NUREG-0800
(Formerly NUREG-75/087)

U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

OFFICE OF NUCLEAR REACTOR REGULATION

Section 7.1. Instrumentation and Controls — Introduction

Version 11.0, June 24, 1997

Review Responsibilities

Primary — Instrumentation and Controls Branch (HICB)

Secondary — None

I. Areas of Review

The instrumentation and control (I&C) systems within the scope of Chapter 7 fall into the following nine categories and are addressed in detail in subsequent sections of the Safety Analysis Report (SAR) Chapter 7 or other sections of the SAR: reactor trip systems (RTS), engineered safety features actuation systems (ESFAS), safe shutdown systems, information systems important to safety, interlock systems important to safety, control systems, diverse I&C systems, data communication systems, and essential auxiliary supporting systems. Protection systems are those I&C systems which initiate safety actions to mitigate the consequences of design basis events. The protection systems include the RTS and the ESFAS.

1. *Reactor trip systems (RTS)* are those systems that initiate rapid control rod insertion to mitigate the consequences of design basis events. The RTS is discussed in Section 7.2 of the SAR.

2. *Engineered safety features actuation systems (ESFAS)* are those I&C systems that initiate and control safety equipment that remove heat or otherwise assist in maintaining the integrity of the three physical barriers to radioactive release (cladding, reactor coolant pressure boundary, and containment). The ESFAS is discussed in Section 7.3 of the SAR.

3. *Safe shutdown systems* are those systems which function to achieve and maintain a safe shutdown condition of the plant. The safe shutdown systems include those I&C systems used to maintain the reactor core in a subcritical condition and provide adequate core cooling to achieve and maintain both hot and cold shutdown conditions. Safe shutdown systems are discussed in Section 7.4 of the SAR.

4. *Information systems important to safety* are those systems which provide information for the safe operation of the plant during normal operation, anticipated operational occurrences, and accidents. The information systems important to safety include those systems which provide information for manual initiation and control of safety systems. They indicate that plant safety functions are being accomplished and provide information from which appropriate actions can be taken to mitigate the consequences of anticipated operational occurrences and accidents. During normal plant operation, the information systems important to safety provide information on the normal status and the bypassed and inoperable status of safety systems. Information systems important to safety are discussed in Section 7.5 of the SAR.

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

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

7. *Diverse instrumentation and control systems* are those systems provided expressly for diverse backup of the reactor protection system and engineered safety features actuation systems. Diverse I&C systems account for the possibility of common-mode failures in the protection systems. The diverse I&C systems category includes the anticipated transient without scram (ATWS) mitigation system as required by 10 CFR 50.62. For plants with digital computer-based instrumentation and controls, diverse I&C systems may also include hardwired manual controls, diverse displays, and any diverse actuation systems specifically installed to meet the guidance of the Staff Requirements Memorandum (SRM) on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." This SRM describes the NRC position on defense-in-depth and diversity. Diverse I&C systems are discussed in Section 7.8 of the SAR.

8. *Data communication systems* transmit signals between systems and between components of systems. Data communications systems may include analog and digital multiplexers as well as non-multiplexed transmission. Where such systems are included in a design, they support one or more of the systems described above. They may also support I&C functions addressed in other sections of the SAR. Data Communications Systems are discussed in Section 7.9 of the SAR.

9. *Essential auxiliary supporting systems* are those systems that function before the I&C systems important to safety can perform their functions. Heating, ventilation and air conditioning systems, electrical power systems, and cooling water systems are typical examples of essential auxiliary supporting systems. Essential auxiliary supporting systems are discussed primarily in Chapters 8 and 9 of the SAR. The I&C aspects of essential auxiliary supporting systems are addressed in the review of those SAR sections which discuss those systems. To the extent that the operation of essential auxiliary

supporting systems are initiated by the protection system, this aspect is included in the review of Sections 7.2 or 7.3 of the SAR.

All other I&C for systems important to safety, such as fire protection, fuel handling control, security systems, radiation monitoring, and control of essential auxiliary supporting systems are addressed in the review of other Standard Review Plan (SRP) sections which discuss these systems. HICB supports the review of these systems as a secondary reviewer. The acceptance criteria and review procedures of Chapter 7, Section 7.7 in particular, are also applicable to these other I&C systems.

HICB is a primary reviewer for one of these other SRP sections, Section 9.5.2, "Voice Communications." HICB is a secondary reviewer for the I&C functions discussed in the other SRP sections. For applications made under 10 CFR 52, HICB also has lead review responsibility for inspections, tests, analyses and acceptance criteria (ITAAC) that demonstrate the adequacy of I&C systems. ITAAC are intended to provide reasonable assurance that, if the inspections, tests, and analyses are performed, the acceptance criteria are met, and a plant is built according to the design, then the plant will operate in accordance with the design certification. SRP Section 14.3 describes the general acceptance criteria and review procedures for ITAAC. Section 14.3.5 describes the specific acceptance criteria and review procedures for I&C system ITAAC.

