U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

OFFICE OF NUCLEAR REACTOR REGULATION

NEW

Appendix 7.0-A
Review Process for Digital Instrumentation and Control Systems

Version 11.0, June 24, 1997

A. Introduction

This appendix provides an overview of the process for reviewing the unique aspects of digital instrumentation and control (I&C) systems. It supplements the description of the process for review of (1) the overall I&C system design described in Section 7.0, (2) the design criteria and commitments described in Section 7.1, and (3) the individual digital I&C systems described in Sections 7.2 through 7.9. This appendix illustrates how the review activities interact with each other and with the overall I&C review process described in Sections 7.1 through 7.9. Additional information relevant to the review process can be found in the references in Section D of this appendix.

More detailed information on the regulatory bases, acceptance criteria, and review processes for specific issues are described in Section 7.1, related branch technical positions (BTPs), and regulatory guides.

Definitions

An *activity group* is a collection of software life cycle activities, all of which are related to a specific life-cycle topic. Eight activity groups are recognized in this appendix: planning, requirements, design, implementation, integration, validation, installation, and operations and maintenance.

Critical characteristics are those properties or attributes that are essential for performance of an equipment's safety function (IEEE Std 934, "Requirements for Replacement Parts for Class 1E Equipment in Nuclear Power Generating Stations"). A similar definition is provided in EPRI NP-5652, "Guideline for the

Utilization of Commercial Grade Items in Nuclear Safety Related Applications," in relation to commercial dedication.

Design output includes documents, such as drawings and specifications, that define technical requirements of structures, systems, and components (ASME Std NQA-1, "Quality Assurance Requirements for Nuclear Facility Applications"). For software, design outputs are the products of the development process that describe the end product that will be installed in the plant. The design outputs of a software development process include software requirements specifications, software design specifications, hardware and software architecture, code listings, system build documents, installation configuration tables, operations manuals, maintenance manuals, and training manuals.

The *design process* comprises technical and management processes that commence with identification of design input and lead to and include the issuance of design output documents (ASME Std NQA-1).

A *design requirement* is a requirement that specifies or constrains the design of a system or system component (IEEE Std 610.12, "IEEE Standard Glossary of Software Engineering Terminology").

Deterministic refers to a property of a computer or communication system such that the time delay between stimulus and response has a guaranteed maximum and minimum.

Embedded software or *firmware* is software that is built into (stored in read-only memory) a computer dedicated to a pre-defined task. Normally, embedded software cannot be modified by the computer that contains it, nor will power failure erase it; some computers may contain embedded software stored in electrically erasable programmable read-only memory (EEPROM), but changing this memory typically requires a special sequence of actions by maintenance personnel.

A *function* is a specific purpose of an entity or its characteristic action (IEEE Std 610.12, "IEEE Standard Glossary of Software Engineering Terminology").

A *functional characteristic* is a trait or property of a design output that implements a functional requirement, a portion of a functional requirement, or a combination of functional requirements. BTP HICB-14 identifies specific functional requirements considered in software reviews.

A *functional requirement* is a requirement that specifies a function that a system or system component must be capable of performing (IEEE Std 610.12). In this appendix, the term functional requirement includes design requirements, interface requirements, performance requirements, and physical requirements, as described in IEEE Std 610.12.

Hardware critical characteristics are those properties or attributes of computer, peripheral, or communication hardware that are essential for performance of the connected equipment's safety function. This includes meeting specifications that are required to execute the software intended to run on the hardware, as well as attributes of reliability, testability, or predictability upon which the Staff's safety findings are based.

Predeveloped software (PDS) is software that already exists, is available as a commercial or proprietary product, and is being considered for use in a computer-based function (IEC Std 880, "Software for Computers in the Safety Systems of Nuclear Power Stations," Supplement 1 draft). Commercial off-the-shelf (COTS) software is a subset of PDS.

Software critical characteristics are those properties or attributes of a software or firmware product that are essential for performance of the related equipment's safety function. This includes functional requirements that are allocated to the software product, as well as attributes of robustness, testability, or dependability upon which the Staff's safety findings are based.

A s*oftware development process characteristic* is a trait or property of a software development process design output that results from the implementation of a design process. BTP HICB-14 identifies specific software development process characteristics considered in software reviews.

A *software development process requirement* describes an activity, or activities, that a software development process must include.

A *software life cycle* is a project-specific, sequenced mapping of activities (Reg. Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorsing IEEE Std 1074, "IEEE Standard for Developing Software Life Cycle Processes"). The software life cycle typically includes a planning phase, requirements phase, design phase, implementation phase, integration phase, validation phase, installation phase, and operation and maintenance phase. The purpose of such a mapping is to permit concurrent execution of related activities, and to provide staged checkpoints at which product and process characteristics are verified during the development process.

B. Background

The fundamental acceptance criteria for I&C systems are described in 10 CFR 50.55a; ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations;" Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," which endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations;" and Appendix A of 10 CFR 50 (General Design Criteria). Appendix B of 10 CFR 50 (Quality Assurance Criteria) provides criteria for quality assurance programs to be applied to the design, fabrication, construction, and testing of I&C safety systems. The criteria of 10 CFR 50 apply to digital I&C systems and are sufficient to support licensing of such systems. For applications under 10 CFR 52, the technical acceptance criteria of 10 CFR 50 apply.

Certain characteristics of digital I&C systems necessitate that augmented review approaches and different review perspectives be used in assessing compliance with the fundamental acceptance criteria of 10 CFR 50. These characteristics are important to the evaluation of (1) design qualification of digital systems, (2) protection against common-mode failure, and (3) selected functional requirements of IEEE Std 603 and the General Design Criteria that pose new assurance challenges when implemented using computers. These topics are discussed in more detail below.

B.1. Qualification of Digital Instrumentation and Control Systems and Components

Digital I&C systems require additional design and qualification approaches than are typically employed for analog systems. The performance of analog systems can typically be predicted by the use of engineering models. These models can also be used to predict the regions over which an analog system exhibits continuous performance. The ability to analyze design using models based upon physics principles, and the ability to use these models to establish a reasonable expectation of continuous performance over substantial ranges of input conditions are important factors used in the qualification of analog systems design. These factors enable extensive use of type testing, acceptance testing, and inspection of design outputs in qualifying the design of analog systems and components. If the design process ensures continuous behavior over a fixed

range of inputs, and testing at a finite sample of input conditions in each of the continuous ranges demonstrates acceptable performance, then performance at intermediate input values between the sampled test points can be inferred to be acceptable with a high degree of confidence.

Digital I&C systems are fundamentally different from analog I&C systems in that minor errors in design and implementation can cause them to exhibit unexpected behavior. Consequently, the performance of digital systems over the entire range of input conditions cannot generally be inferred from testing at a sample of input conditions. The use of inspections, type testing, and acceptance testing of digital systems and components does not alone accomplish design qualification at high confidence levels. To address this issue, the Staff's approach to the review of design qualification for digital systems focuses, to a large extent, upon confirming that the applicant/licensee employed a high-quality development process that incorporated disciplined specification and implementation of design requirements. Inspection and testing is used to verify correct implementation and to validate desired functionality of the final product, but confidence that isolated, discontinuous point failures will not occur derives from the discipline of the development process.

B.2. Defense Against Common-Mode Failure

In digital I&C systems, code, data transmission, data, and hardware may be common to several functions to a greater degree than is typical in analog systems. Although this commonality is the basis for many of the advantages of digital systems, it also raises a key concern: a design using shared data or code has the potential to propagate a common-cause or common-mode failure via software errors, thus defeating the redundancy achieved by the hardware architectural structure. Greater commonality or sharing of hardware among functions within a channel increases the consequences of the failure of a single hardware module and reduces the amount of diversity available within a single safety channel.

