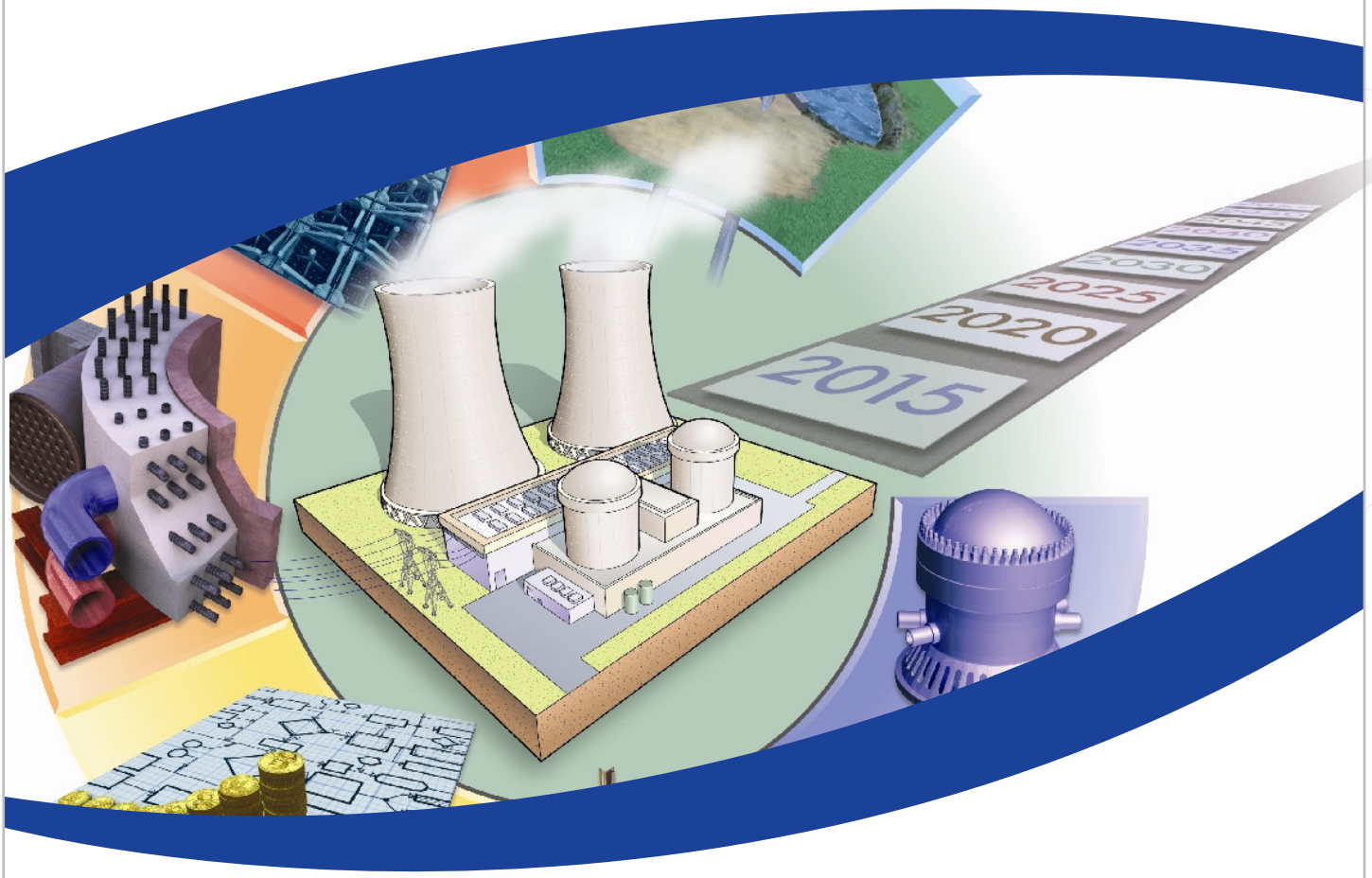
EPRI | ELECTRIC POWER RESEARCH INSTITUTE

2012 TECHNICAL REPORT

Plant Engineering: Guideline for the Acceptance of Commercial-Grade Design and Analysis Computer Programs Used in Nuclear Safety-Related Applications



Plant Engineering: Guideline for the Acceptance of Commercial-Grade Design and Analysis Computer Programs Used in Nuclear Safety-Related Applications

This document does NOT meet the requirements of 10CFR50 Appendix B, 10CFR Part 21, ANSI N45.2-1977 and/or the intent of ISO-9001 (1994)

EPRI Project Manager
M. Tannenbaum

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

3420 Hillview Avenue
Palo Alto, CA 94304-1338
USA

PO Box 10412
Palo Alto, CA 94303-0813
USA

800.313.3774
650.855.2121

askepri@epri.com

www.epri.com

1025243
Final Report, June 2012

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THE FOLLOWING ORGANIZATIONS PREPARED THIS REPORT:

Sequoia Consulting Group, Inc.

Electric Power Research Institute (EPRI)

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Acknowledgments

The following organization prepared this report:

Sequoia Consulting Group, Inc.
9042 Legends Lake Lane
Knoxville, Tennessee 37922

Principal Investigator
M. Tulay

Electric Power Research Institute (EPRI)
1300 West W. T. Harris Blvd.
Charlotte, NC 28262

Principal Investigator
M. Tannenbaum

This report describes research sponsored by EPRI.

EPRI would like to acknowledge the support of the following organizations whose participation and contributions were central to the development of this report:

- ASME NQA-1 Subcommittee on Software Quality Assurance
- EPRI Joint Utility Task Group (JUTG)
- Nuclear Information Technology Strategic Leadership (NITSL)
- Nuclear Procurement Issues Committee (NUPIC)

EPRI would like to thank the following individuals who participated in the Technical Advisory Group and made significant contributions to the development of this report. Their valuable insight and experience were essential to the successful completion of this project.

Tom Ehrhorn	AREVA NP Inc. (USA)
Tracy Rhodes	AREVA NP Inc. (USA)
Dan Baldwin	APS
PJ Maningat	APS
Lynne Valdez	APS
Adrian Johnpillai	Bechtel
Steve Bettinger	Bechtel

This publication is a corporate document that should be cited in the literature in the following manner:

Plant Engineering: Guideline for the Acceptance of Commercial-Grade Design and Analysis Computer Programs Used in Nuclear Safety-Related Applications. EPRI, Palo Alto, CA: 2012. 1025243.

Dominick LoSurdo	Constellation
Ujjal Mondal	CANDU Owners Group
Glen Frix	Duke Energy
Tom Duke	Duke Energy
John Yankoglu	Duke Energy
Theresa Derting	Entergy
Rob Austin	EPRI
Joe Naser	EPRI
Marc Tannenbaum	EPRI
Ray Torok	EPRI
Stanley Mitchell	Exelon / Nuclear Procurement Issues Committee
John Simmons	Luminant/Nuclear Procurement Issues Committee
Rob Santoro	PKMJ, Incorporated
Matt Gibson	Progress Energy
Bhavesh Patel	Progress Energy
Jay Pritchett	Progress Energy
Keith Morrell	Savannah River Nuclear Solutions
William Ware	Southern Nuclear
Michael Tulay	Sequoia Consulting Group, Incorporated
Norm Moreau	Theseus Professional Services, LLC
Mark Harvey	Unistar Nuclear/Nuclear Energy Institute
John O'Connor	URS
Deb Sparkman	U.S. Department of Energy
Milt Conception	U.S. Nuclear Regulatory Commission
Greg Galletti	U.S. Nuclear Regulatory Commission
George Lipscomb	U.S. Nuclear Regulatory Commission
Rich McIntyre	U.S. Nuclear Regulatory Commission
Paul Prescott	U.S. Nuclear Regulatory Commission

Abstract

This report provides methodology that can be used to perform safety classification of non-process computer programs, such as design and analysis tools, that are not resident or embedded (installed as part of) plant systems, structures, and components. The report also provides guidance for using commercial-grade dedication methodology to accept commercially procured computer programs that perform a safety-related function. The guidance is intended for use by subject matter experts in the acceptance of computer programs (that is, software).

Keywords
Analysis
Commercial grade dedication
Computer program
Design
Software
Validation and verification

Executive Summary

Purpose

The basic intent of this report is to provide guidance relative to the acceptance of non-process (that is, not installed in plant systems, structures, or components [SSCs]) computer programs used in the design and analysis of safety-related plant SSCs that have a functional safety classification of safety-related, but are provided as commercial grade.

When a computer program with a functional safety classification of safety-related is furnished as a commercial item, it should be procured as commercial grade and dedicated for use as a basic component in a safety-related application.

This report includes two key elements. First, the report provides a method for determining the functional safety classification of computer programs used in non-process (non-plant equipment) applications. This methodology can be applied to classify any computer program. Second, the report provides guidance for dedicating commercial-grade computer programs for use in a safety-related application. The dedication guidance is primarily targeted at computer programs used for design and analysis, but it can be applied to other types of commercially procured non-process-computer programs that are classified as safety-related by the dedicating entity.

Historically, organizations supporting nuclear power plant operation have accepted non-process computer programs in accordance with their software quality assurance (SQA) programs. In order to be accepted for use in nuclear safety-related applications, software must either be designed and manufactured in accordance with a quality assurance program that meets the requirements of 10CFR50, Appendix B [1] or dedicated for use in accordance with the requirements of 10CFR, Part 21 [2]. This document is not intended to replace existing SQA programs. References made throughout this document to SQA programs are intended to identify and acknowledge existing SQA program elements that are associated with acceptance and use of computer programs.

Background

The use of computer programs in the design and operation of nuclear power plants has evolved significantly since the era in which the current fleet of operating reactors in the United States was constructed. Computer programs are used in an increasing number of applications that support plant design, analysis, construction, operations, and maintenance.

Processes known as *verification* and *validation* are included in typical SQA programs. These processes have been widely applied in the acceptance of commercially produced computer programs in the commercial nuclear power industry and other industries.

In some cases, commercial-grade dedication was not believed to be an option for complex items such as computer programs. This determination was based upon the second sentence in the revised definition of a commercial-grade item included in the 1995 revision to 10CFR21 [2] (shown highlighted below).

> *Commercial grade item*. (1) When applied to nuclear power plants licensed pursuant to 10 CFR Part 50, commercial grade item means a structure, system, or component, or part thereof that affects its safety function, that was not designed and manufactured as a basic component. **Commercial grade items do not include items where the design and manufacturing process require in-process inspections and verifications to ensure that defects or failures to comply are identified and corrected (i.e., one or more critical characteristics of the item cannot be verified)**.

Although discussed in terms of plant structures, systems, and components, the Nuclear Regulatory Commission (NRC) concluded that software could meet the definition of a commercial-grade item in the U.S. NRC Safety Evaluation Report (SER) of Topical Report TR-106439, *Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications* [3]. As discussed in the SER:

> The second sentence of the new Part 21 definition of CGI excludes "items where the design and manufacturing process requires many in-process inspections and verifications to ensure that defects or failures to comply are identified and corrected (i.e., one or more, critical characteristics of the item cannot be verified)." The staff considers verification and validation activities common to software development in digital systems to be a critical characteristic that can be verified as being performed correctly following the completion of the software development by conducting certain dedication activities such as audits, examinations, and tests.

However, existing software quality assurance practices that rely on verification and validation alone may not be sufficient to accept commercial-grade computer programs for use in safety-related applications. In conversations with representatives from the task group that prepared this document, the NRC emphasized that commercially produced computer programs used for safety-related design and analysis are considered to be safety-related, and they reiterated the NRC's position that safety-related items must be either designed and manufactured in accordance with a quality assurance program that meets the requirements of 10CFR, Part 50, Appendix B [1] or dedicated for use in a safety-related application in accordance with the requirements of 10CFR, Part 21 [2].

The NRC staff also stated their expectation that when the computer program is dedicated, the acceptance process should be documented in the form of a commercial-grade item dedication evaluation.

Important elements of commercial-grade item dedication technical evaluation include:

1. Identification of the safety function(s) of the item being dedicated
2. A failure modes and effects analysis (FMEA) for the item being dedicated that postulates failure modes and/or mechanisms of the item that could affect its ability to perform its safety-related function(s)
3. Identification of critical characteristics of the item that can be verified to obtain reasonable assurance that the item is capable of performing its intended safety-related function(s) (that is, the item will not succumb to the failure modes identified in the FMEA)
4. Establishing acceptance criteria for each critical characteristic that will be verified
5. Identification of the acceptance methods and/or activities that will be used to verify each critical characteristic
6. Documenting the technical evaluation and results of acceptance activities

Although verification and validation typically involve comprehensive testing and examination of the computer program, current verification and validation documentation may not always identify specific functions of the computer program as they may relate to the safety-related functions of associated SSCs or impact design analysis activities. In addition, verification and validation may not include an FMEA or other documented means of identifying critical

characteristics. Although commercial-grade dedication technical evaluations for computer programs may incorporate verification and validation activities, the technical evaluation should address each of the six areas noted above.

Safety Classification of Computer Programs

Computer programs with a safety-related function that are provided commercially must be dedicated for use in safety-related applications. Computer programs that do not perform a safety-related function do not need to be dedicated. In order to determine if the computer program must be dedicated for use in a safety-related application, the functional safety classification of the computer program must first be determined. A process for determining the functional safety classification of computer programs is included in Section 5 of this report.

Use of Commercial-Grade Dedication to Accept Computer Programs

The key elements involved in commercial-grade dedication are the technical evaluation and acceptance processes. These processes find basis in the requirements included in 10CFR, Part 21 [2], EPRI NP-5652 [4], EPRI TR-102260 [5], and EPRI TR-106439 [6]. The basic steps in the technical evaluation and acceptance processes are discussed in Section 4 of this report.

Acceptance Versus Design

As defined in 10CFR, Part 21 [2],

> Dedication is an *acceptance* process undertaken to provide reasonable assurance that a commercial-grade item to be used as a basic component will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under an Appendix B, quality assurance program.

Acceptance of computer programs is the process of verifying critical characteristics identified for the computer program using one or more of the acceptance methods to reasonably ensure that the computer program will perform its safety-related function(s). Verification methods may include inspections, tests, or analyses performed by the purchaser or third-party dedicating entity after delivery (Method 1), commercial-grade surveys (Method 2), product inspections or witness at hold points at the manufacturer's facility (Method 3), or evaluation of historical performance of both the supplier and the computer program (Method 4).

Use of commercial-grade dedication as an acceptance process is not intended to validate the suitability of design. Selection of the computer program and suitability of its design are established prior to initiating the commercial-grade dedication acceptance process. Subject matter experts in the types of computations performed by the computer program are typically responsible for selecting the software for use and establishing the suitability of design.

The amount and level of detail of design and qualification information available can impact the types of dedication acceptance methods used as well as the direction in which the inspections and tests are targeted.

In addition to acceptance of computer programs, SQA programs often include provisions for examination and evaluation of the entire software life cycle. The software life cycle includes the processes used by the manufacturer/developer to design, develop, qualify, and accept the software as well as the processes in place to address reported error and control changes to the software. Some of the activities associated with the software life cycle are associated with the design and qualification of the software. In this respect, software verification and validation can extend beyond the acceptance process. The fact that the computer program is being dedicated for use should not be used as a basis to forgo product selection and qualification activities (for example, design reviews) required by SQA programs.

Staff Responsible for Dedication of Computer Programs

Computer programs may be dedicated by licensees as well as other organizations that support plant design, analysis, construction, operations, and maintenance. Safety classification and dedication of computer programs may require the engagement of staff with expertise in several areas. Typically, staff responsible for safety classification and dedication of computer programs could include:

- Design engineers or other technical staff that use the computer program and have in-depth knowledge and understanding of how the computer program is being applied, the intended scope of use, and the theory behind the calculations or functions addressed by the computer program
- Procurement engineers or other individuals with significant experience in the commercial-grade dedication process
- Information technology professionals and other subject matter experts

Table of Contents

Section 1: Introduction and Scope of Use 1-1
1.1 Objectives 1-1
1.2 Applicability of Guidance 1-2
1.2.1 Computer Program Procured as a Basic Component (Scenario A) 1-2
1.2.2 Computer Program Procured as a Commercial Item and Used for Safety-Related Design and Analysis (Scenario B) 1-4
1.2.3 Computer Program Procured as a Commercial Item and Dedicated for Use in Safety-Related Design and Analysis Applications (Scenario C) 1-5
1.3 Applicability of Guidance Provided in This Report 1-6
1.3.1 Commercially Procured Computer Program 1-8
1.3.2 Perform Safety Classification 1-8
1.3.3 Are Controls Greater Than Standard Non-Safety Controls Appropriate? 1-8
1.3.4 Specify Appropriate Augmented Quality Controls 1-8
1.3.5 Procure Using Standard Non-Safety-Related Processes 1-8
1.3.6 Procure as Basic Component or Commercial Grade? 1-8
1.3.7 Independently Verify Output or Pre-Verify Computer Program? 1-9
1.3.8 Accept Using Commercial-Grade Dedication Guidance 1-9
1.3.9 Purchase as a Basic Component 1-9
1.3.10 Apply 10CFR50, Appendix B, Criterion III Controls 1-9
1.4 Scope and Content of This Report 1-9
1.5 Background 1-11
1.6 Basic Premises 1-12
1.6.1 Consistency with Previously Published/Endorsed EPRI Reports 1-12
1.6.2 Suitability of the Design 1-13

1.6.3 Suitability of Computer Program Designs.....1-13
1.6.4 Application of the Guidance in This Report.....1-13
1.6.5 Computer Programs Previously Accepted Via Quality Assurance Programs.....1-13
1.6.6 Maintenance of Computer Programs and Operating Systems.....1-16
1.6.7 Adoption of ASME NQA-1a-2009.....1-16

Section 2: Baseline Terminology – Definitions and Acronyms.....2-1
2.1 Introduction.....2-1
2.2 Definitions of Key Terms.....2-1
2.3 Acronyms.....2-8

Section 3: Types of Design and Analysis Computer Programs.....3-1
3.1 Examples of Design and Analysis Computer Programs.....3-1

Section 4: Generic Technical Evaluation and Acceptance Processes.....4-1
4.1 Overview of Commercial-Grade Dedication.....4-1
4.2 Generic Process for Technical Evaluation.....4-5
4.3 Generic Process for Acceptance of Computer Software.....4-6

Section 5: Functional Safety Classification of Computer Programs.....5-1
5.1 Functional Safety Classification Categories.....5-1
5.2 Safety Classification Guidance.....5-1
5.3 Options for Determining the Safety Classification.....5-2
5.4 Functional Safety Classification.....5-2
5.4.1 Classification Considering Failure Modes and Effects.....5-3
5.4.2 Classification Considering Impact Categorization.....5-9
5.5 Classification of Computer Program Environments.....5-13

Section 6: Acceptance of Commercial-Grade Computer Programs via the Dedication Process.....6-1
6.1 Identify the Computer Program Being Procured.....6-4
6.2 Does the Computer Program Perform a Safety Function?.....6-4

6.3 Is the Computer Program Being Procured as a Basic Component? 6-4
6.4 Identify Critical Characteristics for Acceptance 6-4
6.4.1 Product Selection Attributes 6-6
6.4.2 Product Identification Inspection Attributes 6-6
6.4.3 Physical and Performance Characteristics 6-6
6.4.4 Dependability Characteristics 6-7
6.4.5 Examples of Product Selection, Product Identification, and Critical Characteristics 6-7
6.5 Document Results of Technical Evaluation and Critical Characteristics 6-22
6.6 Select Acceptance Method(s) 6-23
6.6.1 Method 1 – Special Tests and Inspections 6-23
6.6.2 Method 2 – Survey of Commercial-Grade Supplier 6-24
6.6.3 Method 3 – Source Verification 6-25
6.6.4 Method 4 – Supplier and Item Performance History 6-25
6.6.5 Standard Receipt Inspection 6-25
6.7 Dedication Acceptance Activities 6-26
6.8 Considerations When Selecting Acceptance Methods 6-26

Section 7: Commercial-Grade Software Procurement Examples 7-1

7.1 Computer Program Used to Perform Pipe Stress Calculations and Analysis 7-1
7.1.1 Introduction 7-1
7.1.2 Implementation of the Technical Evaluation 7-2
7.1.3 Implementation of the Acceptance Process 7-3
7.2 Computer Program Used in the Design of a Safety-Related Pump 7-4
7.2.1 Introduction 7-4
7.2.2 Implementation of the Technical Evaluation 7-5
7.3 Procurement of an Inventory Management Computer Program 7-6
7.3.1 Introduction 7-6
7.3.2 Implementation of the Technical Evaluation 7-6
7.4 Procurement of a Commercially Procured Computer Program Used to Perform Seismic Analysis of Components in Safety-Related Systems 7-7
7.4.1 Introduction 7-7
7.4.2 Implementation of the Technical Evaluation 7-7

7.5 Procurement of a Computer Program Used for Monitoring the Operation and Control Functions of Plant SSCs 7-8
7.5.1 Introduction 7-8
7.5.2 Implementation of the Technical Evaluation 7-8
7.6 Procurement of a Computer Program Used for Flow-Accelerated Corrosion (FAC) Analysis 7-9
7.6.1 Introduction 7-9
7.6.2 Implementation of the Technical Evaluation 7-9
7.7 Use of Legacy Software for a Previously Accepted Application 7-10
7.7.1 Introduction 7-10
7.7.2 Implementation of the Methodology 7-11
7.8 Use of Legacy Software for a New Application 7-12
7.8.1 Introduction 7-12
7.8.2 Implementation of the Methodology 7-12

Section 8: References and Bibliography 8-1
8.1 In-Text References 8-1
8.2 Bibliography 8-4
8.2.1 Regulatory Documents 8-4
8.2.2 EPRI Technical Reports 8-5
8.2.3 Reference Documents 8-5

Appendix A: Guidance for Specifying Technical, Quality, and Documentation Requirements A-1
A.1 Specifying Technical Requirements A-1
A.2 Specifying Quality Requirements A-2
A.3 Specifying Documentation Requirements A-3

Appendix B: Practical Quality Assurance Considerations for Software Dedication B-1
B.1 Testing Environment B-1
B.2 Scope and Frequency of Dedication B-1
B.3 Applicability of Reporting Requirements B-2
B.4 Applicability of Guidance to Existing Computer Programs B-2
B.5 Applicability of Cyber Security Requirements B-2

Appendix C: Computer Program Categories and Uses C-1
C.1 Computer Programs Integral to Plant SSCs C-1
C.2 Administrative Support Computer Programs C-2
C.3 Operations Support Computer Programs C-3
C.4 Measurement and Test Equipment Computer Programs C-3
C.5 Manufacturing Computer Programs C-4

List of Figures

Figure 1-1 Three Basic Scenarios for Procurement of Commercially Procured Computer Programs for Use in Safety-Related Design and Analysis Applications 1-3

Figure 1-2 Applicability of Dedication Guidance in This Report 1-7

Figure 1-3 Scope and Content of the Report 1-10

Figure 1-4 Applicability of This Guidance to Legacy Computer Programs 1-15

Figure 4-1 Key Elements of Commercial-Grade Dedication 4-1

Figure 4-2 Technical Evaluation and Acceptance Interdependencies 4-3

Figure 4-3 Generic Process for Commercial Grade Dedication 4-4

Figure 5-1 Options for Classifying Computer Programs 5-2

Figure 5-2 Functional Classification Considering Failure Modes and Effects 5-4

Figure 5-3 Functional Classification Considering the Impact of Computer Programs 5-11

Figure 6-1 Commercial-Grade Computer Program Dedication Process 6-3

Figure 6-2 Typical Process Flow (Life Cycle) for Software 6-27

Figure 6-3 Typical Design, Specification, and Acceptance Processes 6-27

List of Tables

Table 4-1 Key Elements of the Technical Evaluation 4-5

Table 5-1 Examples of Failure Mechanisms for Computer Programs 5-8

Table 5-2 Functional Safety Classification Considering Impact of Programs on SSCs 5-12

Table 6-1 Common Failure Mechanisms and Associated Critical Characteristics.....6-5

Table 6-2 Typical Product Selection Attributes 6-9

Table 6-3 Typical Product Identification Attributes.....6-12

Table 6-4 Typical Physical Critical Characteristics 6-13

Table 6-5 Typical Performance Critical Characteristics.....6-13

Table 6-6 Typical Dependability Critical Characteristics.....6-16

Table 6-7 Use of Failure Modes and Effects Analysis in Technical Evaluations of Computer Programs Not Embedded in Plant SSCs.....6-22

Table 6-8 Example of Using Acceptance Methods.....6-28

Section 1: Introduction and Scope of Use

The use of computer programs in the design and operation of nuclear power plants has evolved significantly since the era in which the current fleet of operating reactors in the United States was constructed. Computer programs are used in an increasing number of applications that support operations and maintenance.