The review of Section 7.1 of the SAR includes the tabulation of I&C systems important to safety and the acceptance criteria and guidelines applicable to each of these systems. The review also identifies those I&C systems important to safety that are identical to those previously reviewed by the Staff, and those where the adequacy of the system is based upon prior NRC approval. The bases for prior approval includes the Staff's evaluation of applications for construction permits and operating licenses, preliminary and final design approvals for standardized plants, and topical reports.

Additional background or detailed information relevant to the acceptance criteria and the review process of this section can be found in the references to this section.

II. Acceptance Criteria

The General Design Criteria (GDC) provided in the NRC regulations establish minimum requirements for the design of nuclear power plants. ANSI/IEEE Std 279 is also incorporated in 10 CFR Part 50, 50.55a(h) of the NRC's regulations. These criteria establish the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety. The structures, systems, and components important to safety are those that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public. Although ANSI/IEEE Std 279 contains acceptance criteria only for protection systems, the concepts of ANSI/IEEE Std 279 are applicable as guidance to other I&C safety systems and to non-safety I&C system for which high functional reliability is a goal.

Regulatory guides amplify specific regulations, describe acceptable methods for meeting their requirements, and provide guidance to applicant/licensees. Industry codes and standards set forth requirements and recommended practices applicable to I&C systems for nuclear power plants. These standards are endorsed by regulatory guides, with or without modification, and provide acceptable methods for meeting the requirements of the regulations.

The acceptance criteria consist of the technical requirements of 10 CFR 50 including ANSI/IEEE Std 279 and the GDC, which establish the NRC requirements for I&C systems important to safety. The regulatory guides

and the endorsed industry codes and standards are the guidelines used as a basis for the evaluation of conformance to the requirements of the NRC's regulations. Table 7-1, "Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety," lists the acceptance criteria and guidelines applicable to I&C systems important to safety which are included in the evaluation of these systems as addressed in Chapter 7 of the SAR. Three Mile Island (TMI) Action Plan requirements for I&C systems important to safety are also identified in Table 7-1. Appendix 7.1-A describes the general process for reviewing any I&C system against the acceptance criteria and guidance identified in Table 7-1.

The IEEE superseded ANSI/IEEE Std 279 with IEEE Std 603 "Criteria for Safety Systems for Nuclear Power Generating Stations." The requirements and recommendations of IEEE Std 603, as endorsed by Reg. Guide 1.153 "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," incorporate the requirements and recommendations of ANSI/IEEE Std 279. The guidance described in IEEE Std 603 will be used by the NRC staff in its evaluation of the design, reliability, qualification, and testability of the power, I&C, and control portions of safety systems.

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 safety analysis report (SAR). Therefore, while the guidance of IEEE Std 603 and the requirements of ANSI/IEEE Std 279 are equally applicable to protection systems, IEEE Std 603 is more directly applicable to I&C safety systems other than the protection systems (i.e., information systems, safe shutdown systems, and interlock systems). The guidance of IEEE Std 603 is also more readily adaptable for use in the review of non-safety I&C systems.

Non-safety I&C systems are reviewed to ensure that they 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 SAR. This includes verification that non-safety systems are appropriately isolated from safety systems and that the quality and reliability of these systems is sufficient to minimize challenges to safety systems.

Supplemental Guidance for Digital Computer-Based Safety Systems

For designs that include digital computer-based I&C systems (including hardware, software and firmware), additional issues should be considered when evaluating compliance with 10 CFR 50. Appropriate references to review criteria and review procedures are also included in Appendices A, B, and C to this section.

Reg. Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," SECY-91-292, "Digital Computer Systems for Advanced Light Water Reactors," and SECY-93-087 describe the additional issues involved. These issues and review criteria are summarized below. It is important to note that all criteria of 10 CFR 50 apply to safety-related digital I&C systems. The information here is intended only to clarify the application of certain of these requirements to digital systems, not to replace existing requirements or guidance.

Reg. Guide 1.28, "Quality Assurance Program Requirements (Design and Construction)," endorses the 1983 edition of ASME Std NQA-1, "Quality Assurance Requirements for Nuclear Facility Applications." The 1994 edition of NQA-1 also includes the former ASME Std NQA-2a, Part 2.7 of which addresses computer software. ASME Std NQA-2a, Part 2.7 is referenced by IEEE Std 7-4.3.2, Section 5.3.1, but has not been endorsed by the NRC.

1. Electromagnetic compatibility — Section 3(7) of ANSI/IEEE Std 279 requires that the design basis for protection systems document the range of transient and steady-state conditions throughout which the system must perform. IEEE Std 603 contains similar requirements. For digital computer-based systems, the range of conditions considered should include the electromagnetic environment, including electrostatic discharge. Electrical Power Research Institute (EPRI) topical report TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," and the associated Staff safety evaluation report describe an adequate guideline for qualifying digital I&C equipment for a plant environment. Lightning protection should be addressed as part of the review of electromagnetic compatibility. Lightning protection features should conform to the guidance of NFPA Std 78, "Lightning Protection Code," and ANSI/IEEE Std 665, "Guide for Generation Station Grounding."