Because of this concern, the staff review of digital I&C systems emphasizes quality and defense-in-depth and diversity (D-in-D&D) as protection against propagation of common-mode failures within and between functions.

B.3. System Aspects of Digital Instrumentation and Control

Certain functional requirements that apply to I&C safety systems involve system aspects that pose new assurance challenges when applied to digital systems. These aspects include real-time performance, independence, and on-line testing. The review process for these topics must recognize the special characteristics of digital systems.

C. Review Process

C.1. Summary

The overall process for reviewing the unique aspects of digital I&C systems is outlined in Figure 7.0-A-1. Figure 7.0-A-2 shows the issue-resolution process applicable to each item in 7.0-A-1. The process shown in Figure 7.0-A-1 applies to any digital I&C system or function proposed in a license application or a license amendment application.

The scope of the review process is the same for any I&C safety function; however, the effort required to implement the review will be considerably less for a system that implements only a few safety requirements than it will be for a complex system such as a complete, integrated, digital safety system design. While

acceptance criteria remain the same,[1] the Staff's review emphasis should be commensurate with the safety significance of the given system or aspect of a system's design under review. Probabilistic risk assessments (PRAs), such as those conducted under the Individual Plant Evaluation program (see Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities") or required as part of applications under 10 CFR 52, provide information that may prove helpful in determining the appropriate level of review.

The following seven topics should be addressed in any digital I&C system review:

1. The adequacy of design criteria and guidance to be applied to the proposed system.

2. Identification of review topics — The subsequent review process depends upon the I&C systems addressed in the application.

3. Defense-in-depth and diversity — For applications that involve a reactor trip system (RTS) or an engineered safety features actuation system (ESFAS), the ability of the combination of I&C systems to cope with common-mode failure should be reviewed. This review should confirm that D-in-D&D design conforms to the guidance of Section 7.1 and BTP HICB-19.

4. The adequacy of system functions and commitments for the individual I&C systems — The requirements for each system are outlined in Sections 7.1 through 7.9. For digital systems, this review should address the functional requirements of IEEE 603 and the General Design Criteria that pose new assurance challenges when implemented using computers. The supplemental guidance for digital computer-based safety systems in Section 7.1 describes the system aspects that need careful consideration in digital systems.

5. Life cycle process planning — The adequacy of the computer system development process, particularly the software life cycle activities for digital systems, should be reviewed. This is addressed by confirming that software life cycle plans have commitments to coordinated execution of activity groups, and to staged checkpoints at which product and process characteristics are verified during the development process, as described in Section 7.1 and BTP HICB-14, Section B.3.1.

6. The adequacy of the software life cycle process implementation — A sample of verification and validation, safety analysis, and configuration management documentation for various life-cycle phases should be audited to confirm that the applicant/licensee's life-cycle activities have been implemented as planned. BTP HICB-14, Section B.3.2, describes acceptance criteria and review procedures that provide guidance for the conduct of these audits.

7. Software life cycle process design outputs — The conformance of the hardware and software to the functional and process requirements derived from the design bases should be audited. A sample of software design outputs should be reviewed to confirm that they address the functional requirements allocated to the software, and that the expected software development process characteristics are evident in the design outputs. The review of validation and installation activities should include confirmation of

[1]The Staff discussed the issues of classification and requirements grading in SECY-91-292, "Digital Computer Systems for Advanced Light-Water Reactors," and noted that, "A graded set of requirements based on the importance to safety of the functions being performed with respect to reduction in the potential for radiation exposure could be adopted." IEEE Std 603 and IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," endorsed by Reg. Guide 1.153 and Reg. Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," do not provide for classification, although the foreword to IEEE Std 7-4.3.2 recommends the addition of grading to future versions of IEEE Std 603.

the adequacy of the system test procedures and test results (validation tests, site acceptance tests, pre-operational and start-up tests) that provide assurance that the system functions as intended. BTP HICB-14, Section B.3.3, describes functional characteristics and software development process characteristics that are verified by these audits.

Review of D-in-D&D (topic 3 above) will involve the review of several I&C systems to determine how the overall I&C design functions interact to protect against common-mode failure. This review may involve both non-computer systems and computer-based systems. The review of topics 4, 5, and 6 may be conducted once to evaluate a design process that is common to multiple systems. The review of topic 7 should involve a sample of the products from each digital I&C system described in Chapter 7 of the applicant/licensee's safety analysis report.

For a system incorporating commercial-grade digital equipment, the seven topics still apply, but the review of the commercial-grade elements will be performed differently. For a commercial-grade element of the system, there should be evidence of 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 10 CFR Part 50, Appendix B, quality assurance program. The acceptance process itself is subject to the applicable provisions of 10 CFR Part 50, Appendix B. This process might vary depending on the specifics of the particular commercial-grade equipment and its intended application; however, it must establish the required assurance. The subject of qualification of existing commercial computers is addressed in Reg. Guide 1.152 Rev. 1, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants.” An acceptable process is described in EPRI TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications.”

C.2. Review Process for Software in Digital Instrumentation and Control Systems

For software, the interaction between review topics 4, 5, 6, and 7 is illustrated in Figure 7.0-A-3. In this figure, software requirements are depicted as two subsets of requirements: I&C system-level functional requirements, and software development process requirements. I&C system-level functional requirements describe what function the system is to perform, while software development process requirements describe how the process of building the system is to be performed.

The functional and process requirements come together in the development process. As a result, the design outputs exhibit both functional and process characteristics.

Functional characteristics are described in the design outputs so the resulting system will perform the required functions.

Process characteristics end up in the design outputs as an artifact of the development process. Their presence is evidence that a disciplined development process was employed, and the goal of high-quality software has been achieved. For example, internal consistency of the software requirements specification is a characteristic of a design output. Confirmation that the design output possesses this attribute increases confidence that the development process was disciplined and controlled.

The Staff's review process for software in digital I&C systems, shown in Figure 7.0-A-3, includes each of the following items.

- Review of I&C system-level functional requirements confirms compliance with fundamental requirements embodied in the CFR and guidance in the regulatory guides, standards, and SRP. This review should confirm that the special design considerations of digital systems are appropriately considered and that critical digital hardware and software characteristics are identified.

- Review of software life cycle process plans confirms that the specified software development process requirements documented in the plans establish a commitment to an effective and disciplined software development process and implementation.

- Inspection of the development process confirms that the process life cycle implementation conforms with the software development process requirements described in the plans, and that appropriate safety analysis, verification and validation, and configuration control activities are conducted.

- Audits of design outputs confirm that functional requirements are traceable through all intermediate design products to the final product. Audits of design outputs also confirm that the software development process characteristics and the required software functional characteristics are present.

- Reviews of the acceptance process for PDS, and of the results, confirm that system elements incorporating PDS demonstrate reasonable assurance that they will perform their intended safety function. The reviews should confirm that the critical characteristics of each PDS have been adequately identified and verified.

The review of software in digital I&C systems should be performed within the context of the overall system life cycle stages, shown in Figure 7.0-2. Through the system design activities, system requirements are allocated to components and give rise to hardware and software requirements. Software development activities proceed in parallel with hardware development and become integrated with hardware activities during the system validation stage. Software is validated against software requirements, integrated with hardware, and the complete system is validated against system requirements.

