U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

APPENDIX 7.0-A REVIEW PROCESS FOR DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

REVIEW RESPONSIBILITIES

Primary - Organization responsible for the review of instrumentation and controls

Secondary - None

A. INTRODUCTION

This appendix provides an overview of the process for reviewing 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 Standard Review Plan (SRP) Section 7.0, (2) the design criteria and commitments described in SRP Section 7.1, and (3) the individual digital I&C systems described in SRP 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 SRP Sections 7.2 through 7.9. Additional information relevant to the review process can be found in the references in subsection D of this appendix.

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

Revision 5 - March 2007

1. 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 properties or attributes that are essential for performance of an equipment's safety function (IEEE Std. 934-1987, "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-1-1994, "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-1-1994).

A design requirement specifies or constrains the design of a system or system component (IEEE Std. 610.12-1990, "IEEE Standard Glossary of Software Engineering Terminology").

The term 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 qualified personnel.

A function is a specific purpose of an entity or its characteristic action (IEEE Std. 610.12-1990).

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. SRP BTP 7-14 identifies specific functional requirements considered in software reviews.

A functional requirement specifies a function that a system or system component must be capable of performing (IEEE Std. 610.12-1990). In this appendix, functional requirements include design, interface, performance , and physical requirements, as described in IEEE Std. 610.12-1990.

Hardware critical characteristics are properties or attributes of computer, peripheral, or communication hardware that are essential for performance of the safety function, including specifications that are required to execute the software intended to run on the hardware and the attributes of reliability, testability, or predictability on 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. 60880-2). Commercial off-the-shelf (COTS) software is a subset of PDS.

Software critical characteristics are properties or attributes of a software or firmware product that are essential for performance of the related equipment's safety function. Characteristics include functional requirements that are allocated to the software and the attributes of robustness, testability, or dependability on which the staff's safety findings are based.

A software development process characteristic is a trait or property of a software development process design output that results from the implementation of a design process. SRP BTP 7-14 identifies specific software development process characteristics considered in software reviews.

A software development process requirement describes one or more activities that a software development process must include.

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

B. BACKGROUND

The criteria for I&C systems are described in 10 CFR 50.55a(h), which incorporates IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995; IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations"; and 10 CFR Part 50, Appendix A, General Design Criteria (GDC). 10 CFR Part 50 Appendix B, "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 Part 50 apply to digital I&C systems and are sufficient to support licensing of such systems. For applications under 10 CFR 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants," the technical acceptance criteria of 10 CFR Part 50 apply.

IEEE Std. 7-4.3.2-2003, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by Regulatory Guide 1.152, Revision 2, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," provides additional computer-specific guidance to supplement the requirements of IEEE Std. 603-1991. Guidance on the use of IEEE Std. 7-4.3.2-2003 can be found in SRP Appendix 7.1-D.

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 Part 50. These characteristics are important to the evaluation of (1) design qualification of digital systems, (2) protection against common-cause failure, and (3) selected functional requirements of IEEE Std. 603-1991 and the GDC that pose new assurance challenges when implemented using computers. These topics are discussed in more detail below.

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 on physics principles and to use these models to establish a reasonable expectation of continuous performance over substantial ranges of input conditions are important factors 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 assures 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, 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. Inspections, type testing, and acceptance testing of digital systems and components do 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 on confirming that the applicant/licensee employed a high-quality development process that incorporated disciplined specification and implementation of design requirements. Inspection and testing are 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.

2. Defense Against Common-Cause Failure

In digital I&C safety 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 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's review of digital I&C protection systems emphasizes quality and diversity and defense-in-depth as protection against propagation of common-cause failures within and between functions. Additional guidance on assessment of diversity and defense-in-depth is provided in SRP BTP 7-19.

3. System Aspects of Digital Instrumentation and Control

Certain functional requirements that apply to I&C safety systems involve system aspects that pose 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

1. Summary

The overall process for reviewing digital I&C systems is outlined in Figure 7.0-A-1 of this appendix. Figure 7.0-A-2 of this appendix shows the issue-resolution process applicable to each item in Figure 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 for a complex system such as a complete, integrated, digital safety system design. While acceptance criteria remain the same, 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 (see subsections C.3.1 – C.3.7 of this appendix for a detailed discussion of each topic and subsection C.2 for information on reviewing software in digital I&C systems):

A. Adequacy of design criteria and guidance to be applied to the proposed system.

B. Identification of review topics - The subsequent review process depends on the I&C systems addressed in the application.

C. Diversity and defense-in-depth - For applications that involve a reactor trip system (RTS) or an engineered safety features actuation system (ESFAS), the ability of the combination of I&C systems to cope with common-cause failure should be reviewed. This review should confirm that the diversity and defense-in-depth design conforms to the guidance of SRP Section 7.1 and SRP BTP 7-19.

D. Adequacy of system functions and commitments for the individual I&C systems -

The requirements for each system are outlined in SRP Sections 7.2 through 7.9. For digital systems, this review should address the functional requirements of IEEE Std. 603-1991 and the GDC that pose new assurance challenges when implemented using computers. The supplemental guidance for digital computer-based safety systems in SRP Section 7.1 describes the system aspects that need careful consideration in digital systems.

