C.I.7.6.1 Description

The applicant should provide a description of all systems required for safety not already discussed in the above sections, including initiating circuits, logic, bypasses, interlocks, redundancy, diversity, defense-in-depth design features, and actuated devices. Any supporting systems should be identified and described (reference may be made to other sections of the SAR). The applicant should provide the design basis information required by IEEE Std 603. Sufficient schematic diagrams should be provided to permit an independent evaluation of compliance with the safety criteria.

C.I.7.6.2 Analysis

The applicant should provide analyses to demonstrate conformance with the requirements of the General Design Criteria and IEEE Std 603 are satisfied and the extent to which applicable regulatory guides, and other appropriate criteria and standards are satisfied. These analyses should include, but not be limited to, considerations of the following interlocks:

C interlocks to prevent over-pressurization of low pressure systems

C interlocks to prevent over-pressure of the primary coolant system during low-temperature operations of the reactor vessel

C interlocks for ECCS accumulator valves

C interlocks required to isolate safety systems from non-safety systems

C interlocks required to preclude inadvertent inter-ties between redundant or diverse safety systems

The applicant may reference other sections of the FSAR for supporting systems and analyses.

C.I.7.7 *Control Systems Not Required for Safety*

C.I.7.7.1 Description

The applicant should describe those control systems that can, through normal operation, system failure or inadvertent operation, affect the performance of critical safety functions. The application document should provide an analysis confirming that the design of these control systems conform to the acceptance criteria and guidelines, that the controlled variables can be maintained within prescribed operating ranges, and that effects of operation or failure of these systems are bounded by the accident analyses in Chapter 15 of the FSAR.

C.I.7.7.2 Design Basis Information

The application document for the control systems should address the applicable topics identified in SRP Table 7-1, "Acceptable Criteria and Guidelines for Instrumentation and Control Systems Important to Safety." SRP Appendix 7.1-A describes the staff's review methods for each topic. Major design considerations that should be emphasized in the control systems are identified below:

- Design bases: The control systems should include the necessary features for manual and automatic control of process variables within prescribed normal operating limits.
- Safety classification: The plant accident analysis in Chapter 15 of the FSAR should not rely on the operability of any control system function to assure safety.
- Effects of control system operation upon accidents: The safety analysis should include consideration of the effects of both control systems action and inaction in assessing the transient response of the plant for accident and anticipated operational occurrences.
- Effects of control system failures: The failure of any control system component or any auxiliary supporting system for control systems should not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the FSAR. The application document should address failure modes that can be associated with digital systems such as software design errors as well as random hardware failures.

- Effects of control system failures caused by accidents: The consequential effects of anticipated operational occurrences and accidents should not lead to control systems failures that would result in consequences more severe than those described in the analysis in Chapter 15 of the FSAR.
- Environmental control system: The I&C systems should include environmental controls as necessary to protect equipment from environmental extremes. This would include, for example, heat tracing for safety instruments and instrument sensing lines as discussed in RG 1.151, "Instrument Sensing Lines," and cabinet cooling fans.
- Use of digital systems: To minimize the potential for control system failures that could challenge safety system, control system software should be developed using a structure process similar to that applied to safety system software. Elements of the process may be tailored to account for the lower safety significance of control system software.
- Independence: The independence of safety system functions from the control system should be addressed.
- Defense-in-depth and diversity: Control system elements credited in the defense-in-depth and diversity analysis should be addressed.
- Potential for inadvertent actuation: Control system designs should limit the potential for inadvertent actuation and challenges of safety system functions.
- Control of access: Physical and electronic access to digital computer-based control system software and data should be controlled to prevent changes by unauthorized personnel. Controls should address access via network connections and via maintenance equipment.

C.I.7.7.3 Analysis

The application should provide analyses to demonstrate that these systems are not required for safety. The analyses should demonstrate that the protection systems are capable of coping with all (including gross) failure modes of the control systems.