The nuclear power industry currently uses many types of computer programs and software products. Certain software or computer programs are embedded in plant systems, equipment, and replacement items. Other computer programs are used in engineering design and analysis. Computer programs such as enterprise asset management and resource planning systems, document control systems, corrective action systems, and operations support systems are used to implement a variety of important administrative functions. In addition to licensees, other organizations that support plant design, analysis, construction, operations, and maintenance of plant structures, systems, or components (SSCs) may use computer programs in safety-related applications.

1.1 Objectives

The purpose of this report is to provide guidance for licensees and nuclear suppliers regarding the acceptance of commercial-grade computer programs for use in safety-related applications. Specifically, the objectives of this report are to:

- Establish a baseline vocabulary for discussing the procurement and dedication of commercial-grade computer programs
- Identify different categories of computer programs
- Provide methodologies that can be used to perform functional safety classification of computer programs
- Provide a generic process that can be used to dedicate commercial-grade computer programs that is consistent with the process used to dedicate commercial-grade items
- Identify examples of critical characteristics typically associated with computer programs
- Present commercial-grade item acceptance methods and discuss how they can be applied to accept the computer program

1.2 Applicability of Guidance

Three basic scenarios for procuring and using computer programs in safety-related applications are discussed in this section and illustrated in Figure 1-1. Included is dialogue about the computer program itself, the output of the computer program, and how the computer program is used.

1.2.1 Computer Program Procured as a Basic Component (Scenario A)

Scenario A is represented in Figure 1-1 by boxes 1.2.1 through 1.2.1.3. Scenario A, depicts a computer program procured as a basic component.

In Scenario A, the computer program is being procured to perform safety-related design and/or analysis. The computer program is purchased from a supplier maintaining a nuclear quality assurance program that meets the requirements of 10CFR50, Appendix B [1]. The computer program was either developed or dedicated for use in a safety-related application under the supplier's nuclear quality assurance program.

A hardware analogy for Scenario A would be a part that is being designed and fabricated under a quality assurance program that meets the requirements of 10CFR50, Appendix B. The supplier is on the purchaser's approved supplier list, certifies that the part was produced in accordance with their nuclear quality assurance program, and accepts responsibility for reporting defects in accordance with 10CFR, Part 21 [2] each time the part is supplied to the purchaser.

1.2.1.1 Acceptance for Defined Scope of Use and Installation

In Scenario A, the computer program is accepted by the purchaser for a defined scope of use and is installed in accordance with the purchaser's software quality assurance (SQA) program, processes, and procedures.

1.2.1.2 Control and Use of Computer Program

In Scenario A, the computer program is controlled and used in accordance with the purchaser's SQA program. It is only applied within established boundaries, such as types of calculations, range of input values, installed environment, and so forth. Configuration of the computer program is maintained, changes are controlled, installation of updates (new versions) are controlled, and errors reported by either the supplier or the purchaser are handled in accordance with the purchaser's SQA program.

1.2.1.3 Control and Use of Outputs Using QA Methods

Although control and use of output after acceptance is not the focus of this report, it is worth mentioning that the output generated in Scenario A is controlled and used in an appropriate manner consistent with the requirements of 10CFR50, Appendix B, Criterion III [1], Design Control.

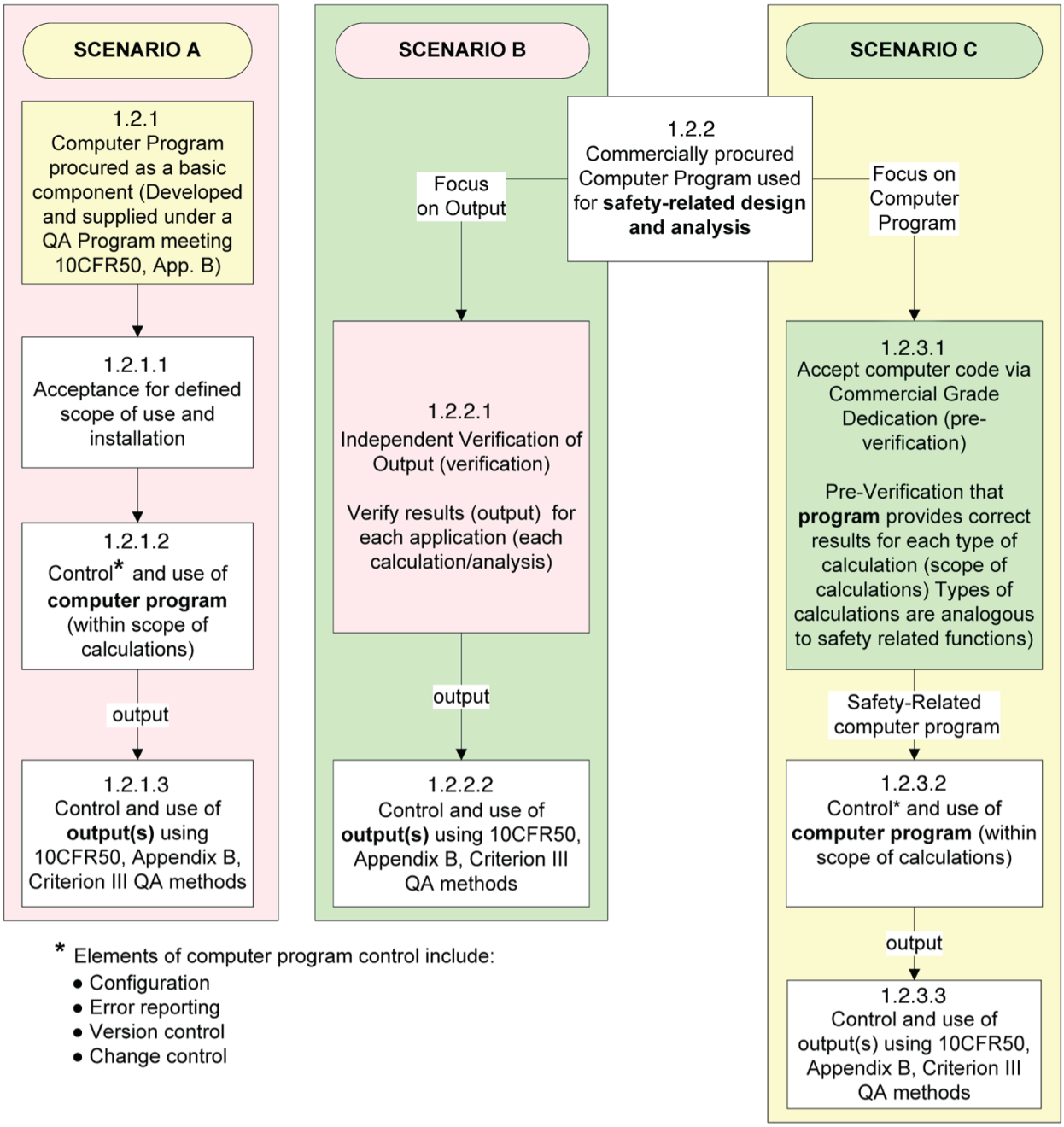


Figure 1-1
Three Basic Scenarios for Procurement of Commercially Procured Computer Programs for Use in Safety-Related Design and Analysis Applications

1.2.2 Computer Program Procured as a Commercial Item and Used for Safety-Related Design and Analysis (Scenario B)

The two remaining scenarios involve use of a commercially developed computer program for use in performing safety-related design and/or analysis. In these scenarios, the computer program is purchased from a commercial supplier that does not maintain a nuclear quality assurance program that meets the requirements of 10CFR50, Appendix B [1].

The computer program was developed and is being supplied as a commercial-grade item.

Output from the computer program is the focus of Scenario B, which is represented in Figure 1.1 by boxes 1.2.2.1 and 1.2.2.2. In Scenario B, each time the computer program is used to generate output, adequacy of the resulting output of the computer program is verified though alternative means. Therefore, the computer program is not being relied upon as the sole basis for performing design and/or analysis calculations. Commercial software used in this manner would be classified as non-safety-related or non-safety-related augmented quality using the safety classification methodology included in Section 5 of this report.

A hardware analogy for this scenario would be a part that is being machined with commercial machinery and cutting tools (such as a drill bit). Each time a finished part is completed, it is subjected to inspections using appropriate metrology and test equipment to verify that it meets the applicable dimensions and tolerances that the machining process is intended to achieve.

1.2.2.1 Independent Verification of Output for Each Calculation

In scenario B, the commercially procured computer program is accepted for use in accordance with the purchaser's SQA program. Each time the commercially procured computer program is used, the output from the program is independently verified using an acceptable method such as hand calculations; calculations using comparable proven programs; or empirical data and information from technical literature.

1.2.2.2 Control and Use of Outputs Using QA Methods

Although control and use of output after acceptance is not the focus of this report, it is worth mentioning that in Scenario B, independently verified output is controlled and used in an appropriate manner consistent with the requirements of 10CFR50, Appendix B, Criterion III [1], Design Control.

1.2.3 Computer Program Procured as a Commercial Item and Dedicated for Use in Safety-Related Design and Analysis Applications (Scenario C)

Scenario C involves using a commercially procured computer program to perform safety-related design and/or analysis. In Scenario C, the computer program is purchased from a commercial supplier that does **not** maintain a nuclear quality assurance program that meets the requirements of 10CFR50, Appendix B [1].

The computer program was developed and is being supplied as a commercial-grade item. The purchaser must dedicate the computer program for use in safety-related design and analysis applications. In a sense, the dedicating entity is pre-verifying that the computer program will provide correct and accurate output.

The ability of the computer program is the focus of Scenario C, which is represented in Figure 1-1 by boxes 1.2.3.1, 1.2.3.2, and 1.2.3.3. In Scenario C, the computer program is relied upon as the sole basis for making design and/or analysis decisions. Commercial computer programs used in this manner would be classified as safety-related using the safety classification methodology included in Section 5 of this report. Therefore, the commercially procured computer program is purchased as a commercial-grade item and dedicated for use in a safety-related design and/or analysis application by the dedicating entity.

Two hardware analogies are discussed for Scenario C. The first involves a part that is manufactured under a commercial quality assurance program and supplied to the purchaser (for example, to an end user) as a commercial-grade item. Each time the part is received by the end user, it is dedicated for use in the intended application. That is, an acceptance process is implemented to verify critical characteristics of the part that provide reasonable assurance that the part will perform its intended safety-related function(s).

Perhaps the second hardware analogy for Scenario C best illustrates the special nature of a computer program used as a basic component in a safety-related application. In the second hardware analogy, the purchaser (for example, a nuclear supplier) has bought commercial machinery and cutting tools that will be used to fabricate safety-related parts. However, for some reason, it is not possible to independently verify the critical characteristics of each part after it is manufactured. Therefore, the purchaser has to ensure the quality of the parts by obtaining reasonable assurance that the machinery used to manufacture them always imparts the desired characteristics. The purchaser must establish the critical characteristics necessary to provide reasonable assurance that the machinery is set up correctly and that the cutting tools are correct and in the condition necessary to ensure that the part has the correct dimensions and configuration. Since the machine and tools will be used at different times, it may be necessary to check the cutting tools (such as drill bits) prior to and after each production run of parts to ensure that the integrity of the cutting tools was maintained throughout the entire production run.

1.2.3.1 Accept Computer Program via Commercial-Grade Dedication

In Scenario C the commercial-grade dedication methodology (included in Section 6 of this report) is used to accept the commercial computer program for safety-related use. Since the output of the computer program will not be independently verified after each use, acceptance focuses on pre-verification that the computer program is capable of producing correct and accurate results for each calculation or function it provides. The types of design and analysis calculations and functions provided by the computer program may be analogous to safety-related functions of plant components.

1.2.3.2 Control and Use of the Computer Program

Although control and use of output after acceptance are not the focus of this report, it is worth mentioning that in Scenario C, the successfully dedicated and accepted computer program is controlled and used in accordance with the purchaser's SQA program. It is applied only within established boundaries, such as types of calculations, range of input values, installed environment, and so forth. Configuration of the computer program is maintained, changes are controlled, installation of updates (new versions) is controlled, and errors that are reported by either the supplier or the purchaser are handled in accordance with the purchaser's SQA program.

1.2.3.3 Control and Use of Output(s) Using QA Methods

Although control and use of output after acceptance are not the focus of this report, it is worth mentioning that the output generated in Scenario C is controlled and used in an appropriate manner consistent with the requirements of 10CFR50, Appendix B, Criterion III [1], Design Control.

1.3 Applicability of Guidance Provided in This Report

The safety classification guidance included in Section 5 of this report can be applied to any commercially procured computer program.

The guidance on accepting commercially procured computer programs using the dedication process outlined in Section 6 of this report is applicable in situations where the commercial program is used in design and analysis applications in which the results provided by the software are not independently verified for each calculation. Figure 1-2 illustrates the applicability of the dedication guidance included in this report.

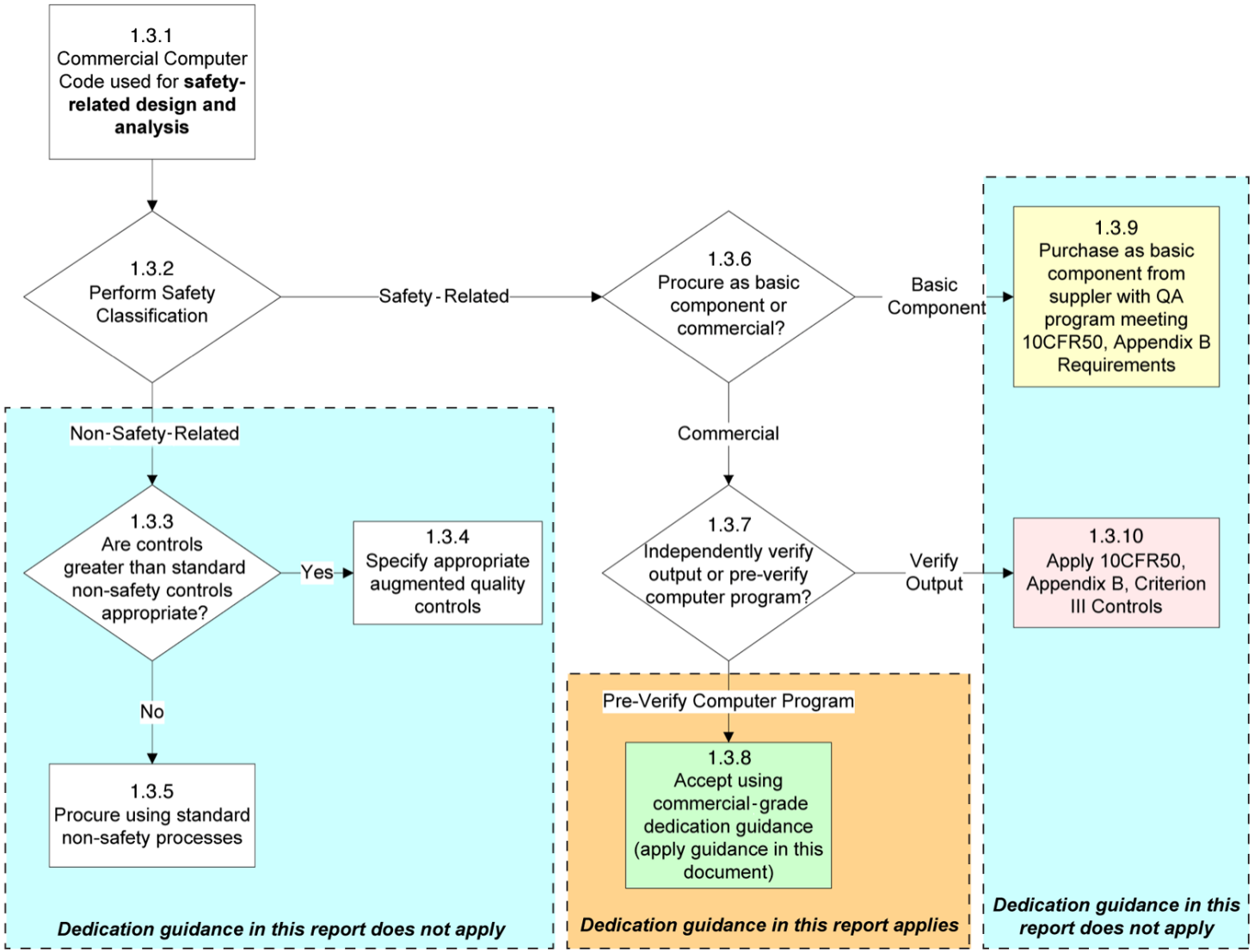


Figure 1-2
Applicability of Dedication Guidance in This Report

1.3.1 Commercially Procured Computer Program

The need or desire to use computer programs that were developed in a commercial environment (not developed under a quality assurance program that meets the requirements of 10CFR50, Appendix B [1]) to perform design or analysis of safety-related SSCs is the event that would initiate screening to determine if the dedication guidance in this report is applicable.

1.3.2 Perform Safety Classification

A safety classification of the computer program is performed to determine if the computer program is classified as safety-related or non-safety-related.

Classification is based on intended use(s). If a computer program is used in multiple applications, classification may be based on the most restrictive end use(s), or classifications may be performed for each specific end use.

1.3.3 Are Controls Greater Than Standard Non-Safety Controls Appropriate?

If the computer program is classified as non-safety-related, the dedication guidance in this report does not apply.

Screening should be performed to determine if controls greater than the controls applied to typical non-safety-related procurements are appropriate. Enhanced controls may be appropriate when the applicable software quality assurance (SQA) plan specifies additional controls, when the computer program is associated with activities subject to regulatory commitments involving augmented quality controls (for example, fire protection and post-accident sampling), or when the computer program is associated with equipment considered critical to generation, equipment considered as a single point vulnerability, and so forth.

1.3.4 Specify Appropriate Augmented Quality Controls

If augmented quality controls are appropriate, they should be specified in procurement documents, acceptance plans, and other documents.

1.3.5 Procure Using Standard Non-Safety-Related Processes

If augmented quality controls are not appropriate, the computer program should be procured as non-safety-related in accordance with applicable requirements.

1.3.6 Procure as Basic Component or Commercial Grade?

Determine if the computer program will be procured as a basic component or as commercial grade. The computer program can be procured as a basic component from a supplier (such as a third-party qualifier) that completes acceptance of the computer program and provides it as a basic component under the supplier's approved quality assurance program that meets the requirements of 10CFR50, Appendix B [1].

1.3.7 Independently Verify Output or Pre-Verify Computer Program?

Determine the manner in which the computer program will be used. If it is not possible to verify the results produced by the computer program, the computer program would have to be accepted using commercial-grade dedication guidance (refer to Section 1.3.8). Will the output (results) derived from use of the computer program be independently verified through alternative means (such as hand calculations; calculations using comparable proven programs; or empirical data and information from technical literature) each time the computer program is applied?

1.3.8 Accept Using Commercial-Grade Dedication Guidance

If the output from the computer program is **not** independently verified for each application, the dedication guidance in this report should be applied to obtain reasonable assurance that use of the computer program will yield correct and accurate results when it is used within the range of applicable functions.

1.3.9 Purchase as a Basic Component

Procure the computer program as a basic component from a supplier that maintains a quality assurance program that is approved by the purchaser and complies with the requirements of 10CFR50, Appendix B [1].

1.3.10 Apply 10CFR50, Appendix B, Criterion III Controls

If output (results) derived from use of the computer program will be verified each time the computer program is applied, the dedication guidance in this report does not apply. Quality controls consistent with Criterion III (Design Control) of 10CFR50, Appendix B are applied to the results obtained through use of the computer program.

1.4 Scope and Content of This Report

Figure 1-3 illustrates the scope and content included in this report.

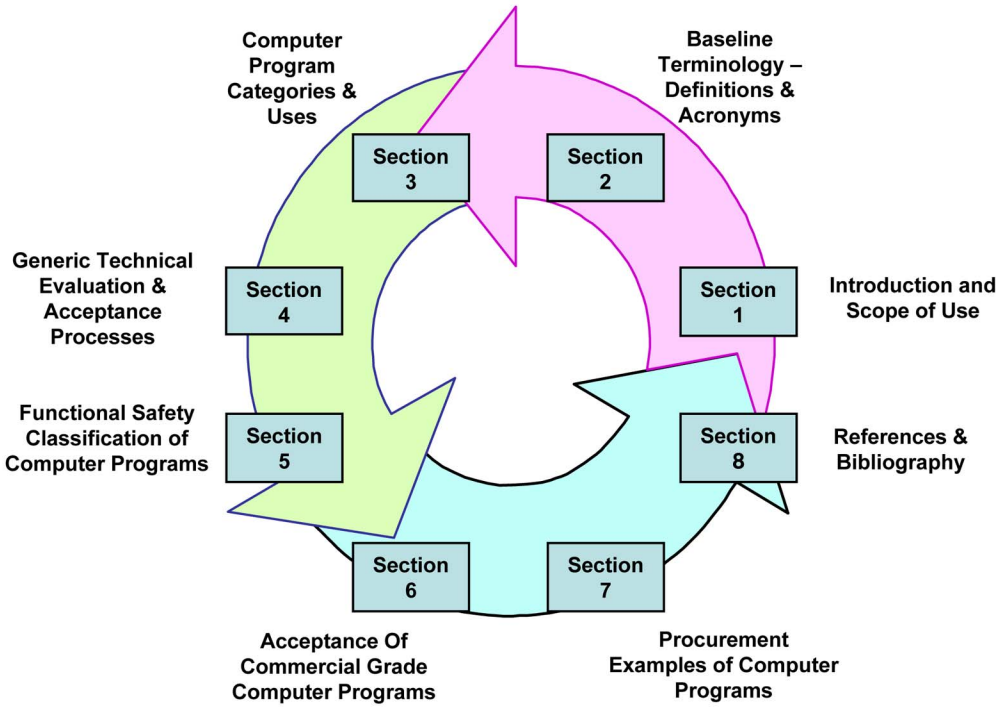


Figure 1-3
Scope and Content of the Report

As shown in the figure, Section 1 is an introduction to the guidance contained in the body of the report. Section 2 provides baseline terminology to establish some commonality of various terms used in the nuclear information technology and procurement areas. Definitions of key terms and acronyms of terms used in the report are provided. Section 3 provides an overview of the different categories of computer programs used at nuclear power plants and the degree to which each type is discussed in this report.

The main focus of the report is the technical evaluation and acceptance guidance contained in Sections 4, 5, and 6. Section 4 discusses these two processes in generic terms. Section 5 discusses how the technical evaluation should be implemented, including safety classification. Section 6 provides guidance for accepting commercial-grade computer programs intended for nuclear safety-related applications. And finally, Section 7 provides illustrative examples of how commercial-grade computer programs might be procured. References are provided in Section 8.

Appendix A contains guidance for specifying technical, quality, and documentation requirements. Appendix B provides practical quality assurance considerations for software dedication. Appendix C provides computer program categories and uses.

1.5 Background

Organizations supporting nuclear power plants maintain an SQA program that has been implemented as part of their overall quality assurance program. Due to the complexities and specialized knowledge associated with computer programs, acceptance activities for software have been conducted in accordance with SQA program requirements. Consistency in methodology employed by utilities is promoted by participation in an industry organization known as Nuclear Information Technology Strategic Leadership (NITSL, formerly Nuclear Utility Software Management Users Group or NUSMG). Similar to utilities, suppliers supporting the nuclear industry generally maintain individual SQA programs, although suppliers were typically not able to access NITSL guidance.

Due to the complexities and specialized knowledge associated with computer programs, acceptance activities for commercial-grade computer programs were not necessarily conducted under the same commercial-grade dedication programs and procedures that were used for accepting commercial-grade items. However, acceptance activities for computer programs were performed under the auspices of the accepting entity's quality assurance program.

In late 2010, the U.S. Nuclear Regulatory Commission (NRC) made presentations in several public forums where they clearly indicated that software can be used in a manner that would result in the software being considered a basic component. In June of 2010, the U.S. NRC endorsed American Society of Mechanical Engineers (ASME) NQA-1-2008 (Edition) [7] and NQA-1a-2009 (Addenda) [8] as a quality assurance program that the NRC considers acceptable for complying with the provisions of Title 10 of the Code of Federal Regulations, Part 50, Domestic Licensing of Production and Utilization Facilities (10 CFR Part 50) [9], and Title 10 of the Code of Federal Regulations, Part 52, Licenses, Certifications, and Approvals for Nuclear Power Plants (10 CFR Part 52) [10].

As of March 2012, no operating units in the United States were currently committed to NQA-1-2008 and NQA-1a-2009. However, some suppliers that support operating plants maintain quality assurance programs that comply with the latest edition and addenda of the standard. NQA-1a-2009, requires that "otherwise acquired" software (software that was not developed in accordance with the requirements of Parts I and II of the NQA-1 Standard [8]) must be accepted using commercial-grade item dedication methodology prior to use as a basic component in a safety-related application. The requirement specifically references NQA-1, Part I, Requirement 7, and Part II, Subpart 2.14 [8], Quality Assurance Requirements for Commercial Grade Items and Services, for guidance on commercial-grade dedication.