E. Life-cycle process planning - The adequacy of the computer system development process, particularly the software life-cycle activities for digital systems, should be reviewed. No specific lifecycle model is required. Adequacy 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 SRP Section 7.1 and SRP BTP 7-14, subsection B.

F. 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. SRP BTP 7-14, subsection B.3.2, describes acceptance criteria and review procedures that provide guidance for the conduct of these audits.

G. 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 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. SRP BTP 7-14, subsection B.3.3, describes functional characteristics and software development process characteristics that are verified by these audits.

Review of diversity and defense-in-depth (topic C above) will involve the review of several I&C systems to determine how the overall I&C design functions interact to protect against common-cause failure. This review may involve both non-computer systems and computer-based systems. The review of topics D, E, and F may be conducted once to evaluate a design process that is common to multiple systems. The review of topic G 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 (SAR).

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 Regulatory Guide 1.152, Revision 2. The process described in EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," was found acceptable by the staff safety evaluation, dated July 17, 1997.

For an upgrade that replaces existing equipment with new equipment, the seven topics still apply but are limited to the change. The review should consider the introduction of new safety impacts that did not exist in the replaced equipment. An example would be common-cause failure of new software.

If the new equipment performs the same function as the existing equipment, the review should determine that the new equipment does indeed perform the same function, that it is at least as reliable as the existing equipment, and that no new safety concerns exist.

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

For software, the interaction between review topics D, E, F, and G is illustrated in Figure 7.0-A-3 of this appendix. In this figure, software requirements are depicted as two subsets of requirements: I&C system-level functional requirements and software development process requirements. The former describe what function the system is to perform while the latter describe how the process of building the system is to be performed.

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 of this appendix, 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 of SRP Section 7.0. 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 D through G. The adequacy of system functional requirements is the subject of topic D. In reviewing these requirements for conformance to IEEE Std. 603–1991 (SRP Appendix 7.1-C) or to IEEE Std. 279-1971 (SRP Appendix 7.1-B), achievement of the design basis characteristics discussed in the appendices (SRP Appendix 7.1-C, subsection 4.2) is an important element in preventing errors in requirements specification. With respect to topics E, F, and G, 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 SRP BTP 7-14, subsection B.3.

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, ladder-logic diagrams) are examples of such methods that 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.

Using 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 these languages may help to accurately specify certain aspects of requirements or design, they may not support complete specification of requirements or design. For example, many formal design methods do not address timing or robustness requirements. Therefore, when formal or high-level design languages are used, care still must be taken to assure that requirements are not overlooked simply because they cannot be described by the specification or language. 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. In such cases, the outputs of one activity must be manually transformed to provide inputs for methods or tools used in subsequent activities. When such combinations of formal methods are used, the review should confirm that the transformations are appropriately verified.

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 on the extent, complexity, and safety significance of the systems involved. Each of these review topics is described in more detail below.

3. Discussion of Digital I&C System Review Topics

This section provides detailed information on the digital I&C system review topics identified above and information on the review of the acceptance of commercial-grade digital equipment. When 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, 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. When 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.

A. Adequacy of Design Criteria and Guidance

SRP 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 Regulatory Guide 1.152, Revision 2, which endorses IEEE Std. 7-4.3.2-2003, and a set of software engineering standards sufficient to describe the software development process. This should include, as a minimum, a commitment to the following software engineering regulatory guides:

- Regulatory Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

- Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."
- Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."
- Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."
- Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."
- Regulatory 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.

B. Identification of Review Topics

Digital I&C review topics to be addressed vary with type of system, as shown in Table 7.0-A-1. The level of review depends on a system's importance to safety.

Table 7.0-A-1. Review Topics for Various Systems

Topic	Type of System				
	Protection	Other Safety	Control	Diverse I&C	Data Communication
	Discussed in SRP Section(s)				
	7.2, 7.3	7.4 - 7.6	7.7	7.8	7.9
Diversity and Defense-in-Depth	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	

* While a diversity and defense-in-depth 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 diversity and defense-in-depth analysis. This includes ensuring compliance with the diversity requirements of 10 CFR 50.62, as discussed in SRP 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 is to assure 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 SRP 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. Review of Diversity and Defense-in-Depth

I&C safety systems incorporating digital computer technology in the reactor protection system or ESFAS should comply with the NRC position on diversity and defense-in-depth 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 of this appendix illustrates the process for review of the system-level diversity and defense-in-depth features to determine compliance with the position. SRP BTP 7-19 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 diversity and defense-in-depth analysis may be very simple. Extensive and detailed analyses may be required for modifications that replace each of the reactor protection and control systems with digital I&C systems.

D. Review of Software Life Cycle Process Planning

The staff's conclusion regarding the quality and reliability of digital computer systems is based on confirmation of the following points:

i. 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.

ii. 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.

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

iv. 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 that define the process requirements and the commitments the applicant/licensee makes regarding software life-cycle activities. Figure 7.0-A-5 of this appendix 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 subsection C.3.1 above. Figure 7.0-A-6 of this appendix outlines the procedures for reviewing software life-cycle process planning. SRP BTP 7-14 describes the detailed regulatory bases and material to be reviewed for evaluating software development life-cycle process planning. SRP BTP 7-14, subsection B.3.1, 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 NRC staff.