C.I.7.8 *Diverse Instrumentation and Control Systems*

C.I.7.8.1 System Description

The applicant should provide a description of the diverse instrumentation and control system that includes initiating circuits, logic, bypasses, interlocks, redundancy, diversity, defense-in-depth design features, and actuated devices. Supporting systems should be identified and described. Anticipated transient without scram (ATWS) mitigation functions should be described. Diverse manual controls and diverse display provisions also should be addressed.

C.I.7.8.2 Analysis

The applicant should provide analyses to demonstrate (1) conformance of the proposed diverse instrumentation and control system with the requirements of 10 CFR 50.62, "ATWS rule," (2) the adequacy of manual controls and displays supporting control room operator actions to place the nuclear plant in a hot shutdown condition, and to perform reactivity control, core heat removal, reactor coolant inventory control, containment isolation, and containment integrity actions, and (3) for plant designs using digital computer-based protection systems, the conformance of the proposed diverse instrumentation and control system with the guidance of SRP Chapter 7, BTP 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems."

C.I.7.9 *Data Communication Systems*

C.I.7.9.1 System Description

This section addresses both safety and non-safety communication systems. The applicant should provide a description of all data communication systems (DCS) that are part of or support the systems described in Section 7.2 through 7.8 of the applicant's FSAR. The scope and depth of the system description will vary according to the systems's importance to safety. This section includes communication between systems and communication between computers within a system.

C.I.7.9.2 Design Basis Information

The applicant should address the applicable criteria according to the importance to safety of the system. Major design considerations that should be emphasized in the data communication systems are identified below:

- Quality of components and modules.
- DCS software quality (See SRP Chapter 7, BTP 7-14).
- Performance of the protocol selected for the DCS should meet the performance requirements of all supported systems. The performance requirements include:
    - Real-time performance
    - System deterministic timing
    - Time delays within the DCS
    - Data rates
    - Data bandwidths
    - Interfaces with other DCSs
    - DCS test results commensurate with the system requirements.
- Reliability: The potential hazards to the DCA, inadvertent actuation, error recovery, self-testing and surveillance testing should be addressed in the application.
- Control of access: The DCS should not present an electronic path by which unauthorized personnel can change plant software or display erroneous status information to the operators.
- Single-failure-criterion: The use of a DCS as a single path for multiple signals or data raises particular concerns regarding extensive consequential failure as the result of a single failure. The application document should address the appropriate channel assignments to individual communication subsystems to ensure that both redundancy and diversity requirements within the supported systems are met.
- Independence: See IEEE Std 603 requirements.
- 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 (GDC 23).
- System testing and surveillances should be addressed in the application.
- EMI/RFI susceptibility: The data communication media should not present a fault propagation path for environmental effects (e.g., high-energy electrical faults and lightning) from one redundant portion of a system to another, or from another system to a safety system.

- Defense-in-depth and diversity analyses should address each potential failure mode.
- DCS exposed to seismic hazard: If data communication or multiplexer equipment connected to the safety system is located in a non-seismic Category I structure, simultaneous seismic destruction or perturbation can affect the DCS equipment. The design should consider that type of seismic hazard.

C.I.7.9.3 Analysis

The application should provide analyses to demonstrate that these DCS systems conform to the guidelines in the regulatory guides and industry codes and standards applicable to these systems, and are in conformance with the guidance of GDC 1 and the requirements of 10 CFR 50.55a(a)(1) have been met.

Appendix C.I.7-A.
Digital Instrumentation and Control Systems Application Guidance

The overall scope of the application should include information on (1) the design qualification of digital systems, (2) protection against common-mode failure, and (3) functional requirements of IEEE Std 603 and the General Design Criteria when implementing a digital protection system.

The following seven topics should be addressed in digital I&C system application documents:

(14) The design criteria to be applied to the proposed system.

(15) Identification of the I&C design as applicable to the final safety analysis report (FSAR) Sections 7.2 through 7.9.