Requirements specification and allocation activities, particularly for software, have proven to be an important source of errors in system development. Much of the software life cycle is devoted to ensuring faithful implementation of the specified software requirements. Therefore, appropriate attention should be given to requirements when addressing topics 4 through 7. The adequacy of system functional requirements is the subject of topic 4. In reviewing these requirements for conformance to ANSI/IEEE Standard 279 (Appendix 7.1-B) or to IEEE Standard 603 (Appendix 7.1-C), achievement of the design basis characteristics discussed in the appendices (7.1-B, Section 3 and 7.1-C, Section 4) is an important element in preventing errors in requirements specification. With respect to topics 5, 6, and 7, the planning and implementation activities should exhibit appropriate emphasis on the allocation of system functional requirements to components, the capture of functional and related software requirements, and the verification and control of those system and software requirements. The software requirements specification should exhibit the functional and process characteristics described in Section 3.3.a of BTP HICB-14.

Formal or semi-formal methods are available for use in preparing some design outputs. Formal specification languages and high-level design languages (e.g., function block diagrams, logic diagrams, and ladder logic diagrams) are examples of such methods which can be useful for specifying certain aspects of software requirements. For example, function block diagrams are usually sufficient to specify the logical functions to be performed by a protection system.

The use of such languages reduces ambiguity and can make incomplete and inconsistent requirements easier to recognize. Furthermore, analytical tools are often available to support evaluation of ambiguity, completeness, consistency, and correctness. While the use of such languages may help to accurately specify certain aspects of requirements or design, existing languages do not support complete specification of requirements or design. For example, many formal design methods do not address timing or robustness requirements. Therefore where such formal or high-level languages are used, care must be taken to ensure that requirements are not overlooked simply because they cannot be described by the specification or design language selected. All requirements must be identified and addressed. Requirements or designs may be described by any combination of languages, including any effective combination of formal languages, high-level languages, and natural languages, provided the interfaces between requirements expressed in different forms are appropriately addressed.

Many formal methods deal only with a single life cycle activity. Often the outputs of one activity must be manually transformed to provide inputs for methods or tools used in subsequent activities. Where such combinations of formal methods are used, the review should confirm that the transformations are appropriately verified.

Note that in some methods a single high-level description may be part of more than one design output. For example, in some programmable logic controller (PLC) implementations a single ladder logic description may describe logic requirements in the SRS, describe logic design in the SDD, and serve the function of source code. Such uses are acceptable provided that the BTP HICB-14 criteria for each design output are met.

The review process described above is applicable to any digital I&C system. However, the complexity and depth of the review can vary substantially depending upon the extent, complexity, and safety significance of the systems involved. Each of these review topics is described in more detail below.

C.3. Discussion of Digital System Review Topics

This section provides detailed information on each of the digital system review topics identified above; information on the review of the acceptance of commercial-grade digital equipment is also provided. Where an applicant/licensee proposes a digital system that the NRC staff has previously approved, the staff review scope would be significantly reduced and would focus only on plant-specific issues associated with the modification (e.g., environmental qualification and configuration management). The staff would not review again generic aspects of the proposed design, such as the software development process, products, and documents, unless these aspects have changed or been affected by plant-specific differences. Where differences exist between prior approvals, they should be identified and the review should confirm that an adequate basis has been provided to accommodate the differences. The review should include an evaluation of differences to confirm that they are acceptable.

C.3.1. Adequacy of Design Criteria and Guidance

Section 7.1 discusses the general review of design criteria and guidance. For new digital systems, the applicant/licensee should have committed to the guidance in Reg. Guide 1.152, which endorses IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," and a set of software engineering standards sufficient to describe the software development process. This should include, as a minimum, a commitment to the software engineering regulatory guides (Reg. Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.170, "Software Test

Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," and Reg. Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants") or an acceptable alternative approach.

C.3.2. Identification of Review Topics

The digital I&C review topics to be addressed depend upon the system under review, as outlined in Table 7.0-A-1.

Table 7.0-A-1. Review Topics Depend on the System Under Review

Topic	Protection System (7.2–7.3)	Other Safety Systems (7.4–7.6)	Control System (7.7)	Diverse I&C System (7.8)	Data Communication System (7.9)
D-in-D&D	Review	*	*	*	Same review as supported system(s)
Functional Requirements	Review	Review	Limited review	Review	Same review as supported system(s)
Development Process	Review	Review	Limited review	Review	Same review as supported system(s)
Process Implementation	Review	Review	Limited review	Review	Same review as supported system(s)
Design Outputs	Review	Review	Limited review	Review	Same review as supported system(s)

* While D-in-D&D analysis is not required for systems other than RTS and ESFAS, changes to other I&C systems in plants that have existing digital RTS and ESFAS should be reviewed to confirm that the proposed changes do not affect assumptions and commitments made in the existing D-in-D&D analysis. This includes ensuring compliance with the diversity requirements of 10 CFR 50.62, as discussed in Section 7.8.

The level of review depends upon the importance to safety of the system under review. Control systems receive a limited review as necessary to confirm that control system failures cannot have an adverse effect on safety system functions and will not pose frequent challenges to the safety systems. An area of special emphasis for control systems will be to ensure that the control system design is consistent with the commitments for control system/safety system independence. Isolation of safety systems from control system failures should be addressed.

Data communication systems are treated as support systems (see Section 7.9), although they are often composed of specialized hardware, embedded software, and communication protocol software that runs on the computers linked together by the data communication system. They may support protection systems, other safety systems, diverse I&C systems, control systems, or any combination thereof. A design may provide separate safety and non-safety data communication systems. The review topics applicable to any data communication system are the combination of topics applicable to the I&C systems supported by that data communication system.

Computer internal data communication is at present accomplished by high-speed databuses that are usually designed by the makers of the computer system package itself. There are a number of standardized computer internal buses, and, unlike data communication systems, no software is involved (other than operating system software). Operation of computer internal buses is usually under the control of hardware. Unless this situation changes, computer internal data communication should be reviewed by confirming critical hardware characteristics. If software is involved in computer internal data communication, the review should proceed as described above under data communication systems.

C.3.3. Review of Defense-in-Depth and Diversity

I&C safety systems incorporating digital computer technology in the reactor protection system or ESFAS must comply with the NRC position on D-in-D&D described in the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." Figure 7.0-A-4 illustrates the process for review of the system-level D-in-D&D features to determine compliance with the position. BTP HICB-19 describes in detail the regulatory bases, material to be reviewed, acceptance criteria, and review process. For simple modifications, such as incorporating a single digital function into an otherwise analog I&C system, the D-in-D&D analysis may be very simple. Extensive and detailed analyses may be required for completely integrated computer-based reactor protection and control systems.

C.3.4. Review of Software Life Cycle Process Planning

The Staff's conclusion regarding the quality and reliability of digital computer systems will be based upon confirmation of the following points:

1. Plant and overall I&C system requirements are correctly decomposed into the digital I&C system requirements for each digital I&C system under review. Critical hardware and software characteristics are identified.

2. A development process is specified and documented such that implementation of the process gives a high degree of confidence that the functional requirements will be or are implemented in the computer system. The life cycle process plan describes a coordinated engineering process in which design outputs at each planned stage of the design process are verified to implement the input requirements of the stage.

3. The specified process and products, including design outputs, are designed to be inspected at staged checkpoints.

4. The installed system functions as designed. Validation and integration tests, acceptance tests, and on-site pre-operational and start-up functional tests demonstrate that the identified critical hardware and software characteristics are verified.

As discussed above, the Staff's determination of the qualification of digital I&C systems and components is based in part on confirmation that the software for the systems is developed using a disciplined engineering process. Typically, this process is described in a set of software life cycle process development planning documents, which define the process requirements and the commitments the applicant/licensee makes regarding software life cycle activities. Figure 7.0-A-5 identifies the software life cycle planning topics that should be considered for review. These commitments must be consistent with the commitments made for the design criteria and guidance discussed in Section C.3.1 above. Figure 7.0-A-6 outlines the procedures for reviewing software life cycle process planning. BTP HICB-14 describes the detailed regulatory bases and

material to be reviewed for evaluating software development life cycle process planning. Section B.3.1 of that BTP describes the acceptance criteria for this review. In addition to confirming the acceptability of the applicant/licensee's plans, this review activity should also identify the higher-risk activities of the software life cycle process for subsequent audit by the NRC staff.