2. Computer system quality — In order for safety-related, digital computer-based I&C systems to comply with the quality and reliability requirements of ANSI/IEEE Std 279, GDC 1, GDC 21, GDC 29, and 10 CFR 50 Appendix B, the computers (including embedded software) must be of high quality. The quality requirements applicable to hardware are well documented in ANSI/IEEE Std 279, IEEE Std 603, and ASME Std NQA-1. IEEE Std 7-4.3.2 identifies five areas where additional guidance is needed to support evaluation of digital systems with respect to these requirements.

    a. Software development and hardware/software integration — An acceptable means of ensuring the quality of computer systems and their embedded software includes developing the software and then performing system integration using a well-structured and well-executed software engineering process. This process should (1) be in accordance with the requirements of 10 CFR 50 Appendix B, (2) be consistent with the guidance of ASME Std NQA-2a Part 2.7, and (3) implement a software engineering life cycle in accordance with the guidance of Reg. Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." BTP HICB-14 describes the characteristics of an acceptable software engineering process in more detail. The inspections and tests conducted as part of this process should demonstrate that the final product exhibits the qualities that characterize high quality software and the computer system, with its embedded software, performs as designed. BTP HICB-14 describes the characteristics the Staff expects I&C system software and software life cycle processes to exhibit.

    b. Qualification of existing commercial computers, including predeveloped software (PDS) — To meet the fundamental quality requirements, the following should be qualified for use in the plant instrumentation systems: existing computers and predeveloped software (commercial off-the-shelf software, or PDS produced for another purpose). All software, including operating systems, resident on safety system computers at run time must be qualified for their intended applications. IEEE Std 7-4.3.2, Section 5.3.2 describes an acceptable set of fundamental requirements for this qualification process. This standard allows the use of engineering judgment for the acceptance of existing software, and the use of compensating factors to substitute for missing elements of the software development process. These provisions should not be interpreted to permit unsupported subjectivity in the acceptance of existing software. EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," provides more detail on the characteristics of an acceptable process for qualifying existing software, and discusses the use of engineering judgment and compensating factors.

        Programmable logic controllers (PLCs) are a possible means of implementing safety-related I&C using existing commercial computers. BTP HICB-18 describes an acceptable process for applying the recommendations of this section to PLC implementations.

c. Software tools — Compliance with the fundamental quality requirements necessitates that computer-based tools used in the design of digital I&C not introduce faults into the software which is resident on the computer at run time. IEEE Std 7-4.3.2, Section 5.3.3 describes an acceptable means of preventing such faults. The qualification process described in EPRI TR-106439 and the development process described in BTP HICB-14 are acceptable alternative processes for ensuring the quality of software tools is adequate to minimize the introduction of faults into plant software.

d. Verification and validation — As described in Section 5.3.4 of IEEE Std 7-4.3.2, an acceptable software development process and hardware/software integration process will include verification and validation that provides adequate confidence that both the safety system requirements and those requirements defined at each stage of development, including handling of credible abnormal conditions, have been implemented. Implementation of a software engineering process as described by BTP HICB-14 will ensure adequate verification and validation. Reg. Guides 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," and 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," describe acceptable approaches to planning and conducting certain verification and validation activities of a software engineering process.

e. Software configuration management — As described in Section 5.3.5 of IEEE Std 7-4.3.2, an acceptable software development process will include software configuration management in accordance with ASME NQA-2a Part 2.7. BTP HICB-14 describes the characteristics that the Staff expects software configuration management processes will exhibit. Reg. Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," describes an acceptable method for implementing software configuration management.

3. Equipment qualification — To comply with the requirements of GDC 4, 10 CFR 50.49, and ANSI/IEEE Std 279 Sections 3.7, 4.4, & 4.5, environmental qualification must demonstrate that the design basis and performance requirements of the I&C system are met when the equipment is exposed to normal and adverse environments. SRP Appendices 7.1-B and 7.1-C describe the review of qualification for all environments.

4. System integrity — ANSI/IEEE Std 279, Section 4.5 and GDC 21 require that all protection system channels maintain necessary functional capability under extremes of conditions relating to environment, energy supply, malfunctions, and accidents. Section 5.5 of IEEE Std 603 includes similar requirements for safety systems. Evaluation of digital systems with respect to these requirements includes assuring design for computer integrity and design for test and calibration.

a. Design for computer integrity — As discussed in Section 5.5.1 of IEEE Std 7-4.3.2, digital systems must be designed to perform their safety function when subjected to all conditions that have significant potential for defeating their safety function. Evaluation with respect to the other topics discussed for computer-based systems addresses many aspects of design for integrity. In addition, design for computer integrity involves selecting system architectures and design standards to ensure that system real-time performance is predictable and within design requirements. BTP HICB-21 describes the review of digital computer real-time performance.

b. Design for test and calibration — Digital computer-based systems generally cannot be designed such that all failure modes are either "fail-safe" or revealed by indication of the failure. Therefore, automated self-test features may be necessary for failure detectability. Special features may also be needed to provide the capability to support surveillance testing. IEEE Std 603, Section 5.7 describes the fundamental guidance applicable to test and calibration features. BTP HICB-17 describes the automatic self-testing and surveillance testing features characteristic of an acceptable digital system.