(16) Defense-in-depth and diversity — For applications that involve a reactor trip system (RTS) or an engineered safety features actuation system (ESFAS), the ability of the combination of I&C systems to cope with common-cause failure should be addressed. The application should confirm that defense-in-depth and diversity design features conform to the guidance of SRP Chapter 7, BTP 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems."

(17) The application should address the functional requirements, commitments to comply with IEEE 603, and the General Design Criteria. In addition, the application should include information on conformance or commitments to NRC Regulatory Guide 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants." Regulatory Guide 1.152, Revision 2, provides guidance on minimum functional and design requirements for computers used as components of a nuclear power generating plant safety systems. RG 1.152, Revision 2, also provides digital safety system security guidance.

(18) Life cycle process planning — The computer system development process, particularly the software life cycle activities for digital systems, should be provided. The software life cycle plans should have commitments to coordinate execution of activity groups, and checkpoints at which product and process characteristics are verified and validated during the development process, as described in SRP Chapter 7 Appendix 7.1-D, and BTP 7-14, "Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems."

(19) Life cycle process requirements - The computer system functional requirements should be documented using a systematic process. A statistically valid sample of system requirements should be selected to confirm that the applicant/licensee's life-cycle activities have been implemented as planned. The sample size should be such that the staff can conclude with at least 95% assurance that the quality of the design has been validated. BTP 7-14 describes functional characteristics and software development process characteristics that should be verified by staff reviews.

(20) Software life cycle process design outputs — The conformance of the hardware and software to the functional and performance requirements is derived from the design bases. A statistically valid sample of software design outputs should be provided to confirm with at least 95% assurance that they address the functional requirements and have been allocated to the software appropriately, and to confirm that the expected software development process characteristics are evident in the design outputs. The system test procedures and test results (validation tests, site acceptance tests, pre-operational and start-up tests) should provide assurance that the system functions as intended. BTP 7-14 describes functional characteristics and software development process characteristics that can be verified by staff reviews.

For a system incorporating commercial-grade digital equipment, the preceding seven topics still apply. There should be evidence in the application of an acceptance process that has determined that there is reasonable assurance that the equipment will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under a quality assurance program consistent with Appendix B to 10 CFR Part 50. The commercial-grade dedication process should be described in detail. This should include information on how the commercial equipment was originally designed and tested. The acceptance process itself is subject to the applicable provisions of Appendix B to 10 CFR Part 50. An acceptable process is described in EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications."

Appendix C.I.7-B.
Conformance with IEEE Std 603

The scope of IEEE Std 603 includes all I&C safety systems, which are the systems covered in Sections 7.2 through 7.6 of the final safety analysis report (FSAR). Applicable considerations include design bases, redundancy, independence, single failures, qualification, bypasses, status indication, and testing. Digital data communication systems as described in FSAR Section 7.9 are support systems for other I&C systems. As such, they inherit the applicable requirements and guidance that apply to the supported systems. Consequently, the guidance of IEEE Std 603 is directly applicable to those parts of data communication systems that support safety system functions.

All functional requirements for the I&C system and the operational environment for the I&C system should be described. As a minimum, each of the design basis aspects identified in IEEE Std 603 Sections 4.1 through 4.12 should be addressed.

C.I.7.B-1 Safety System Design Basis

The application should address the safety system design basis for the following design aspects:

(1) Single-Failure Criterion: Any single failure within the safety system shall not prevent proper protective action at the system level when required. The applicant/licensee's analysis should confirm that the requirements of the single-failure criterion are satisfied.

(2) Completion of Protective Action: The application document should include functional and logic diagrams indicating "seal-in" features that are provided to enable system-level protective actions to go to completion.

(3) Quality: The applicant/licensee should confirm that the safety protection system conforms to the quality assurance provisions of Appendix B to 10 CFR Part 50. For digital computer-based systems, the applicant/licensee should address the quality requirements described in Section 5.3 of IEEE Std 7-4.3.2. EPRI TR-106439 "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," provides guidance for the evaluation of existing commercial computers and software to comply with Section 5.3.2 of IEEE Std 7-4.3.2. The guidance of BTP 7-14 or the guidance of EPRI TR-106439 may be applied to the qualification of software tools, as discussed in Section 5.3.3 of IEEE Std 7-4.3.2.