In discussions pursuant to development of this report, NRC staff emphasized that they consider commercially produced computer programs used in certain applications (such as design and analysis of safety-related SSCs to be safety-related and that safety-related items must be either designed and manufactured in accordance with a quality assurance program that meets the requirements of 10CFR, Part 50, Appendix B [1] or dedicated for use as a basic component in a

safety-related application in accordance with the requirements of 10CFR, Part 21 [2]. The NRC staff also communicated their expectation that when the computer program is dedicated, the acceptance process should be documented in the form of a commercial-grade item dedication evaluation.

1.6 Basic Premises

1.6.1 Consistency with Previously Published/Endorsed EPRI Reports

The guidance presented in this report is consistent with previously published/endorsed EPRI technical reports that address nuclear procurement processes, which include:

- *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*, TR-107330 [11]
- *Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications (NCIG-07)*, NP-5652 [4]
- *Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications*, TR-106439 [6] and U.S. NRC Safety Evaluation Report "Review of EPRI Topical Report TR-106439, *Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications*," Adams Accession number 9810150223 [3]
- *Guidelines for the Technical Evaluation of Replacement Items in Nuclear Power Plants*, 1008256 [12]
- *Handbook for Evaluating Critical Digital Equipment and Systems*, 1011710 [13]
- *Plant Support Engineering: Information for Use in Conducting Audits of Supplier Commercial Grade Item Dedication Programs*, 1016157 [14]
- *Supplemental Guidance for the Application of EPRI Report NP-5652 on the Utilization of Commercial Grade Items*, TR-102260 [5]

The suggested methods for performing the technical evaluation and acceptance process are identical to those described in the EPRI reports developed in response to the Nuclear Management and Resources Council (NUMARC, now the Nuclear Energy Institute) industry procurement initiative of the early 1990s [15], and that have been effectively implemented by both licensees and nuclear suppliers since that time. Guidance provided in this report builds upon current industry practice, lessons learned, and existing regulatory requirements.

1.6.2 Suitability of the Design

One of the basic premises derived from the definition of *dedication* in 10CFR21 [2] is that dedication is an acceptance process. The suitability of design must be established prior to initiating procurement of the item. In other words, the technical evaluation and acceptance activities involved in dedication are not substitutes for design; they may not be used to change the design of a given item, nor are they a means to verify the suitability of a given design.

The organization purchasing an item communicates design requirements in purchasing documents or specifications and selects a product that meets the applicable design requirements. In some cases, the design of the item must be qualified through testing or analysis as meeting the applicable design requirements. Once design qualification and selection of the item to be procured is completed, procurement can begin. Design requirements are translated into appropriate technical procurement specification requirements, including an acceptance plan that will provide reasonable assurance that the design requirements are met. Together, these processes should provide reasonable assurance that the item being procured will perform its safety-related functions.

1.6.3 Suitability of Computer Program Designs

For the purposes of this report, the term *suitability* is used in the same context as it is used when verifying the suitability of equipment design. Qualification of computer programs entails knowledge of the manufacturer's or developer's life-cycle process, which in the case of commercially available computer programs may not always be accessible to end users.

This being the case, licensees may not be able to use commercial software in safety-related applications by reliance on the qualification activities performed by the commercial supplier. Instead, commercial-grade dedication may be the only feasible option, which for commercial-grade computer programs being procured, is described in Sections 3 and 4 of this report.

1.6.4 Application of the Guidance in This Report

This report has been prepared for use by both nuclear licensees (domestic and international) and nuclear suppliers.

1.6.5 Computer Programs Previously Accepted Via Quality Assurance Programs

The guidance in this document is intended to ensure future procurements of commercial-grade computer programs for use in safety-related applications include the technical evaluation and acceptance activities required to perform adequate commercial-grade item dedication. This report is not intended to create new requirements in addition to those described in existing nuclear QA and SQA programs, but rather to provide methodologies and tools for more effectively accepting computer programs in accordance with regulatory, licensing, and customer expectations.

Similarly, the guidance in this report need not be used for providing additional assurance of the quality of computer programs that have already been accepted for use in accordance with nuclear QA/SQA programs. As noted in the Executive Summary, this guidance is not intended to be used for assuring the quality of computer programs used in safety-related applications that have been accepted prior to the issuance of this guidance, provided the following conditions have been met, as illustrated in Figure 1-4:

1. Evidence of the following activities exists for the computer program:

    a. Established capabilities and limitations for its intended end use were identified and proven.

    b. The intended use is within parameters previously approved.

2. The computer program has been controlled under the supplier/licensee's QA program.

Illustrative examples demonstrating the use of this methodology described in Figure 1-4 are provided in Section 7 of this report.

However, changes in or expansion of the use of the computer program or a revision to the computer program itself (for example, software updates) should subject the computer program to the guidance contained here. Each licensee or nuclear supplier should address the adequacy of past procurement activities on a case-by-case basis.

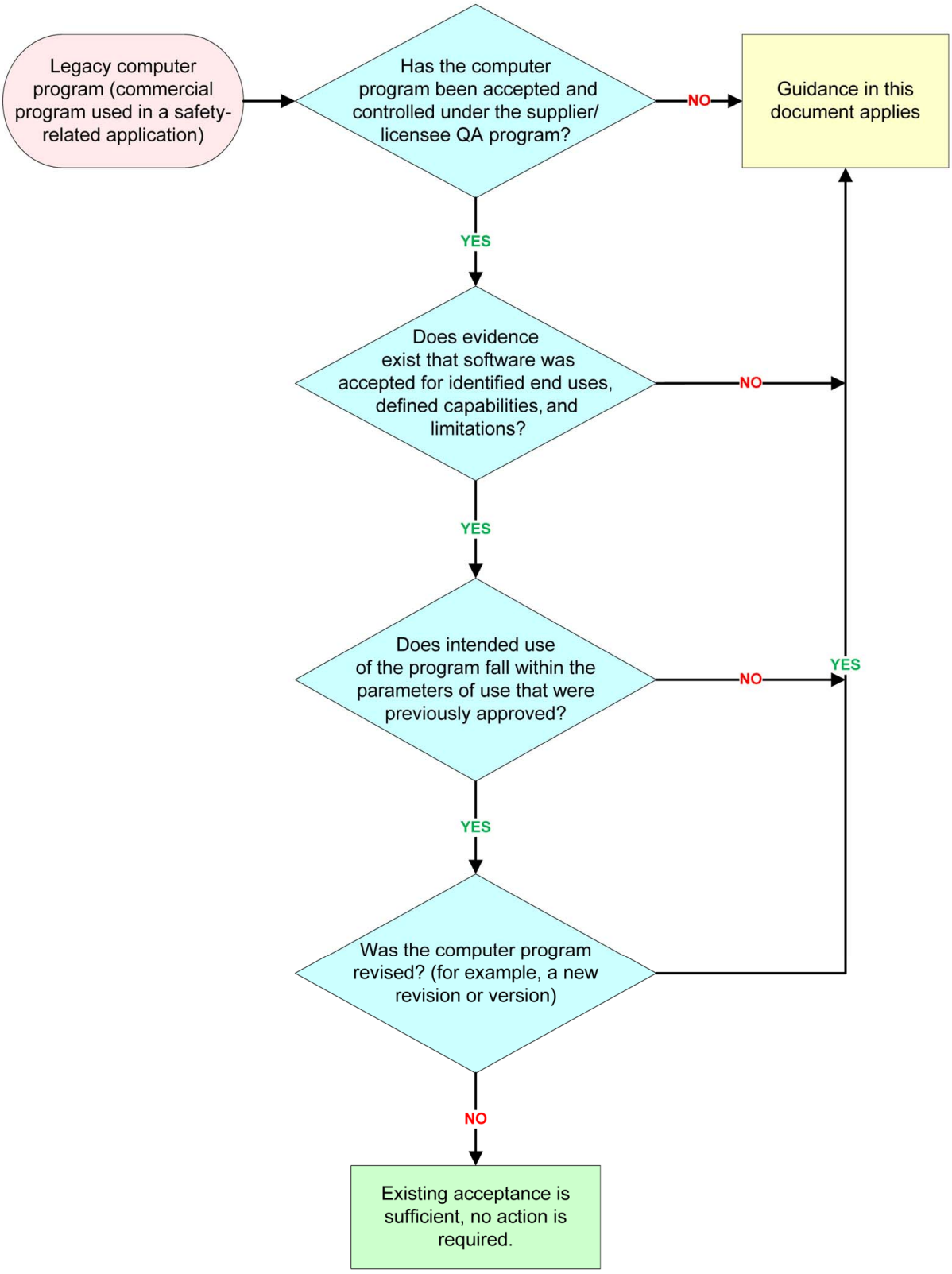


Figure 1-4
Applicability of This Guidance to Legacy Computer Programs

1.6.6 Maintenance of Computer Programs and Operating Systems

Initial identification of the computer program (version, build, and so forth) being procured is necessary. Identification characteristics are discussed in Section 6 of this report.

Maintenance and configuration management of computer programs and their operating systems subsequent to initial acceptance are outside the scope of this document. Although these activities are important, they are not part of the dedication acceptance process. Guidance regarding the installation of patches, auto-updates, etc. to computer programs or their operating systems is not provided in this report, and the licensee or nuclear supplier is encouraged to implement the appropriate controls described in their current quality assurance program.

1.6.7 Adoption of ASME NQA-1a-2009

Special care should be taken by organizations adopting the requirements of ASME NQA-1a-2009 [8], which includes modified criteria for accepting software that has not been previously approved under a QA program consistent with ASME NQA-1a-2009 requirements. For "Otherwise Acquired Software" (Part II, Subpart 2.7, Paragraph 302), the 2009 addendum prescribes using Part I, Requirement 7, and Part II, Subpart 2.14, Quality Assurance Requirements for Commercial Grade Items and Services. This guidance would apply to organizations that want to do any of the following :

1. Operate under an ASME NQA-1a-2009 [8] compliant Quality Program.

2. Augment a pre-NQA-1a-2009 [8] Quality Program to use commercial-grade dedication as the process for satisfying paragraph 302, "Otherwise Acquired Software."

3. Facilitate a future adoption of ASME NQA-1a-2009 [8] by proactively incorporating commercial-grade dedication in their quality processes.

Conditions 2 and 3 are not mandatory and can be executed at the discretion of an organization. Furthermore, since conditions 2 and 3 are voluntary, this implies no requirement to reassess computer programs used in previously executed analysis and design. Once an organization institutes procedures to comply with ASME NQA-1a-2009 Part II, Subpart 2.7, paragraph 302, non-complying computer programs [8] (that is, legacy programs) must be brought up to the standard before they can be used.

Section 2: Baseline Terminology – Definitions and Acronyms

2.1 Introduction

Terminology associated with computer programs or software is defined in a wide variety of codes and standards. Definitions for terms are not always consistent from one standard to another standard or among various user communities.

2.2 Definitions of Key Terms

acceptance	The employment of methods to produce objective evidence that provides reasonable assurance that a commercial-grade item to be used as a basic component will perform its intended safety function Reference EPRI NP-5652 [4] and 10CFR21 [2].
audit	A planned and documented activity performed to determine by investigation, examination, or evaluation of objective evidence the adequacy of and compliance with established procedures, instructions, drawings, and other applicable documents and the effectiveness of implementation. An audit should not be confused with surveillance or inspection activities performed for the sole purpose of process control or product acceptance. Reference ASME NQA-1a-2009 [8].
augmented quality	As used in this report, *augmented quality* is an optional subset of the classification category non-safety-related. It may be applied to any item that is subject to non-safety-related regulatory requirements or special requirements imposed by the utility. The scope of the classification category is station specific. Reference EPRI NP-6895 [16].

basic component	An item procured either as safety-related or as a commercial-grade item that has been accepted and dedicated for safety-related application. Reference EPRI NP-5652 [4].
classification	A documented technical evaluation process that results in the determination of an item's safety classification, design requirements, (including environmental and seismic qualification), and QA requirements. Adapted from EPRI TR-102260 [5].
commercial-grade item (CGI)	A structure, system, or component, or part thereof that affects its safety function that was not designed and manufactured as a basic component. Commercial-grade items do not include items where the design and manufacturing process requires many in-process inspections and verifications to ensure that defects or failures to comply are identified and corrected (that is, one or more critical characteristics of the item cannot be verified). Reference the 1995 revision of 10CFR21 [2]. An item is a commercial-grade item if its critical characteristics can be verified during the dedication process. Reference the NEI clarification of the NRC definition included in the 1995 revision of 10CFR21 [2].
commercial-grade survey	Activities conducted by the purchaser or its agent to verify that a supplier of commercial-grade items controls, through quality activities, the critical characteristics of specifically designated commercial-grade items as a method to accept those items for safety-related use. Reference EPRI NP-5652 [3].
commercial supplier	An organization in the supply chain that does not provide items in accordance with a quality assurance program that meets the requirements of 10CFR50, Appendix B [1].
computer program	A combination of computer instructions and data definitions that enables computer hardware to perform computational or control functions (Reference ASME NQA-1a-2009 [7])
credible failure mechanism	The manner by which an item may fail, degrading the item's ability to perform the component or system function under evaluation. Reference IEEE STD. 500-1984 [17].

critical characteristics	The important design, material, and performance characteristics of a CGI that—once verified—will provide reasonable assurance that the item will perform its intended safety function. Reference the 1995 revision of 10CFR21 [2].
critical characteristics for acceptance	Identifiable and measurable attributes/variables of a commercial-grade item, which once selected to be verified, provide reasonable assurance that a commercial-grade item to be used as a basic component will perform its intended safety function.
critical characteristics for design	The properties or attributes that are essential for the item's form, fit, and functional performance. Critical characteristics for design are the identifiable and/or measurable attributes of a replacement item that provide assurance that the replacement item will perform its design function. Reference EPRI 1008256 [12].
dedicating entity	The organization that performs the dedication process. Dedication may be performed by the manufacturer of the item, a third-party dedicating entity, or the licensee itself. Reference the 1995 revision of 10CFR21 [2].
dedication	An acceptance process that is undertaken to provide reasonable assurance that a commercial-grade item to be used as a basic component will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under a 10CFR50, App. B QA program. Reference 1995 revision of 10CFR21 [2].
design function	The operation that an item is required to perform to meet the component or system design basis. Reference EPRI 1008256 [12].
development	The process by which computer programs (including source code) are written or modified. Reference NITSL-SQA-2005-02 [18].
equivalency evaluation	A technical evaluation performed to confirm that an alternative item, not identical to the original item, will satisfactorily perform its design function. Reference EPRI 1008256 [12].

equivalent change	A change that does not result in a change to those bounded technical requirements that 1) ensure performance of design basis functions, or 2) ensure compliance with the plant licensing bases of either the item(s) or applicable interfaces. Reference EPRI TR-1008254 [19].
failure	A mechanism that prevents an item from accomplishing its function. Reference EPRI NP-6895 [16].
failure mode	The effects or conditions that result from an item's credible failure mechanisms. Reference EPRI 1008256 [12].
failure modes and effects analysis	An evaluation of an item's credible failure mechanisms and their effect on system and/or component function. Reference EPRI 1008256 [12].
graded approach	The selective assignment of the quality assurance elements that the software must comply with based on its assigned quality classification. This is determined by the evaluation of the functional process(es) that the software supports. Reference NITSL-SQA-2005-02 [18].
legacy software	A term used to describe computer software that has been accepted by means other than those described in the most current regulatory/licensing/QA requirements.
like-for-like procurement	The replacement of an item with an item that is identical. Reference EPRI 1008256 [12].
non-process computer program	Computer program applications that do not run on permanent plant equipment; that is, they are not installed in plant systems, structures, or components.
nuclear supplier	An organization in the supply chain that has developed a nuclear quality assurance program and, as such, is capable of furnishing basic components and must comply with the requirements of 10CFR21 [2].

performance-based supplier audit	An audit using a methodology that evaluates processes or activities on the basis of their performance and allows subsequent conclusions about the products of the process or activity and the quality assurance program of the supplier audited. Reference EPRI NP-6630 [20].
post-installation tests	Activities conducted after installation of a commercial-grade item to verify required critical characteristics prior to placement in operation. An element of the "Special Tests and Inspection" method to accept an item for safety-related use. Reference EPRI NP-5652 [4].
process computer program	Any computer program that controls, monitors, interfaces, or communicates with permanent plant equipment governed by the design change process.
procurement document	Contractually binding documents that identify and define the requirements that items or services must meet in order to be considered acceptable by the purchaser. Reference EPRI TR-102260 [5].
qualification: computer program	The process for ensuring that a computer program design is suitable for its intended application. (See software verification and validation.)
qualification: personnel	The characteristics or abilities gained through education, training, or experience, as measured against established requirements, such as standards or tests that qualify an individual to perform a required function. Reference ASME NQA-1a-2009 [8].
qualification: supplier	The process used to establish that a supplier is adequately implementing their quality assurance program requirements and, as such, is capable of furnishing an acceptable item or service as defined by the customer. Adapted from EPRI NP-6630 [20].
reasonable assurance	A justifiable level of confidence based on objective and measurable facts, actions, or observations from which adequacy can be inferred. Reference EPRI TR-102260 [5].
replacement item	An item that replaces an original or installed item, either identical or alternate. Reference EPRI 1008256 [12]

safety-related

A plant structure, system, component, part, or item used in a nuclear power plant that is relied upon during or following design basis accidents to assure:

1. The integrity of the reactor coolant pressure boundary,
2. The capability to shut down the reactor and maintain it in a safe shutdown condition, or
3. The capability to prevent or mitigate the consequences of accidents which could result in potential offsite radiation exposures comparable to those referred to in l0CFR Part 100.11.

Safety-related services include design, engineering, testing, inspecting, and consulting services which could, if they contained defects, create a substantial safety hazard. Examples of these types of safety related services and software are:

- Nondestructive examination of safety-related welds,
- Design of safety-related pipe hangers and supports,
- Seismic and geologic surveys for a reactor site,
- Specification of safety-related hardware characteristics,
- Computer codes for reactor analysis,
- Emergency procedures, and
- Fire protection inspections by fire consultants

Reference 10CFR21.3 [2], 10CFR50.49 [21], and 10CFR100, Appendix A [22], NUREG 0302, Revision 1 [23], Review of EPRI topical report TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications” [3].

software

Computer programs and associated documentation and data pertaining to the operation of a computer system. Reference ASME NQA-1a-2009 [8].

software configuration management

Procedures that include, but are not limited to configuration identification, change control, and status control. Reference ASME NQA-1a-2009 [8].

software life cycle	The period of time that begins when a software product is conceived and ends when the software is no longer available for use. Reference NITSL-SQA-2005-01 [24].
software quality assurance (SQA)	The program that establishes quality controls for the development, procurement, operation, use, maintenance, and retirement of software commensurate with its importance to nuclear safety. Reference NITSL-SQA-2005-01 [24].
software verification and validation	Processes that determine whether the development products of a given activity conform to the requirements of that activity and whether the software satisfies its intended use and the user needs. Reference IEEE 1012 [25].
source verification	Activities witnessed at the supplier's facilities by the purchaser or its agent for specific items to verify that a supplier of a commercial-grade item controls the critical characteristics of that item, as a method to accept the item. Reference EPRI NP-5652 [4].
special tests and inspection	Activities conducted after the receipt of a commercial-grade item to verify one or more critical characteristics as a method to accept the item for safety-related use. Reference EPRI NP-5652 [4].
standard receipt inspection	Activities conducted upon receipt of items including commercial-grade items in accordance with ANSI N45.2.2-1978 [26] or other applicable quality assurance standard to check such elements as the quantity received, part number, general condition of items, and damage. Adapted from EPRI NP-5652 [4].
supplier	The organization furnishing a commercial-grade item or basic component. This could include an original equipment manufacturer, part manufacturer, or distributor. Reference EPRI NP-5652 [4].
system	A group of subsystems united by some interaction or interdependence, performing many duties but functioning as a single unit. Reference EPRI TR-102260 [5].

technical evaluation	An evaluation performed to ensure that the correct technical requirements for an item are specified in a procurement document. Reference EPRI NP-5652 [4].
technical requirements	Parameters that define the function or performance of a given SSC in a particular application/end use or group of applications/end-uses. Reference EPRI TR-1008254 [19].
validation	Confirmation by examination and provisions of objective evidence that the particular requirements for a specific intended use are fulfilled. Reference IEEE 1012-1998 [25].
verification	Confirmation by examination and provisions of objective evidence that specified requirements have been fulfilled. Reference IEEE 1012-1998 [25].

2.3 Acronyms

ANS – American Nuclear Society

ANSI – American National Standards Institute

AOP – abnormal operating procedure

ARP – alarm response procedure

ASME – ASME International (formerly American Society of Mechanical Engineers)

CDR – critical digital review

CFR – Code of Federal Regulations

CGI – commercial-grade item

CMMI - capability maturity model integration

COTS – commercial off-the-shelf

DOE – Department of Energy

EAM – enterprise asset management

EOP – emergency operating procedure

EPRI – Electric Power Research Institute

ERP – enterprise resource planning

EPROM – erasable programmable read-only memory

FAC – flow-accelerated corrosion

FMEA – failure modes and effects analysis

FSAR – Final Safety Analysis Report

IEEE – Institute of Electrical and Electronics Engineers

ISO – International Standards Organization

M&TE – measurement and test equipment

NCIG – Nuclear Construction Issues Group

NEI – Nuclear Energy Institute

NITSL - Nuclear Information Technology Strategic Leadership

NP – nuclear power

NRC – Nuclear Regulatory Commission

NSSS – nuclear steam system supplier

NUMARC – Nuclear Utility Management and Resource Council, now the Nuclear Energy Institute

NUSMG – Nuclear Utility Software Management Users Group

PROM – programmable read-only memory

QA – quality assurance

R&D – research and development

SEI - Software Engineering Institute

SME – subject matter expert

SQA – software quality assurance

SSC – structure, system, or component

TR – technical report

V&V – verification and validation

Section 3: Types of Design and Analysis Computer Programs

The purpose of this section is to discuss various types of design and analysis computer programs addressed in the scope of this report. Examples of other computer programs are included in Appendix C.

3.1 Examples of Design and Analysis Computer Programs

Design and analysis computer programs are the primary focus of this report. Examples of these types of computer programs may include (depending on the use of the output):

- Piping stress and flexibility analysis computer programs such as NU-Pipe II, SuperPipe, ADLPipe, and CAESAR-II[1]
- Steady-state thermal-hydraulics and pipe flow analysis programs such as AFT Fathom[2]
- Accident analysis programs such as CFAST, ALOHA, MACCS2, EPIcode, GENII, Hotspot, IMBA, and MELCOR[3]
- Finite element analysis computer programs such as GT Strudl[4]
- Electrical power system computer programs such as ETAP[5]
- Engineering simulation computer programs such as ANSYS[6]

[1] NU-Pipe II is a trademark of Quadrex Energy Systems; SuperPipe is a trademark of ABB Impell; ADLPipe is a trademark of ADLPIPE., Inc.; and CAESAR-II is a trademark of Intergraph Cadworx & Analysis Solutions, Inc.

[2] AFT Fathom is a trademark of Applied Flow Technology.

[3] CFAST is a trademark of the U.S. Department of Commerce, National Institute of Standards and Technology (NIST); ALOHA is a trademark of the U.S. Department of Commerce, National Oceanic and Atmospheric Administration (NOAA; MACCS2 is a trademark of the U.S. NRC and Sandia National Laboratories; EPIcode is a trademark of Homann Associates, Inc.; GENII is a trademark of Pacific Northwest National Laboratory; Hotspot is a trademark of Lawrence Livermore National Laboratories; IMBA is a trademark of United Kingdom Health Protection Agency; and MELCOR is a trademark of the U.S. NRC and Sandia National Laboratories.

[4] GT Strudl is a trademark of Georgia Tech CASE Center Research and Development Team.

[5] ETAP is a registered trademark of ETAP automation, Inc.

[6] ANSYS is a trademark of ANSYS, Inc.

Products like these that are not purchased as a basic component from a supplier that maintains a nuclear quality assurance program (that complies with the requirements of 10CFR50, Appendix B [1]) and assumes responsibility for reporting of defects and noncompliance in accordance with 10CFR21 [2] are considered commercial-grade computer programs.

The examples included are intended to illustrate the types of computer programs that might be used in safety-related design and analysis applications.

Note that some of the examples of computer programs included in Section 3.1 may be available as both commercial software or as basic components from the supplier that developed the computer program or from a third-party supplier who has dedicated the computer program and can furnish it as a basic component. A computer program purchased as a basic component from a supplier that maintains a nuclear quality assurance program (that complies with the requirements of 10CFR50, Appendix B [1]) and assumes responsibility for reporting of defects and noncompliance in accordance with 10CFR21 [2] does not need to be dedicated.

Section 4: Generic Technical Evaluation and Acceptance Processes

The purpose of this section is to provide guidance for implementing the technical evaluation process associated with commercial-grade computer program dedication.

4.1 Overview of Commercial-Grade Dedication

As shown in Figure 4-1, successful commercial-grade dedication involves two key elements. First is the technical evaluation, which ensures that the computer program is classified and specified correctly. Second is the acceptance process, which provides reasonable assurance that the computer program procured meets specified requirements.