Almost every computer system will involve some use of PDS. PDS may be used directly in plant computers or in processes used to develop in-plant software. The applicant/licensee's process for qualification of PDS should be reviewed as part of the evaluation of the development process.

For new applications and license amendment applications, review of software life cycle process plans is confined to any changes in the plans if all of the following conditions hold: (1) the applicant/licensee has previously developed a digital I&C safety system under a process acceptable to the Staff, (2) the applicant/licensee has made commitments to software development plans similar to those identified in BTP HICB-14, and (3) these plans have been accepted by the NRC staff.

C.3.5. Review of Functional Requirements for Individual Systems

The functional requirements and commitments for each I&C system must be reviewed against the requirements of 10 CFR 50, as described in Section 7.1 and the individual SRP sections applicable to the system under review. Certain review topics need to be considered differently for digital systems. These topics are:

- Equipment qualification, including electromagnetic compatibility.
- Real-time, deterministic performance.
- On-line and periodic test provisions.
- Communications independence.
- Control of access.

Figure 7.0-A-7 outlines the review of these topics. Detailed regulatory bases, material to be reviewed, acceptance criteria, and review processes for each of these topics are contained in Sections 7.1 and 7.9, Appendix 7.1-C, and BTPs HICB-17 and HICB-21.

C.3.6. Audit of Software Life Cycle Process Implementation

The applicant/licensee's implementation of life cycle activities should be audited to confirm that the planned process is being implemented. Figure 7.0-A-8 provides an overview of the process for auditing the implementation process. Figure 7.0-A-5 identifies the software life cycle process implementation topics that should be considered as candidates for audit. BTP HICB-14, Section B.3.2, describes the acceptance criteria for software life cycle process implementation. The scope and depth of the inspection should be consistent with the extent and complexity of the proposed digital system and the potential safety impact of system failure. For simple, limited, low-impact retrofits to existing systems, the process audit may be a very limited-scope "desk audit" of selected examples of process documentation. Review of extensive digital I&C systems, such as an integrated digital control and protection system, should involve detailed reviews of a wide range of software process documentation. Ideally, these reviews would occur in process audits of several of the life cycle phases, as indicated in Figure 7.0-A-5. The audit of a given set of life cycle activities and the

inspection of products generated by those activities, as discussed in Section C.3.7 below, may be combined into a single audit.

One effective audit technique is the string audit, in which the reviewer selects a sample of specific software development process requirements and specific functional requirements and confirms that they are implemented throughout the life cycle.

C.3.7. Audit of Software Life Cycle Process Design Outputs

The products of a design process include both the design outputs that describe the technical requirements of systems and components, and the systems and components themselves. The review of digital systems should include inspection of these products on an audit basis to confirm that the systems and components meet the functional requirements. Figure 7.0-A-9 provides an overview of the process for inspection of design outputs. Candidate items for inspection include the items described in Appendix 7-B, BTP HICB-17, HICB-21, and HICB-14, Section B.3.3.

Software product inspection is performed by inspecting a representative sample of the design outputs, i.e., software requirements specifications, software design specifications, hardware and software architecture, code listings, build documents, configuration tables, operations manuals, maintenance manuals, and training manuals.

The inspections should examine functional characteristics to confirm that system functional requirements have been properly implemented at each phase of the software development process. Verification and validation analyses and test reports should also be examined to extract information about the design output's conformance with system functional requirements and to verify critical hardware and software characteristics.

The inspections should also examine software development process characteristics to confirm that the products embody characteristics that are evidence of an effective and visible software development process. This step provides confidence that positive findings for the sample functional requirements to be inspected are representative of the software product as a whole. The combination of positive findings in the review of development plans, process implementation, and design outputs provides a high degree of confidence that all of the software conforms with the fundamental system requirements.

This approach requires that the integrity of design outputs be maintained in the translation of code to machine language. Consequently, the Staff's review should include confirmation of the integrity of this conversion. This will normally be accomplished by confirming the qualification of the mechanism and tools for performing this translation (e.g., a COTS compiler and linker) and reviewing integrated system testing, installation, and pre-operational test reports.

One approach to conducting product inspections that has proved successful is the use of string audits that follow selected functional requirements through the design outputs previously described. The scope and depth of the product inspections should be tailored to the extent, complexity, and safety significance of the digital system under review. BTP-14, Section B.3.3, presents specific criteria from which the inspection activities for a specific product may be derived.

For operating license, operating license amendment, or combined license applications, the product inspections should also confirm that the systems reviewed are installed, operated, and maintained appropriately. NRC Inspection Manual, Part 2500, "Digital Retrofits Receiving Prior Approval," provides guidance for inspecting these activities.

C.3.8. Review of the Acceptance of Commercial-Grade Digital Equipment

All software, including operating systems, resident on safety system computers at run time must be qualified for their intended applications. Qualification may be established either by producing the PDS items under a 10 CFR Appendix B quality assurance program or by dedicating the item for use in the safety system as defined in 10 CFR Part 21. Review topics for the former case are described above. Review in the latter case requires a determination that a suitable acceptance process has demonstrated reasonable assurance that the equipment will perform its intended safety function. 10 CFR Part 21 states that "this assurance is achieved by identifying the critical characteristics of the item and verifying their acceptability by inspections, tests, or analyses performed by the purchaser or third-party dedicating entity after delivery, supplemented as necessary by one or more of the following: commercial grade surveys; product inspections or witness at holdpoints at the manufacturer's facility, and analysis of historical records for acceptable performance."

An acceptable set of fundamental requirements for this process is described in IEEE 7-4.3.2, Section 5.3.2, and guidance given in Annex D (Informative) of the standard. This standard is endorsed in Reg. Guide 1.152, Rev. 1. In this guidance, the qualification process is accomplished by comparing the commercial-grade item to the design criteria of the standard. 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. The guidance provided herein for the review of newly developed software provides technical background pertinent to evaluating the use of the engineering judgment and compensating factors provisions. The standard requires the acceptance, and its basis, to be documented and maintained with the qualification documentation.

In order to demonstrate reasonable assurance, the acceptance process for most PDS can be expected to comprise a variety of technical activities conducted in significant detail. Guidance on these activities has been provided in EPRI TR-106439. The NRC has issued a safety evaluation report (SER) on the EPRI guideline in which it determined that "TR-106439 contains an acceptable method for dedicating commercial grade digital equipment for use in nuclear power plant safety applications."

If the guidance in EPRI TR-106439 is applied in the dedication of a component, the following items should be noted by the reviewer:

- TR-106439 is not intended to be used as a detailed "how-to" manual. There may be significant variation in specific steps taken depending on vendors, components, and applications. Detailed specific information, in addition to that provided in the report examples, will be needed to perform an actual commercial dedication. Use of TR-106439 in connection with a license amendment or 10 CFR 50.59 evaluation should include descriptions of alternatives selected and deviations from the guidance in the documentation of the acceptance process.

- The dedication effort can be "graded" based on safety significance and relative complexity.

- TR-106439 references EPRI NP-5652, which discusses four methods for use in commercial dedication:(1) special tests and inspections, (2) commercial-grade survey of supplier, (3) source verification, and (4) acceptable supplier/item performance record. As noted in TR-106439, supported by Generic Letters 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products," and 91-05, "Licensee Commercial-Grade Procurement and Dedication Programs," for typical applications no one method will suffice by itself, and it is likely that methods 1, 2, and 4 will all be needed.