Almost every computer system involves 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 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 SRP BTP 7-14, and (3) these plans have been accepted by NRC staff.

E. 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 Part 50, as described in SRP 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 of this appendix 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 SRP Sections 7.1 and 7.9, SRP Appendix 7.1-C, and SRP BTPs 7-17 and 7-21.

F. 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 of this appendix provides an overview of the process for auditing the implementation process. Figure 7.0-A-5 of this appendix identifies the software life-cycle process implementation topics that should be considered as candidates for audit. SRP BTP 7-14, subsection 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 replacement of the protection and control systems, 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 of this appendix. The audit of a given set of life-cycle activities and the inspection of products generated by those activities, as discussed in subsection C.3.7 below, may be combined into a single audit.

One effective audit technique is the string audit. Reviewers examine the implementation of a randomly selected, statistically significant sample of software development process requirements and functional requirements and confirms that they are implemented throughout the life cycle.

G. Audit of Software Life-Cycle Process Design Outputs

The products of a design process include 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 of this appendix provides an overview of the process for inspection of design outputs. Candidate items for inspection include the items described in SRP Appendix 7-B, and SRP BTPs 7-17, 7-21, and 7-14, subsection 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. SRP BTP 7-14, subsection 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 reviewed systems are installed, operated, and maintained appropriately. NRC Inspection Manual, Chapter 52001, "Digital Retrofits Receiving Prior Approval," provides guidance for inspecting these activities.

H. Review of the Acceptance of Commercial-Grade Digital Equipment

All software, including operating systems, that is resident on safety system computers at run time must be qualified for the 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 21. Review topics for the former are described above. Review for the latter requires a determination that a suitable acceptance process has demonstrated reasonable assurance that the equipment will perform its intended safety function.

10 CFR 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 Std. 7-4.3.2-2003, Clause 5.4.2, as endorsed by Regulatory Guide 1.152, Revision 2. 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.

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 is 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:

- EPRI 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 EPRI TR-106439 in connection with a license amendment or 10 CFR 50.59 evaluation should include descriptions of the alternatives selected and deviations from the guidance in the documentation of the acceptance process.

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

- EPRI 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 EPRI 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 EPRI 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.

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

D. REFERENCES

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

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

3. 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.

4. IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."

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

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

7. IEEE Std. 7-4.3.2-2003, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

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

9. IEC Std. 60880-2, "Software for Computers Important to Safety for Nuclear Power Plants - Part 2: Software Aspects of Defense Against Common Cause Failures, Use of Software Tools and of Pre-Developed Software," IEC Publication, 2000.

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

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

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

13. NRC Inspection Manual, Inspection Procedure 52001, "Digital Retrofits Receiving Prior Approval," March 2, 1998.

14. Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Revision 2, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, January 2006.

15. Regulatory Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 2004.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

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

22. Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," July 21, 1993.