5. Communications independence — Sections 4.6 and 4.7 of ANSI/IEEE Std 279 require independence between redundant channels of the protection system and between safety systems and non-safety systems. IEEE Std 603, Section 5.6 contains similar requirements as do GDC 21, 22, and 24. Evaluation of digital systems with respect to these requirements should consider the effect of data communications on independence and the isolation of safety and non-safety portions of computer software. This is in addition to the need to consider electrical and physical independence within any I&C system as discussed elsewhere in this chapter. Annex G of IEEE Std 7-4.3.2 describes acceptable approaches to computer communication independence. The preferred approach to communication independence ensures that (1) redundant safety-grade equipment communicate via one-way communications paths, (2) safety-grade systems do not receive information from non-safety-grade systems except when under test, (3) if two-way communications are used, failure of coordination or handshaking between sending and receiving systems does not prevent either system from functioning correctly, and (4) the control of communications links resides in the sending system. SRP Appendix 7.1-C provides guidance for the review of communications independence.

6. Reliability — GDC 21 and ANSI/IEEE Std 279 require that protection systems be designed with high functional reliability. IEEE Std 603 requires the analysis of system design to confirm that safety systems achieve the reliability goals established by the design basis. As discussed in Section 5.15 of IEEE Std 7-4.3.2, when reliability goals are established at the system level, the proof of meeting the goals must address software reliability.

   The Staff does not endorse the concept of quantitative reliability goals as a sole means of meeting the NRC's regulations for the reliability of digital computers used in safety systems. The NRC staff's acceptance of the reliability of the computer system is based on deterministic criteria for both the hardware and software rather than on quantitative reliability goals. This topic is discussed further in Reg. Guide 1.152 and SRP Appendix 7.1-C.

   Nevertheless, qualitative reliability estimation using a combination of analysis, testing, and operating experience can provide an added level of confidence in a system's reliable performance. Qualitative estimation of software reliability should address the fact that software failures that are not the consequence of hardware failures are caused by design errors and, therefore, do not follow the random failure behavior used for hardware reliability.

   Software that complies with the quality criteria of item 2 above and that is used in safety systems that provide measures for defense against common mode failures as described below are considered by the Staff to comply with the fundamental reliability requirements of GDC 21, ANSI/IEEE Std 279, and IEEE Std 603.

7. Defense against common-mode failures — Experience shows that flaws in requirements and design can be expected to exist in even the highest quality software despite good engineering processes and testing. These residual flaws pose the concern that the use of common software has the potential to propagate

common-cause or common-mode failures that can defeat the redundancy provided by hardware architectural structure. To address this issue, designs that incorporate digital computer-based protection systems must comply with the NRC position on defense-in-depth and diversity as described in the Staff Requirements Memorandum on SECY-93-087. BTP HICB-19 describes acceptable means for complying with this position.

8. Use of emerging software methods — Software engineering is a maturing field. Certain techniques that are still under development may be proposed by applicant/licensees. Two general areas of emerging methods are formal methods and the use of non-procedural languages. There may be other methods that should be considered. Proposal of such techniques for development of systems or components important to safety, or the use of commercial items using such techniques in systems important to safety, will require careful consideration by the reviewer.

    a. Formal methods — Formal methods are approaches based on the use of mathematical techniques and notations for describing and analyzing properties of software systems. Descriptions of the system are written using notations based on mathematical expressions rather than a natural language such as English. This allows formal proof that the specification has certain properties such as completeness and internal consistency. Formal methods, knowledgeably applied, can improve the software development process. Therefore, the Staff encourages the informed use of formal methods as part of a applicant/licensee's software engineering process. The Staff, however, neither requires the use of formal methods nor will allow the use of formal methods to replace compliance with the fundamental acceptance criteria described in items 1 through 7 above. Section C.3.7 of Appendix 7.0-A discusses in more detail the use of formal and semiformal languages for describing software requirements and design.

    b. Non-procedural languages — Non-procedural software techniques include expert systems, neural networks, fuzzy systems, and genetic algorithms. These methods are not sufficiently mature at this time to support the definition of processes for evaluating conformance with the acceptance criteria of 10 CFR 50 and ANSI/IEEE Std 279.