- The examples listed in TR-106439 are not all-inclusive. Depending on application and product specifics, some of the evaluations may not be needed or additional verification activities, beyond those listed in the example, might be necessary.

- Engineering judgement applied in the acceptance process must be documented sufficiently to allow a comparably qualified individual to reach the same conclusion.

- The validity of the commercial-grade item dedication must be maintained as long as the item remains in service. Dedicated software items should not be updated to new revision levels without prior evaluation to determine if a design change is required. Commercially dedicated items should not be operated in a configuration outside the bounds of the original dedication.

- The utility should arrange to be notified by the vendor when defects are discovered. This requires confirmation that the vendor's processes will support this need.

- TR-106439 notes that not all commercial items can be successfully dedicated.

D. References

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

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

EPRI NP-5652. "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications." Final Report, Electric Power Research Institute, June 1988.

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.

Generic Letter 88-20. "Individual Plant Examination for Severe Accident Vulnerabilities." November 23, 1988.

Generic Letter 89-02. "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products." 1989.

Generic Letter 91-05. "Licensee Commercial-Grade Procurement and Dedication Programs." 1991.

IEC Std 880. "Software for Computers in the Safety Systems of Nuclear Power Stations." IEC Publication, 1986.

IEC Std 880, Supplement 1 Draft. "Software for Computers in the Safety Systems of Nuclear Power Stations." IEC Publication, October 1996.

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

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

IEEE Std 610.12-1990. "IEEE Standard Glossary of Software Engineering Terminology."

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

IEEE Std 934-1987. "Requirements for Replacement Parts for Class 1E Equipment in Nuclear Power Generating Stations."

NRC Inspection Manual, Chapter 52001. "Digital Retrofits Receiving Prior Approval."

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Rev. 1. Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, January 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Rev. 1. Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

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

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

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

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

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

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

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

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

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.

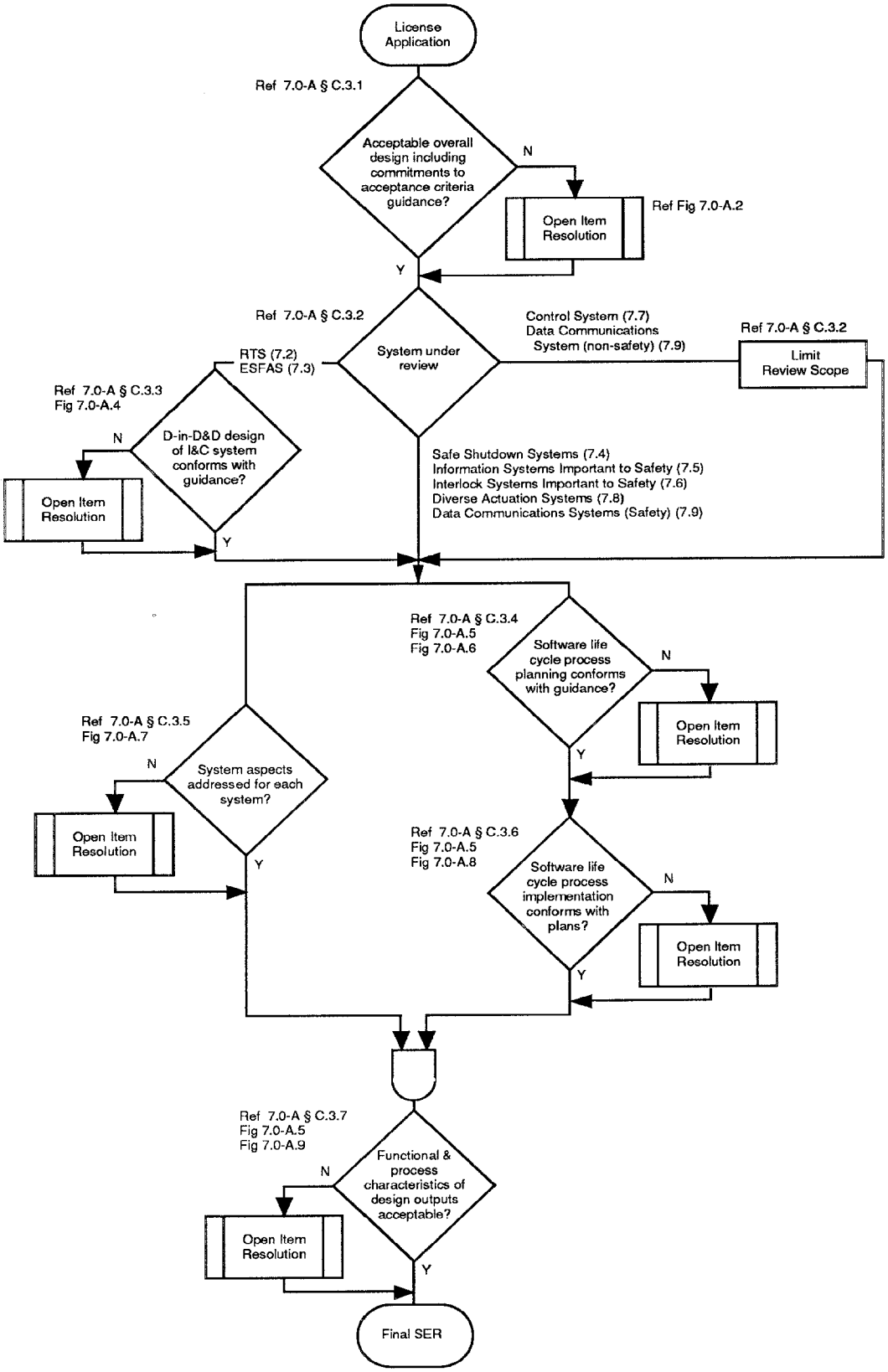

Figure 7.0-A-1. Overview of the Process for Reviewing the Unique Aspects of Digital Instrumentation and Control Systems

