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 ESF 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. The regulations at 10 CFR 50.55a(h) require that applications filed on or after May 13, 1999, for preliminary and final design approvals (Appendix O, "Standardization of Design: Staff Review of Standard Designs," to 10 CFR Part 52), design certifications, and construction permits, operating licenses, and COLs that do not reference a final design approval or design certification must meet the requirements for safety systems in IEEE Std 603-1991, and the correction sheet dated January 30, 1995. IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by RG 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," provides guidance on applying the safety system criteria to computer-based systems. Other IEEE standards referenced in this guide should be the revision endorsed by the current version of a regulatory guide unless the guide indicates a specific revision of a standard. The applicant should provide analysis of control systems and instrumentation, with particular consideration of transients induced by the control system, which, if not terminated in a timely manner, could result in fuel damage and subsequent fission product release to the environment.

The applicant should also provide instrumentation for accident monitoring 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 offer reasonable assurance that the applicant will comply with the regulations of 10 CFR Part 50 Chapter I and that public health and safety will be protected.

The COL applicant should describe the applicable life-cycle development activities. The application should describe the system requirements and demonstrate how the final system meets these requirements. Nondigital 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 COL application submittals related to digital I&C 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 applicant may submit the information described in these appendices in topical reports.

C.I.7.1 Introduction

C.I.7.1.1 *Identification of Safety-Related Systems*

The COL application should list all instrumentation, control, and supporting systems that are safety-related, including alarm, communication, and display instrumentation. The application should identify, as applicable, the designers responsible for providing the I&C designs included for the facility. The application should identify systems that are identical to those of a nuclear power plant of similar

design that has recently received a COL license, design approval, or design certification. This section should also identify systems that are different and discuss the differences and their effects on safety-related systems.

C.I.7.1.2 ***Identification of Safety Criteria***

The COL application should provide a regulatory requirements applicability matrix that lists all design bases, criteria, regulatory guides, standards, and other documents to be implemented in the design of the systems listed in Section C.I.7.1.1. This section of the FSAR should include the specific information identified in NUREG-0800, SRP Chapter 7, Appendix 7.1-A.

The acceptance criteria and guidelines given in SRP Appendix 7.1-A are divided into four categories—(1) the regulations in 10 CFR 50.55a(h) including guidance in IEEE Std 603, (2) the GDCs 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 (BTPs) (10 CFR 50.34(h), conformance with the SRP).

The COL applicant should describe the technical design bases for all protection system functions, including the reactor trip function, ESF, emergency power, interlocks, bypasses, and equipment protection. The applicant should also state diversity requirements.

C.I.7.2 Reactor Trip System

C.I.7.2.*1* *Description*

C.I.7.2.1.1 *System Description*

The COL 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. This section should identify and describe any supporting systems and also identify those parts of the reactor trip system that are not required for safety.

C.I.7.2.1.2 *Design-Basis Information*

For a reactor trip system, the COL application should address all topics listed in Appendix C.I.7-B to this document. The application should emphasize the following major design considerations:

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

The applicant should include a commitment to supplement the application, as necessary, with final design drawings.

C.I.7.2.2 ***Analysis***

The COL applicant should provide analyses, including a failure mode and effects analysis, to demonstrate how it has satisfied the requirements of the GDCs and IEEE Std 603 and IEEE Std 7-4.3.2 and the extent to which it has satisfied applicable regulatory guides and other appropriate criteria and standards. 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 the following:

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

The analyses should also 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. The analyses may refer to other sections of the FSAR for discussions of 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 COL applicant should provide a description of the I&Cs associated with the ESFs, including initiating circuits, logic, bypasses, interlocks, sequencing, redundancy, diversity, defense-in-depth design features, and actuated devices. This section should identify and describe any supporting systems and identify those parts of the ESF system not required for safety.

C.I.7.3.1.2 ***Design-Basis Information***

For ESF systems, the COL application should address all topics listed in Appendix C.I.7-B to this document. The application should emphasize the following major design considerations:

- 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

In the FSAR, the COL applicant should provide preliminary logic diagrams, piping and instrumentation diagrams, and location layout drawings of all ESF systems and supporting systems. The COL applicant should include a commitment to supplement the application, as necessary, with final design drawings.

C.I.7.3.2 ***Analysis***

The COL applicant should provide analyses, including a failure mode and effects analysis, to demonstrate how it has satisfied the requirements of the GDCs and the guidance in IEEE Std 603, and IEEE Std 7-4.3.2, and the extent to which it has satisfied applicable regulatory guides and other appropriate criteria and standards. 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 applicant should also describe the method for periodic testing of ESF I&C equipment consists of technical specification basis and the effects on system integrity during testing.