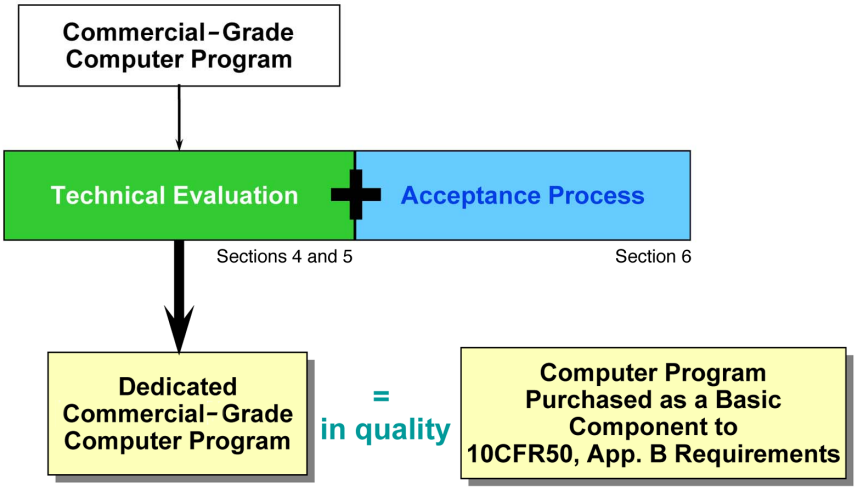


Figure 4-1
Key Elements of Commercial-Grade Dedication [4]

Together, the technical evaluation and acceptance processes constitute dedication, which in accordance with the definition in 10CFR21 [2], should:

> …provide reasonable assurance that a commercial grade item to be used as a basic component will perform its intended safety function, and in this respect, is deemed equivalent to an item designed and manufactured under a 10CFR50, App. B QA program.

Consistent with the requirements provided in ASME NQA-1 [8], the following key points should be considered when dedicating commercial-grade computer programs that have been classified as safety related:

- The acquired computer program should be identified and controlled during the dedication process.
- The dedication process should be documented and include the following:
  - Identification of the capabilities and limitations for intended use as critical characteristics
  - Utilization of test plans and test cases as the method of acceptance to demonstrate the capabilities within the limitations
  - Instructions for use (for example, the user manual) within the limits of the dedicated capabilities
- The dedication process should be documented, and the performance of the actions necessary to accept the software should be reviewed and approved. The resulting documentation and associated computer program(s) should establish the current baseline.

As depicted in Figure 4-2, the procurement process begins after completion and verification of the design. Although dedication is primarily an acceptance activity, it involves many elements of the technical evaluation.

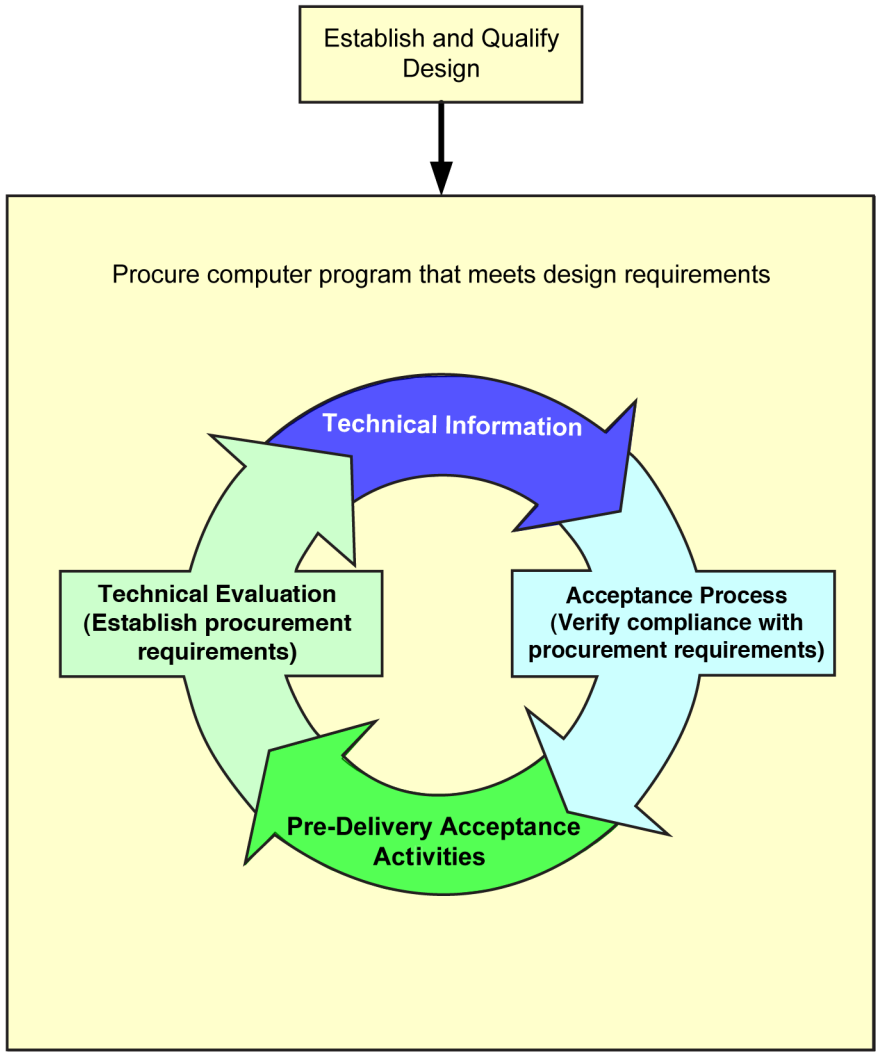


Figure 4-2
Technical Evaluation and Acceptance Interdependencies

Technical information derived from the technical evaluation process is necessary to establish acceptance criteria, and in some cases, additional evaluation and information may be required to support acceptance. Likewise, technical and quality requirements may need to be updated to reflect activities necessary to support acceptance, such as commercial-grade surveys and source surveillance.

Figure 4-3 illustrates the relationship between the technical evaluation and acceptance processes in more detail by depicting the generic process for commercial-grade dedication based on the original process published in EPRI NP-5652 [4]. The flow chart has been modified for the purposes of this report to denote a computer program instead of "item," but the basic flow of procurement activities remains unchanged.

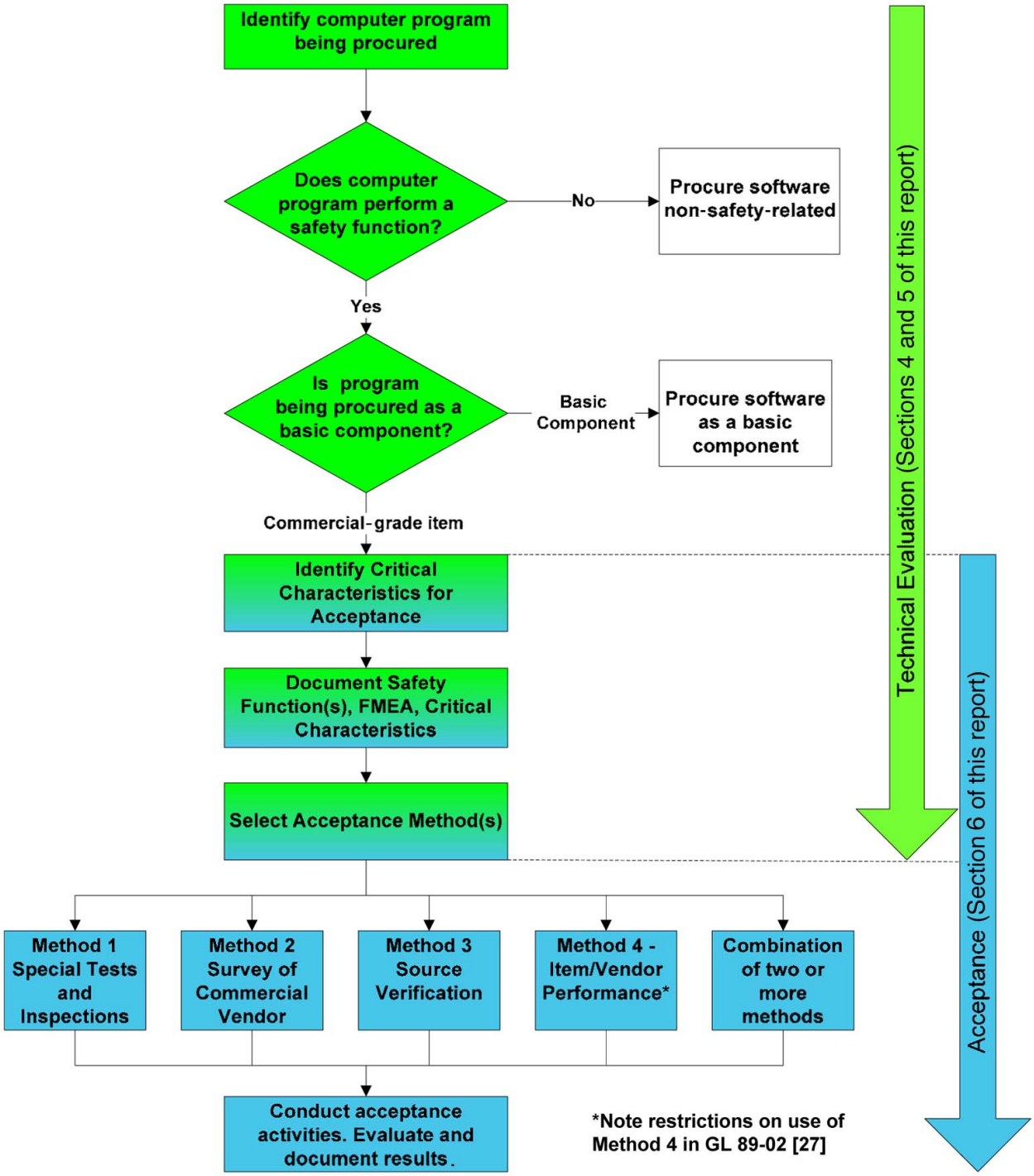


Figure 4-3
Generic Process for Commercial Grade Dedication

Of particular note is the reiteration of the four acceptance methods (that is, the means to verify selected critical characteristics), which remain identical to those in EPRI NP-5652. As the figure illustrates, acceptance methods associated with commercial-grade dedication include:

1. Special tests and inspections
2. Commercial-grade surveys
3. Source verification
4. Acceptable item/supplier performance record

Organizations performing commercial dedication have the latitude to use one or more of these methods, as appropriate (that is, two or more in combination). U.S. NRC Generic Letter 89-02 [27] and Information Notice 2011-01 [28] provide conditions applicable to the use of Methods 2 (commercial-grade surveys) and 4 (acceptable item/supplier performance record).

4.2 Generic Process for Technical Evaluation

The generic process for technical evaluation of replacement items is outlined in EPRI 1008256, *Plant Support Engineering: Guidelines for the Technical Evaluation of Replacement Items in Nuclear Power Plants, Revision 1* [12]. A technical evaluation for computer program would typically include the following key elements shown in Table 4-1.

Table 4-1
Key Elements of the Technical Evaluation

Technical Evaluation Element	Source of Implementation Guidance
Identifying the computer program scope of use and function	Based upon the dedicating entity's application(s).
Determining the *safety classification* of the computer program being procured, and identifying applicable safety functions	Refer to Section 5 of this report.
Performing failure modes and effects analyses to help identify if failure of the computer program could result in failure of plant SSCs and to identify characteristics of the computer program necessary to ensure that it will perform its safety functions	Refer to Sections 5 and 6 of this report.
Identifying the critical characteristics and acceptance methods that will be used to verify critical characteristics	Refer to Section 6 of this report.
Specifying the appropriate technical, quality, and documentation requirements	Refer to Appendix A of this report.

Table 4-1 (continued)
Key Elements of the Technical Evaluation

Technical Evaluation Element	Source of Implementation Guidance
When necessary, determining the *suitability of a proposed replacement computer program* that is not identical to the original	Refer to current industry guidance regarding the verification and validation of updated versions/editions of computer programs.
Documenting the technical evaluation and ensuring that provisions are in place to document the acceptance process and results of acceptance activities	Refer to Sections 5 and 6 of this report.

4.3 Generic Process for Acceptance of Computer Software

The technical evaluation and functional safety classification processes depicted in Figures 4-1 and 4-2 are discussed in detail in Section 5 of this report. The acceptance process, including the selection and verification of critical characteristics, are discussed in detail in Section 6 of this report.

Section 5: Functional Safety Classification of Computer Programs

Functional safety classification provides a way to group items in accordance with their relative importance to facilitate the application of appropriate quality assurance controls and processes. The following explanation of safety classifications is based upon EPRI NP-6895 [16] and 10CFR21 [2] and is adapted to specifically address computer programs.

Classification of a computer program that is not integral to a structure, system, or component can be similar to the classification processes that licensees routinely perform when procuring replacement items and services. Classification facilitates proper procurement, installation, testing, operation, and maintenance activities. The classification process is typically included in the technical evaluation and should be performed by qualified engineering or technical personnel.

The safety classification of an item typically has a direct impact on its design requirements, quality assurance requirements, technical procurement requirements, and acceptance requirements. Figure 1-2 in this report shows how the safety classification of a computer program is related to the guidance in this document.

5.1 Functional Safety Classification Categories

The two functional safety classifications are **safety-related** and **non-safety-related**. A subset of non-safety-related items may be classified as **augmented quality**.

5.2 Safety Classification Guidance

It is acceptable practice to conservatively assume that an item, service, or computer program performs a safety-related function and should be treated as a basic component. However, industry experience since the procurement initiatives of the early 1990s suggests that it is beneficial to perform a functional safety classification evaluation. Licensees and nuclear suppliers should make this determination on a case-by-case basis using the tools provided in this report, which are consistent with the guidelines developed since the industry procurement initiative.

Information Notice No. 86-77: Computer Program Error Report Handling [29], states the following:

> A computer program is a basic component use [*sic*] in 10 CFR 21 when used in a safety-related design activities [*sic*].

This statement is true for any item because an item is a basic component when it is used in a safety-related application. This statement should **not** be interpreted to mean that all computer programs are basic components. Similar to systems, structures, and components, computer programs should be evaluated and assigned a safety classification based upon how they are being used and the functionality that they provide. It is incumbent upon the entity using the computer program (licensee or nuclear supplier) to determine an appropriate safety classification on a case-by-case basis by evaluating the actual function(s) of the computer program and its intended end use(s). The technical evaluation should document the computer program's functional safety classification, safety function(s) and performance requirements, and application requirements (service conditions such as installed platform, requirements, etc.).

5.3 Options for Determining the Safety Classification

Figure 5-1 summarizes the options for classifying computer programs.

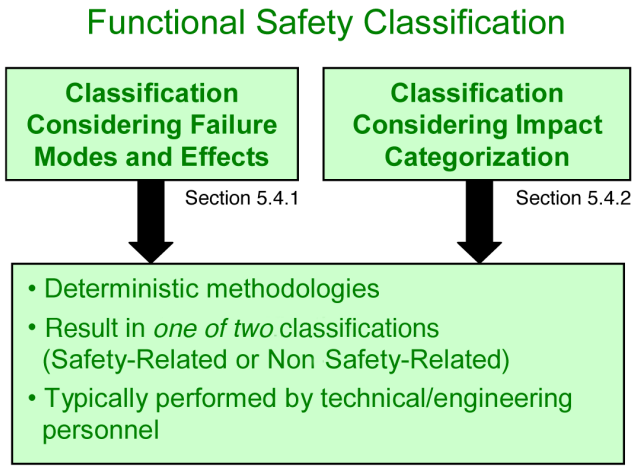


Figure 5-1
Options for Classifying Computer Programs

5.4 Functional Safety Classification

Functional safety classification is the process of evaluating an item to determine its safety classification based upon its function(s). The two basic safety classifications resulting from functional safety classification are **safety-related** and **non-safety-related**. As defined in 10CFR21 [2], items classified as safety-related are those items (structure, system, or component, or part thereof) that affect safety functions necessary to assure: (A) the integrity of the reactor coolant

pressure boundary; (B) the capability to shut down the reactor and maintain it in a safe shutdown condition; or (C) the capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to those referred to in §50.34(a)(1) [30]or §100.11 of Title 10 of the Code of Federal Regulations [22]. Items that are not safety-related are classified as non-safety-related.

A subset of non-safety-related items may be classified as **augmented quality** items. As referred to in this report, *augmented quality items* are items subject to non-safety-related regulatory requirements or other special requirements imposed by the licensee or nuclear supplier. The scope of items considered augmented quality is typically unique to each facility.

EPRI NP-6895, *Guidelines for the Safety Classification of Systems, Components, and Parts used in Nuclear Power Plant Applications* [16], documents the functional safety classification process for plant SSCs in detail.

The safety classification of computer programs is performed to determine if any function(s) performed by the computer program could prevent associated SSCs from performing their safety-related functions. If a postulated failure of a computer program (failure of a function performed by the computer program) could impact the ability of an associated SSC to perform its safety-related function(s), the computer program is safety-related. Therefore, functions of a computer program associated with SSCs should be identified as part of the safety classification process for computer programs.

As shown in Figure 5-1, there are two deterministic methodologies that result in a functional safety classification—one that considers failure modes and effects and one that considers the impact that the computer software has on associated SSCs. These two methodologies are discussed in the following sections.

5.4.1 Classification Considering Failure Modes and Effects

Figure 5-2 illustrates a methodology for functionally classifying a computer program by considering failure modes and effects. This methodology, which considers failure modes and their effects, has been successfully implemented since it was first introduced prior to the industry-wide procurement initiative in the early 1990s. The technical evaluation should include performing a documented failure modes and effects analysis (FMEA) to identify the credible failure mechanisms of the item in the specific application(s) under consideration.

When using FMEA to perform safety classification of plant SSCs, the effect of failure on the SSC(s) itself is evaluated. Application of this methodology differs when it is applied to safety classification of design and analysis computer programs. When using failure modes and effects analysis to perform safety classification of design and analysis computer programs, failure of the computer program must be extrapolated to determine if it could also result in failure of plant SSCs that the computer program is being used to design or analyze.

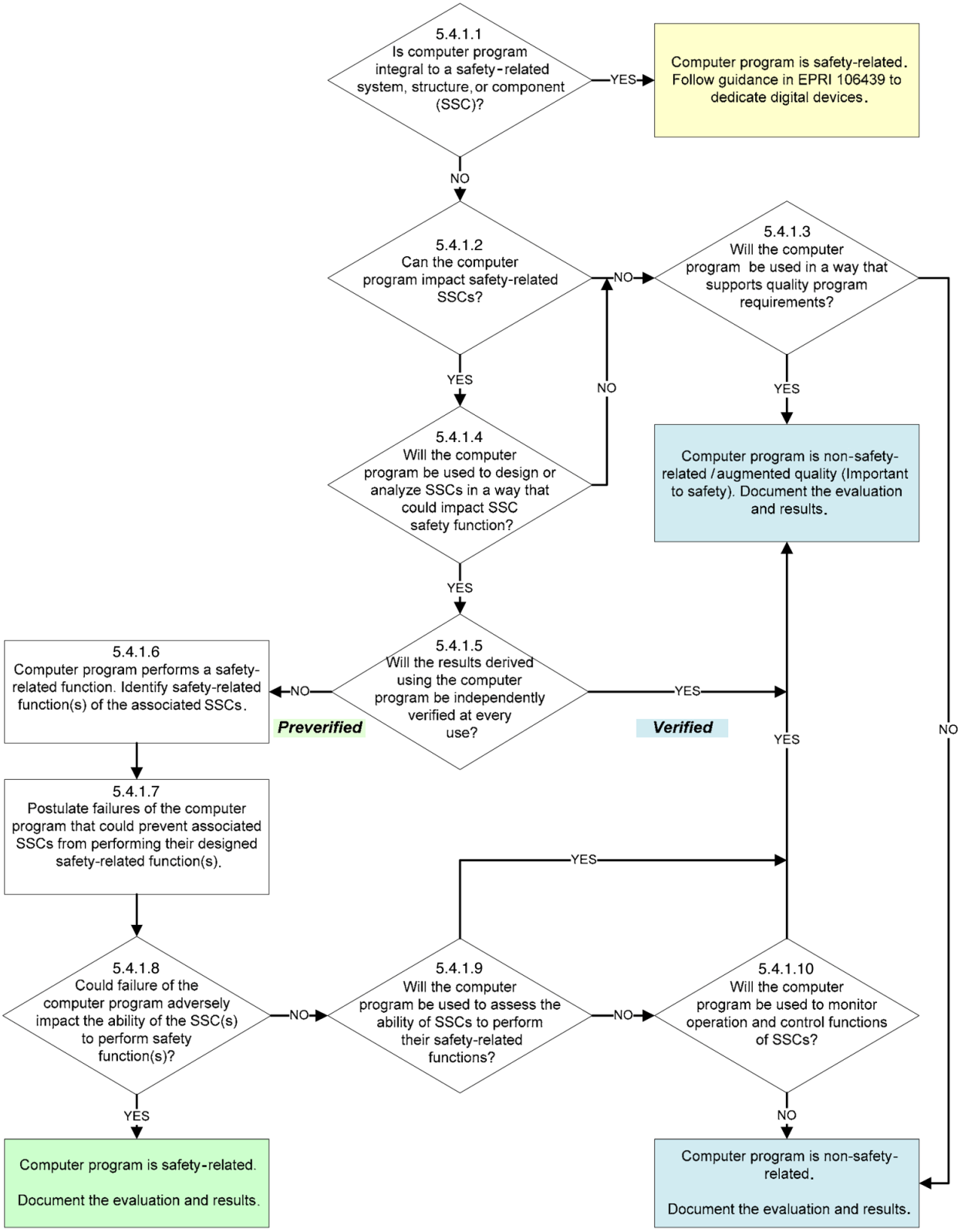


Figure 5-2
Functional Classification Considering Failure Modes and Effects

5.4.1.1 Is the Computer Program Integral to a Safety-Related SSC?

Determine if the computer program is integral to safety-related plant SSCs. If the computer program is integral to a safety-related SSC (for example, a computer program embedded in a programmable logic controller installed in the plant), the computer program is necessary for the component to perform its safety function(s), and the computer program should be classified as safety-related.

Appendix C, Section C.1 of this report, includes some discussion pertaining to computer programs that are integral to a safety-related SSC. Additional guidance for addressing digital equipment used in safety-related SSC's can be found in EPRI TR-106439, *Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications* [6], and EPRI TR-107339, *Evaluating Commercial Digital Equipment for High Integrity Applications: A Supplement to EPRI Report TR-106439* [31].

5.4.1.2 Can the Computer Program Impact Safety-Related SSCs?

This is a preliminary screening performed to determine if the computer program function(s) can impact safety-related SSCs. Computer program functions that typically impact SSCs include:

- The computer program is used to facilitate design of the safety-related SSC.
- The computer program is used to analyze how the safety-related SSC will function or withstand design conditions.
- The computer program is used to monitor operation or control functions of a safety-related SSC.

A computer program that cannot impact safety-related SSCs is non-safety-related.

5.4.1.3 Will the Computer Program Be Used in a Way That Supports Quality Program Requirements?

Determine if the computer program is used in a way that supports quality program requirements. Examples of this would be any of the following:

- The computer program is associated with a document control or records management system.
- The computer program is associated with a dose management system.
- The computer program is used for tracking corrective actions.
- The computer program is used to maintain training records and transcripts.
- The computer program used for emergency response preparedness.

In applications similar to those above, the computer program in itself does not meet the definition of safety-related, but is a tool used to implement quality assurance processes or controls necessary to implement 10CFR50, Appendix B [1] requirements. A computer program that is used in a way that supports quality program requirements is non-safety-related, but may be important to plant safety. As such, augmented quality controls should be considered.

5.4.1.4 Will the Computer Program Be Used to Design or Analyze SSCs in a Way That Could Impact SSC Safety Function(s)?

Determine if the computer program is used in a way that influences the design or use of an SSC in a way that could impact the SSC's ability to perform its designed safety functions.

Computer programs that may not have a direct active effect on an SSC's ability to perform safety functions may still affect the capability of the SSC to perform its intended safety function(s). For example, design computer program that is used to develop equipment design could indirectly affect the ability of the equipment being designed to perform its safety function(s) subsequent to manufacture and installation in the plant.

If the computer program is used to design or analyze SSCs in a way that could impact SSC safety functions, then it should be determined whether the results are independently verified. If the computer program is not used to design or analyze SSCs in a way that could impact SSC safety functions, then further evaluation of failure modes should be performed.

5.4.1.5 Will the Results Derived Using the Computer Program Be Independently Verified for Every Use?

Determine if the results (that is, the design output) provided by the computer program will be independently verified for each use of the computer program by other acceptable methods. The independent verification of the computer program results may be performed during the design process.

If the computer program is not providing the sole basis for design or analysis decisions, it may not be considered as safety-related. If the computer program is being relied upon as the sole basis for decisions that could impact the ability of safety-related SSCs to perform their intended safety function, then further evaluation of failure modes should be performed.

