Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications

TR-106439

Final Report, October 1996

Prepared by
EPRI Working Group on Use of
Commercial Digital Equipment in
Nuclear Safety Applications
with
MPR Associates, Inc.
Alexandria, Virginia

Prepared for
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, California 94304

EPRI Project Manager
R. C. Torok
O&M Cost Control Technology Target
Nuclear Power Group

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS REPORT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS REPORT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS REPORT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS REPORT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS REPORT.

ORGANIZATION(S) THAT PREPARED THIS REPORT

MPR ASSOCIATES, INC.

ORDERING INFORMATION

Requests for copies of this report should be directed to the EPRI Distribution Center, 207 Coggins Drive, P.O. Box 23205, Pleasant Hill, CA 94523, (510) 934-4212. There is no charge for reports requested by EPRI member utilities.

Electric Power Research Institute and EPRI are registered service marks of Electric Power Research Institute, Inc.

Copyright © 1996 Electric Power Research Institute, Inc. All rights reserved.

REPORT SUMMARY

Nuclear power plants are increasingly upgrading their instrumentation and control (I&C) systems with commercial digital equipment, which allows them to continue meeting safety and reliability requirements while controlling operating costs. However, the use of commercial software-based devices for safety-related applications has raised new issues that impact design, procurement, and licensing activities. This guideline describes a consistent, comprehensive approach for the evaluation and acceptance of commercial digital equipment for nuclear safety systems.

BACKGROUND

In response to growing challenges of obsolescence and increasing maintenance costs, nuclear utilities are replacing and upgrading selected I&C equipment. Upgrades typically involve changes from analog to digital technology, with proven commercial products often providing practical solutions. New concerns, however, have accompanied the use of digital equipment for safety-related applications, including the potential for common-mode failure of redundant components, electromagnetic interference (EMI), and human-machine interface problems. When commercial off-the-shelf software is used, added complications arise, primarily related to demonstrating the adequacy of the supplier's software development process and documentation. The commercial-grade item dedication process nuclear utilities commonly use to evaluate and accept commercial components for use in safety-related applications was not developed with software-based equipment in mind. Hence, for software-based systems, utilities require a consensus approach to help standardize the treatment of commercial equipment while ensuring safety, reliability, and cost-effectiveness.

OBJECTIVES

To guide utilities in evaluating and accepting commercial-grade digital equipment for nuclear safety-related applications.

APPROACH

An EPRI-sponsored working group of utility and industry representatives developed this guideline document. Their consensus approach addresses digital issues within the context of the commercial-grade item dedication process, providing supplemental guidance as necessary. Working group participation and review by industry representatives and regulators proved invaluable in strengthening and refining the

document. This project may serve as a useful model for future activities that have regulatory impacts.

RESULTS

This guideline will help utilities evaluate, design, and implement digital upgrades involving commercial software-based equipment. It will also prove useful in obtaining regulatory approvals for such equipment, when required. The guideline relies on the established commercial-grade item dedication process, with supplemental guidance to help the user address digital-specific issues. It emphasizes testing, analysis, vendor assessments, and careful review of operating experience to ensure adequate safety and reliability and address the associated technical and regulatory issues.

This guidance is designed for use by utilities and other organizations that dedicate commercial-grade equipment for nuclear safety applications. Not developed as a new standard, the guide references existing industry standards and guidelines, as appropriate. It is intended to be compatible with utility-specific change processes, including graded approaches for quality assurance. While the guideline is designed primarily for digital upgrades to safety systems, it should also be helpful in nonsafety applications that require high reliability.

EPRI PERSPECTIVE

Both the nuclear power industry and the NRC have recognized the potential for enhanced safety and reliability afforded by commercial digital equipment. This guideline will help its users avoid problems that nuclear plants and other industries have experienced with digital equipment. Most often, problems arise because digital devices are treated as "black boxes," with inadequate understanding leading to unexpected and unwanted behaviors. For both cost and safety reasons, nuclear utilities must have sufficient knowledge of the workings of the device to anticipate the types of failures and abnormal conditions that could arise. Accordingly, design engineers, system engineers, and users should be active in all phases of a plant change that involves software-based equipment. EPRI expects the framework in this guideline to be compatible with future guidelines and standards that apply to the evaluation and use of commercial software-based equipment. It is hoped that this guideline will receive endorsement and wide usage by the nuclear power community.

INTEREST CATEGORIES

Plant support engineering
Instrumentation and control
Assessment and optimization

KEY WORDS

Digital upgrade
Instrumentation and control
Licensing
Commercial-grade item dedication
Commercial off-the-shelf (COTS) software

ABSTRACT

In response to growing challenges of obsolescence and increasing maintenance costs, nuclear utilities are replacing and upgrading selected instrumentation and control equipment. Upgrades typically involve changes from analog to more modern, digital technology, and in many cases proven commercial products offer practical solutions. However, the use of commercial software-based equipment raises concerns, especially in nuclear safety-related applications. For commercial software-based systems, not developed strictly in accordance with nuclear standards, appropriate methods and criteria must be used in judging the acceptability of this equipment for use in safety-related applications.