C.I.7.4 Systems Required for Safe Shutdown

C.I.7.4.1 ***Description***

The COL 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. The applicant should also identify and describe any supporting systems.

For shutdown safety systems, the COL application should address all topics listed in Appendix C.I.7-B to this document. The applicant should emphasize the following major design considerations:

- 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)

For remote shutdown capability, the applicant should describe the provisions taken in accordance with GDC 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.

In the FSAR, the COL applicant should provide preliminary logic diagrams, piping and instrumentation diagrams, and location layout drawings of all safe shutdown systems and supporting systems. The COL applicant should include a commitment to supplement the application, as necessary, with final design drawings.

C.I.7.4.2 ***Analysis***

The COL applicant should provide analyses that demonstrate how it has satisfied the requirements of the GDCs and 10 CFR 50.55a(h) (IEEE 603-1991). The applicant should provide justification for any deviation from meeting the agency's regulation. These analyses should include considerations of instrumentation installed to permit a safe shutdown in the event of the following:

- 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. The analyses may refer to other sections of the FSAR for supporting systems.

C.I.7.5 Information Systems Important to Safety

C.I.7.5.1 ***Description***

The COL application should describe the following instrumentation systems that provide information to enable the operator to perform required safety functions:

- accident monitoring instrumentation (RG 1.97)
- bypassed and inoperable status indication for safety systems (RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems")
- plant annunciators (alarms) (use of digital systems; see SRP Appendix 7.0-A)
- safety parameter displays (10 CFR 50.34, "Contents of applications; technical information," requirement related to TMI)
- information systems associated with the emergency response facilities and nuclear data link (10 CFR 50.34 requirement related to TMI)

The COL applicant should provide preliminary logic diagrams, piping and instrumentation diagrams, and location layout drawings of all information systems important to safety. The COL applicant should include a commitment to supplement the application, as necessary, with final design drawings.

C.I.7.5.2 ***Analysis***

The COL 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 ESF operations, possible unanticipated postaccident 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. In the FSAR, the applicant should identify appropriate safety criteria and demonstrate compliance with these criteria.

The applicant should identify the information readouts and indications provided to the operator for monitoring conditions in the reactor, the RCS, and the containment and safety-related process systems, including ESFs. The information available to the operator should include all operating conditions of the plant, including AOO, and accident and postaccident 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: the number of channels provided and their range, accuracy, and location; and a discussion of the adequacy of the design. The range and accuracy should be consistent with system requirements defined in the FSAR.

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, ESF systems, safe shutdown systems, information system, or any of their supporting systems. These other systems include interlock systems to prevent overpressurization of low-pressure systems when these systems are connected to high-pressure systems, interlocks to prevent overpressurizing the primary coolant system during low-temperature operations, interlocks to isolate safety systems from nonsafety 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 COL applicant should provide a description of all systems required for safety not already discussed in Sections 7.2 through 7.5 of the FSAR, including initiating circuits, logic, bypasses, interlocks, redundancy, diversity, defense-in-depth design features, and actuated devices. The applicant should identify and describe any supporting systems (the application may refer to descriptions included in other sections of the FSAR). The applicant should provide the design-basis information required by IEEE Std 603. In the FSAR, the applicant should provide preliminary logic diagrams, piping and instrumentation diagrams, and location layout drawings of interlock systems important to safety. The COL applicant should include a commitment to supplement the applications, as necessary, with final design drawings.

C.I.7.6.2 *Analysis*

The COL applicant should provide analyses to demonstrate how it has satisfied the requirements of the GDC and IEEE Std 603 and the extent to which it has satisfied applicable regulatory guides and other appropriate criteria and standards. These analyses should include, but not be limited to, considerations of the following interlocks:

- interlocks to prevent overpressurization of low-pressure systems
- interlocks to prevent overpressurization of the primary coolant system during low-temperature operations of the reactor vessel
- interlocks for ECCS accumulator valves
- interlocks required to isolate safety systems from nonsafety systems
- 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 COL applicant should describe those control systems that can, through failure of normal operation, 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 conforms to the acceptance criteria and guidelines, the controlled variables can be maintained within prescribed operating ranges, and the 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*

For the control systems, the COL application should address the applicable topics identified in SRP Table 7-1. The application should emphasize the following major design considerations in the control systems:

- 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 on accidents—The safety analysis should consider the effects of both control system action and inaction in assessing the transient response of the plant for accidents and AOO.
- 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 AOO 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 and random hardware failures.
- Effects of control system failures caused by accidents—The consequential effects of AOO 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 and cabinet cooling fans.
- Use of digital systems—To minimize the potential for control system failures that could challenge safety systems, control system software should be developed using a structured 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 application should address the independence of safety system functions from the control system.