23. Safety Evaluation by the Office of Nuclear Reactor Regulation, "EPRI Topical Report TR-106439," July 17, 1997.

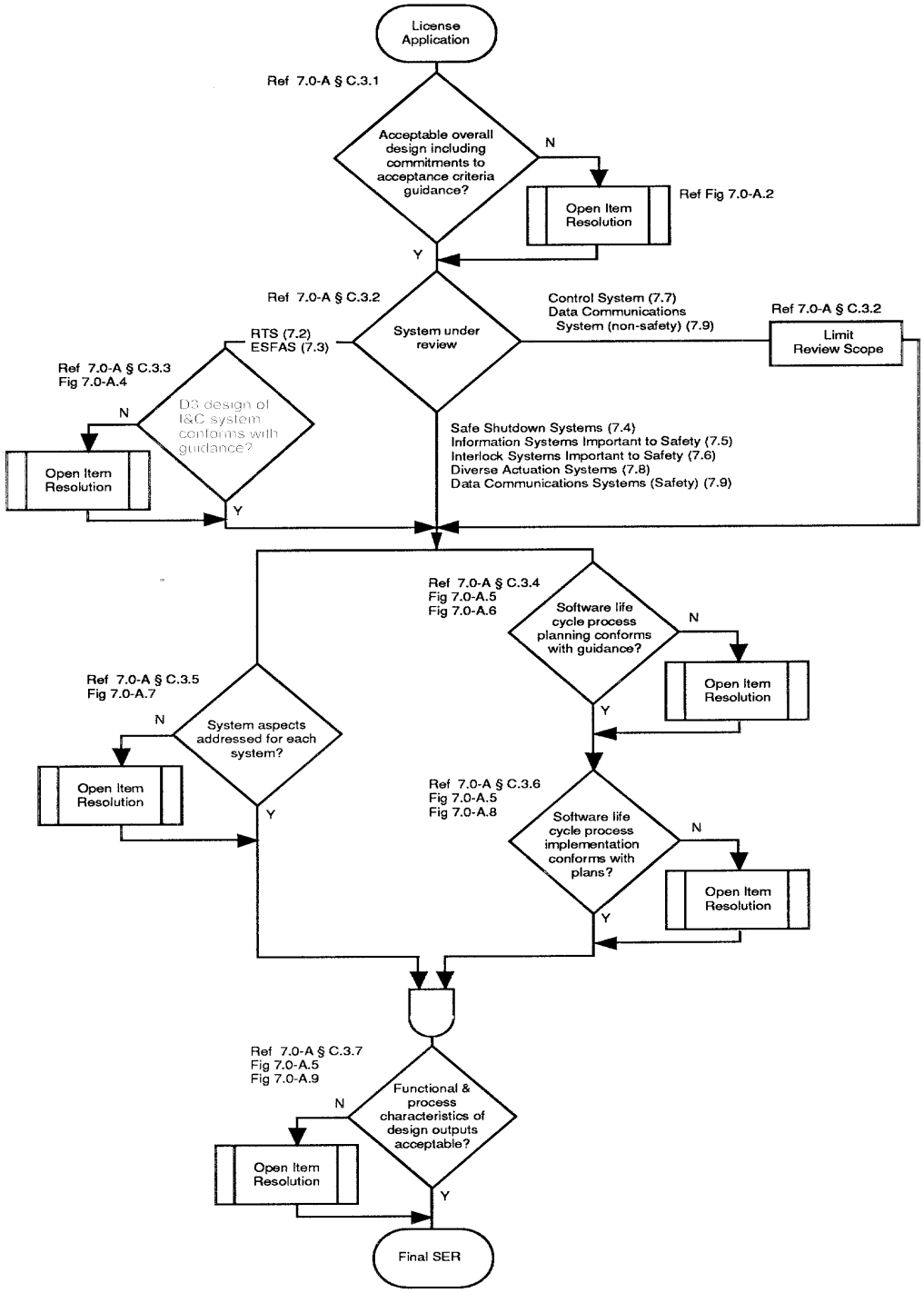

Figure 7.0-A-1. Overview of the process for reviewing digital instrumentation and control

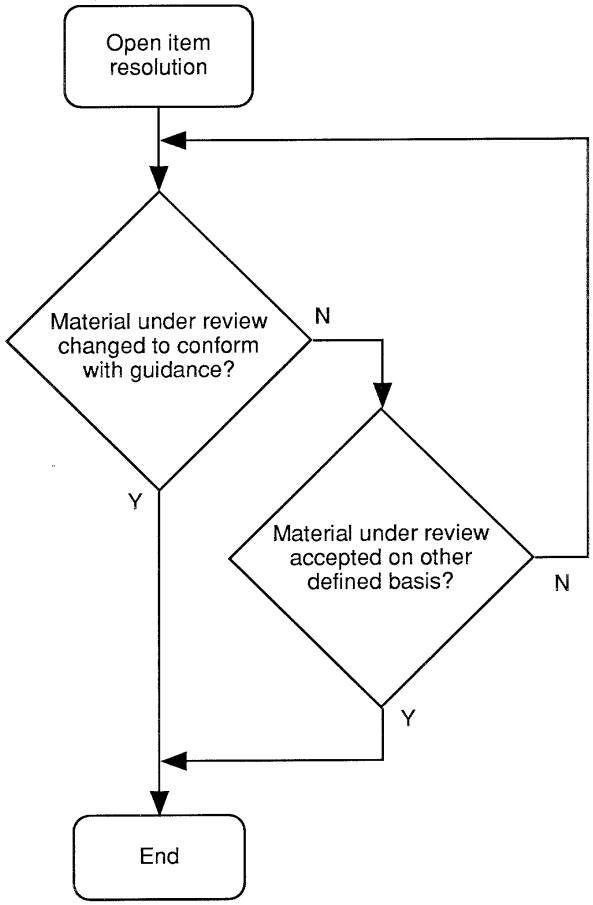

Figure 7.0-A-2. Open item resolution process.