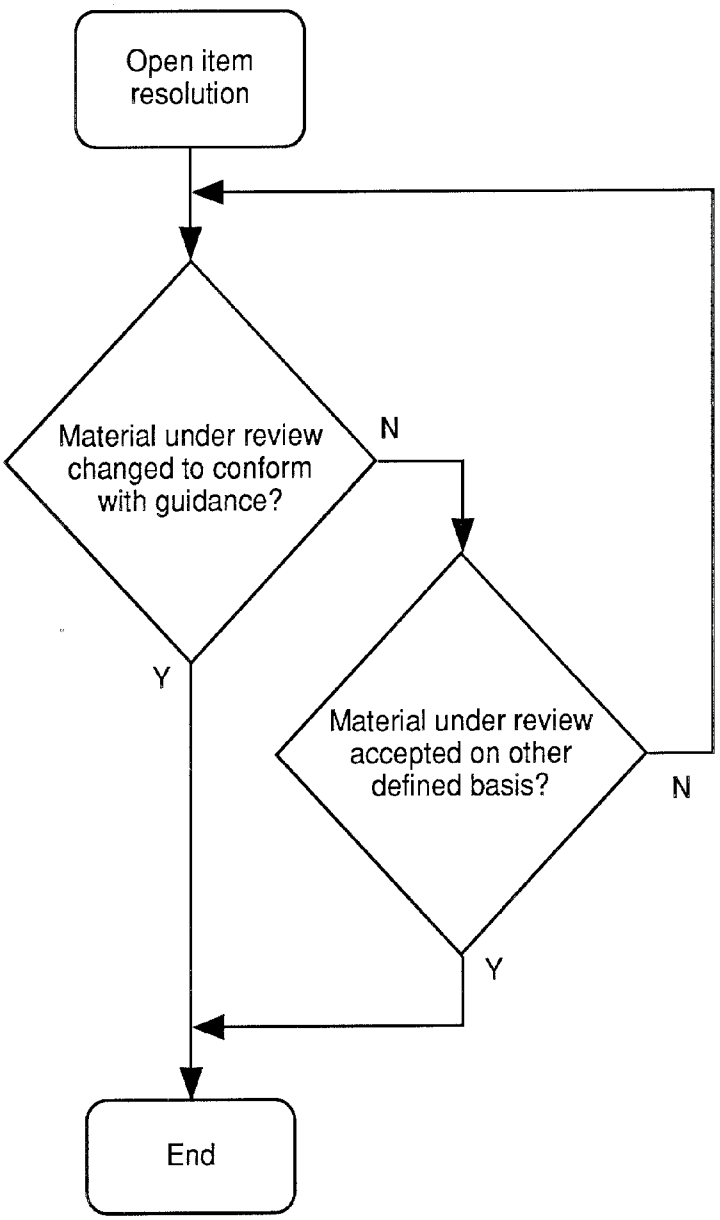

Figure 7.0-A-2. Open Item Resolution Process

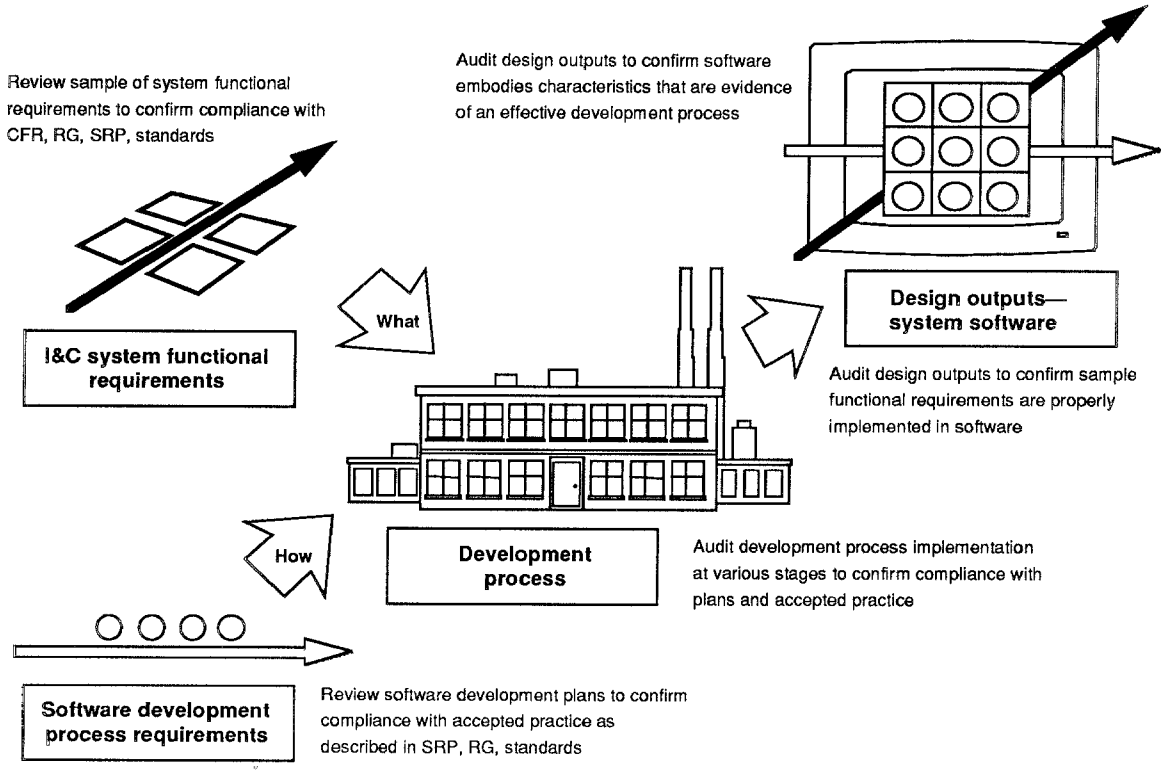

Figure 7.0-A-3. Software Review Process

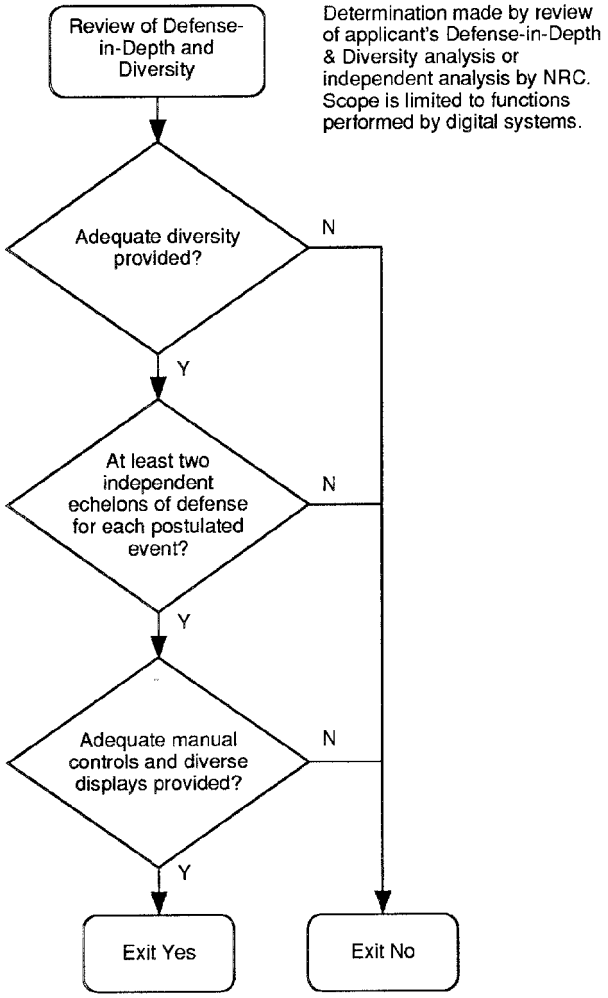

Figure 7.0-A-4. Defense-in-Depth and Diversity Review