(4) Equipment Qualification: The applicant/licensee should confirm that the safety system equipment is designed to meet the functional performance requirements over the range of normal and worst case (e.g., any transient, accident or anticipated operational occurrence) environmental conditions where the equipment is expected to operate. The applicant/licensee should address mild environment qualification and electromagnetic interference (EMI) qualification of safety system I&C equipment. The applicant/licensee should confirm that there is independence between environmental control systems and sensing systems that would indicate the failure or malfunctioning of environmental control systems. The application also should include confirmation that the environmental protection for instrument sensing lines conforms with the guidance of RG 1.151, "Instrument Sensing Lines." EMI qualification should conform with the guidance of RG 1.180, Rev.1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation Control Systems."

(5) System Integrity:

- The application document should confirm that tests have been conducted on safety system equipment components and the system racks and panels to demonstrate that the safety system performance is adequate to ensure completion of protective actions over the range of transient and steady-state conditions of both the energy supply and the environment. Where tests have not been conducted, the applicant/licensee should confirm that the safety system components are conservatively designed to operate over the range of service conditions.
- For digital computer-based systems, the confirmation of system real-time performance is adequate to ensure completion of protective action within the critical points of time identified as required.
- The application should confirm that the design provides for protection systems 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, or adverse environment conditions are experienced.
- The application document should include a failure modes and effects analysis. The analysis should justify the acceptability of each failure effect.
- Failure of computer system hardware or software should not inhibit manual initiation of protective functions or the operator performance of preplanned emergency or recovery actions.
- Lightning protection should be addressed as part of the electromagnetic compatibility. Lightning protection features should conform with the guidance of RG 1.204, "Guidelines for Lightning Protection of Nuclear Power Plants."

(6) Independence: The application document should demonstrate the independence between (a) redundant portions of a safety system, (b) safety systems and the effects of design basis events, and (c) safety systems and other systems. Three aspects of independence should be addressed in each case:

- Physical independence,
- Electrical independence, and
- Communications independence.

Guidance for evaluation of physical and electrical independence is provided in RG 1.75, "Physical Independence of Electrical Systems," which endorses IEEE Std 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." The applicant/licensee should confirm that the safety system design precludes the use of components that are common to redundant portions of the safety system, such as common switches for actuation, reset, calibration, or test; common sensing lines; or any other features that could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers. Electrical independence should include the utilization of separate power sources. Transmission of signals between independent channels should be through isolation devices, and should be such that signals from one channel can not adversely affect the proper operation of other channels.

Additional guidance is provided in SRP Chapter 7, Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," Appendix 7.1-C, "Guidance for Evaluation of

Conformance to IEEE Std 603," Appendix 7.1-D, "Guidance for Evaluation of Conformance to IEEE Std 7-4.3.2," and Section 7.9, "Data Communication Systems."

(7) Capability for Test and Calibration: Guidance on periodic testing of the protection system is provided in RG 1.22, "Periodic Testing of Protection System Actuation Functions," and in RG 1.118, "Periodic Testing of Electric Power and Protection Systems," which endorses IEEE Std 338, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems." The extent of test and calibration capabilities provided bears heavily on whether the design meets the single-failure criterion. Periodic testing should duplicate, as closely as practical, the overall performance required of the protection system. The testing should confirm operability of both the automatic and manual circuitry. The capability to permit testing during power operation should be provided. When this capability can only be achieved by overlapping tests, the test scheme should 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 during power operation should be avoided.

(8) Information Displays: The information displays for manually controlled actions should include confirmation that displays will be functional (e.g., power will be available and sensors are appropriately qualified) during plant conditions under which manual actions may be necessary. Safety system bypass and inoperable status indications should conform with the guidance of RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."