An example of independent verification might be verifying that the results obtained through the use of a commercial computer program are accurate by comparing them with results obtained by hand calculations or other computer program applications that have been evaluated and approved for the intended use.

Another example might be using an alternative method, such as seismic testing of a product prototype, to verify a product design based upon the use of a commercially available computer program. In this case, failure mechanisms of the computer program that result in inaccuracies could not adversely impact the ability of the SSC to perform safety functions because the worst outcome of using a faulted computer program would be design flaws that would be identified during seismic testing of the prototype (design verification).

5.4.1.6 Identify the Safety Functions Associated with the Computer Program

Understanding the functions of the computer program and the relationship between computer program functions and SSC functions is necessary to perform functional safety classification.

Typically, safety functions for safety-related SSCs are identified in plant information systems, procurement engineering evaluations, and system descriptions. The computer program functions that will be relied upon may include all capabilities of the computer program or a subset of specific functions.

Communication with computer program end users and subject matter experts may be required to clearly identify safety-related computer program functions.

When computer programs are used generically to address certain categories of SSCs, it may be appropriate to generically identify and characterize safety functions of the plant SSCs.

For example, if a computer program is used to perform analysis on safety-related piping, the associated SSC might be identified as "safety-related piping." The safety function of the plant SSCs could be described as "maintain pressure boundary integrity." (Subsequently, the effect of failure of the computer program could be described as "In the event computer program yields incorrect results, safety-related piping could lose the ability to maintain pressure boundary integrity at designed conditions."

5.4.1.7 Postulate Failures of the Computer Program That Could Prevent SSCs from Performing Their Designed Safety-Related Functions

The next step in the process is to determine how the computer program might fail and, in turn, prevent associated SSCs from performing their designed safety-related functions. Failure of the computer program must be extrapolated to determine if it could also result in failure of plant SSCs that the computer program is being used to design or analyze.

Failure modes and mechanisms for computer programs differ from failure modes and mechanisms typically associated with equipment because computer programs do not age or wear out in the sense that a mechanical or electrical device would.

A computer program can and does fail when it behaves in an unexpected way, fails to produce a result, or produces an erroneous result. Unknowingly using an erroneous result in a design or analysis process could, in turn, cause failure of the SSC(s) involved in the design or analysis.

The types of failures introduced during the design and development process may be common to many types of computer programs. In addition, a computer program may be subject to unique failures associated with specific functions, capabilities, and limitations of the computer program.

Common types of computer program failure mechanisms that may be postulated during the functional safety classification process and that would be evident once the program was designed are summarized in Table 5-1:

Table 5-1
Examples of Failure Mechanisms for Computer Programs

Postulated Failure	Description
Conceptual Error	Errors resulting when the computer program is applied outside its intended use or when the computer program is syntactically correct, but the programmer or designer intended it to do something else.
Arithmetic Error	Errors such as division by zero, stack over/underflow, and loss of precision resulting from incorrect programmatic calculations.
Interface Errors	Errors generated by or through incorrect interfacing of the computer program with other programs, hardware, or operating systems.

5.4.1.8 Could Failure of the Computer Program Adversely Impact the Ability of an SSC to Perform Its Safety Function?

Determine if postulated failure modes and mechanisms of the computer program would result in a situation that could adversely impact the ability of an SSC to perform its safety function. When considering failure of the computer program to perform safety classification, the effect of failure on the computer program must be extrapolated to determine the impact it might have on plant SSCs. For example, consider the failure of a computer program that causes inaccurate results to be used during a design or analysis process applicable to plant SSCs. Extrapolation would involve determining if use of the inaccurate calculations could result in failure of the plant SSC(s) (designed or analyzed using the computer program) to perform its safety-related function(s).

If postulated failure mechanisms of the computer program can result in inaccuracies or malfunctions that could lead to an adverse impact on the ability of SSCs to perform safety functions, then the computer program should be classified as safety-related. If postulated failure mechanisms of the computer

program cannot result in inaccuracies or malfunctions that could adversely impact the ability of SSCs to perform safety functions, then further evaluation is necessary to determine if it is used to assess SSC functionality or to monitor operation or control functions of SSCs.

5.4.1.9 Will the Computer Program Be Used to Assess the Ability of SSCs to Perform Their Safety-Related Function(s)?

Computer programs used to assess the ability of SSCs to perform their safety-related functions, but that do not directly impact SSCs capability to perform safety functions should be classified as non-safety-related, augmented quality.

Although this type of computer program is not safety-related, it is considered to be important to safety. Therefore, the dedicating entity may elect to implement appropriate controls similar to those included in elements of their nuclear quality assurance program. Additional guidance regarding the application of certain 10CFR50, Appendix B criteria for non-safety-related augmented quality computer programs is provided in Nuclear Information Technology Strategic Leadership (NITSL) NITSL-SQA-2005-02, Guidance Document to Implement Policy for Software Quality Assurance in the Nuclear Power Industry, Revision 1 [18].

5.4.1.10 Will the Computer Program Be Used to Monitor Operation and Control Functions of SSCs?

A computer program used to monitor operation and control functions of SSCs should be classified as non-safety-related, augmented quality because its failure does not adversely impact the ability of the SSC to perform its safety function. Augmented quality controls may be applicable because the computer program has the potential of an indirect impact on the SSC performing its safety-related function and, in this regard, is considered to be important to plant safety.

5.4.2 Classification Considering Impact Categorization

NITSL outlines a method for classification of software into one of four categories: high impact, medium impact, low impact, and other in NEI/NITSL document NITSL-SQA-2005-02 Rev. 1 [18]. Section 5.2.1, Software Quality Classification, of that document includes the following guidance:

> Criteria to classify software important to nuclear safety should be established and reflected in quality levels using a graded approach. Optional sub-categories may be included in SQA programs similar to those levels suggested below.
>
> 1. High Impact
>
> Software that has a direct active effect on the ability of a safety-related structure, system or component (SSC) to perform its intended safety functions.

Software used for the design of SSC that assures the SSC meets its intended design basis safety function as defined in the nuclear license documents without using alternate methods to verify the results.

2. Medium Impact

Software used to assess the ability of SSC to meet its intended safety function.

Software used to monitor "operation and control functions" of plant SSC.

3. Low Impact

Software used to support activities that have no direct impact on nuclear operations, design or license commitments but may be used to monitor compliance or optimize performance.

4. Other

Software not included in the above classifications.

NITSL-SQA-2005-02 Rev. 1 Attachment 1, "Suggested Minimum Requirements for Software Based upon Classification" [18] suggests that high impact software be controlled under the full scope of the licensee's SQA program, in effect requiring the elements of 10CFR50, Appendix B [1] program to be implemented. It also suggests that medium and low impact software be controlled using the graded approach, implementing only selective criteria from 10CFR50, Appendix B [1].

Suggesting that all of the elements of 10CFR50, Appendix B be implemented through each licensee's SQA program for high impact software is in essence classifying this type of software as safety-related. By suggesting that only some of the elements of 10CFR50, Appendix B be implemented through each licensee's SQA program for medium and low impact software, the determination is, in essence, classifying these types of software as non-safety-related or non-safety-related, augmented quality when the non-safety-related software is subject to additional quality activities.

The relationship between functional safety classifications and NITSL software impact categories is illustrated in Figure 5-3 and Table 5-2.

Table 5-2 illustrates an example of a functional safety classification that corresponds with the NITSL impact categories.

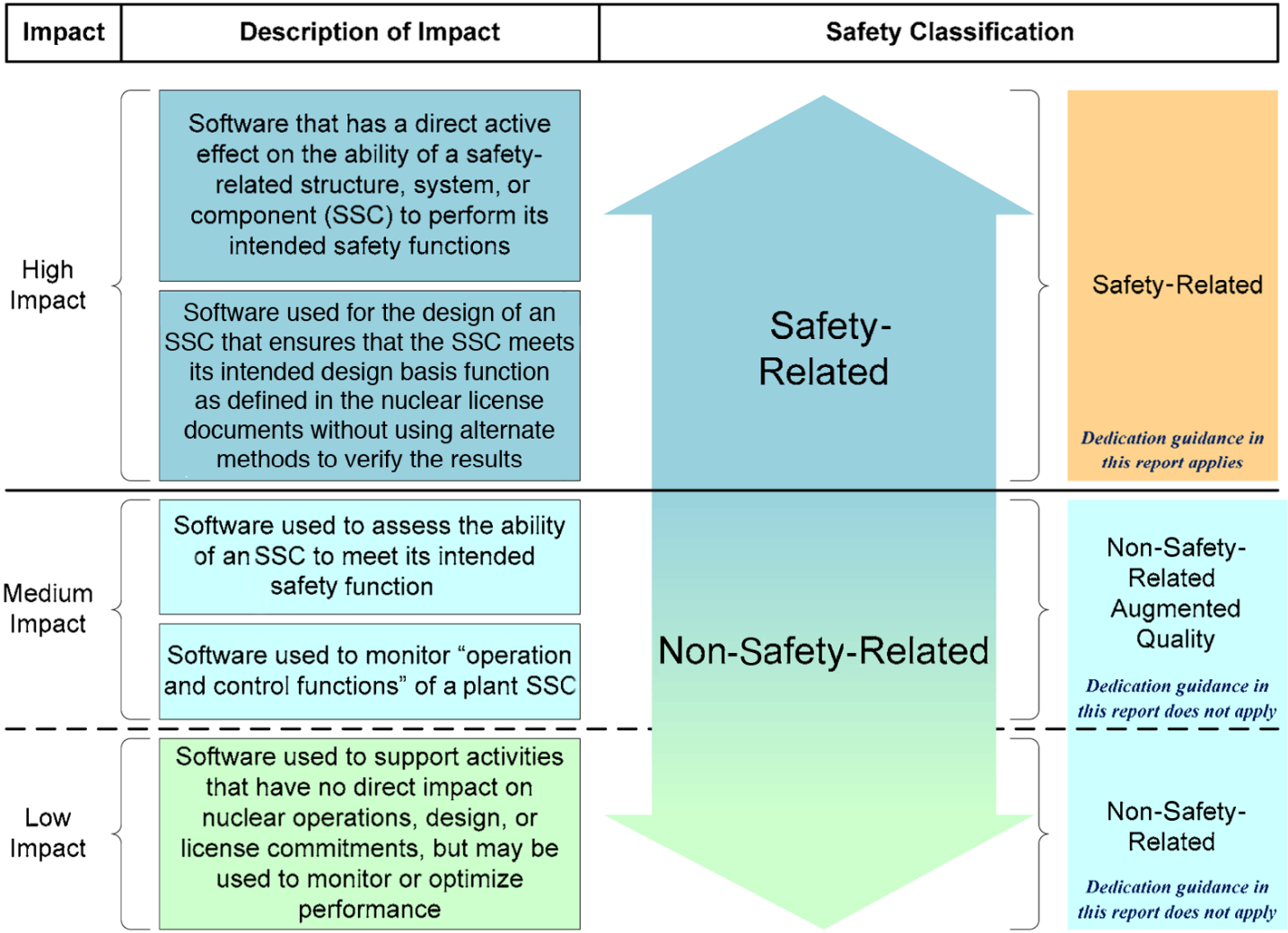


Figure 5-3
Functional Classification Considering the Impact of Computer Programs

Table 5-2
Functional Safety Classification Considering Impact of Programs on SSCs

Impact	Safety-Related	Augmented Quality (Non-Safety-related)/Non-Safety-Related SSCs – Significant Contributors to Plant Safety	Non-Safety-Related
High Impact (Note 1)	Software that has a direct active effect on the ability of a safety-related SSC to perform its intended safety functions.		
High Impact (Note 2)	Software used for the design of an SSC that ensures that the SSC meets its intended design basis safety function as defined in the nuclear license documents without using alternative methods to verify the results.		
Medium Impact (Note 3)		Software used to assess the ability of an SSC to meet its intended safety function.	
Medium Impact (Note 4)		Software used to monitor operation and control functions of a plant SSC.	
Low Impact			Software used to support activities that have no direct impact on nuclear operations, design, or license commitments, but may be used to monitor compliance or optimize performance.

Notes:

1. Software used in these applications is integral to the SSC and, as such, is outside the scope of this report.
2. Software is used as a design tool.
3. Software is used for assessing the functionality of SSCs.
4. Software is used as an operations tool.

5.5 Classification of Computer Program Environments

A hierarchical relationship exists between safety-related SSCs. That is, if a part is classified as safety-related, the component to which the part belongs is classified as safety-related, and the system to which the component belongs is classified as safety-related.

This hierarchical relationship is not the same for computer programs that are not embedded in plant SSCs.

A computer program classified as safety-related that is not embedded in plant SSCs (such as a computer program used to design or analyze safety-related equipment) can reside in an environment that is not safety-related. That is, the computer program could be installed on a non-safety-related workstation using a non-safety-related operating system, etc. However, the necessary controls must be in place to ensure that the safety-related computer program is capable of performing its safety-related functions in that environment.

Although not the primary focus of this report, typical controls might include:

- Ensuring that dedication acceptance activities address the computer program's environment
- Controlling configuration and security of the workstation and applicable operating system and associated software
- Performing applicable testing after the configuration of the host environment is modified
- Performing applicable testing at sufficient intervals to ensure that the computer program is capable of performing its safety-related functions

Section 6: Acceptance of Commercial-Grade Computer Programs via the Dedication Process

The purpose of this section is to provide guidance for implementing the acceptance of computer programs via commercial-grade dedication. As defined in Revision 2 of 10CFR21 [2]:

> Dedication is an acceptance process undertaken to provide reasonable assurance that a commercial grade item to be used as a basic component will perform its intended safety function, and in this respect, is deemed equivalent to an item designed and manufactured under a 10CFR50, App. B QA program.

It is important to emphasize that dedication is an *acceptance* process that occurs after other key processes including design, product selection, and qualification are complete. Dedication is not intended to establish or confirm acceptability of the existing design. Dedication is used as an acceptance process to provide reasonable assurance that the items being dedicated are capable of performing their safety-related functions.

Existing verification and validation practices may cover a broader range of activities than acceptance. In some cases, verification and validation may include:

- Confirmation that a product conforms with applicable design (specification) requirements
- Qualification that the product meets design (specification requirements)
- Acceptance of the purchased product for use

The guidance in this report addresses dedication as the "acceptance process undertaken to provide reasonable assurance that a commercial-grade item to be used as a basic component will perform its intended safety function, and in this respect, is deemed equivalent to an item designed and manufactured under a 10CFR50, App. B QA program" [2]. **It is important to ensure that other applicable processes, such as design and qualification, are also completed**.

Figure 6-1 illustrates the generic process for dedicating commercial-grade computer programs that are based on the process originally published in EPRI NP-5652 [4]. As noted in Section 4 of this report, the dedication process relies upon key elements of the technical evaluation, such as safety classification and determining whether the item (a computer program in this case) will be furnished as a basic component or commercial grade.

While the technical evaluation and acceptance processes overlap to a certain extent, the dedication acceptance process primarily focuses on the verification of critical characteristics. The objective of implementing the technical evaluation and acceptance process (that is, commercial-grade dedication) is to provide reasonable assurance that the computer program will perform its intended safety-related function(s).

EPRI TR-102260 [5] defines reasonable assurance as:

> A justifiable level of confidence based on objective and measurable facts, actions, or observations which infer adequacy.

Reasonable assurance is achieved by selecting appropriate critical characteristics that when verified provide a justifiable level of confidence that the computer program will perform as it is designed to perform. Verification is performed by selecting one or more of the acceptance methods described in EPRI NP-5652 [4], as appropriate. These acceptance methods are rooted in Criterion VII of 10CFR50, Appendix B [1].

This section will briefly summarize the purpose and implementation of each step of the generic process, but will primarily focus on the selection and verification of critical characteristics.

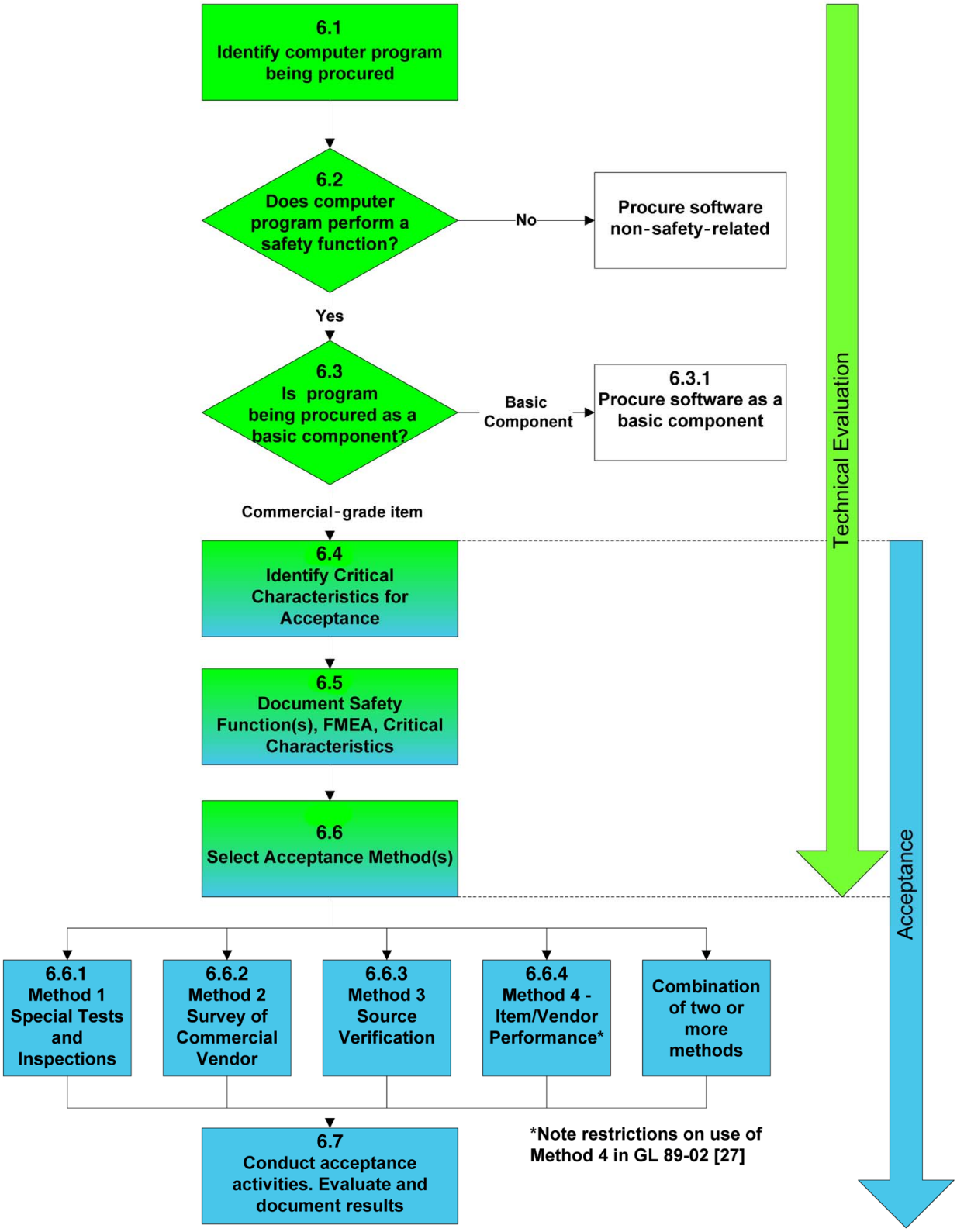


Figure 6-1
Commercial-Grade Computer Program Dedication Process (Based on EPRI NP-5652 [4])

6.1 Identify the Computer Program Being Procured

The computer program being procured should be clearly identified, including the applicable version, build, release number, and other identifying information.

6.2 Does the Computer Program Perform a Safety Function?

If the functional safety classification resulted in the computer program being classified as safety-related, the computer program performs a safety function and should be procured as either a basic component or as a commercial-grade item and dedicated for use as a basic component in a safety-related application.

If the functional safety classification that was performed resulted in the computer program being classified as non-safety-related (including non-safety-related, augmented quality), the computer program should be procured as a non-safety-related item.

6.3 Is the Computer Program Being Procured as a Basic Component?

A computer program that has been classified by the licensee or nuclear supplier as safety-related may be procured from a supplier with an audited and approved nuclear quality assurance program as a basic component. Otherwise, the computer program must be procured commercial grade and dedicated for use as a basic component in a safety-related application.

A computer program that is designed and manufactured under a nuclear quality assurance program should be procured as a basic component. Procurement documents would as a minimum require the computer program to be furnished in accordance with the supplier's QA program that meets the requirements of 10CFR50, Appendix B [1] and would require reporting of defects and noncompliance in accordance with 10CFR21 [2].

6.4 Identify Critical Characteristics for Acceptance

A computer program with a functional safety classification of safety-related that is not designed and manufactured under a nuclear quality assurance program can be furnished as a commercial-grade item. That is, it is procured as commercial grade and dedicated for use as a basic component in a safety-related application.

Identifying critical characteristics is an essential step in the dedication process. Critical characteristics identified during the technical evaluation are verified during the acceptance process to provide reasonable assurance that the computer program being accepted is capable of performing its intended safety-related function.

Critical characteristics are defined in revision 2 of 10CFR21 [2] as:

> Those important design, material, and performance characteristics of a commercial grade item that once verified, will provide reasonable assurance that the item will perform its intended safety function.

When detailed design information is available, critical characteristics for the computer program can be derived from the design information, specified in the procurement documents, and subsequently verified during acceptance activities. If design information is not available, an FMEA based on the function of the computer program can be performed to derive critical characteristics.

Consideration of failure modes can be helpful in identifying characteristics of a computer program that are necessary for it to perform its safety function(s). Table 6-1 lists some common failure mechanisms for computer programs and the critical characteristics that may be selected for verification.

Table 6-1
Common Failure Mechanisms and Associated Critical Characteristics

Type of Failure	Critical Characteristics
Conceptual Error	Accurate/correct results are obtained for calculations performed within the specified range of use.
Arithmetic Error	Accurate/correct results are obtained for calculations performed within the specified range of use, engineering parameters.
Interface Errors	Accurate/correct results are obtained when computer program is installed and interfacing with other programs, hardware, or operating systems.

Due to the complex nature of computer programs and the limited availability of detailed design and development information, it may not always be feasible to identify a specific critical characteristic that correlates with each specific failure mechanism considered. In these cases, it may be possible to develop critical characteristics that inherently address identified failure modes. For example, verifying a critical characteristic of "accuracy" using special testing (Acceptance Method 1) can provide reasonable assurance that the computer program would be capable of performing its safety-related function. Test cases could be developed that use the computer program in an environment (platform, operating systems, etc.) equal to the environment in which it will be used, where the test cases would address the applications (types of calculations) for which the computer program will be used, as well as the intended range of input values. If this special testing provides results of the desired accuracy, then reasonable assurance would be provided that failure modes (software faults) are not triggered when the computer program is used as intended.

In some cases, critical characteristics can be derived by considering the computer program's inputs, outputs, and operating environment. The following factors should be considered when identifying critical characteristics:

- Input should be provided by the vendor (or developed through interfacing with the vendor) that identifies and characterizes the design and functional parameters..
- The number and nature of the critical characteristics are to be based on the intended safety function, application requirements, complexity, credible failure modes and effects, and performance requirements.
- Critical characteristics that cannot be effectively verified during post-receipt inspection and testing should be identified so that an appropriate verification method can be implemented during development or through a review of the development review process.

6.4.1 Product Selection Attributes

Product selection attributes (Refer to Table 6-2) are characteristics that the computer program must possess to fulfill its intended scope of use. Product selection attributes are typically considered during the initial stages of product selection or design, well in advance of the acceptance process. Documenting the selection attributes can be helpful when identifying scope of use, safety functions, and critical characteristics.

6.4.2 Product Identification Inspection Attributes

Product identification inspection attributes (Refer to Table 6-3) should be verified as an integral part of the commercial-grade dedication process. Although product identification characteristics may not be directly related to computer program safety function(s), verification of identity is an important part of the overall acceptance process and may provide indication of changes in the computer program that have occurred subsequent to previous procurements.

In addition, product identification attributes can be an important aspect of computer program control because identification often indicates a version or release number.

6.4.3 Physical and Performance Characteristics

When determining critical characteristics for mechanical and electrical items, consideration is given to identifying two categories of critical characteristics including *physical characteristics* (such as dimensions, materials of construction, and configuration) as well as *performance characteristics* (such as opening time, closing time, spring constant, resistance, etc.).

Examples of physical and performance characteristics applicable and relevant to computer programs are included in Tables 6-4 and 6-5.

6.4.4 Dependability Characteristics

Whereas hardware failures can typically be attributed to fabrication defects and failure mechanisms associated with aging, computer program failures are typically attributed to errors in computer program design or coding, that is, the ability of the computer program to provide dependable results.