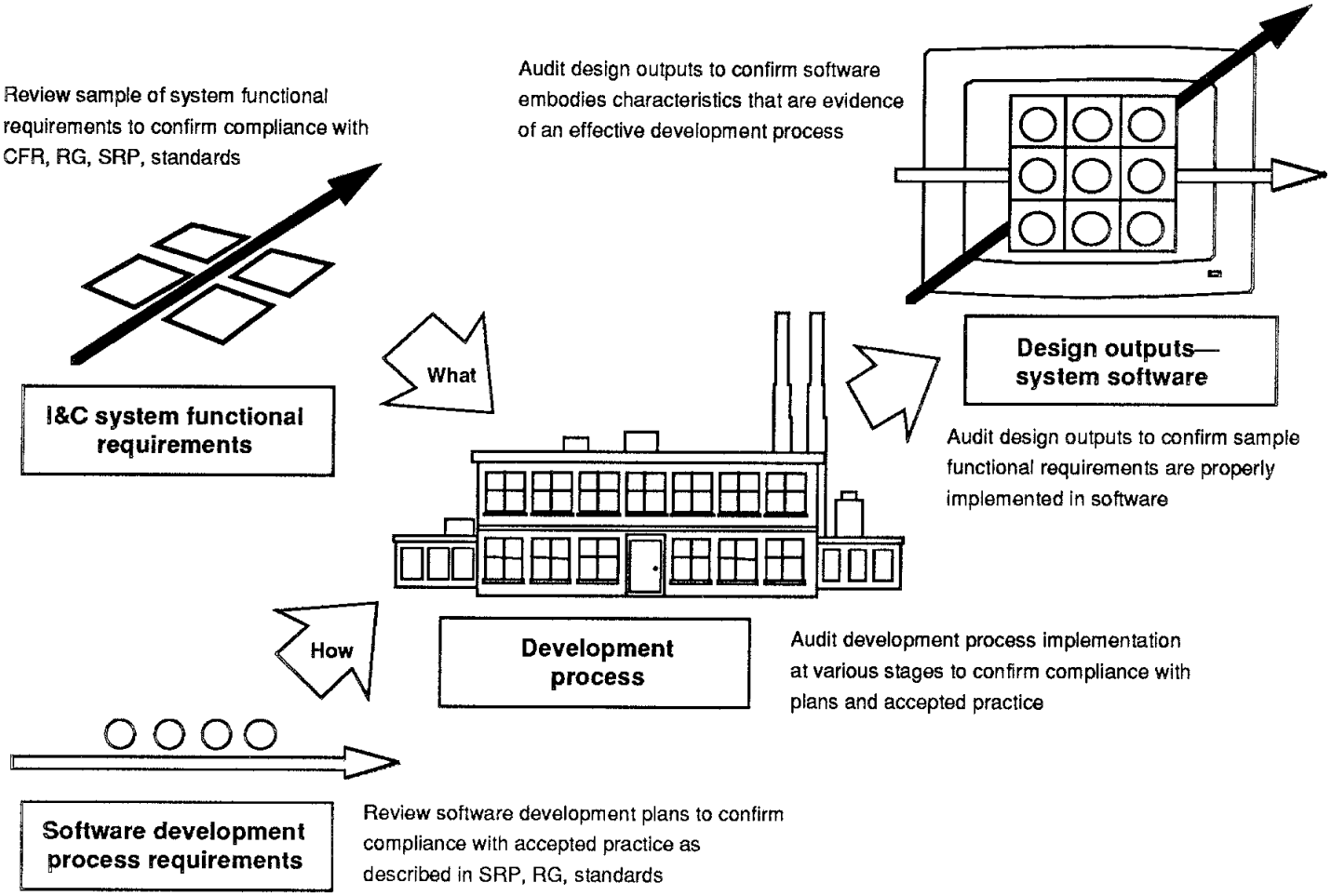

Figure 7.0-A-3. Software review process.

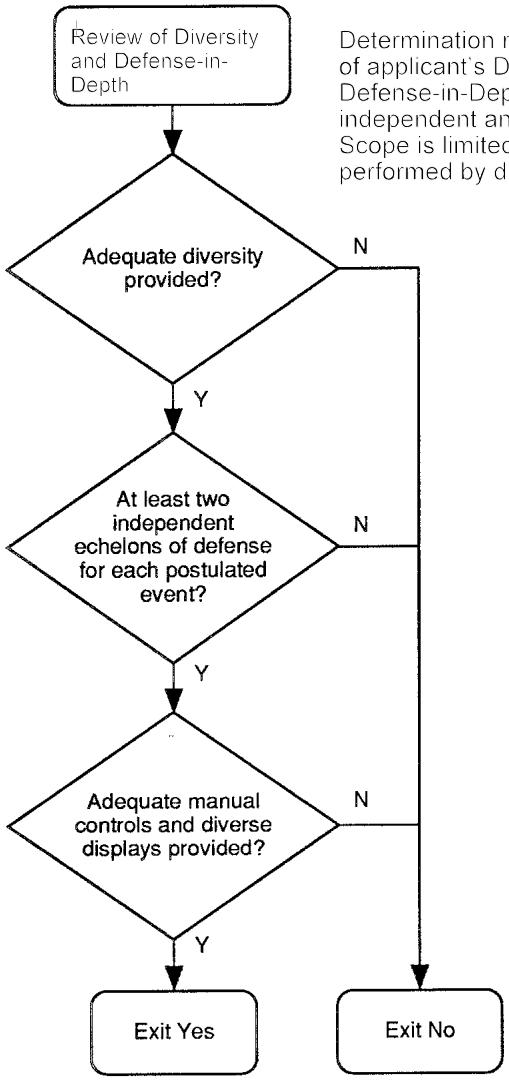

Figure 7.0-A-4. Diversity and Defense-in-depth review.