Application of the Supplemental Guidance to Computer-Based Systems Important to Safety

Digital computers may be used in non-safety systems that are important to safety and are provided to comply with:

- GDC 13 (Instrumentation & Control)
- GDC 19 (Remote Shutdown)
- 10 CFR 50 Appendix R, Section III.G.1.b (Remote Cold Shutdown)
- 10 CFR 50 Appendix R, Section III.L.1 (Alternate or Dedicated Shutdown)
- 10 CFR 50.62 (ATWS)
- 10 CFR 50.63 (Station Blackout)

- 10 CFR 50.47 (Emergency Response)

GDC 1 and 10 CFR 50.55a(a)(1) require that these systems be designed to quality standards commensurate with the importance of the safety function to be performed. Items 1, 2, 4, 6, and 8 above should be considered when evaluating such systems with respect to these criteria. Item 3 above should also be considered for systems whose failure under postulated environmental conditions could prevent satisfactory accomplishment of safety functions. Item 5 above should also be considered for reactivity control systems required for remote, alternate, or dedicated shutdown systems required by GDC 19 or 10 CFR 50 Appendix R.

Other acceptance criteria which are applicable to I&C systems important to safety are not included when the evaluation of conformance to such criteria is addressed in the review of other SAR sections. For example, GDC 3, "Fire Protection," is not included in Table 7-1 since conformance to the requirements of GDC 3 is addressed in the review of Section 9.5.1 of the SAR.

Appendix A to this SRP section provides guidance on the applicability and review methods to be used in evaluating conformance to the acceptance criteria and guidelines for I&C systems important to safety. Appendix B to this SRP section provides guidance to be used in the evaluation of conformance to the requirements of ANSI/IEEE Std 279. Appendix C to this SRP section provides guidance for evaluation of conformance to IEEE Std 603.

III. Review Procedures

Section 7.0 provides an overview of the review process for I&C systems. Within this process, the objectives of the review of Section 7.1 of the SAR are to confirm that the I&C systems important to safety are addressed in Chapter 7 of the SAR and that the applicant/licensee commits to appropriate acceptance criteria and guidelines applicable to each of these systems. This identification meets the applicable requirements of General Design Criterion 1, "Quality Standards and Records," of 10 CFR Part 50 Appendix A. General Design Criterion 1 requires that, "Structures, systems and components important to safety shall be designed, fabricated, erected and tested to quality standards commensurate with the importance of the safety function to be performed." Therefore, the review of Section 7.1 should confirm that the SAR includes (1) a discussion regarding the applicability of each criterion and guideline for each system important to safety, and (2) a statement that the criteria and guidelines are implemented or will be implemented in the design of I&C systems important to safety. If exceptions to the guidelines are taken, the review confirms that an acceptable basis has been provided for those exceptions.

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

1. Section 7.1 is reviewed to confirm that all I&C systems important to safety are included in Chapter 7. Normally, Chapter 7 of the SAR should address each of the I&C systems included in the areas of review for Section 7.1 of the SRP. This review should confirm that all I&C systems, including embedded computers and software necessary to support the operation of safety systems, are identified in Section 7.1 and discussed in subsequent sections of Chapter 7. The safety systems supported by the I&C system are described in other sections of the SAR (particularly in Chapters 5, 6, 8, 9, 10, 15, and 18). The review of the systems identified is coordinated with the branches which have primary review responsibility for the supported systems.

2. The acceptance criteria applicable to each of the I&C systems important to safety are reviewed to confirm that the appropriate criteria have been identified for each system. Appendix 7.1-A identifies the

acceptance criteria applicable to the I&C systems important to safety, and describes the method and scope of the review to verify conformance.

3. The guidelines applicable to each of the I&C systems important to safety are reviewed to confirm that the appropriate guidelines have been identified for each system. Appendix 7.1-A identifies the guidelines applicable to the I&C systems important to safety, and describes the method and scope of the review to verify conformance.

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

5. When the applicant/licensee proposes I&C systems that incorporate digital computers, the review includes the supplemental guidance for digital computer based systems described in part II above. Appendix 7.0-A describes the review process.

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

7. If the proposed systems employ technologies that have not previously been accepted by the Staff, the reviewer should identify these technologies and establish a basis for acceptance prior to proceeding with the review.

8. The proposed resolution of unresolved safety issues (USIs) and medium- and high-priority generic safety issues (GSIs) are reviewed. Appendix 7.1-A identifies the guidance for review of the resolution of USIs and GSIs.

Additional Review Steps for Design Certification or Combined License Applications Under 10 CFR Part 52:

9. The certified design material (CDM) is reviewed to confirm that it describes the key characteristics, performance requirements and proposed inspections, tests, analyses and acceptance criteria (ITAAC) for each instrumentation system important to safety. SRP Chapter 14 contains guidance for the review of CDM. Additionally, the ITAAC implementation is reviewed to confirm that the as-built systems conform to the certified design.

IV. Evaluation Findings

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

The applicant/licensee has identified the I&C systems which are important to safety in accordance with Reg. Guide 1.70, Revision 3, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants," November 1978.