EPRI TR-106439, *Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications* [6], identified *dependability characteristics* (see Table 6-5) as a category of characteristics that should be considered when determining critical characteristics for digital devices installed in plant SSCs.

The concept of dependability characteristics extends to computer programs used in safety-related design and analysis applications. Dependability characteristics are typically associated with the reliability of the device under the entire range of operating conditions and event sequences. Therefore, dependability characteristics are directly related to the design or built-in capabilities of the device or computer program to correctly perform all safety-related functions and handle anticipated as well as unexpected inputs, fault conditions, etc.

Dependability characteristics, which may include attributes such as reliability and built-in quality, are heavily dependent upon the computer program development process and the individuals who develop, verify, and validate the software integral to the computer program. Examples of dependability critical characteristics are included in Table 6-6.

6.4.5 Examples of Product Selection, Product Identification, and Critical Characteristics

The following tables are provided for consideration when identifying product selection and product identification inspection attributes. Although product selection takes place prior to dedication, documenting the selection criteria can be helpful in identification of end uses, functions, and failure modes. Documenting product identification characteristics facilitates the standard receipt inspection process.

- Typical Product Selection Attributes: Table 6-2
- Typical Product Identification Inspection Attributes: Table 6-3

The following tables are provided for consideration when selecting critical characteristics to dedicate a commercial-grade computer program:

- Typical Physical Critical Characteristics: Table 6-4
- Typical Performance Critical Characteristics: Table 6-5
- Typical Dependability Critical Characteristics: Table 6-6

Critical characteristics should be selected based on the specific application(s) for which the computer program will be used and the associated safety function(s). The critical characteristics included in the tables are not intended to be a complete list of all critical characteristics that a licensee or nuclear supplier may opt to verify. Similarly, inclusion of the tables does not imply that **all** of the critical characteristics listed in this report would need to be verified for every computer program dedication. Note that the "possible methods of verification column" is provided for information purposes only, and the user of this report can use other methods as appropriate.

Table 6-2
Typical Product Selection Attributes

Product Selection Attribute	Description	Acceptance Criteria	Possible Methods of Evaluation During Product Selection/ Qualification for Use
Functionality required for intended end use(s) The computer program is capable of performing the desired calculations, analyses, and so forth.	When correctly installed in the designated environment, the computer program is capable of performing the types of calculations required over the identified range of inputs.	The computer program includes the capabilities specified/ necessary to support design and analysis. Note: Verification of the capabilities for acceptance takes place after product design, selection, and qualification are complete.	Review of published product literature.
Validity of scientific basis for computer program functionality The computer program basis is consistent with the appropriate engineering scientific research and professional technical approaches.	The degree to which the computer program's sample or complete data sets of results correlate with experimental data, expected data results, or professional analyses and to which any erroneous data sets do not correlate with the experimental data or professional analyses. This attribute may be particularly important for computer programs used to perform the analysis of an accident and structural integrity analyses for determining the proper design of safety components.	Consistency with research and professional technical approaches is based upon peer-reviewed published technical papers or industry-accepted computer programs performing a similar function. The output of the computer program can be viewed as how closely the computer program's output matches the technical report or baseline computer program output (for example, the computer program output correlates with experimental data to ± 3σ.)	Engineering and/or subject matter expert review of documentation associated with the computer program. Evaluation may include: • A comparison of peer-reviewed technical publication detail results against the computer program's output for a similar problem being solved. • A comparison of the baseline computer output against the computer program's output that is being dedicated. The baseline computer program must solve the same or closely similar physical problem as the dedicating computer program. • A review of the computer program's current user base and its applicability to the intended use.

Table 6-2 (continued)
Typical Product Selection Attributes

Product Selection Attribute	Description	Acceptance Criteria	Possible Methods of Evaluation During Product Selection/ Qualification for Use
Effective problem reporting	An institutionalized process used by the supplier to both receive problem reports from customers and to notify customers of potential computer program errors or weaknesses and rollout patches, updates, and so forth.	A formal, documented problem or error reporting program exists and is effectively implemented. A documented process exists to track customers and provide notification when appropriate. Evaluation criteria for determining when notification is warranted are documented and include an appropriate threshold. Problem reporting metrics are maintained and indicate an appropriate number of notifications to users over time.	Verification is performed by a review of communications regarding errors with users, a review of any website or other form of communication with the supplier, and a review of a communications log.

Table 6-2 (continued)
Typical Product Selection Attributes

Product Selection Attribute	Description	Acceptance Criteria	Possible Methods of Evaluation During Product Selection / Qualification for Use
Supportability/maintainability	The ability of the supplier to continue providing support for the computer program over the life of its use.	Supportability/maintainability: • Standard financial models used to evaluate suppliers • Other evaluation factors include stability of the supplier/business longevity (for example, the number of years in business) • Size of the customer base (for example, the number of customers worldwide) • Plans for future product updates or releases (for example, supplier R&D has updates scheduled for the next three years) • Supplier's history of discontinuing products (for example, have product lines been regularly discontinued?)	Review of the supplier history for the specific computer program as well as the history in supporting similar computer programs or products.
Supportability/maintainability	(If applicable) The computer program is designed in a way that permits modifications to be performed. This attribute may be more appropriate for computer programs whose failure or unavailability could result in few or no alternatives or alternatives that are not financially feasible.	Time and skills required to modify the computer program (mean time to change or mean time to fix).	Review of supplier metrics associated with the length of time to evaluate the change/error correction, make the code change/correction, test the change/correction, update all computer program documentation, and release the change.

Table 6-2 (continued)
Typical Product Selection Attributes

Product Selection Attribute	Description	Acceptance Criteria	Possible Methods of Evaluation During Product Selection/ Qualification for Use
Environmental compatibility: portability	The measure of the effort required to migrate the computer program to a different hardware platform, component, or environment. This critical characteristic may be important only for computer programs that are expected to be executed in a different environment.	As described in computer program requirements. Portability criteria can be expressed as a unit of time (for example, 16 hours or 15 days).	Performing migration to one or more environments equivalent to the dedicating entities. (Method 1)

Table 6-3
Typical Product Identification Attributes

Inspection Attribute	Description	Acceptance Criteria	Possible Methods of Verification During Standard Receipt Inspection
Host computer/operating environment identification	Information that identifies the host computer system(s) or operating environment(s) suitable for execution of the computer program.	Identifying information matches the host computer system(s) or operating environment(s) included in the applicable specification and/or procurement document.	Review of product identification and documentation during receipt inspection
Computer program identification	Complete information required to identify the base computer program as well as build number, version number, included patches, and so forth.	Computer program identification matches the criteria specified in the applicable specification and/or procurement document	Review of product identification and documentation during receipt inspection.

Note: Product identification attributes may be used for maintaining configuration control, traceability, etc., as deemed appropriate by each end user.

Table 6-4
Typical Physical Critical Characteristics (Adapted from ASME NQA-1 [8] and EPRI TR-106439 [6])

Physical Critical Characteristic	Description	Acceptance Criteria	Possible Methods of Verification
Format	The media format in which the computer program is provided, for example, CD, DVD, etc.	The format matches the format specified in the applicable specification and/or procurement document.	Inspection and testing. (Method 1)

Table 6-5
Typical Performance Critical Characteristics (Adapted from ASME NQA-1 [8] and EPRI TR-106439 [6])

Performance Critical Characteristic	Description	Acceptance Criteria	Possible Methods of Verification
Accuracy of output	The degree to which there is a close correlation with the expected or desired outcome.	Objective evidence through testing or similar means (such as verification and/or validation) that the computer program results meet the user's specified requirements. Criteria may be expressed similar to the following: Accuracy - ± X%	Inspection and testing. (Method 1) Commercial-grade survey of testing activities and documentation Observation and review of design. (Method 3) Review of the installed base to determine performance history. (Method 4)
Precision of output	The degree of repeatability or degree of measure.	Objective evidence through testing or similar means (such as verification and / or validation) that the computer program results meet the user's specified requirements. Criteria may be expressed similar to the following: Precision - ± 0.000X	Inspection and testing. (Method 1) Commercial-grade survey of testing activities and documentation Observation and review of design. (Method 3) Review of the installed base to determine performance history. (Method 4)

Table 6-5 (continued)
Typical Performance Critical Characteristics (Adapted from ASME NQA-1 [8] and EPRI TR-106439 [6])

Performance Critical Characteristic	Description	Acceptance Criteria	Possible Methods of Verification
Tolerance of output	The allowable possible error in measurement.	Objective evidence through testing or similar means (such as verification or validation) that the computer program results meet the user's specified requirements. Criteria may be expressed similar to the following: Tolerance - ± 0.0000X	Inspection and testing. (Method 1) Commercial-grade survey of testing activities and documentation Observation and review of design. (Method 3) Review of the installed base to determine performance history. (Method 4)
Functionality: Specific safety functions and algorithms	Critical functions or calculations are performed. For example, time-dependent functions and functionality to allow only authorized users access to perform the safety-related calculations.	As described in computer program requirements or procurement specification documentation. Each functionality criterion may be expressed similar to the following: Given source input data, calculate dose exposure at 10 meters and 0 receptor height.	Inspection and testing. (Method 1) Observation and review of design. (Method 2 and/or 3) Review of the installed base to determine performance history. (Method 4)
Functionality: Completeness and correctness	The degree to which the computer program requirements, design, and implementation satisfy applicable requirements. Formal techniques may be used to mathematically prove that the computer program satisfies its specified requirements. This critical characteristic is important to identify the risks of the computer program failing to execute its safety functions.	Completeness and correctness are based upon how many of the computer program's requirements have been verified to be successfully implemented (for example, 100% of the allocated safety requirements are correctly implemented).	Performing a review of the functional requirements' traceability to test cases and verification that the test results indicate correct functionality. If the requirements' traceability is unavailable, the dedicating entity can develop the traceability matrix from the computer program's requirements or procurement specifications and test cases performed. (Method 2)

Table 6-5 (continued)
Typical Performance Critical Characteristics (Adapted from ASME NQA-1 [8] and EPRI TR-106439 [6])

Performance Critical Characteristic	Description	Acceptance Criteria	Possible Methods of Verification
Interfaces: Critical input parameters and valid ranges	The set of input parameters that are used in the critical functions of the computer program and the range of their valid values. This critical characteristic is important to ensure that the computer program will function properly for all possible ranges of operational inputs required for safety-related computations.	As described in computer program requirements or procurement specification documentation. This criteria may be expressed similar to the following: Deposition receptor height (for example, 0 to 1 ft), time: (dd/mm/yyyy hh:mm:ss); and length (1.00 to 5.00 meters).	Inspection and testing. (Method 1) Inspection of user's manual. (Method 1) Observation and review of design and/or implementation. (Method 2 and/or 3) Review the installed base to determine performance history. (Method 4)
Interfaces: Output parameters	The characteristics of the critical output parameters. The characteristics of the critical output parameters include file formats and mathematical notations. This critical characteristic is important to ensure that the computer program output is expressed in the required expected format or units of measure.	As described in computer program requirements or procurement specification documentation. This criterion can include parameters such as the output file name (for example, 28 characters, case-insensitive with a file extension of pdf), output format specification (for example, comma-delimited, scientific notation, and units of measure (such as psig expressed to the Xth decimal place).	Inspection and testing. (Method 1) Observation and review of design. (Method 3) Review of the installed base to determine performance history. (Method 4)

Table 6-6
Typical Dependability Critical Characteristics (Adapted from ASME NQA-1 [8] and EPRI TR-106439 [6])

Dependability Critical Characteristic	Description	Acceptance Criteria	Possible Methods of Verification
Built-in quality Effective quality and oversight of development process	The development process is performed under the auspices of documented, effective quality assurance procedures, program, and/or plan (for example, IEEE-730 [32], IEEE/EIA Standard 12207.0 [33], IEC 60880 [34], ISO-9001 [35], etc.).	Objective evidence that demonstrates that: The computer program was developed under the auspices of a documented quality assurance (or oversight) program that was effectively implemented throughout the development process. The quality assurance program includes measures to ensure that the computer program is capable of performing functions included in the requirement specifications/ design documents. In the case of accredited quality assurance programs, accreditation of the developing organization throughout the development process.	Method 2 – Commercial-grade survey with a technical subject matter expert participation. Method 3 – Source surveillance with a technical subject matter expert participation to examine documented quality program documents and records associated with the development process. Review of third-party certification/accreditation reports and documentation. Review of internal/external audit reports.
Built-in quality Structured development process Documentation	Development process is structured and documented. The process is clearly designed to achieve the functionality specified and to meet the requirements that are defined and documented.	Objective evidence demonstrates that: The development process is documented in procedures or other types of work instructions. The process is designed to achieve the defined and documented functionality.	Commercial-grade survey with subject matter expert participation. (Method 2) Source surveillance with a technical subject matter expert at key points in the development process and associated testing. (Method 3)

Table 6-6 (continued)
Typical Dependability Critical Characteristics (Adapted from ASME NQA-1 [8] and EPRI TR-106439 [6])

Dependability Critical Characteristic	Description	Acceptance Criteria	Possible Methods of Verification
Built-in quality Structured development process Adherence to coding practices	The computer program complies with applicable coding standards, or use of code libraries. Adherence to coding practices typically reduces the likelihood of unidentified errors in the computer program.	Coding practices can be expressed in terms of the amount (such as percentage) of code developed independent of applicable coding practices or without the use of applicable code libraries.	Commercial-grade survey with subject matter expert participation. (Method 2) Source surveillance with a technical subject matter expert at key points in the development process and associated testing. (Method 3)
Built-in quality Structured development process Configuration control and traceability	Changes in the program are controlled and documented. Changes are traceable to specific builds or versions so that customers may be notified of problems, etc. Changes are subject to acceptance testing commensurate with testing applied to the original code.	Configuration of the computer program is controlled by use of an automated configuration management tool or other effective method. The configuration of the computer program is controlled as well as alignment with and revision of the associated software and documentation. The ability to support incoming and outgoing problem reporting processes (that is, traceability) is maintained.	Commercial-grade survey with subject matter expert participation. (Method 2) Source surveillance with a technical subject matter expert at key points in the development process and associated testing. (Method 3)

Table 6-6 (continued)
Typical Dependability Critical Characteristics (Adapted from ASME NQA-1 [8] and EPRI TR-106439 [6])

Dependability Critical Characteristic	Description	Acceptance Criteria	Possible Methods of Verification
Built-in quality: Code structure (complexity, conciseness)	The measure to which the computer program is legible, the complexity is minimized, and the code length is minimized. This critical characteristic can be used to provide an indicator as to the difficulty to verify through reviews and testing that the code will perform as expected.	Code structure criteria can be quantitative, through the use of static analysis tools, or qualitative, through reviews of the documented design or inspection of the code. Code structure criteria may take the form of number of internal subroutine interfaces, number of do-loops, number of exits from a module, straightforward flow of logic in code module, and code module depth and breadth.	Review of supplier documented evidence from the use of a static analysis tool or the dedicating entity performing an inspection and manual analysis of the documented design or computer program code. (Method 2)
Built-in quality: Conformance to national codes, standards, and industry-accepted certifications	The computer program's compliance with applicable national codes and standards or industry-accepted certifications.	Conformance criterion can be a measure of how well the computer program meets industry-accepted practices that provide a qualitative pedigree of the computer program. The criteria can be the degree to which a national code, standard, or third-party certification or recertification programs is achieved (for example, 90% achievement of compliance to Capability Maturity Model Integration Software Engineering Institute (CMMI SEI) maturity level 4 or achieved pertinent ISO 9001 [35] registration).	Inspection of supplier-performed assessments of the computer program against the national code or standard. (Method 1) Inspection of the proof of third-party certification. (Method 1) Review of computer program documentation and artifacts against the selected national code or standard. (Method 2)

Table 6-6 (continued)
Typical Dependability Critical Characteristics (Adapted from ASME NQA-1 [8] and EPRI TR-106439 [6])

Dependability Critical Characteristic	Description	Acceptance Criteria	Possible Methods of Verification
Built-in quality: Internal reviews and verifications	Effective use of analysis methods (for example, peer reviews) during development of the computer program to confirm compliance with requirements and identify errors and noncompliance with supplier procedures and standards.	Criteria for internal reviews and verifications effectiveness are based upon the ratio of errors identified during the review/ verification and the number of errors that are discovered in the next life-cycle phase (for example, the ratio of the number of requirements errors identified during the requirements review and the number of errors detected during the design phase).	Inspection and analysis of results from reviews or verification and validation activities performed in two or more adjacent life-cycle phases. (Method 2 and/or Method 3).

Table 6-6 (continued)
Typical Dependability Critical Characteristics (Adapted from ASME NQA-1 [8] and EPRI TR-106439 [6])

Dependability Critical Characteristic	Description	Acceptance Criteria	Possible Methods of Verification
Built-in quality: Testability and thoroughness of testing	A measure of the completeness of the computer program verification, validation, and installation testing to ensure that the computer program is correct and complete. This critical characteristic may be appropriate to use for ensuring that tests performed by the supplier or developer were adequate to provide the reasonable assurance that the safety functions can be performed satisfactorily.	Testability criteria are based on the ease or difficulty in conducting verification and validation activities as well as the breadth and depth of the testing performed. Testability criteria may include: the number of hours needed to perform peer reviews, pretest a module, and develop test cases. The thoroughness of computer program testing criteria can be measures that identify the quantity of errors discovered during the various testing activities (for example, trend analysis of errors per module, comparison of pre- and post-release errors) and traceability of tests performed to the safety requirements for the computer program (for example, 95% of the requirements were tested).	Inspection of documented review reports and test records that include the time spent to prepare, conduct, and perform post-review or test activities. (Method 1) Review of the objective evidence of the errors identified during the testing processes or traceability of safety requirements to the tests completed. If objective evidence is not available, the dedicating entity may be able to create the traceability of the safety requirements to the tests performed from the computer program's documented requirements and test reports. (Method 2)

Table 6-6 (continued)
Typical Dependability Critical Characteristics (Adapted from ASME NQA-1 [8] and EPRI TR-106439 [6])

Dependability Critical Characteristic	Description	Acceptance Criteria	Possible Methods of Verification
Built-in quality: Training, knowledge, and proficiency of the personnel performing the work	Staff training, knowledge, and proficiency associated with the design, development, testing, oversight of the computer program, experience in similar projects and familiarity with specific tools, languages used in design, and implementation. This critical characteristic can be used to provide an indicator of the errors remaining in the computer program.	Staff training, knowledge, and proficiency criteria may include how well the specific staff member satisfies the supplier's qualification requirements for the position held. The criterion can be the percentage of qualification requirements met.	Review of objective evidence of attendance at courses, staff resumes, and on-the-job training against the supplier qualification requirements to determine how well the staff member satisfies the requirements. (Method 2)

6.5 Document Results of Technical Evaluation and Critical Characteristics

The results of the technical evaluation and critical characteristics should be clearly documented, including:

- Computer program safety function(s)
- FMEA or other process used to derive critical characteristics
- Critical characteristics of the computer program

As mentioned in 5.4.1.6, the FMEA is used differently when identifying critical characteristics for computer programs than it is for performing safety classification. During safety classification of computer programs, the FMEA focuses on the effects that failures could have on plant equipment. Therefore, failure of the computer program must be extrapolated to determine if it could also result in failure of plant SSCs that the computer program is being used to design or analyze.

When identifying critical characteristics, the FMEA focuses on the effects that failures could have on computer program functions in order to help identify characteristics required to prevent computer program failure modes and mechanisms from occurring and impacting the ability of the computer program to perform its safety-related functions.

Table 6-7
Use of Failure Modes and Effects Analysis in Technical Evaluations of Computer Programs Not Embedded in Plant SSCs

Application of FMEA	Safety Classification	Commercial-Grade Dedication
Objective	Determine the functional safety classification of the computer program.	Identify critical characteristics of the computer program.
Intent	Determine if failure of the item being classified could prevent safety-related plant SSCs from performing their safety-related function(s).	Recognize failure modes and mechanisms to facilitate the identification of characteristics necessary to prevent failures from occurring.
Technique	Extrapolate to determine if failures of the computer program could result in the inability of associated plant SSCs to perform one or more safety functions.	Analyze failure modes and effects to determine computer program characteristics required to prevent failure of the computer program.

Some of the most serious faults have a subtle effect on the program's functionality and may, thus, be undetected for a long time. Other failures may cause the program to crash or freeze, leading to a denial of service. Others qualify as security problems and might, for example, enable a malicious user to bypass access controls in order to obtain unauthorized privileges.

Results of the technical evaluation may be documented in various formats. For example, critical characteristics might be identified by the dedicating entity in various types of documentation, such as:

- Software requirement specification
- Procurement specification
- Verification plans
- Test or inspection results
- Procedures or work instructions
- User guides

The basis or reasons for critical characteristic selection should also be evident in the documentation. Documentation should be clear and understandable enough to ensure that another person with similar training and qualification can arrive at the same conclusions included in the technical evaluation and critical characteristics identification.

6.6 Select Acceptance Method(s)

As Figure 6-1 illustrates, acceptance methods associated with commercial-grade dedication include:

1. Special tests and inspection
2. Commercial-grade surveys
3. Source verification
4. Acceptable item and supplier performance record

Organizations performing commercial dedication have the latitude to use one or more of these methods, as appropriate (that is, two or more in combination).

6.6.1 Method 1 – Special Tests and Inspections

Special tests and inspections, often referred to as Method 1, are often the only practical means available to the dedicating entity for verifying selected critical characteristics. Testing of the computer program should ensure that the selected critical characteristics are verified. Testing should include run tests of the computer program installed in its operating environment or system and respective hardware and may also include test cases, test scenarios, or verification via alternative calculations.

If test cases developed by organizations other than the dedicating entity are used, care should be taken to ensure that the test cases adequately verify the selected critical characteristics.

Although developed for digital control systems,-EPRI report TR-103291, *Handbook for Verification and Validation of Digital Systems* [36], contains guidance that can be applied when testing non-process computer programs.

6.6.2 Method 2 – Survey of Commercial-Grade Supplier

Conducting a commercial-grade survey of a supplier is often referred to as Method 2. A commercial-grade survey is a performance-based assessment of a supplier conducted to determine the adequacy of supplier quality controls that are directly related to ensuring that the critical characteristics of the product being dedicated are acceptable.

A survey plan is developed that identifies the critical characteristics as well as the types of programmatic and process controls that should be assessed during the survey. The controls must be captured in writing by the supplier. Although no specific format is required, controls are often documented in quality assurance program requirements, procedures, work instructions, testing plans, and so forth. During conduct of the survey, the controls that the supplier has in place are evaluated to determine if they effectively ensure that the computer program is imparted with the identified critical characteristics. The survey should be performance-based, meaning that in addition to reviewing the documented controls, the supplier's effectiveness in implementing the controls is also evaluated.

Controls determined to be effective during the survey are documented in a survey report. The controls are subsequently specified as quality requirements in procurement documents issued to the supplier. The procurement document also requires the supplier to provide certification attesting to the fact that the computer program was developed or is being provided in accordance with the specified controls. The certification is verified during receipt inspection and is maintained as objective evidence that the critical characteristics associated with the specified controls are acceptable.

The dedicating entity may not have an opportunity to conduct a commercial-grade survey of a computer program supplier as a way to evaluate commercial quality controls as they are implemented throughout the entire life cycle of the computer program being purchased. However, a commercial-grade survey can provide the dedicating entity with an opportunity to examine (and develop confidence in) the processes that were used to develop the computer program. The extent to which the supplier implements design control measures (such as those described in commercial industry standards, such as IEEE) and the effectiveness of the supplier's implementation can be evaluated during the survey. In some cases, it may also be possible to review the documentation associated with the development of the computer program being purchased by the dedicating entity.

EPRI report 1011710, *Handbook for Evaluating Critical Digital Equipment and Systems* [13], includes guidance on performing a critical digital review (CDR) of digital process equipment to identify issues associated with dependability and integrity of the device. Application of CDR methodology may provide useful input for a commercial-grade survey plan relative to dependability critical characteristics.

6.6.3 Method 3 – Source Verification

Source verification is often referred to as Method 3. Source verification entails verification of critical characteristics during the design and development of the computer program being procured. Source verifications are typically performed in conjunction with key milestones in the production process or development life cycle so that important activities can be witnessed by the dedicating entity.

Due to the inherent complexity of computer programs, in-process inspections and verifications are typically required to ensure that defects or failures to comply with design requirements (for example, the computer program requirements specification) are identified and corrected. It is unlikely that the dedicating entity would have an opportunity to verify in-process tests and inspections during the development of commercial off-the-shelf computer programs.

EPRI report TR-103291, *Handbook for Verification and Validation of Digital Systems* [36], provides insight into the key steps of the software life-cycle development process and the types of testing and verification activities associated with each step. Although the guidance in the document was developed for digital control systems, it may prove useful in planning and conducting source verifications for computer programs.

6.6.4 Method 4 – Supplier and Item Performance History

Performance history (good or bad) of the item and supplier is a consideration when determining the use of the other acceptance methods and the rigor to which they are used on a case-by-case basis. Specific regulatory expectations for the use of supplier or item performance history are included in NRC Generic Letter 89-02 [27]. Supplier and item performance history is typically used as a factor in the selection of sampling plans when verifying physical and performance characteristics associated with hardware.