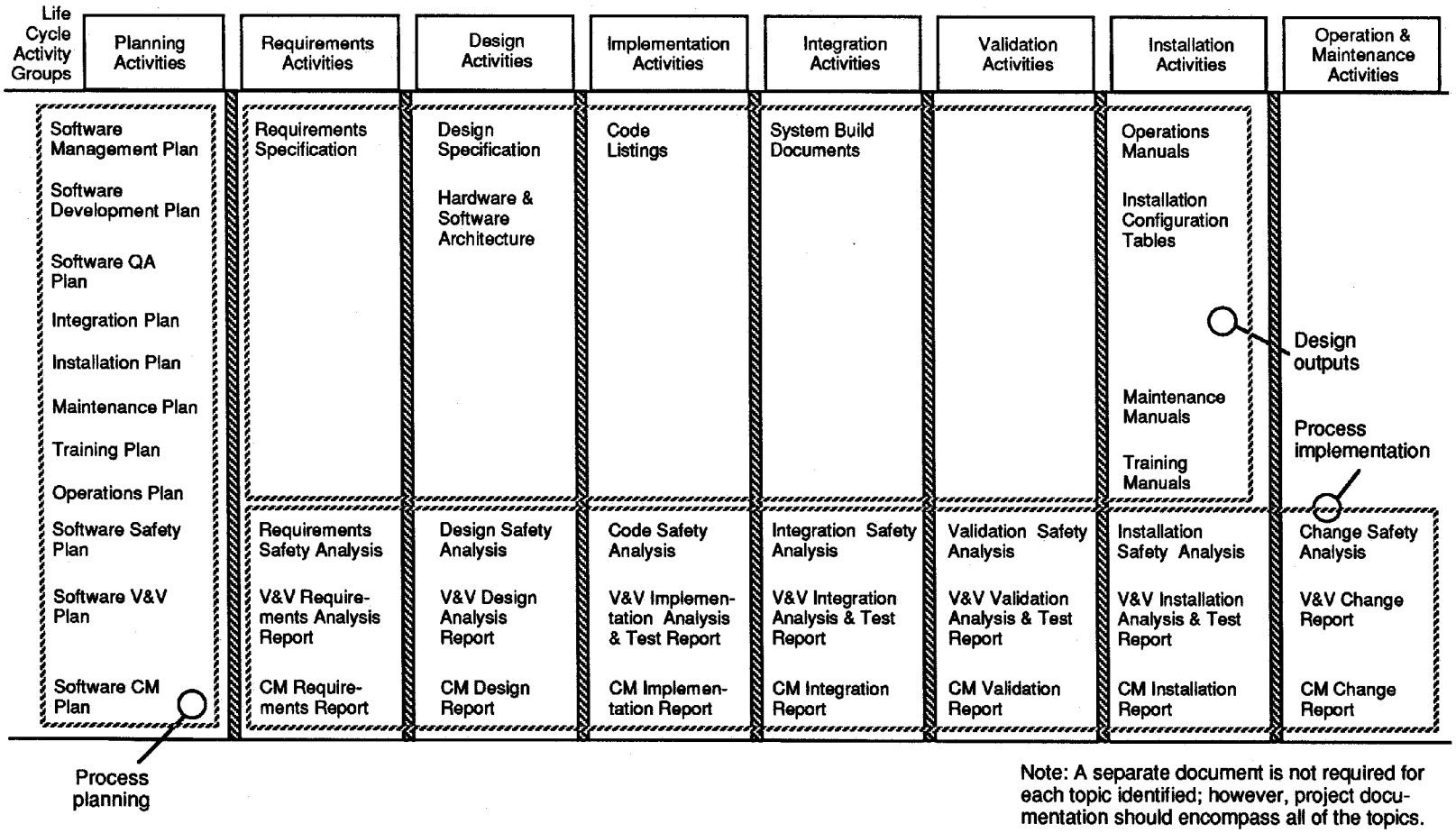

Figure 7.0-A-5. Software Life Cycle Activities

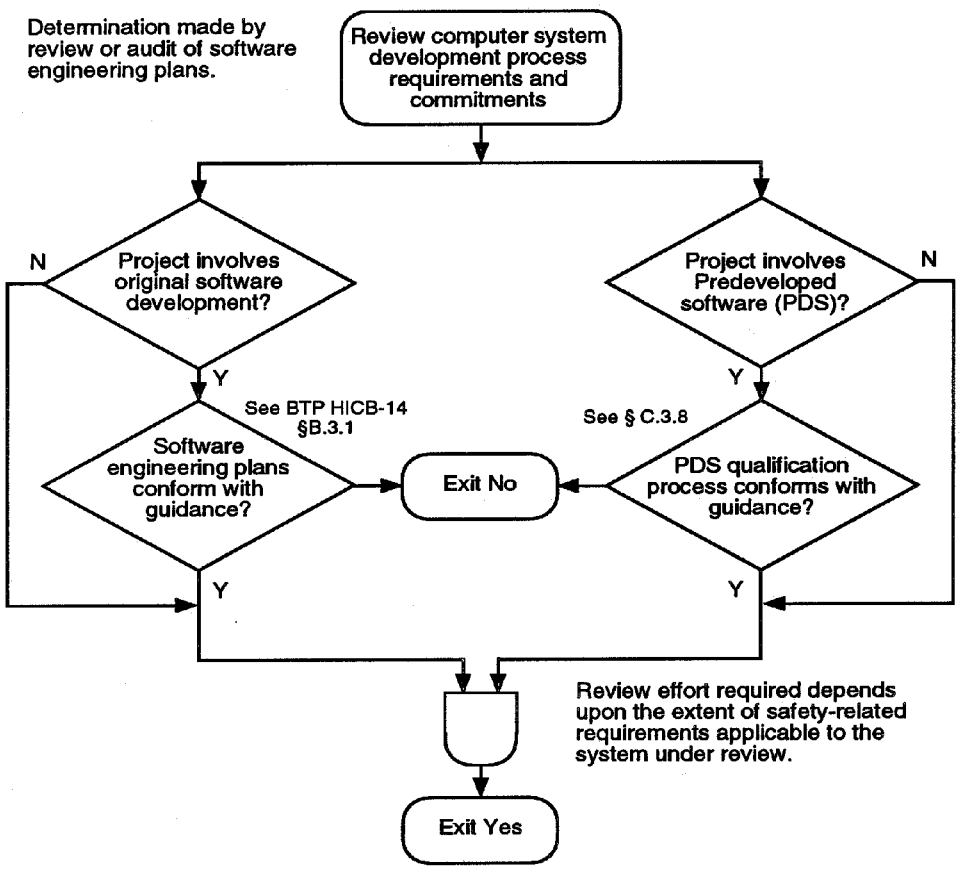

Figure 7.0-A-6. Review of Software Life Cycle Process Planning

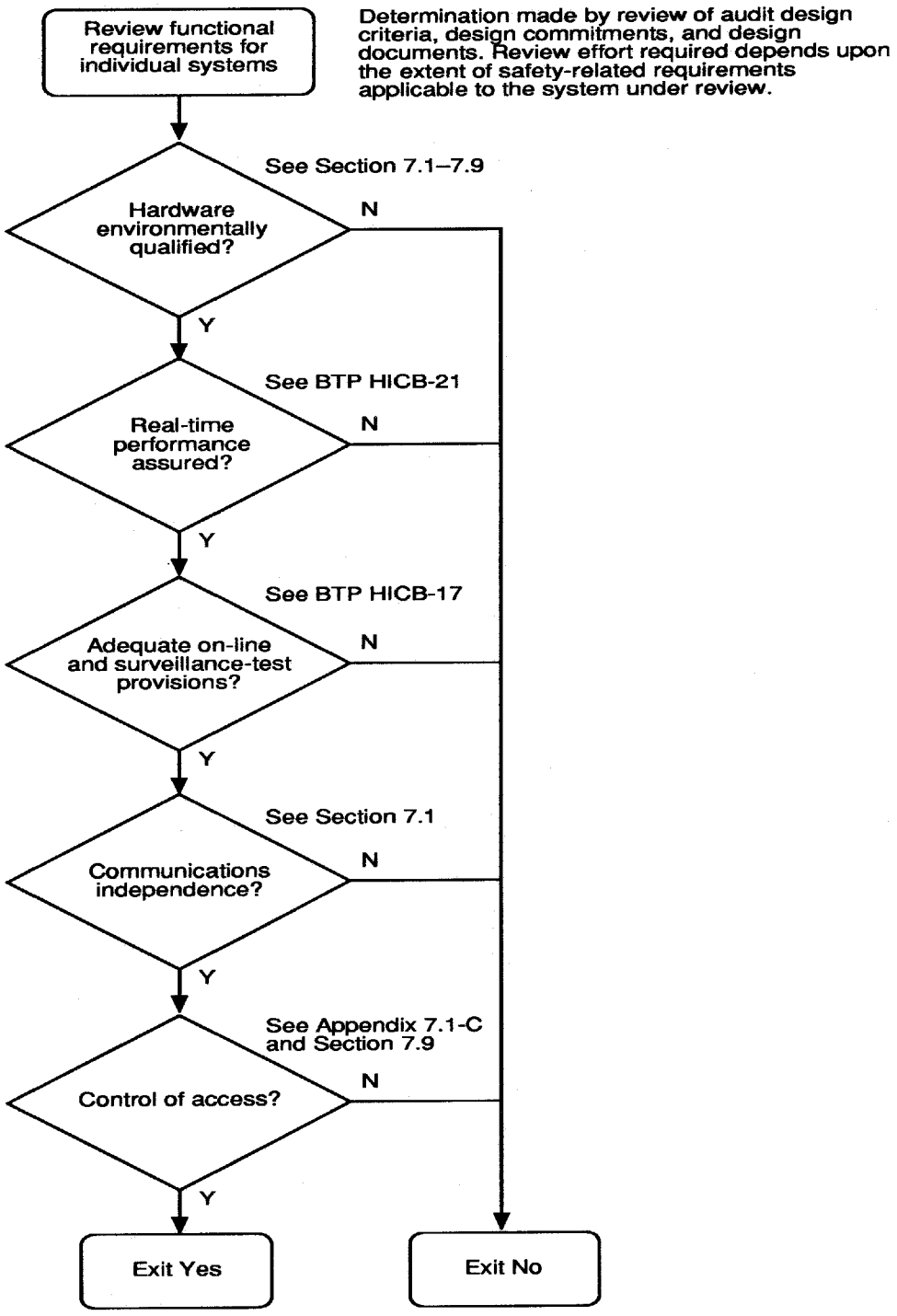

Figure 7.0-A-7. Special Considerations in the