The applicant/licensee has identified the acceptance criteria consisting of the General Design Criteria and ANSI/IEEE Std. 279, included in the NRC's regulations, which are applicable to those systems as identified in the SRP. The applicant/licensee has also identified the guidelines consisting of the regulatory guides and the industry codes and standards which are applicable to the systems as identified in the SRP. [If exception to the guidelines has been taken by the applicant/licensee, an evaluation of the exception or a reference to the section of the SER which addresses those exceptions should be provided.] The Staff concludes that the implementation of the identified acceptance criteria and guidelines satisfies the requirements of GDC 1 with respect to the design, fabrication, erection, and testing to quality standards commensurate with the importance of the safety functions to be performed.

Note: the following finding applies only to applications under 10 CFR 52.

The review confirms that each of the safety systems identified in the SAR also has an associated design description and ITAAC.

V. Implementation

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

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

VI. References

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

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

ANSI/IEEE Std 323-1974. "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."

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

ANSI/IEEE Std 665-1987. "Guide for Generation Station Grounding."

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

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

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

ASME Std NQA-1-1994. "Quality Assurance Requirements for Nuclear Facility Applications."

ASME Std NQA-2a-1990 Part 2.7. "Quality Assurance Requirements of Computer Software for Nuclear Facility Applications."

EPRI Topical Report TR-102323. "Guidelines for Electromagnetic Interference Testing in Power Plants." Electric Power Research Institute, September 1994.

EPRI Topical Report TR-106439. "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." Electric Power Research Institute, October 1996.

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

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

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

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

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

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

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

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

IEEE Std 1074-1991. "IEEE Standard for Developing Software Life Cycle Processes."

ISA-S67.02-1980. "Nuclear-Safety-Related Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants."

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

NFPA Std 78. "Lightning Protection Code." National Fire Protection Association, 1992.

NUREG/CR-6421. "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications." March 1996.

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

NUREG-0718 R01. "Licensing Requirements for Pending Applications for Construction Permits and Manufacturing License." 1981.

NUREG-0737. "Clarification of TMI Action Plan Requirements." 1980.

NUREG-0933. "A Prioritization of Generic Safety Issues." Updated periodically.

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

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

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

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

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

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

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

Regulatory Guide 1.28. "Quality Assurance Program Requirements (Design and Construction)." 1985.

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

Regulatory Guide 1.89. "Environmental Qualification of Certain Electric Equipment Important to Safety in Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1984.

Safety Evaluation by the Office of Nuclear Reactor Regulation. "EPRI Topical Report TR-102323." April 17, 1996.

Safety Evaluation by the Office of Nuclear Reactor Regulation. "EPRI Topical Report TR-106439." March 1997.

SECY-91-292. "Digital Computer Systems for Advanced Light Water Reactors." September 16, 1991.

SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." April 2, 1993.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." July 15, 1993.

Table 7-1. Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety

Version 12.0, May 2, 1997

The matrix of Table 7-1 identifies the acceptance criteria (denoted by "A") and the guidelines (denoted by "G") and their applicability to the various sections of Chapter 7 of the SAR. These acceptance criteria include the applicable General Design Criteria and ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," which establish the NRC requirements for the instrumentation and control systems important to safety. The guidelines for implementation of these requirements are provided in the current versions of regulatory guides, the endorsed industry standards, and the branch technical positions (BTPs) of the Instrumentation and Control Systems Branch (HICB). The BTPs listed in this table are contained in Appendix 7-A. The guidelines are not mandatory and only set forth acceptable methods of implementing the acceptance criteria. The BTPs are used when a particular design problem has an identified and acceptable solution; they also are not mandatory. In all cases, the primary basis for acceptance of the design is conformance to the acceptance criteria.

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

TMI action plan requirements for instrumentation and control systems important to safety are imposed by 10 CFR 50.34(f) for applications approved after February 16, 1982. For operating reactors that had approved construction permits prior to February 16, 1982, the TMI action plan requirements were imposed by Generic Letters that required conformance with NUREG-0718, "Licensing Requirements for Pending Applications for Construction Permits and Manufacturing License," NUREG-0737, "Clarification of TMI Action Plan Requirements," NUREG-0737, Supplement 1, "Clarification of TMI Action Plan Requirements — Requirements for Emergency Response Capability," and NUREG-0694, "TMI-Related Requirements for New Operating Reactor Licenses." Table 7.1 identifies both the CFR and TMI action plan reference numbers for the TMI action plan requirements relevant to Chapter 7 of the safety analysis report. The Action Plan references are given in brackets under the reference to the equivalent requirement of 10 CFR 50.34(f). Appendix 7.1-A presents specific acceptance criteria for TMI Action Plan items. However, important context information is found in the concepts contained in the referenced reports.