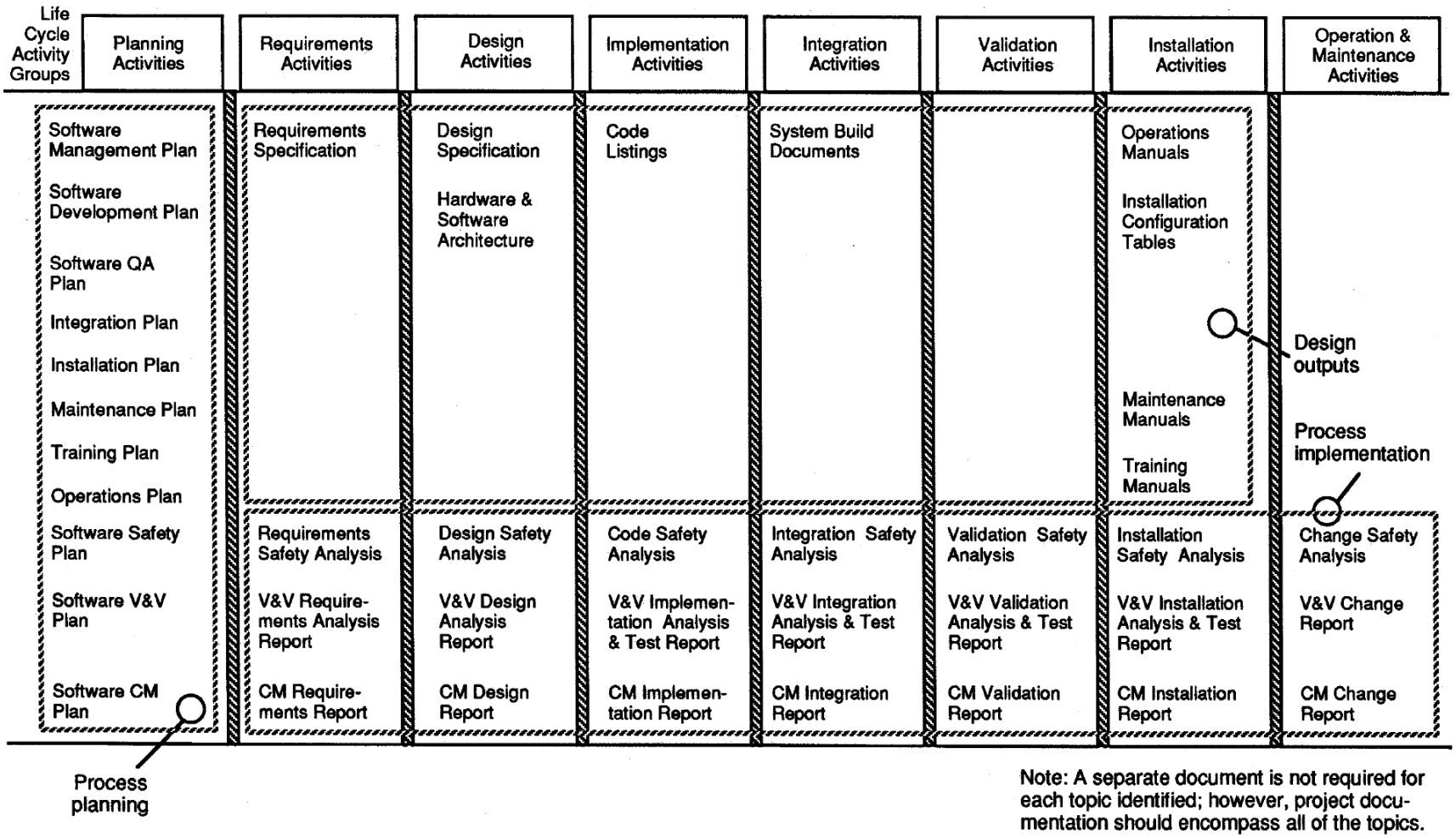

Figure 7.0-A-5. Software life-cycle activities.