6.6.5 Standard Receipt Inspection

Standard receipt inspection verifications should be integral to all commercial-grade acceptance methods. Standard receiving activities are typically performed before acceptance of critical characteristics that take place after delivery of the product to ensure that the correct item has been received in the correct quantities, format, and so on.

The following are examples of product attributes that can be verified as part of the standard receiving process:

- Software authenticity and registration key
- Firmware revision number
- Software revision level
- General condition of the software media
- Condition of the packaging
- Supplier documentation

6.7 Dedication Acceptance Activities

All of the acceptance activities specified in the dedication evaluation to verify critical characteristics for acceptance must be successfully completed. Some verification activities such as commercial-grade surveys of the supplier or source verification may be conducted well in advance of receiving the computer program. Dedication acceptance activities include (1) special tests and inspections (including verification and validation activities), (2) commercial-grade surveys, (3) source verification(s), and (4) consideration of historical performance of the computer program and/or the computer program developer/supplier.

The results of acceptance activities should be documented and clearly identified as acceptable or not acceptable. Documentation should be clear and understandable enough to ensure that another person with similar training and qualification can easily arrive at the same conclusions included in the evaluation and acceptance package.

6.8 Considerations When Selecting Acceptance Methods

Existing software development standards, such as IEEE software engineering standards, include a "life-cycle" approach to ensuring the overall quality of the software. These standards are based on a model that starts with a concept for proposed software and ends with a finished software product. The standards advocate implementation of quality assurance controls that are applied throughout the product's life cycle, including controls associated with refining the software concept, designing the software, testing the software, managing updates and revisions, and so forth.

During selection of acceptance methods for commercially procured computer programs, it may not be possible to adequately verify each element of the typical software quality assurance life cycle through source verification or commercial-grade survey, particularly if development of the computer program is complete before the dedication process is started.

Acceptance may rely more heavily on testing in the installed environment when it is not possible to verify implementation of earlier elements in the software development life cycle.

Elements comprising the life-cycle approach are shown below in Figure 6-2.

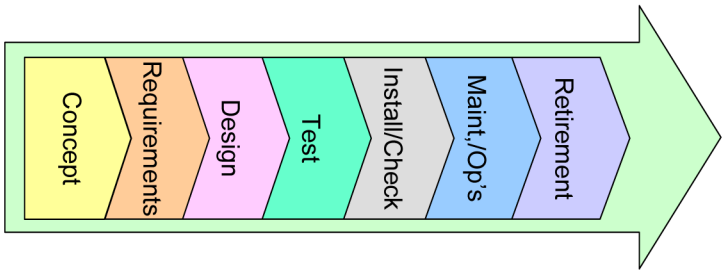


Figure 6-2
Typical Process Flow (Life Cycle) for Software (Based on NITSL-SQA-2005-02)

Figure 6-3 attempts to illustrate where, in a typical computer program development life cycle, the types of design, specification, and acceptance processes associated with plant structures might occur. Earlier stages of the computer development life cycle may be more focused on designing the computer program and establishing that various parts of the program perform as intended, while middle stages may be more focused on developing integrated testing scenarios and conducting verification and validation of the computer program, and later stages may involve maintenance and configuration management of the computer program.

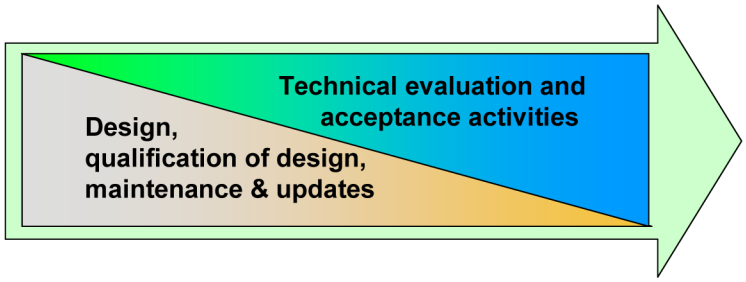


Figure 6-3
Typical Design, Specification, and Acceptance Processes

The selection of acceptance methods is dependent upon the degree to which the dedicating entity is able to participate in implementation of the computer program life cycle and the level of access that the application developer is willing to provide to the dedicating entity. In the case of commercial-grade computer programs, it may or may not be possible to implement controls over the entire software life cycle. Although Method 2 (commercial-grade survey) or Method 3 (source verification) could be used to provide assurance that effective controls are in place throughout the software life cycle, the ability to implement these methods is dependent upon when the licensee begins planned coordination with the manufacturer, as well as the manufacturer's willingness to provide access to these life-cycle activities. Therefore, acceptance of commercially procured computer programs using the dedication process may rely heavily on special testing and inspection (including verification and validation) of the completed computer program.

In a case where the dedicating entity is permitted to perform a commercial-grade survey at the supplier's facility and is provided access to records of the software development and testing processes, it may be possible to verify applicable dependability characteristics to build confidence that the computer program is capable of performing its safety-related functions. In this scenario, it may be feasible to rely more upon "built-in" quality controls and less on performance testing. In a case where the dedicating entity is unable to perform a survey and does not have access to records of the software development and testing processes, the dedication may have to rely more upon performance testing and less upon verification of "built-in" dependability.

Table 6-8 is provided as an illustrative example of how some critical characteristics may be verified using one or more of the acceptance methods. Tables 6-2 through 6-5 also suggest acceptance methods that might be appropriate for verifying each critical characteristic included.

Table 6-8
Example of Using Acceptance Methods

Inspection Attribute/ Critical Characteristics	Acceptance Criteria	Possible Method(s) of Acceptance
Software revision number	Software revision conforms to the number identified in the procurement document.	Standard receipt inspection
Update (configuration) control	Current configuration remains suitable for the application.	Method 2 (CG survey)
Platform compatibility (operating system, etc.)	Computer program is compatible with the current operating system.	Method 1 (Testing)
Hardware compatibility	Computer program is compatible with the current hardware.	Method 1 (Testing)
Built-in quality	Appropriate in-process tests and inspections are performed.	Method 2 (CG survey)
Quality of design and implementation	Design controls are performed in accordance with SQA.	Method 2 (CG survey)
Functions/applications	Outputs are consistent and accurate for various applications.	Method 1 (Testing), Method 2 (CG survey)

Table 6-8 (continued)
Example of Using Acceptance Methods

Inspection Attribute/ Critical Characteristics	Acceptance Criteria	Possible Method(s) of Acceptance
Range (input variables, limits of application, etc.)	Outputs are consistent and accurate over a range of inputs and applications.	Method 1 (Testing), Method 2 (CG survey)
Accuracy	Outputs are mathematically accurate.	Method 1 (Testing), Method 2 (CG survey)
Consistency repeatability	Outputs are consistent and accurate over numerous times the computer program is used.	Method 1 (Testing), Method 2 (CG survey)

Section 7: Commercial-Grade Software Procurement Examples

The purpose of this section is to provide several examples that demonstrate the implementation of a technical evaluation for computer programs. Each example includes implementation of a classification methodology, and in the cases where the computer program was classified safety-related, the example includes the acceptance process for a commercial-grade computer program.

These examples are provided for illustrative purposes only and demonstrate how the methodology can effectively be implemented. The user of this report should ensure that good engineering judgment is used for each procurement of new computer programs as well as for expanded usages of existing computer programs, and that appropriate procedures are followed when performing the technical evaluation and acceptance activities.

7.1 Computer Program Used to Perform Pipe Stress Calculations and Analysis

7.1.1 Introduction

This example describes a scenario where a design engineer at a nuclear power plant is procuring an analysis computer program that will be used to perform pipe stress analysis that will provide input for the design, selection, and layout of a large number of pipe supports. The calculations performed by the computer program are very complex and will not be independently verified by hand calculations or other means.

In this example, the computer program is classified **safety-related**, procured commercial-grade, and dedicated.

7.1.2 Implementation of the Technical Evaluation

The first step of the technical evaluation is to determine the classification of the analysis computer program. In this case, the engineer opts to perform a functional safety classification considering failure modes and effects. The methodology described in Section 5.4.1 of this report is used, with the following results:

- Is the computer program integral to a safety-related SSC?
  - NO. Thus, the guidance provided in this report is applicable.
- Can the computer program impact safety-related SSCs?
  - YES. The program will provide pipe stress data that are associated with piping in the reactor coolant system.
- Will the computer program be used to design or analyze SSCs in a way that could impact SSC safety functions?
  - YES. The computer program is used to design the safety-related pipe hangers installed in the reactor coolant system.
- Will the results derived using the computer program be independently verified for every use?
  - NO. The engineer proceeds to perform a failure modes and effects analysis.

    The safety-related functions of the associated equipment under normal and accident conditions are documented in the plant FSAR, Technical Specifications, systems descriptions, and design basis documents. The engineer documents the function of the analysis computer program—to accurately calculate pipe stress based on verified design input (flow rate, pressure, fluid type, temperature, etc.). The computer program is used as a tool to perform calculations that replicate a series of mathematical equations.

    The engineer postulates that it is credible that the computer program has unrevealed or undetected faults.
- Could failure of the computer program adversely impact the ability of the SSC to perform safety functions?
  - YES. Faults in the computer program software could produce results that directly affect the design, selection, and layout of pipe supports, which—if not correct—could cause failure of the piping itself.

In this case, the engineer classifies the computer program as **safety-related**.

The next step is to determine if the computer program will be furnished as a basic component from a supplier maintaining an audited or approved nuclear QA program or furnished commercial grade. The engineer determines that the computer program is a commercial-grade product and that it was not designed or manufactured under a nuclear QA program. The engineer completes the technical evaluation by specifying the appropriate technical procurement requirements.

7.1.3 Implementation of the Acceptance Process

The engineer then documents that the commercial-grade computer program must be dedicated for this particular safety-related application.

The engineer reviews records documenting product selection (performed earlier by subject matter experts) to confirm that the computer program functionality was determined to be consistent with applicable engineering methods and approaches. This review also provides insight into the required functionality, intended scope, and range of use.

Based upon identified functions and intended usage, the tables in Section 6 of this report are used to help identify a set of critical characteristics that, once verified, will provide reasonable assurance that the computer program will perform its safety-related function and conform to the procurement document. Characteristics identified include:

- Required functionality
  - Completeness and correctness
  - Specific safety functions and algorithms
- Accuracy/precision/tolerance outputs
- Required interfaces
  - Critical input parameters and valid ranges
  - Output parameters

During the technical evaluation, it became clear that the developer of the commercial off-the-shelf software (COTS) would not allow the use of either Method 2 (commercial-grade survey) or Method 3 (source verification). Therefore, the engineer determined that dedication would have to rely upon special tests and inspections (Method 1) to verify the identified critical characteristics. The engineer works with staff responsible for software acceptance and subject matter experts in the type of analysis being performed to devise a set of tests that will be performed to verify the computer program's critical characteristics:

- The test will be performed with the program installed in its intended operating environment, and testing frequency and intervals will be established that are appropriate for the type of configuration and security controls maintained for the operating environment.
- The commercial computer program testing will involve multiple test scenarios for each type of calculation or function. Scenarios will include sets of design input values that cover the ranges of the input parameters as well as values outside the parameters.
- The acceptable results/range of results for each of the testing scenarios will be determined in advance and verified independently (as correct and accurate) by alternative means.

The engineer recognizes that a standard receipt inspection should be an integral part of the acceptance process, so the following product identification attributes are included in the acceptance plan for verification upon receipt:

- Host computer operating environment identifiers
- Computer program name
- Computer program version identifier
- General condition of the computer program media
- Condition of the packaging

Upon completion of the acceptance activities, the engineer is reasonably assured of the following:

- The computer program is capable of performing its safety function(s).
- Use of the program within specified parameters will result in piping analysis that is accurate and technically correct.
- The resulting design of pipe supports will be appropriate.
- Use of the accepted commercially procured computer program in this application will not have an adverse effect on the safety-related functions of the associated piping.

Note that, in this example, the commercially procured computer program was successfully dedicated for one particular application. This same commercial computer program would not require dedication if it was designated only for use in non-safety-related applications. If the commercial computer program is subsequently required for use in a different safety-related application with different design input parameters and values (for example, analyzing pipe stress in the main steam system), an additional dedication applying the same rigor would be necessary to accept the program for use in the new application.

7.2 Computer Program Used in the Design of a Safety-Related Pump

7.2.1 Introduction

This example describes a scenario where an equipment manufacturer who maintains a nuclear QA program is required to design a replacement pump that the licensee has classified as safety-related (that is, a basic component). The function of the pump is to provide cooling water under normal and accident conditions, thus requiring the pump to perform safety functions during and after an earthquake. The software is used to size critical dimensions associated with the pump casing and impeller and to assist the design engineer with the selection of appropriate materials that will exhibit the necessary strength. The manufacturer's processes require that when a pump is designed using the commercial software, a prototype pump is fabricated based upon the new design and subjected to testing to qualify the design. Once the design is qualified, a new pump will be fabricated for the customer in accordance with the qualified design.

In this example, the computer program is classified **non-safety-related**, thus negating the need for dedication.

7.2.2 Implementation of the Technical Evaluation

The first step of the technical evaluation is to determine the classification of the design computer program. In this case, the engineer opts to perform a functional safety classification considering failure modes and effects. The methodology described in Section 5.4.1 of this report is used, with the following results:

- Is the computer program integral to a safety-related SSC?
  - NO. The computer program being furnished is not integral to the pump.
- Can the computer program impact safety-related SSCs?
  - YES. The computer program will directly affect certain critical dimensions of the pump casing and impeller.
- Will the computer program be used to design or analyze SSCs in a way that could impact SSC safety functions?
  - YES. The computer program is used to design the configuration of the pump casing and impeller.
- Will the results derived using the computer program be independently verified for every use?
  - NO. The mathematical results of calculations will not be independently verified. The engineer proceeds to perform a failure modes and effects analysis keeping in mind that the design that incorporated the results of the software will be independently verified through qualification testing.

    The engineer documents the safety-related functions of the pump under normal and seismic conditions. The engineer documents the function of the design software—to accurately calculate critical dimensions based on verified design input (flow rate, pressure, fluid type, temperature, etc.). The software is used as a tool to perform calculations that replicate a series of mathematical equations.

    The engineer postulates that it is credible that the software has unrevealed or undetected faults.
- Could failure of the computer program adversely impact the ability of the SSC (that is, the pump) to perform safety functions?
  - NO. Failure of the computer program cannot impact the ability of the pump to perform its safety functions. This is because once the design of the pump is completed; a prototype will be built and qualified (as capable of performing its function under normal and accident conditions) via testing as part of the design verification. The worst outcome of using a faulted computer program in this case is an unsuitable design for the licensee's plant-specific application, which will be revealed through failure of the pump when the prototype is subjected to qualification testing.

- Will the computer program be used to assess the ability of SSCs to perform their safety-related function(s)?
  - NO.
- Will the computer program be used to monitor operation and control functions of SSCs?
  - NO.

Therefore, in this case, the engineer classifies the computer program as **non-safety-related**.

7.3 Procurement of an Inventory Management Computer Program

7.3.1 Introduction

This example describes a scenario where a licensee is procuring a commercially available inventory management computer program to upgrade and enhance material control capabilities across their fleet of nuclear power plants.

In this example, the computer program is classified **non-safety-related**, thus negating the need for dedication; but implementation of augmented quality controls is deemed appropriate.

7.3.2 Implementation of the Technical Evaluation

The first step of the technical evaluation is to determine the classification of the computer program. In this case, the engineer opts to perform a functional safety classification considering failure modes and effects. The methodology described in Section 5.4.1 of this report is used, with the following results:

- Is the computer program integral to a safety-related SSC?
  - NO. Thus the guidance provided in this report is applicable.
- Can the computer program impact safety-related SSCs?
  - YES. In this application, the computer program performs administrative functions that could adversely impact the procurement of safety-related SSCs.
- Will the computer program be used to design or analyze SSCs in a way that could impact SSC safety functions?
  - NO. The computer program can in no way alter the design of safety-related SSCs.
- Will the computer program be used in a way that supports quality program requirements (but is not a basic component)?
  - YES.

Therefore, in this case, the engineer classifies the computer program as **non-safety-related,** but applies augmented quality controls in accordance with the organization's QA program to achieve a reasonable level of confidence that the computer program will perform its design functions.

7.4 Procurement of a Commercially Procured Computer Program Used to Perform Seismic Analysis of Components in Safety-Related Systems

7.4.1 Introduction

Specifically, the example describes a scenario where a design engineer at an architectural/engineering organization maintaining an audited and approved nuclear QA program is procuring an analysis computer program that will be used to perform seismic analysis of components installed in safety-related piping systems.

In this example, the computer program is classified **non-safety-related**, thus negating the need for dedication; but implementation of augmented quality controls is deemed appropriate.

7.4.2 Implementation of the Technical Evaluation

The first step of the technical evaluation is to determine the classification of the analysis computer program. In this case, the engineer opts to perform a functional safety classification considering failure modes and effects. The methodology described in Section 5.4.1 of this report is used, with the following results:

- Is the computer program integral to a safety-related SSC?
  - NO. Thus the guidance provided in this report is applicable.
- Can the computer program impact safety-related SSCs?
  - YES. The program will provide data that are associated with the ability of certain components to withstand an earthquake.
- Will the computer program be used to design or analyze SSCs in a way that could impact SSC safety functions?
  - YES. The computer program is used to perform seismic analysis of SSCs.
- Will the results derived using the computer program be independently verified for every use?
  - YES, integral to their design verification process is the requirement that the mathematical accuracy of design and analysis tools is independently verified by alternative calculation. Procedures require that every time the software is used, the mathematical results are verified by independent means. (Design control practices used to ensure correctness and accuracy of results are in accordance with Criterion III of 10CFR50, Appendix B and the architect/engineering organization's design control procedures. It is important to recognize that the design control practices are not

referred to in the architect/engineering organization's procedures as "dedication." In essence, the architect/engineering organization is verifying critical characteristics of the computer program through the implementation of the documented design verification process that is applied for every use of the program.)

Therefore, in this case, the engineer classifies the computer program as **non-safety-related,** but applies augmented quality controls in accordance with the organization's QA program to achieve a reasonable level of confidence that the computer program will perform its design functions.

7.5 Procurement of a Computer Program Used for Monitoring the Operation and Control Functions of Plant SSCs

7.5.1 Introduction

Specifically, the example describes a scenario where a licensee is procuring a commercially available computer program that will be used to monitor the operation and control functions of plant SSCs.

In this example, the computer program is classified **non-safety-related**, thus negating the need for dedication; but implementation of augmented quality controls is deemed appropriate.

7.5.2 Implementation of the Technical Evaluation

The first step of the technical evaluation is to determine the classification of the computer program. In this case, the engineer opts to perform a functional safety classification by considering impact categorization. The methodology described in Section 5.4.2 of this report is used, with the following results:

- Is the computer program High Impact?
  - Does the software have a direct active effect on the ability of a safety-related SSC to perform its intended safety functions?
    - NO.
  - Is the software used for the design of an SSC that ensures that the SSC meets its intended design basis safety function as defined in the nuclear license documents without using alternative methods to verify the results?
    - NO.
- Is the computer program Medium Impact?
  - Is the software used to assess the ability of an SSC to meet its intended safety function?
    - NO.
  - Is the software used to monitor operation and control functions of plant SSCs?
    - YES.

As such, in this case, the engineer categorizes the computer program as **Medium Impact** and thus classifies the computer program as **non-safety-related,** but applies augmented quality controls in accordance with the organization's QA program to achieve a reasonable level of confidence that the computer program will perform its design functions.

7.6 Procurement of a Computer Program Used for Flow-Accelerated Corrosion (FAC) Analysis

7.6.1 Introduction

Specifically, the example describes a scenario where a licensee is ordering a commercially available computer program, EPRI CHECWORKS®, that will be used to assist in the implementation of their flow-accelerated corrosion program. The function of the program is to help prioritize inspections of piping to evaluate corrosion.

In this example, the computer program is classified **non-safety-related**, thus negating the need for dedication; but implementation of augmented quality controls is deemed appropriate.

7.6.2 Implementation of the Technical Evaluation

The first step of the technical evaluation is to determine the classification of the design computer program. In this case, the engineer opts to perform a functional safety classification considering failure modes and effects. The methodology described in Section 5.4.1 of this report is used, with the following results:

- Is the computer program integral to a safety-related SSC?
  - NO. The computer program being furnished is not integral to the piping.
- Can the computer program impact safety-related SSCs?
  - YES. The computer program is not used to design piping, but is used to help analyze piping system corrosion that is experienced during operation. However, the computer program can have some impact on plant piping systems as it is used to help establish programmatic controls associated with monitoring flow-accelerated corrosion of piping systems such as the feedwater system.
- Will the computer program be used to design or analyze SSCs in a way that could impact SSC safety functions?
  - YES. The engineer believes that some impact on piping safety function it might be possible. However, the engineer knows that results derived using CHECWORKS® are only one input considered by the licensee when establishing flow-accelerated corrosion program controls, so impact is unlikely. To be conservative, the engineer selects yes.

- Will the results derived using the computer program be independently verified for every use?
  - NO. Although the results of ultrasonic testing are compared to the results predicted by the program and actual ultrasonic testing results can be used as input for future calculations, the results calculated by the program are not independently verified. Therefore, the engineer will perform a failure modes and effects analysis on the software and postulates that it is credible that the software has unrevealed or undetected faults.
- Could failure of the computer program adversely impact the ability of the SSC to perform safety functions?
  - NO. After careful consideration, the engineer determines that failure of the computer program could not adversely impact the ability of piping systems to perform their safety function. This is because results derived using CHECWORKS® are only one input considered by the licensee when establishing flow-accelerated corrosion program controls. Actual ultrasonic testing results and other inputs are also considered when establishing corrosion control program activities. CHECKWORKS® data are only one of several inputs used by engineers who perform analysis of flow accelerated corrosion. performed Therefore, CHECWORKS® is not the sole means of determining when or where to perform flow-accelerated corrosion inspections. The licensee's flow-accelerated corrosion program includes multiple controls, such as engineering knowledge and expertise, qualification in performance of analyzing the readings/data from calibrated instruments, and review of historical and identified bounding data.
- Will the computer program be used to assess the ability of SSCs to perform their safety-related function(s)?
  - YES. The engineer determines that this question could be answered as YES or NO. After careful consideration of how CHECKWORKS® is used in his organization, he selects YES to be conservative.

Therefore, in this case, the engineer classifies the computer program as non-safety-related, but applies augmented quality controls in accordance with the organization's QA program to achieve a reasonable level of confidence that the computer program will perform its design functions.

7.7 Use of Legacy Software for a Previously Accepted Application

7.7.1 Introduction

In this example, the civil engineering department at a nuclear power plant is conducting the static structural analysis of a safety-related diesel generator building using the finite element software ANSYS that has been previously approved for use within the organization's software QA program.

A model of the building is created using ANSYS SHELL43 elements, the number of degrees of freedom is 200,000, and ANSYS PCG solver is used to obtain the solution.

In determining the applicability of this guidance in the use of ANSYS Release 12 to solve the above problem, the engineer used the methodology described in Figure 1-4, "Applicability of Guidance to Legacy Computer Programs," of this report.

7.7.2 Implementation of the Methodology

- Has the computer program been accepted and controlled under the supplier/licensee quality assurance program?
  - YES.
- Does evidence exist that the software was accepted for identified end uses, defined capabilities and limitations?
  - YES. Test plans were prepared with test results obtained by running sample problems provided by ANSYS to confirm operation of the program for its intended use within the specified limitations.
- Does intended use of the program fall within the parameters of use that were previously approved?
  - YES. The Engineer verified that ANSYS was applicable and capable for use of models with up to 300,000 degrees of freedom, which encompass the requirements of this problem.
- Was the computer program revised (for example, a new revision or version)?
  - NO. A legacy version of the software will be used (that is, ANSYS Release 12.)

Accordingly, the engineer determined that the existing acceptance of ANSYS Release 12 to conduct the static analysis of the diesel generator building using ANSYS SHELL43 elements and PCG solver is sufficient, and no action is required.

In this example, it was **not** necessary to subject the legacy computer program to the requirements of this guidance.

7.8 Use of Legacy Software for a New Application

7.8.1 Introduction

In this example, the civil engineering department at a nuclear power plant is conducting the dynamic analysis of a safety-related piping system using the finite element software ANSYS that has been previously approved for use within the organization's software QA program.

The model of the piping system is analyzed using the multi-point response spectrum method, the model is created using ANSYS PIPE16 and PIPE18 elements, the number of degrees of freedom is 1000, and ANSYS sparse block lanczos solver is used to obtain the solution.

In determining the applicability of this guidance in the use of ANSYS Release 12 to solve the above problem, the engineer used the methodology described in Figure 1-4, "Applicability of Guidance to Legacy Computer Programs," of this report.