(9) Control of Access: The application should confirm that design features provide means to control physical access to protection system equipment, including access to test points and the means for changing setpoints. Typically the access controls should include provisions such as alarms and locks on safety system panel doors, or control of access to rooms in which safety system equipment is located. The digital computer-based systems should have controls over electronic access to safety system software and data. Controls should address access via network connections, and via maintenance equipment.

(10) Repair: Digital safety systems may include self-diagnostic capabilities to aid in troubleshooting. The application should describe the characteristics of the digital computer-based diagnostic capabilities.

(11) Identification: Guidance on identification is provided in RG 1.75, "Criteria for Independence of Electrical Safety Systems," which endorses IEEE Std 384, "Standard Criteria for Independence of Class 1E Equipment and Circuits." The preferred identification method is color coding of components, cables, and cabinets. For computer-based systems, the configuration management plan should describe the identification process for computer software.

(12) Human Factors Considerations: The safety system human factors design features should be consistent with the applicant/licensee's commitments documented in Chapter 18 of the FSAR.

(13) Reliability: The applicant/licensee should justify that the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed. For computer systems, both hardware and software reliability should be analyzed. RG 1.152 Revision 2, describes the NRC position on software reliability determination.

C.I.7B-2 Functional and Design Requirements

The applicant should address the functional and design requirements for the following design aspects:

(1) Automatic Control: The application document should include an analysis to confirm that the safety system has been qualified for the requisite performance requirements. The evaluation of the precision of the protection system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis. For digital computer-based systems, the application should confirm that the general functional requirements have been appropriately allocated into hardware and software requirements. The application should also confirm that the system's real-time performance is deterministic and known.

(2) Manual Control: Features for manual initiation of protective action should conform with RG 1.62, "Manual Initiation of Protection Action." The application should include confirmation that the controls will be functional (e.g., power will be available and command equipment will be appropriately qualified) for the plant conditions under which manual actions may be necessary.

(3) Interaction Between the Sense and Command Features and Other Systems: The application should confirm that non-safety system interactions with protection systems are limited such that the requirements of 10 CFR Part 50 Appendix A, GDC 24, "Separation of Protection and Control System," are met. Where the event of concern is single failure of a sensing channel shared between control and protection functions, previously accepted approaches have included:

- Isolating the protection system from channel failures by providing additional redundancy.
- Isolating the control system from channel failures by using data validation techniques to select a valid control input.
- Designing the communications path to be a broadcast only (simplex) path from the protection system to the control system.

(4) Derivation of System Inputs: For both direct and indirect parameters, the applicant/licensee should verify that the characteristics (e.g., range, accuracy, resolution, response time, sample rate) of the instruments that produce the protection system inputs are consistent with the analysis provided in Chapter 15 of the FSAR. A safety system that requires loss of flow protection would, for example, normally derive its signal from flow sensors (a direct parameter). An indirect flow indication design might use a parameter such as a pressure signal or pump speed. In selecting an indirect parameter, the applicant/licensee should verify that the indirect parameter provides a valid representation of the desired direct parameter for all events.

(5) Capability for Testing and Calibration of System Inputs: The most common method used to verify the availability of the input sensors is by cross checking between redundant channels that have available instrumentation signal displays. When only two channels of signal displays are provided, the applicant/licensee should state the basis used to ensure that an operator will not take incorrect action when the two channel signals differ. The applicant/licensee should state the method to be used for checking the operational availability of non-indicating sensors. SRP Chapter 7, BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions," discusses issues that should be considered in sensor checks and surveillance tests for digital computer I&C systems.

(6) Operating Bypasses: The requirement of Section 7.4 in IEEE 603 for automatic removal of operational bypasses requires that the reactor operator shall have no role in such removal. The operator may take action, however, to prevent the unnecessary initiation of a protective action. The application document should address this issue.

(7) Maintenance Bypass: The application document should address the provision of any maintenance bypass and confirm that the required action is consistent with the proposed plant technical specifications.