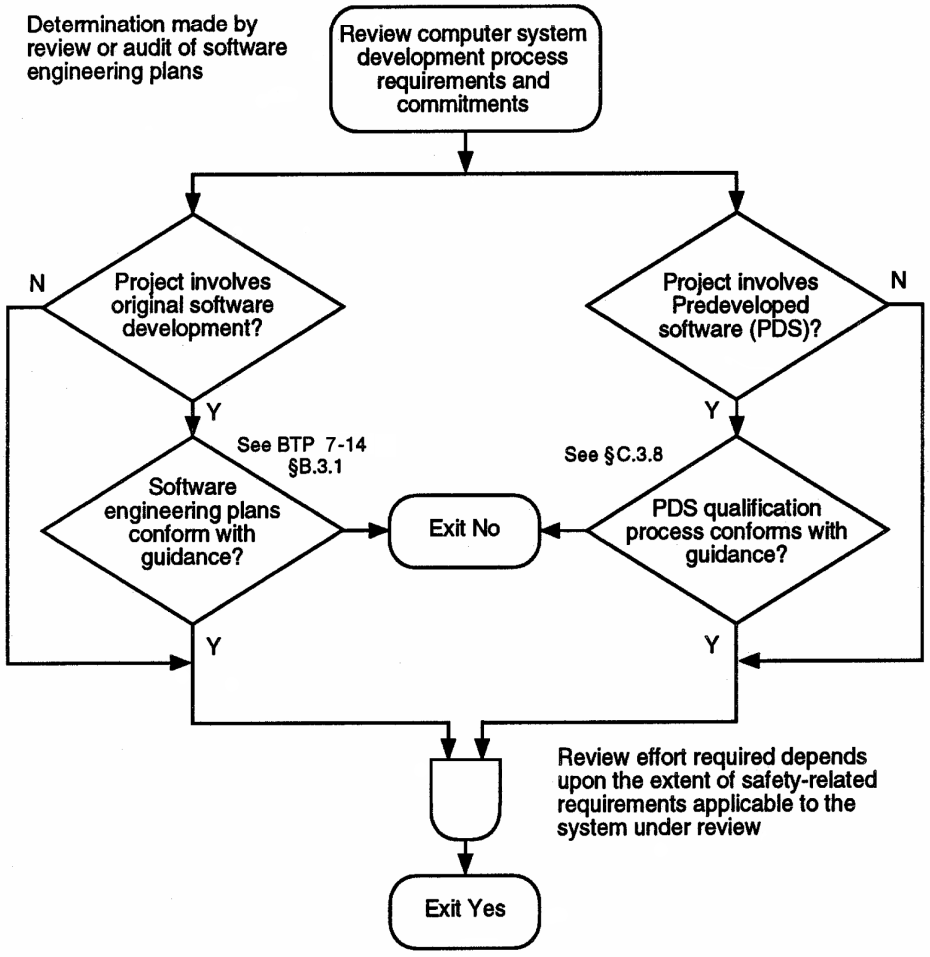

Figure 7.0-A-6. Review of software life-cycle process planning.

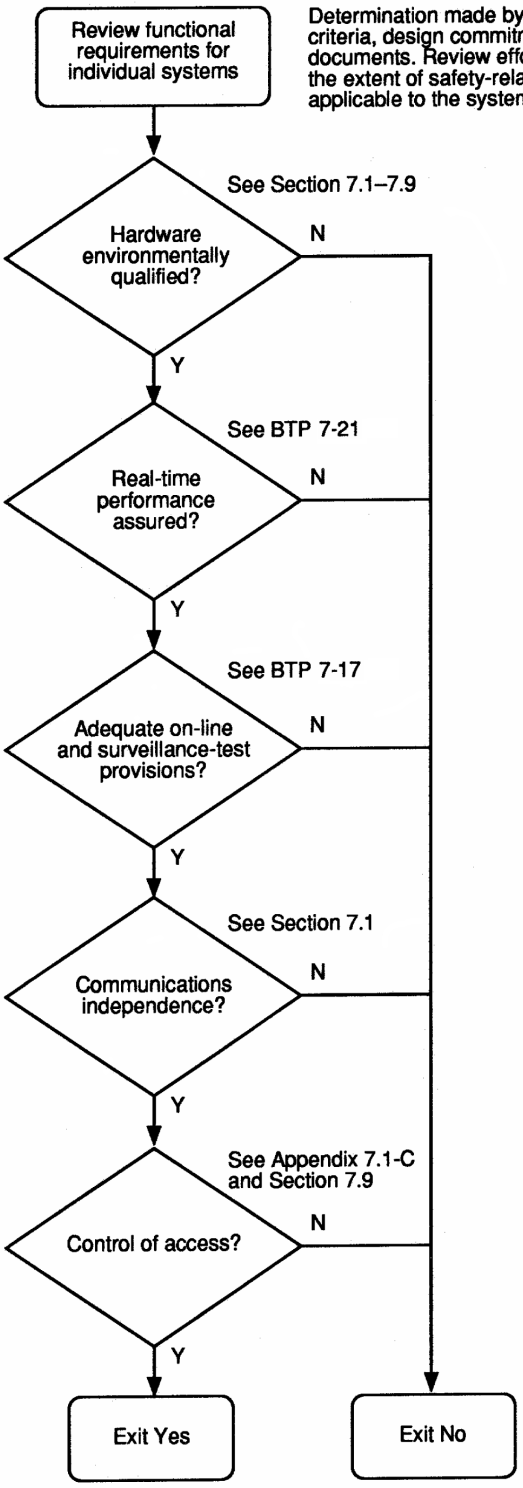

Figure 7.0-A-7. Special considerations in the review of functional requirements for digital instrumentation and control systems.