Table 7-1. Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety

Criteria		Title	Applicability								Remarks
			7.2	7.3	7.4	7.5	7.6	7.7	7.8	7.9	
1. 10 CFR Parts 50 and 52											
a.	50.55a(a)(1)	Quality Standards for Systems Important to Safety	A	A	A	A	A	A	A	A	
b.	50.55a(h)	Criteria for Protection Systems for Nuclear Power Generating Stations (ANSI/IEEE Std 279)	A	A	*	*	*	*	*	**	
c.	50.34(f)(2)(v) [I.D.3]	Bypass and Inoperable Status Indication	A	A		A	A			**	See NUREG-0718, -0737, -0737 Supplement 1, and -0694
d.	50.34(f)(2)(xii) [II.E.1.2]	Auxiliary Feedwater System Automatic Initiation and Flow Indication		A		A					Applies only to PWRs. See NUREG-0718, -0737, and -0694
e.	50.34(f)(2)(xvii) [II.F.1]	Accident Monitoring Instrumentation				A					See NUREG-0718, -0737 Supplement 1, and -0694
f.	50.34(f)(2)(xviii) [II.F.2]	Inadequate Core Cooling Instrumentation				A					See NUREG-0694
g.	50.34(f)(2)(xiv) [II.E.4.2]	Containment Isolation Systems		A							See NUREG-0737
h.	50.34(f)(2)(xix) [II.F.3]	Instruments for Monitoring Plant Conditions Following Core Damage				A					See NUREG-0718
i.	50.34(f)(2)(xx) [II.G.1]	Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves			A	A					Applies only to PWRs. See NUREG-0737
j.	50.34(f)(2)(xxii) [II.K.2.g]	Failure Mode and Effect Analysis of Integrated Control System						A			Applies only to B&W plants. See NUREG-0718, -0737, and -0694
k.	50.34(f)(2) (xxiii)(II.K.2.10)	Anticipatory Trip on Loss of Main Feedwater or Turbine Trip	A								Applies only to B&W plants. See NUREG-0737, and -0694

* The ANSI/IEEE Std 279 requirement to provide adequate separation between protection and control function (item 4.7.2) applies to all instrumentation and control systems. The requirements for display of bypass and inoperable status indication (item 4.13) also apply to information systems important to safety (Section 7.5). Although not required by NRC regulations, the other criteria of ANSI/IEEE Std 279 and Reg. Guide 1.153 address considerations such as design bases, redundancy, independence, single failures, qualification, bypasses, status indication, and testing that are used as guidance, where appropriate, for systems addressed in these sections of the SRP.

** The data communication systems (DCS) addressed by Section 7.9 are support systems for one or more of the systems addressed by Section 7.2 through 7.8. Acceptance criteria for a specific DCS derive from the acceptance criteria for the systems supported by that DCS. The criteria marked as ** are likely to apply to the DCS in one or more possible DCS applications. Section 7.9 gives more detailed guidance on the applicability of these criteria to specific DCS applications.

Criteria		Title	Applicability								Remarks
			7.2	7.3	7.4	7.5	7.6	7.7	7.8	7.9	
l.	50.34(f)(2)(xxiv) [II.K.3.23]	Central Reactor Vessel Water Level Recording				A					Applies only to BWRs. See NUREG-0718
m.	50.62	Requirements for Reduction of Risk from Anticipated Transients without Scram							A	**	
n.	52.47(a)(1)(iv)	Resolution of Unresolved and Generic Safety Issues	A	A	A	A	A	A	A	A	Applies only to applications for design certification or licensing of certified designs under Part 52
o.	52.47(a)(1)(vi)	ITAAC in Design Certification Applications	A	A	A	A	A	A	A	A	Applies only to applications for design certification or licensing of certified designs under Part 52
p.	52.47(a)(1)(vii)	Interface Requirements	A	A	A	A	A	A	A	A	Applies only to applications for design certification or licensing of certified designs under Part 52
q.	52.47(a)(2)	Level of Detail	A	A	A	A	A	A	A	A	Applies only to applications for design certification or licensing of certified designs under Part 52
r.	52.47(b)(2)(i)	Innovative Means of Accomplishing Safety Functions	A	A	A	A	A			A	Applies only to applications for design certification or licensing of certified designs under Part 52
s.	52.79(c)	ITAAC in Combined Operating License Applications	A	A	A	A	A	A	A	A	Applies only to applications for combined licenses under Part 52.
2. General Design Criteria (GDC) 10 CFR Part 50 Appendix A											
a.	GDC 1	Quality Standards and Records	A	A	A	A	A	A	A	A	
b.	GDC 2	Design Bases for Protection Against Natural Phenomena	A	A	A	A	A			**	
c.	GDC 4	Environmental and Missile Design Bases	A	A	A	A	A			**	
d.	GDC 13	Instrumentation and Control	A	A	A	A	A	A	A	**	
e.	GDC 19	Control Room	A	A	A	A	A	A	A	**	
f.	GDC 20	Protection System Functions	A	A							
g.	GDC 21	Protection Systems Reliability and Testability	A	A						**	