- Defense in depth and diversity—The application should address control system elements credited in the defense-in-depth and diversity analyses.
- Potential for inadvertent actuation—Control system designs should limit the potential for inadvertent actuation and challenges of safety system functions.
- Control of access—The applicant should control physical and electronic access to digital computer-based control system software and data to prevent changes by unauthorized personnel. Controls should address access via network connections and via maintenance equipment.

The COL applicant should provide preliminary logic diagrams, piping and instrumentation diagrams, and location layout drawings of all control systems in the FSAR. The COL applicant should include a commitment to supplement the application, as necessary, with final design drawings.

C.I.7.7.3 ***Analysis***

The COL 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 COL applicant should provide a description of the diverse I&C systems that includes initiating circuits, logic, bypasses, interlocks, redundancy, diversity, defense-in-depth design features, and actuated devices. This section should identify and describe supporting systems (the applicant may refer to other applicable sections of the FSAR). The applicant should describe mitigation functions for anticipated transient without scram and address diverse manual controls and diverse display provisions.

In the FSAR, the COL applicant should provide preliminary logic diagrams, piping and instrumentation diagrams, and location layout drawings of all diverse I&C systems. The COL applicant should include a commitment to supplement the application, as necessary, with final design drawings.

C.I.7.8.2 ***Analysis***

The COL applicant should provide analyses to demonstrate (1) conformance of the proposed diverse I&C system with the requirements of 10 CFR 50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants," (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 I&C system with the guidance of SRP Chapter 7, BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," Revision 5, issued February 2007.

C.I.7.9 Data Communication Systems

C.I.7.9.1 *System Description*

This section addresses both safety and nonsafety communication systems. The COL applicant should describe all data communication systems (DCSs) that are part of or support the systems described in Sections 7.2 through 7.8 of the applicant's FSAR. The scope and depth of the system description will vary according to the system'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 COL applicant should address the applicable criteria according to the importance to safety of the system. The applicant should emphasize the following major DCS design considerations:

- The applicant should consider the quality of components and modules.
- The applicant should consider DCS software quality (see SRP Chapter 7, BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Controls Systems," Revision 5, issued February 2007).
- The protocol selected for the DCS should meet the performance requirements of all supported systems. The performance requirements include the following:
  - 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
  - communication protocols
- The application should address the potential hazards to the DCS, including inadvertent actuation, error recovery, self-testing, and surveillance testing.
- To control 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.
- 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 the assignments meet both redundancy and diversity requirements within the supported systems.
- See IEEE Std 603 requirements for independence.
- The protection system should be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis (GDC 23).
- The application should address system testing and surveillances.

- The application should address the status of DCSs in the design of bypass and inoperable status indications.
- To limit susceptibility to electromagnetic and radiofrequency interference, 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.
- The design should consider the exposure of DCSs to seismic hazards. If data communication or multiplexer equipment connected to the safety system is located in a nonseismic Category I structure, simultaneous seismic destruction or perturbation can affect the DCS equipment.

The COL applicant should describe DCSs and provide preliminary layout drawings and network routing information. The COL applicant should include a commitment to supplement the application, as necessary, with final design drawings.

C.I.7.9.3 ***Analysis***

The application should provide analyses to demonstrate that these DCS systems conform to the recommendations in the regulatory guides and industry codes and standards applicable to these systems, are in conformance with the guidance of GDC 1 and meet the requirements of 10 CFR 50.55a(a)(1). The operability of supporting data communication clearly affects the operability of supported I&C safety functions. The means and criteria for determining if a function has failed as a result of communications failure are not necessarily obvious, and therefore, the application should describe them.

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-cause failure, and (3) functional requirements of IEEE Std 603 and the GDC when implementing a digital protection system.

The applicant should address the following seven topics in I&C system application documents:

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

(2) The I&C design as applicable to the FSAR Sections 7.2 through 7.9.

(3) Defense in depth and diversity—For applications that involve a reactor trip system or an ESF actuation system, the applicant should address the combined ability of the I&C systems to cope with common-cause failure. The application should confirm that defense-in-depth and diversity design features conform to the guidance of NUREG-0800, Chapter 7, BTP 7-19.

(4) Functional requirements and commitments—The application should address the functional requirements, commitments to comply with IEEE 603, and the GDC. In addition, the application should include information on conformance or commitments to NRC RG 1.152. RG 1.152 provides guidance on minimum functional and design requirements for computers used as components of a nuclear power generating plant safety system. RG 1.152 also provides digital safety system security guidance.