Review of Functional Requirements for Digital Instrumentation and Control Systems

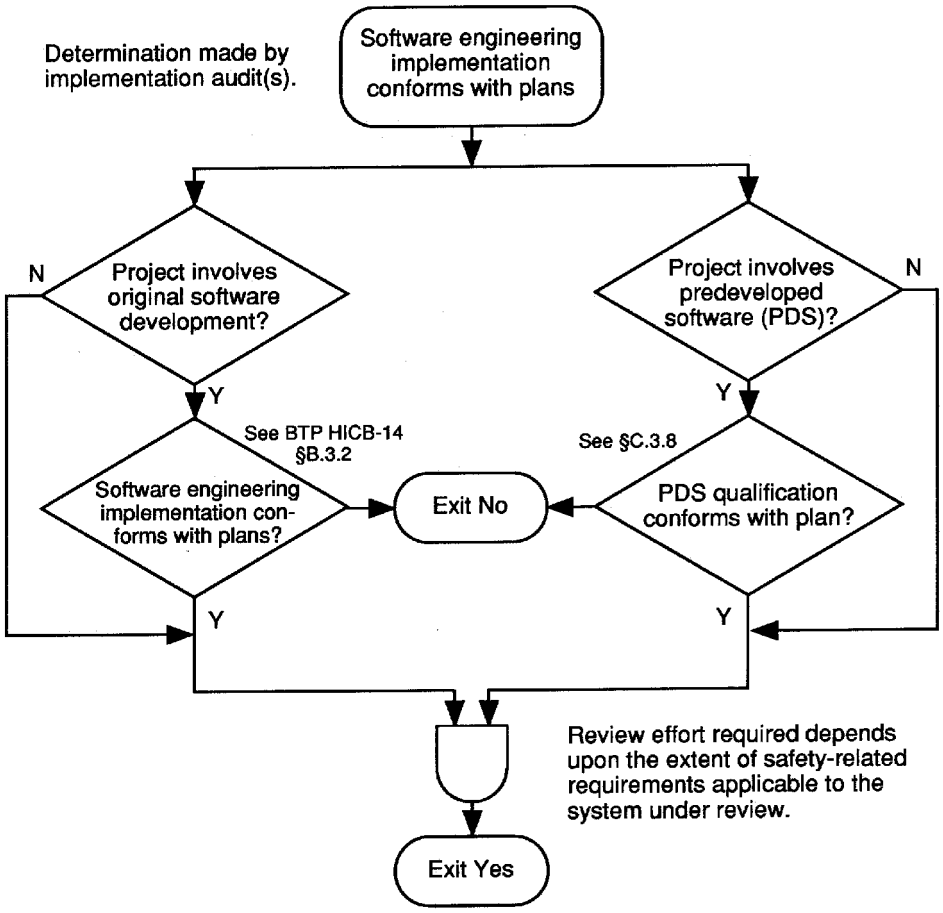

Figure 7.0-A-8. Review of Software Development Process Implementation

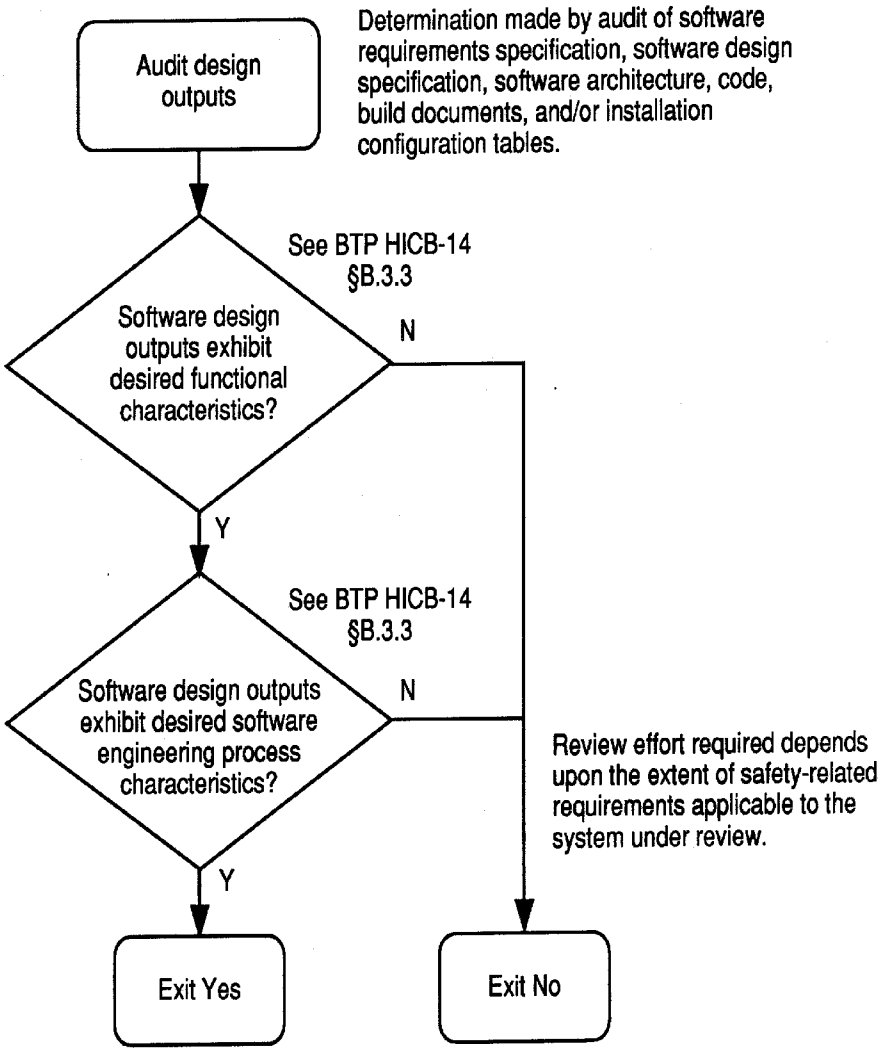

Figure 7.0-A-9. Review of Design Outputs