7.8.2 Implementation of the Methodology

- Has the computer program been accepted and controlled under the supplier/licensee quality assurance program?
  - YES.
- Does evidence exist that the software was accepted for identified end uses, defined capabilities and limitations?
  - NO. The program dynamic capabilities were tested for the dynamic analysis of SSCs using the single-point response spectrum method, whereas the multi-point response spectrum method is intended/proposed for the current application.

Although no longer a deciding factor at this point in this example, the engineer still verified that ANSYS was applicable and capable for use in the solution of dynamic models with up to 300,000 degrees of freedom, which encompass the requirements of this problem. Also, the engineer verified that a newer version of the software was not available or being considered for use in this application.

Because the previous acceptance of ANSYS Release 12 did NOT sufficiently validate or test this software for the new application, the engineer determined that the use of ANSYS Release 12 for this new application should be subjected to the requirements of this guidance. The engineer will use the guidance provided in Sections 4, 5, and 6 of this report to determine the appropriate classification and acceptance of this software for the intended use.

Section 8: References and Bibliography

The following references were used during the development of this report.

8.1 In-Text References

1. U.S. Code of Federal Regulations, Title 10, Chapter 1, Appendix B to Part 50, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Facilities, Office of the Federal Register, National Archives and Records Administration, U.S. Government Printing Office, Washington, DC.

2. U.S. Code of Federal Regulations, Title 10, Chapter 1, Part 21, Reporting of Defects and Noncompliance, Office of the Federal Register, National Archives and Records Administration, U.S. Government Printing Office, Washington, DC.

3. U.S. Nuclear Regulatory Commission, Safety Evaluation Report (SER), "Review of EPRI Topical Report TR-106439, *Guideline on Evaluation & Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications*," (TAC No. M94127), (ADAMS accession number 9810150223).

4. *Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications (NCIG-07).* EPRI, Palo Alto, CA: June 1988. NP-5652.

5. *Supplemental Guidance for the Application of EPRI Report NP-5652 on the Utilization of Commercial Grade Items.* EPRI, Palo Alto, CA: March 1994. TR-102260.

6. *Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications.* EPRI, Palo Alto, CA: November 1996. TR-106439.

7. Quality Assurance Requirements for Nuclear Facility Applications (QA), ASME NQA-1-2008 (edition). American Society of Mechanical Engineers, New York, NY: 2008.

8. Quality Assurance Requirements for Nuclear Facility Applications (QA), ASME NQA-1a-2009 (addenda). American Society of Mechanical Engineers, New York, NY: 2009.

9. U.S. Code of Federal Regulations, Title 10, Chapter 1, Part 50, Domestic Licensing of Production and Utilization Facilities, Office of the Federal Register, National Archives and Records Administration, U.S. Government Printing Office, Washington, DC.

10. Combining Licenses, 10CFR50.52. Licenses, Certifications, and Approvals For Nuclear Power Plants, Government Printing Office, Washington, D.C.

11. *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants.* EPRI, Palo Alto, CA: December 1996. TR-107330.

12. *Guidelines for the Technical Evaluation of Replacement Items in Nuclear Power Plants: Revision 1.* EPRI, Palo Alto, CA: June 2006. 1008256.

13. *Handbook for Evaluating Critical Digital Equipment and Systems.* EPRI, Palo Alto, CA: November 2005. 1011710.

14. *Plant Support Engineering: Information for Use in Conducting Audits of Supplier Commercial Grade Item Dedication Programs.* EPRI, Palo Alto, CA: June 2008. 1016157.

15. *"Nuclear Procurement Program Improvements." Nuclear Utility Management and Resources Council, Incorporated, Washington, D.C.:1990. NUMARC 90-13*

16. *Guidelines for the Safety Classification of Systems, Components, and Parts Used in Nuclear Power Plant Applications (NCIG-17).* EPRI, Palo Alto, CA: February 1991. NP-6895.

17. *IEEE STD-500, IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations Institute of Electrical and Electronics Engineers: Computer Society, Washington, D.C.: 1984.*

18. Nuclear Information Technology Strategic Leadership, Guidance Document to Implement Policy for Software Quality Assurance in the Nuclear Power Industry, Revision 1, NITSL-SQA-2005-02, January 2009.

19. *Guidelines for Optimizing the Engineering Change Process for Nuclear Power Plants, Revision 2, EPRI, Palo Alto, CA: November 2007. 1008254*

20. *Guidelines for Performance-Based Supplier Audits (NCIG-16).* EPRI, Palo Alto, CA: June 1990. NP-6630.

21. 10CFR50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants.

22. Determination of Exclusion Area, Low Population Zone, and Population Center Distance, 10CFR100.11. Government Printing Office, Washington, D.C.

23. NUREG-0302 Rev. 1 Remarks Presented (Questions/Answers Discussed) at Public Regional Meetings to Discuss Regulations (10 CFR Part 21) for Reporting of Defects and Noncompliance July 12–26, 1977.

24. NITSL-SQA-2005-01, Policy for Software Quality Assurance in the Nuclear Power Industry, Revision 0, March 2005.

25. IEEE Standard for Software Verification and Validation. IEEE 1012-1998.

26. Packaging, Shipping, Storage and Handling of Items for Nuclear Power Plants, American Society of Mechanical Engineers, New York, NY: 1978. ANSI/ASME N45.2.2, 1978

27. U.S. Nuclear Regulatory Commission. Generic Letter 89-02: Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products (Agencywide Reports Access and Management System (ADAMS) Accession No. ML031140060). Government Printing Office, Washington, D.C. March 1989.

28. U.S. Nuclear Regulatory Commission Information Notice 2011-01, Commercial-Grade Dedication Issues Identified During NRC Inspections (Agencywide Reports Access and Management System (ADAMS) Accession No. ML103220180), Government Printing Office, Washington, D.C.: February 2011.

29. U.S. Nuclear Regulatory Commission, Computer Program Error Report Handling, Information Notice 86-77. (Agencywide Reports Access and Management System (ADAMS) Accession No. ML31250196) Government Printing Office, Washington, D.C.: August 1986.

30. U.S. Code of Federal Regulations, Title 10, Chapter 1, Part 50, Section 34(a)(1), Contents of Applications; Technical Information, 10CFR50.34(a)(1). Government Printing Office, Washington, D.C.: June 2009.

31. *Evaluating Commercial Digital Equipment for High-Integrity Applications: A Supplement to EPRI Report TR-106439.* EPRI, Palo Alto, CA: December 1997. TR-107339.

32. IEEE 730-2002, IEEE Standard for Software Quality Assurance Plans. Institute of Electrical and Electronics Engineers: Computer Society, Washington, D.C.: 2002.

33. *IEEE/EIA 12207.0, IEEE Standard for Information Technology – Software Life Cycle Processes,* Institute of Electrical and Electronics Engineers: Computer Society, Washington, D.C.: 1996

34. *IEC 60880, Nuclear Power Plants-Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions, International Electrotechnical Commission, Geneva, Switzerland*.

35. *ANSI/ISO/ASQ Q9001*:2008, American National Standard, Quality Management Systems – Requirements, American National Standards Institute/International Organization for Standardization/American Society for Quality, 2008.

36. *Handbook for Verification and Validation of Digital Systems.* EPRI, Palo Alto, CA: December 1998. TR-103291.

8.2 Bibliography

8.2.1 Regulatory Documents

10CFR50.2, Definitions, Office of the Federal Register, National Archives and Records Administration, U.S. Government Printing Office, Washington, DC.

Canadian Nuclear Safety Commission. Computer Programs Used in Design and Safety Analysis of Nuclear Power Plants and Research Reactors, G-149. CNSC, Ottawa, Ontario: October 2000.

Conditions of Construction Permits, Early Site Permits, Combined Licenses, and Manufacturing Licenses, 10CFR50.55(e). Government Printing Office, Washington, D.C.: August 2007.

NUREG 0800, Chapter 7, BTP 7-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, Revision 5, Washington, D.C.: March 2007.

NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems. Lawrence Livermore National Laboratory, Livermore, CA: January 1994.

U.S. Nuclear Regulatory Commission, Computers in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.152. Government Printing Office, Washington, D.C.

U.S. Nuclear Regulatory Commission. Generic Letter 91-05: Licensee Commercial-Grade Procurement and Dedication Programs. Government Printing Office, Washington, D.C. April 1991.

U.S. Nuclear Regulatory Commission. Inspection of Commercial-Grade Dedication Programs: IP43004. Government Printing Office, Washington, D.C. October 2007.

U.S. Nuclear Regulatory Commission. Regulatory Issue Summary 2000-18: Guidance on Managing Quality Assurance Records in Electronic Media. Government Printing Office, Washington, D.C. 2000.

U.S. Nuclear Regulatory Commission. Criteria for Use of Computers in Safety Systems of Nuclear Power Plants. USNRC Regulatory Guide 1.152, Revision 2, Washington, D.C.: January 2006.

U.S. Nuclear Regulatory Commission. Quality Assurance Program Requirements (Operational). USNRC Regulatory Guide 1.33, Revision 2, Washington, D.C., February 1978.

U.S. Nuclear Regulatory Commission. Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants. USNRC Regulatory Guide 1.168, Revision 1, Washington, D.C.: February 2004.

8.2.2 EPRI Technical Reports

Computerized Procedure Systems Guidance on the Design, Implementation, and Use of Computerized Procedure Systems, Associated Automation, and Soft Controls. EPRI, Palo Alto, CA: August 2010. 1015313.

Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants. EPRI, Palo Alto, CA: December 1996. TR-107330.

8.2.3 Reference Documents

ANS-10.7-201: Non-Real Time, High Integrity Software for the Nuclear Industry (new draft standard). American Nuclear Society, La Grange Park, IL.

ANSI N45.2, Quality Assurance Program Requirements for Nuclear Power Plants. American National Standards Institute, Washington, D.C.

ANSI/ANS-10.2-2000; R2009: Portability of Scientific and Engineering Software. American Nuclear Society, La Grange Park, IL: 2009. 240243.

ANSI/ANS-10.4-2008, Verification and Validation of Non-Safety-Related Scientific and Engineering Computer Programs for the Nuclear Industry. American Nuclear Society, La Grange Park, IL: 2008. 240277.

IEEE Guide to the Software Engineering Body of Knowledge. Institute of Electrical and Electronics Engineers: Computer Society, Washington, D.C.: 2004.

IEEE Standard Computer Dictionary. A Compilation of IEEE Standard Computer Glossaries. IEEE 610-1991.

IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations. IEEE 7-4.3.2 (2003).

IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations. IEEE 603-1998.

IEEE Standard for Software Reviews and Audits. IEEE 1028-2008.

Software Engineering - Guide to the Software Engineering Body of Knowledge (SWEBOK). International Organization for Standardization and the International Electrotechnical Commission, Genève, Switzerland: September 2005. ISO/IEC TR 19759:2005.

U.S. Department of Energy, Quality Assurance: Improving Safety Software Quality. DOE O 414.1C, Washington, D.C.: June 2005.

U.S. Department of Energy, Safety Software Guide for Use with 10 CFR 830, Subpart A, Quality Assurance Requirements. DOE G 414.1-4, Washington, D.C.: June 2005.

Appendix A: Guidance for Specifying Technical, Quality, and Documentation Requirements

As part of the technical evaluation, the software being procured is specified correctly. This typically involves specifying the correct technical, quality and documentation requirements in the procurement document.

A.1 Specifying Technical Requirements

Technical requirements should be a translation of the design of the software into procurement requirements. The licensee should develop procurement documents that specify the software requirements to ensure that the vendor meets the design intent.

Software that is purchased as commercial off-the-shelf (COTS) or "shrink wrapped" should be subjected to adequate testing to ensure that it meets the expectations of the requesting organization. Many times, this requires the organization to develop a functional requirements document and acceptance tests to demonstrate that their expectations are met.

During the proposal stage, especially for customized software, it is important to ensure that the vendor or consultant understands and commits to the quality of the deliverables. Organizations should develop a functional requirements document to assist with vendor and customer understanding of expectations.

Vendor deliverables should be similar to those generated by in-house staff although some may be considered proprietary and may not be included in the deliverable. At a minimum, the vendor should supply test cases that demonstrate that the software meets the expected requirements.

The vendor or consultant should understand and have experience producing appropriate quality documentation so that a proposal adequately covers the effort required to generate these documents.

If planning to dedicate commercial-grade software for a safety-related application, the purchasing organization should:

- Identify and document, in the functional requirements, those critical design characteristics that the software must possess to accomplish the intended safety functions.
- Carry out mock-up testing at the vendor facility and/or the utility.
- Establish critical acceptance characteristics, and in test documentation, demonstrate that the safety functions the computer program must perform are acceptably implemented.

A.2 Specifying Quality Requirements

The quality requirements for computer software should be developed and specified in the procurement document to invoke the necessary supplier controls over manufacturing, design, and purchasing activities that ensure that the specified technical requirements of the software are met. The specification should also delineate anticipated quality assurance program responsibilities between the licensee and various organizations in the supply chain.

Appropriate quality requirements should be specified that reflect the supplier's software quality program/controls that have been audited (in the case of suppliers with nuclear QA programs) or surveyed (in the case of suppliers with commercial QA programs). The licensee should establish conditions in procurement documents to ensure the control of quality by the supplier or consultant when providing software and/or services.

Quality requirements do not take the place of or substitute for technical requirements. Computer software that is technically inadequate can be produced under an acceptable software quality assurance program, but it will remain technically inadequate (that is, unsuitable) for the application.

When specifying computer software quality requirements, it is necessary to understand the supplier's use of sub-suppliers and material sources to ensure that appropriate quality requirements are passed on and specified correctly through the supply chain.

Suppliers or consultants who provide software that is included in safety-related plant systems or as basic components are required to maintain an SQA program equivalent to that maintained by the utility. In these cases, the supplier's nuclear QA program—as well as 10CFR21—should be specified. These programs should be audited by the utility for adequacy. Information regarding the adequacy of the supplier's or consultant's QA program, to implicitly include software, should be maintained on a list of vendors approved to provide basic components.

The quality requirements for commercial-grade computer software to be used in nuclear safety application need special consideration. Commercial-grade purchases should not have nuclear-unique standards imposed in the purchase documents (that is, 10CFR50 Appendix B and 10CFR21).

Typically, the quality requirements specified in the procurement document will include the following:

- Quality Assurance Program Requirements – For safety-related computer software, this would typically be the specification of a nuclear QA program. Supplier QA programs such as 10CFR50 Appendix B or ASME/ANSI NQA-1 are typically recognized as nuclear QA programs acceptable for use in providing the licensee with a basic component. - For non-safety-related computer programs, commercial QA program requirements such as compliance with ISO-9001 may be specified as appropriate.
- Other special quality requirements may include any of the following:
  - Rights of access provisions for inspection/audit/surveillance
  - Error notification from the supplier (if within their capabilities and contractually defined)
  - Hold points necessary to perform inspection, audit, and surveillance activities.
  - Special shipping, storage, and handling requirements for media or firmware in procurement documents, taking into consideration temperature, humidity, electromagnetic interference, etc.
  - QA and development record retention requirements (period of time that seller must maintain applicable records)
  - Provisions to maintain a copy of source code in escrow that can be released to the buyer if defined circumstances render the seller unable to support the products

A.3 Specifying Documentation Requirements

The amount of supplier documentation necessary will vary depending on how the computer software has been classified (that is, safety-related or non-safety-related). In general, supplier documentation is required to furnish the licensee with objective evidence that the technical and quality requirements of purchased software have been met. Documentation should be considered as a tool in the verification of the software's technical adequacy and quality compliance, but it should not be relied upon without confirmation of its validity.

Supplier documentation requirements should correlate with the specified technical and quality requirements and be specific as to the content. Care should be taken not to request excessive or meaningless documents or test reports that are not applicable to the software or its associated safety-related components. Certificates of Conformance should not rely solely on generalized statements such as, "This software meets the requirements of the purchase document." Instead the documentation should be validated by the licensee and should contain specific statements enabling the supplier to verify specified requirements. In any case, the licensee should be involved in the acceptance process.

The range of supplier documentation typically includes, as applicable, the following (including consideration of quantity and type of media):

- Personnel certifications and qualifications
- Inspection reports
- SQA manual (if provided and available)
- Test reports
- Certificates of Conformance/Compliance
- Audit reports of sub-suppliers, if appropriate

A submittal schedule should be specified to inform the supplier when each required document needs to be made available to the licensee for review. Retention time of records should also be specified, as well as the quality and legibility of the records, where necessary, to ensure future reproduction capability.

Appendix B:Practical Quality Assurance Considerations for Software Dedication

B.1 Testing Environment

Computer programs should be tested on the same platform (that is, operating system) and in the same environment (that is, hardware) in which they will be used. Considerations should be made for controlling the installation and use of safety-related software.

B.2 Scope and Frequency of Dedication

Commercial-grade dedication is based upon identified safety functions or applications. It is possible to dedicate commercial-grade software with multiple capabilities for use in an application that requires only a subset of the computer program's capabilities. The dedication could be further limited to a certain range of inputs or variables, based upon the scope of work for which the software is being used.

When software dedication is application- or range-specific, use of the safety-related software should be controlled in accordance with the scope of applications for which it is dedicated.

Additional or different critical characteristics may be required to be verified prior to using dedicated software to perform functions not addressed in the original dedication evaluation:

- To take advantage of computational capabilities (functions) that were not included in the original dedication
- To perform calculations that are beyond the scope or range of calculations for which the software was originally dedicated.

New versions of computer programs (or those not previously dedicated) require revisiting the technical evaluation and acceptance processes to ensure that they remain suitable for their intended use and that they are acceptable.

B.3 Applicability of Reporting Requirements

The requirements of 10CFR21 for reporting defects and noncompliance apply to basic components, including computer programs when they are considered a basic component.

Provisions should be in place to ensure that proper screening is conducted and applicable reporting in accordance with 10CFR21 is initiated when errors or "bugs" are identified that could impact the functions of computer programs that are dedicated for safety-related use. Errors may be identified by the entity using the computer program, or they may be reported to the computer program user by the computer program developer or other computer program users.

B.4 Applicability of Guidance to Existing Computer Programs

The guidance in this report is not required to be used for ensuring the quality of computer programs used in safety-related applications that have been accepted prior to the issuance of this guidance if the following conditions have been met:

1. Documentation of the following activities exists for the computer program:
   - Capabilities and limitations for its intended use
   - Test plans and results to demonstrate the capabilities within the limitations
2. Control of the computer program under the supplier/licensee QA program

However, changes in or expansion of the use of the computer program or a revision to the computer program itself (that is, a software update) will subject the computer program to the guidance contained in this report.

B.5 Applicability of Cyber Security Requirements

Successful commercial-grade dedication does not exclude the dedicating entity from meeting applicable cyber security requirements., -. Cyber security precautions should be implemented in accordance with applicable requirements when necessary.

It may be necessary to implement measures designed to ensure that the integrity of the computer program has not been compromised from a cyber security perspective. For example, testing to ensure that the computer program is functioning as intended could be performed prior to and after use of the program to provide assurance that the computer program was not compromised (in a way that impacts critical characteristics) before or during the testing program.

Appendix C:Computer Program Categories and Uses

Many types of computer programs are used by nuclear power generation facilities and the organizations that support them, including:

- Design computer programs
- Analysis computer programs
- Computer programs integral to plant SSCs
- Administrative support computer programs
- Operations support computer programs
- Measurement and test equipment computer programs
- Manufacturing computer programs

Section 3 of this report discusses examples of design and analysis computer programs. Other categories are discussed below.

C.1 Computer Programs Integral to Plant SSCs

A computer program that is integral to a plant SSC is not included in the scope of this report because guidance for accepting this type of software is already available and has been evaluated for use by the U.S. Nuclear Regulatory Commission.

Examples of plant SSCs that rely upon integral computer programs include devices such as:

- Programmable logic controllers
- Plant computers
- Digital control systems
- Smart transmitters
- Embedded microprocessors, programmable read-only memory devices (PROMs)
- Erasable programmable read-only memory devices (EPROMs)

Guidance for accepting devices with integral computer programs may be found in the following EPRI reports:

- *Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications*, TR-106439 [6] and U.S. NRC Safety Evaluation Report "Review of EPRI Topical Report TR-106439, *Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications*," (TAC No. M94127), Adams Accession number 9810150223 [3]
- *Evaluating Commercial Digital Equipment for High-Integrity Applications: A Supplement to EPRI Report TR-106439*, TR-107339 [31]
- *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*, TR-107330 [11]
- *Handbook for Evaluating Critical Digital Equipment and Systems*, 1011710 [13]

C.2 Administrative Support Computer Programs

Many administrative processes are facilitated by the use of computer programs. These computer program applications range from programs with a single function to complex, integrated systems that integrate plant processes to enhance reporting, tracking, scheduling, and access to information.

Examples of computer programs that might support administrative processes include the following:

- Computer-aided design programs such as Microstation from Bentley Systems, Incorporated and AutoCAD from Autodesk, Incorporated.
- Engineering process computer programs such as Intergraph's SmartPlant foundation
- Office-oriented computer programs such as Microsoft Word, Excel, Access, Outlook, and PowerPoint; Sun's OpenOffice; and so forth
- Integrated inventory, maintenance, and procurement systems including enterprise resource planning (ERP) and enterprise asset management (EAM) suites such as Ventyx Asset Suite (PassPort), IBM Maximo, and SAP
- Record and document management computer programs such as EMC Corporation's Documentum and IBM's FileNet
- Corrective action tracking systems such as DevonWay's AIM Express
- Software used to develop/conduct training such as Microsoft PowerPoint and the Institute of Nuclear Power Operations NANTeL
- Computer programs used to manage historical information such as OSIsoft's PI and InStep Software, LLC's eDNA
- Network and interface programs

These types of computer programs typically perform non-safety-related functions. However, additional (that is, augmented) quality controls may be warranted depending upon the way in which the programs are implemented, configured, relied upon, and used to meet licensee-specific commitments, regulatory commitments, and/or quality program requirements. A functional safety classification should be performed to evaluate the computer program based upon its specific functions.

C.3 Operations Support Computer Programs

Computer programs used by operations personnel include computerized procedure systems as well as other computer programs that provide real-time information regarding equipment status or reference data. These procedures may include normal operating procedures, abnormal operating procedures (AOPs), alarm response procedures (ARPs), surveillance procedures, and/or emergency operating procedures (EOPs). Operators may use computerized procedures inside or outside the main control room (for example, at the remote shutdown station). In some cases, these systems may be used by craftspeople to support plant maintenance activities.

Operations support computer programs can be designed to provide different levels of functionality and automation. Because the guidelines and criteria that are applicable to design and implementation of computerized procedure systems depend upon the types of functionality provided, it is helpful to define categories of computerized procedure systems based on their functionality.

C.4 Measurement and Test Equipment Computer Programs

Measurement and test equipment (M&TE) computer programs include software that is integral to M&TE as well as computer programs used to manage the calibration program. An example of M&TE software is National Instrument's LabVIEW (Laboratory Virtual Instrumentation Engineering Workbench), which is a platform and development environment for visual programming used to automate the use of laboratory processing and measuring equipment.

M&TE computer programs are controlled in accordance with licensees' QA programs in accordance with Criterion XII. "Control of Measuring and Test Equipment" of 10CFR50, Appendix B [1], which states:

> Measures shall be established to assure that tools, gages, instruments, and other measuring and testing devices used in activities affecting quality are properly controlled, calibrated, and adjusted at specified periods to maintain accuracy within necessary limits.

An example of these measures is the use of known standards (traceable to the National Institute of Standards and Technology) at appropriate intervals (such as before and after each calibration) to verify accuracy and functionality of the automated M&TE.

Detailed guidance regarding the quality and calibration of measurement and test equipment is included in licensee implementing standards and procedural control. Therefore, computer programs associated with measurement and test equipment are not considered to be in the scope of computer programs that might require commercial-grade item dedication when measures (such as verification using know standards) are in place to ensure and maintain accuracy.

C.5 Manufacturing Computer Programs

Examples of computer programs used during the manufacture of plant SSCs include computer programs that control machinery, statistical process control computer programs, process automation computer programs, and so forth.

Computer programs used in manufacturing applications that are used to produce items are not safety-related when the items produced are verified as meeting design requirements using independent verification methods such as inspection and testing.

The extent to which this type of computer program may or may not perform a safety-related function depends upon the way in which the programs are implemented, configured, relied upon, and used. Quality control processes are typically in place to verify product conformance and acceptability after manufacturing is complete. In these cases, manufacturing software is typically classified as non-safety-related. However, a functional safety classification can be performed to evaluate the computer program based upon its specific functions and relationship with safety-related plant components and parts. If the computer program is the sole means of communicating quality information (such as quality control acceptance criteria cited in work documents), a functional safety-classification should be performed.

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute Inc., (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent more than 90 percent of the electricity generated and delivered in the United States, and international participation extends to 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together...Shaping the Future of Electricity

Programs:

Nuclear Power

Plant Engineering

1025243

Electric Power Research Institute

3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA

800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com