(5) Life-cycle process planning—The applicant should describe the computer system development process, particularly the software life-cycle activities for digital systems. 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 NUREG-0800, Chapter 7, Appendix 7.1-D, and BTP 7-14.

(6) Life-cycle process requirements—Using a systematic process, the applicant should document the computer system functional requirements. The applicant/licensee[1] should select a statistically valid sample to confirm that it has implemented the life-cycle activities as planned. The applicant should identify documentation available for NRC inspection that confirms implementation. The type of documents should be similar to the documents shown on SRP BTP 7-14, Figure 7-A-1. Staff reviews should verify the functional characteristics and software development process characteristics described in BTP 7-14.

(7) Software life-cycle process design outputs—The conformance of the hardware and software to the functional and performance requirements derives from the design bases. The applicant should identify documentation available for NRC inspection that confirms implementation. The type of documents should be similar to the documents shown on SRP BTP 7-14, Figure 7-A-1. The system test procedures and test results (validation tests, site acceptance tests, preoperational and startup tests) should provide assurance that the system functions as intended. Staff reviews

---

[1] The guidance uses the terminology "applicant/licensee" to describe the life-cycle activities because these activities span the application period and postapplication period following issuance of the license as some of these activities are likely to be included in the ITAAC.

can verify the functional characteristics and software development process characteristics described in SRP BTP 7-14.

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 QA program consistent with Appendix B to 10 CFR Part 50. The applicant should describe the commercial-grade dedication process in detail and include information on the original design and test of the commercial equipment. The acceptance process itself is subject to the applicable provisions of Appendix B to 10 CFR Part 50. EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," issued October 1996, describes an acceptable process to qualify a commercial equipment product.

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 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 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.

The applicant should describe all functional requirements for the I&C system and the operational environment for the I&C system. At a minimum, the applicant should address each of the design-basis aspects identified in IEEE Std 603, Sections 4.1 through 4.12.

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

The COL applicant 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[1] analysis should confirm that it has satisfied the requirements of the single-failure criterion.

(2) Completion of Protective Action—The COL application 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 QA 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 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 applicant/licensee may use the guidance of SRP BTP 7-14 or the guidance of EPRI TR-106439 for 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 AOO) environmental conditions where the equipment is expected to operate. The applicant/licensee should address mild environment qualification and electromagnetic interference qualification of safety system I&C equipment. The applicant 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. Electromagnetic interference qualification should conform with the guidance of RG 1.180.

(5) System Integrity

- The application document should confirm that tests conducted on safety system equipment components and the system racks and panels 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 application should confirm that 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 occur.
- The application 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.
- The application should address lightning protection 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 DBEs, and (c) safety systems and other systems. In each case, the application should address the following aspects of independence:

- physical independence
- electrical independence
- communications independence

Guidance for evaluation of physical and electrical independence appears 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.

SRP Chapter 7, Appendix 7.0-A, Appendix 7.1-C, Appendix 7.1-D, and Section 7.9 provide additional guidance.

(7) Capability for Test and Calibration—Guidance on periodic testing of the protection system appears 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. Testing should be possible during power operation. When this capability can be achieved only by overlapping tests, the test scheme should be such that the tests do, in fact, overlap from one test segment to another. The applicant/licensee should avoid test procedures that require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment during power operation.

(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 a 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—RG 1.75, which endorses IEEE Std 384, provides guidance on identification. 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) Auxiliary Features—Auxiliary supporting features shall meet all requirements of IEEE Std 603-1991. Other auxiliary features that (1) perform a function that is not required for the safety systems to accomplish their safety functions, and (2) are part of the safety systems by association (that is, not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. SRP Appendix 7.1-C, provides additional guidance.

(13) 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.

(14) 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, the

applicant should analyze both hardware and software reliability. RG 1.152 describes the NRC position on software reliability determination.

C.I.7.B-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 analysis should evaluate the precision of the protection system by showing the extent to which the analysis factors in setpoints, margins, errors, and response times. For digital computer-based systems, the application should confirm that hardware and software requirements have incorporated the general functional 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 confirm 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 nonsafety system interactions with protection systems are limited such that the system meets the requirements of GDC 24, "Separation of Protection and Control System," in Appendix A to 10 CFR Part 50. Where the event of concern is single failure of a sensing channel shared between control and protection functions, previously accepted approaches have included the following:

- 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 in Chapter 15 of the FSAR. The applicant's design specification should include this information. The design specification documents should be available for NRC staff audit. 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 cross-checking between redundant channels that have available instrumentation signal displays. When only two channels of signal displays are provided, the applicant should state the basis used to ensure that an operator will not take incorrect action when the two channel signals differ. The applicant should state the method to

beused for checking the operational availability of nonindicating sensors. NUREG-0800, Chapter 7, BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions," Revision 5, issued February 2007, 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 Std 603 for automatic removal of operational bypasses states 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 TS.