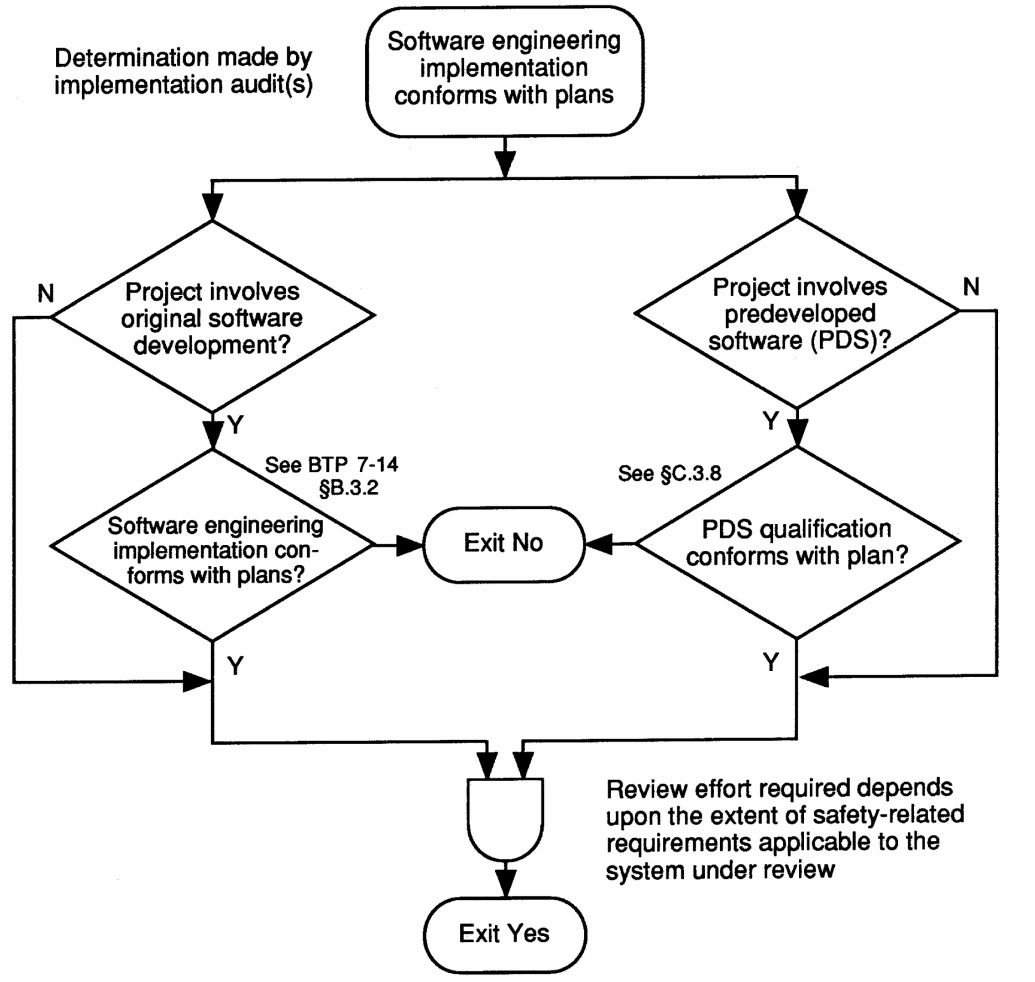

Figure 7.0-A-8. Review of software development process implementation.

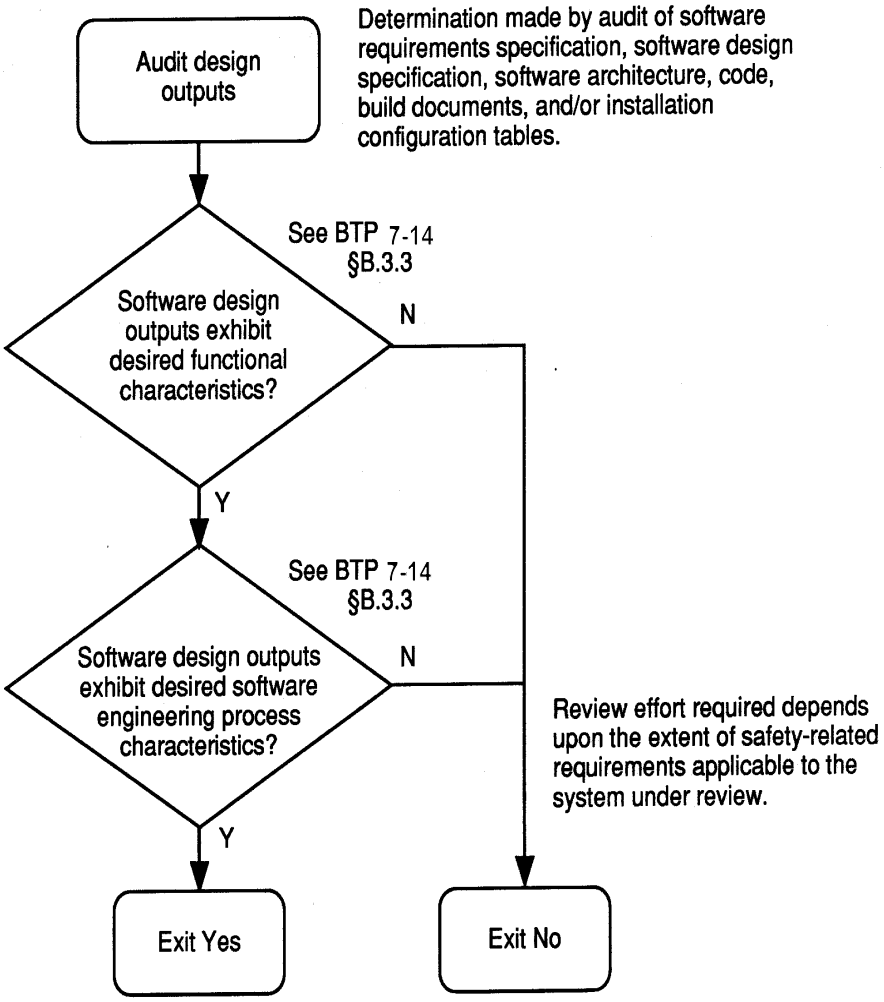

Figure 7.0-A-9. Review of Design Outputs