Criteria		Title	Applicability								Remarks
			7.2	7.3	7.4	7.5	7.6	7.7	7.8	7.9	
h.	GDC 22	Protection System Independence	A	A						**	
i.	GDC 23	Protection System Failure Modes	A	A						**	
j.	GDC 24	Separation of Protection and Control Systems	A	A	A	A	A	A	A	A	
k.	GDC 25	Protection System Requirements for Reactivity Control Malfunctions	A				A				
l.	GDC 29	Protection Against Anticipated Operational Occurrences	A					A		**	
3. Staff Requirements Memoranda											
a.	SRM to SECY 93-087 II.Q	Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems	A	A				A	A	**	See BTP HICB-19
b.	SRM to SECY 93-087 II.T	Control Room Annunciator (Alarm) Reliability				A				**	Applies only to advanced light water reactors
4. Regulatory Guides											
a.	Reg. Guide 1.22	Periodic Testing of Protection System Actuation Functions	G	G					G	**	See BTP HICB-8
b.	Reg. Guide 1.47	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System	G	G		G	G			**	
c.	Reg. Guide 1.53	Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems	G	G	G	G	G			**	See ANSI/IEEE Std 379 (ANSI N41.2)
d.	Reg. Guide 1.62	Manual Initiation of Protection Actions	G	G					G		
e.	Reg. Guide 1.75	Physical Independence of Electric Systems	G	G	G	G	G	G	G	G	See ANSI/IEEE Std 384 (ANSI/N41.14)
f.	Reg. Guide 1.97	Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident				G					See ANSI/ANS 4.5
g.	Draft Reg. Guide DG-1045	Proposed Revision 3 to Reg. Guide 1.105, "Instrument Spans and Setpoints"	G	G	G	G	G	G	G	G	See ISA Std S67.04 and BTP HICB-12
h.	Reg. Guide 1.118	Periodic Testing of Electric Power and Protection Systems	G	G	G	G	G		G	**	See IEEE Std 338
i.	Reg. Guide 1.151	Instrument Sensing Lines	G	G	G	G	G	G	G		See ANSI/ISA-S67.02
j.	Reg. Guide 1.152	Digital Computers in Safety Systems of Nuclear Power Plants	G	G	G	G	G	G	G	G	See IEEE Std 7-4.3.2
k.	Reg. Guide 1.153	Power Instrumentation and Control Portions of Safety Systems	G	G	G	G	G	*	*	**	See IEEE Std 603

Criteria		Title	Applicability								Remarks
			7.2	7.3	7.4	7.5	7.6	7.7	7.8	7.9	
l.	Reg. Guide 1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	G	G	G	G	G	G	G	G	See IEEE Std 828 and IEEE Std 1042
m.	Reg. Guide 1.168	Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	G	G	G	G	G	G	G	G	See ANSI/IEEE Std 1012 and IEEE Std 1028
n.	Reg. Guide 1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	G	G	G	G	G	G	G	G	See IEEE Std 830
o.	Reg. Guide 1.170	Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	G	G	G	G	G	G	G	G	See ANSI/IEEE Std 829
p.	Reg. Guide 1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	G	G	G	G	G	G	G	G	See ANSI/IEEE Std 1008
q.	Reg. Guide 1.173	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	G	G	G	G	G	G	G	G	See IEEE Std 1074
5. Branch Technical Positions (BTP) HICB											
a.	BTP HICB-1	Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System					G				
b.	BTP HICB-2	Guidance on Requirements on Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines					G				
c.	BTP HICB-3	Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service	G	G							
d.	BTP HICB-4	Guidance on Design Criteria for Auxiliary Feedwater Systems		G							
e.	BTP HICB-5	Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors	G				G	G			
f.	BTP HICB-6	Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode		G							
g.	BTP HICB-7	Not used									

Criteria		Title	Applicability								Remarks
			7.2	7.3	7.4	7.5	7.6	7.7	7.8	7.9	
h.	BTP HICB-8	Guidance on Application of Regulatory Guide 1.22	G	G						**	
i.	BTP HICB-9	Guidance on Requirements for Reactor Protection System Anticipatory Trips	G								
j.	BTP HICB-10	Guidance on Application of Regulatory Guide 1.97				G					
k.	BTP HICB-11	Guidance on Application and Qualification of Isolation Devices	G	G	G	G	G	G	G	**	
l.	BTP HICB-12	Guidance on Establishing and Maintaining Instrument Setpoints	G	G	G	G	G		G	G	
m.	BTP HICB-13	Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors	G	G	G	G					
n.	BTP HICB-14	Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems	G	G	G	G	G	G	G	G	
o.	BTP HICB-15	Not used									
p.	BTP HICB-16	Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52.	G	G	G	G	G	G	G	G	
q.	BTP HICB-17	Guidance on Self-Test and Surveillance Test Provisions	G	G	G	G	G	G	G	G	
r.	BTP HICB-18	Guidance on Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems	G	G	G	G	G	G	G	G	
s.	BTP HICB-19	Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems	G	G				G	G	G	
t.	BTP HICB-20	Not used									
u.	BTP HICB-21	Guidance on Digital Computer Real-Time Performance	G	G	G	G	G	G	G	G	