(8) Setpoints—The applicant/licnesee'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 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. RG 1.105, "Setpoint for Safety-Related Instrumentation," provides guidance for setpoint determination. The setpoint calculation documents should be available for NRC staff audit.

Appendix C.I.7-C

Conformance with IEEE Std 7-4.3.2

The scope of IEEE Std 7-4.3.2-2003 and RG 1.152 includes all safety-related digital I&C systems that are computer-based. IEEE Std 7-4.3.2-2003 amplifies the criteria in IEEE Std 603-1998, (IEEE Std 603-1998 evolved from IEEE Std 603-1991, although 10 CFR 50.55a(h) requires the use of IEEE Std 603-1991 to address the role of computers as part of safety systems in nuclear power generating stations (i.e., systems covered by Sections 7.2 through 7.6 of the plant FSAR). For nonsafety digital I&C systems covered by FSAR Sections 7.7 and 7.8 (i.e., systems with a high degree of importance to safety based on risk), the applicant can consider a graded application of the criteria of IEEE Std 7-4.3.2-2003. 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 QA 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 criteria described in Clause 5.3 of IEEE Std 7-4.3.2-2003. IEEE Std 603 addresses hardware quality, and IEEE/EIA Std 12207.0-1996, "IEEE/EIA Standard Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information Technology Software Life Cycle Processes," and supporting standards address software quality. To meet the quality criterion, the application should address conformance to the criteria in 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 QA 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
- validation
- installation
- operations
- maintenance

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

- software requirements specifications
- hardware and software architecture descriptions
- major hardware component description and qualifications
- software design specifications
- 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 life-cycle phases:

- concepts
- requirements

- design
- implementation
- test
- installation, checkout, and acceptance testing
- operation
- maintenance
- retirement

The activities during the life-cycle phases are summarized below:

- 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

NUREG-0800, SRP BTP 7-14 describes the characteristics of a software development process that the NRC staff evaluates when assessing compliance with the quality criteria of 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 steps 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. The testing should exercise all portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions. 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 equipment meets the performance requirements related to safety functions.

(b) Qualification of Existing Commercial Computers—As guidance, the applicant should use EPRI TR-106439 and the safety evaluation approving this topical report for reference. 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 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 Subclauses 5.5.1 through 5.5.3 on designs for computer integrity, test and calibration, and fault detection and self-diagnostics activities. The application 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 meeting the requirements of IEEE Std 603, data communication between safety channels or between safety and nonsafety systems should not inhibit the performance of the safety function.

(7) Capability for Test and Calibration—The safety system equipment should have the capability for testing and calibration while retaining the capability to accomplish its safety functions. It should be possible to test and calibrate the safety system equipment during power operation, and the test should duplicate, as closely as practicable, the performance of the safety function. Testing of Class 1E systems should be in accordance with the requirements of IEEE Std 338, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."

(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. The requirement documentation should be available for NRC staff audit.

(9) Control of Access—The design should permit the administrative control of access to safety system equipment. Provisions within the safety systems, provision in the generating station design, or a combination of the two should support these administrative controls.

(10) Repair—The design of the safety systems should facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

(11) Identification—To ensure that the required computer system hardware and software are installed in the appropriate system configuration, the system should meet the following identification criteria specific to software systems:

- Firmware and software identification should ensure that the correct software is installed in the correct hardware component.
- The software should have a means to retrieve identification from the firmware by using software maintenance tools.
- Physical identification requirements of the digital computer system hardware should be in accordance with the identification requirements in IEEE Std 603.

(12) Auxiliary Features—There is no guidance beyond the requirements of IEEE Std 603-1991.

(13) Human Factors Considerations—The design should consider human factors at the initial stages and throughout the design process to ensure that the human operator(s) and maintenance personnel can successfully accomplish the functions allocated to them in whole or in part to meet the safety system design goals, in accordance with IEEE Std 1023, "Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities."

(14) 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 and may also involve software error recording and trending. RG 1.152, 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 Cyber Security Requirements

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

The life-cycle 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 through 2.9 of RG 1.152 describe digital safety system security guidance for the individual phases of the life cycle.