(8) Setpoints: The applicant/licensee's analysis should confirm that an adequate margin exists between operating limits and setpoints, such that there is a low probability for inadvertent actuation of the system. The application document should include an analysis to confirm that an adequate margin exists between setpoints and safety limits, such that the system initiates protective actions before safety limits are exceeded. Regulatory Guide 1.105, "Setpoint for Safety-Related Instrumentation," provides guidance for setpoint determination.

Appendix C.I.7-C.
Conformance with IEEE Std 7-4.3.2

The scope of IEEE Std 7-4.3.2-2003 and Regulatory Guide 1.152, Revision 2 includes all safety digital instrumentation and control (I&C) systems that are computer-based. IEEE Std 7-4.3.2-2003 serves to amplify criteria in IEEE Std 603-1998 (IEEE Std 603-1998 was evolved from IEEE Std 603-1991 and it should be recognized that IEEE Std 603-1991 is required by 10 CFR 50.55a(h)) to address the use of computers as part of safety systems in nuclear power generating stations - systems covered by Sections 7.2 through 7.6 of the plant final safety analysis report (FSAR). For non-safety digital I&C systems covered by FSAR Sections 7.7 and 7.8, which are systems that have a high degree of importance-to-safety based on risk, a graded application of the criteria of IEEE Std 7-4.3.2-2003 could be considered. Data communication systems covered by FSAR Section 7.9 are support systems to I&C systems. Hence, the requirements and guidance for the communication systems are the same as those for the principal I&C systems they support.

C.I.7.C-1 Computer-Based Safety System Design Basis

The applicant should address the computer-based safety system design basis for the following design aspects:

(1) Single-Failure Criterion: Clause 5.1 in IEEE std 603 defines the single failure criterion.

(2) Completion of Protective Action: The application should demonstrate that the safety systems are designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features will continue until completion. Deliberate operator action should be required to return the safety systems to normal. This requirement should not preclude the use of equipment protective devices identified in IEEE 603 Section 4.11 of the design basis or the provision for deliberate operator interventions. Seal-in of individual channels is not required.

(3) Quality: The application document should confirm that quality assurance provisions of Appendix B to 10 CFR Part 50 are applied to the safety system. For digital computer-based systems, the application should address the quality requirements described in Clause 5.3 of IEEE Std 7-4.3.2-2003. Hardware quality is addressed in IEEE Std 603. Software quality is addressed in IEEE/EIA Std 12207.0-1996 and supporting standards. In addition to the requirements of IEEE Std 603, the following activities necessitate additional requirements that are necessary to meet the quality criterion. The application document should address conformance to the requirements of the following clauses of IEEE Std 7-4.3.2-2003:

5.3.1	Software development
5.3.2	Use of software tools
5.3.3, 5.3.4	Verification and validation
5.3.5	Configuration management
5.3.6	Risk management
5.4.2	Qualification of existing commercial computers.

The application document should address life cycle activities in the following three areas:

(1) **Software Life Cycle Process Planning**

- Software management plan
- Software development plan
- Software test plan
- Software quality assurance plan
- Integration plan
- Installation plan
- Maintenance plan
- Training plan
- Operations plan
- Software safety plan
- Software verification and validation plan
- Software configuration management plan

(2) **Software Life Cycle Process Implementation**

- Safety analyses
- Verification and validation analysis and test reports
- Configuration management reports
- Requirement traceability matrix

One or more sets of these reports should be available for each of the following activity groups:

- Requirements
- Design
- Implementation
- Integration
- Test
- Installation
- Operations
- Maintenance

(3) **Software Life Cycle Process Design Outputs**

- Software requirements specifications (SRS)
- Hardware and software architecture descriptions (SAD)
- Major hardware component description and qualifications
- Software design specifications (SDS)
- Code listings
- System Build documents
- Installation configuration tables
- Operations manuals
- Maintenance manuals
- Training manuals

The application should address the computer system development process, which typically consists of the following computer lifecycle phases:

- Concepts
- Requirements
- Design
- Implementation
- Test
- Installation, Checkout and Acceptance Testing
- Operation
- Maintenance
- Retirement

The activities during the lifecycle phases are summarized as:

- Creating the conceptual design of the system
- Translating the concepts into specific system requirements
- Using the requirements to develop a detailed system design
- Implementing the design into hardware and software functions
- Testing the functions to assure the requirements have been correctly implemented
- Installing the system and performing site acceptance testing
- Operating and maintaining the system
- Retiring the system

SRP BTP 7-14 describes the characteristics of a software development process that the NRC staff evaluates when assessing compliance with the quality requirements of the Clause 5.3 "Quality" of IEEE Std 7-4.3.2-2003.

(4) Equipment Qualification: In addition to the equipment qualification criteria provided by IEEE Std 603, the following requirements are necessary to qualify digital computers for use in safety systems.

(a) Computer System Testing: Computer system equipment qualification testing should be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, should be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the central processing unit, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing should demonstrate that the performance requirements related to safety functions have been met.

(b) Qualification of Existing Commercial Computers: EPRI TR-106439 "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," and the Safety Evaluation approving this topical for reference should be used as guidance. The dedication process for the computer should entail identification of the physical, performance, and development process requirements necessary to provide adequate confidence that the proposed digital system or component can achieve the safety function. The dedication process applies to the computer hardware, software, and firmware that are required to accomplish the safety function. The dedication process for software and firmware should include an evaluation of the design process.

(5) System Integrity: In addition to the system integrity criteria provided by IEEE Std 603, and the guidance in SRP Appendix 7.1-C, IEEE Std 7-4.3.2-2003 includes criteria in Sub-Clauses 5.5.1 through 5.5.3 on designs for computer integrity, test and calibration, and fault detection and self-diagnostics activities. The application document should address the following design features to achieve system integrity in digital equipment for use in safety systems:

- Design for computer integrity
- Design for test and calibration
- Fault detection and self-diagnostics

(6) Independence: In addition to the requirements of IEEE Std 603, data communication between safety channels or between safety and non-safety systems should not inhibit the performance of the safety function.

(7) Capability for Test and Calibration: Capability for testing and calibration of safety system equipment should be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment should be provided during power operation and should duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems should be in accordance with the requirements of IEEE Std 338-1987.

(8) Information Displays: The requirements for information displays are contained in IEEE Std 603-1991, section 5.8. The application should provide documentation of compliance with these requirements.

(9) Control of Access: The design should permit the administrative control of access to safety system equipment. These administrative controls should be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.

(10) Repair: The safety systems should be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

(11) Identification: To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, the following identification criteria specific to software systems should be met:

(a) Firmware and software identification should be used to assure the correct software is installed in the correct hardware component.

(b) Means should be included in the software such that the identification may be retrieved from the firm-ware using software maintenance tools.

(c) Physical identification requirements of the digital computer system hardware should be in accordance with the identification requirements in IEEE Std 603.

(12) Human Factors Considerations: Human factors should be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintenance e personnel can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988.

(13) Reliability: In addition to the requirements of IEEE Std 603, when reliability goals are identified, the proof of meeting the goals should include the software. The method for determining reliability may include combinations of analysis, field experience and testing. Software error recording and trending may be used in combination with analysis, field experience and testing. Regulatory Guide 1.152, Revision 2, which endorses IEEE Std 7-4.3.2-2003, indicates that the concept of quantitative reliability is not recommended as a sole means of meeting the NRC's regulations for reliability of digital computers in safety systems. However, quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the I&C system.

C.I.7.C-2 The Application Should Address Cyber Security Requirements

The digital safety system development process should address potential security vulnerabilities in each phase of the digital safety system lifecycle.

The lifecycle phase-specific security requirements should be commensurate with the risk and magnitude of the harm resulting from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the digital safety system. Regulatory Positions 2.1 – 2.9 of Regulatory Guide 1.152, Revision 2 describe digital safety system security guidance for the individual phases of the lifecycle.