This guideline document describes an approach for evaluation and acceptance of commercial software-based equipment in nuclear safety systems. The guidance is intended for use by utilities or other organizations who perform dedication of commercial grade digital equipment for nuclear safety applications. The approach is based on the use of the existing commercial grade item dedication process, with supplemental guidance provided to help the user address digital-specific issues. The approach emphasizes identification of appropriate critical characteristics with subsequent verification through testing, analysis, vendor assessments and careful review of operating experience. This guide is not intended to be a new standard; it references existing industry standards and guidelines as appropriate. The guide is intended primarily for digital upgrades to safety systems, but it should also be useful in non-safety applications that require high reliability. The guidance is intended to be compatible with utility-specific change processes, including graded approaches for quality assurance.

ACKNOWLEDGMENTS

The following individuals are members of the EPRI Working Group on Use of Commercial Digital Equipment in Nuclear Safety Applications and contributed to the development of this document. Their support is gratefully acknowledged.

Bruce Geddes, Chairman	Baltimore Gas and Electric
Charles Waite, Past Chairman	Public Service Electric and Gas
Janardan G. Amin	TU Electric
Jess Betlack	MPR Associates
Martin Cohen	Johnson Yokogawa Corporation
Randy Crane	NUS Idaho Center
James M. Dean	Applied Energy Services
Ray DiSandro	PECO Energy Company
Bob Fink	MPR Associates
Wayne H. Glidden	Duquesne Light Company
Diljit Gulati	Commonwealth Edison Company
Dennis A. Harris	Triconex Corporation
John Hefler	Pacific Gas & Electric
Dave Herrell	Public Service Electric and Gas
Kevin Holmstrom	Northern States Power
Timothy E. Hurst	Hurst Consulting, Inc.
Ron Jarrett	Tennessee Valley Authority
James T. Keiper	Foxboro Company
Chris Kelly	Westronics
David A. Kulp	Yankee Atomic Electric Company
Paul Lantz	Fluke Corporation
Rory Mackie	Houston Lighting & Power
Antonio Mancini	Eaton Corporation
Randall S. May	S. Levy Incorporated
Joseph Naser	Electric Power Research Institute
Walt Pelenski	GPU Nuclear - Oyster Creek NGS
Ifti Rana	Southern Company Services
Dave Reigel	GE Nuclear Energy
Marty Ryan	ABB Combustion Engineering
Jim Stewart	U.S. Nuclear Regulatory Commission
Keith Swing	Raytheon Nuclear, Inc.
Ray Torok	Electric Power Research Institute
Gerard van Noordennen	Northeast Utilities System, Millstone NPS
Carl A. Vitalbo	Westinghouse Electric Corporation

CONTENTS

1 INTRODUCTION 1-1
1.1 Background 1-1
1.2 Purpose 1-3
1.3 Scope 1-4
1.4 Content of This Guideline 1-5

2 DEFINITIONS AND TERMINOLOGY 2-1

3 OVERVIEW 3-1
3.1 The Problem: Obtaining an Adequate Level of Assurance with Commercial Digital Equipment 3-1
Assurance for Nuclear Grade Equipment 3-3
Equivalent Assurance for Commercial Equipment 3-3
Supplemental Effort and Cost 3-6
Demonstrating vs Adding Quality 3-7
3.2 Existing Guidance on Design and Licensing of Digital Systems 3-7
3.3 Existing Guidance on Commercial Grade Item Dedication 3-8

4 EVALUATION AND ACCEPTANCE 4-1
4.1 The Process: A Combination of Design and Procurement Activities 4-1
4.2 Guidance on Defining and Verifying Critical Characteristics 4-4
4.3 Additional Guidance 4-15
Application to Different Types of Changes 4-15
Timing of Activities in the Process 4-15
Technical Reviews and Expertise Required 4-16
Who and Where to Survey 4-17
Iteration on Requirements and Critical Characteristics 4-17
Requirements on the Dedicator 4-18
Dedicating for Multiple Applications 4-18

Documenting Engineering Judgment *4-19*

5 MAINTENANCE OF A COMMERCIAL DEDICATION 5-1
5.1 Product Changes Including Software/Firmware Revisions 5-1
5.2 Operating Within the Bounds of the Original Dedication 5-2
5.3 10 CFR 21 Reporting 5-2
5.4 Third Party Dedicators 5-3
5.5 Long-Term Support Issues 5-4

6 EXAMPLES 6-1
6.1 Simple Indicator 6-1
6.2 Indicator With Contact Output 6-6
6.3 Multi-Function Controller 6-11
6.4 ESFAS Upgrade Using PLCs 6-19

7 REFERENCES 7-1

LIST OF FIGURES

Figure 3-1 Overview: Approaches for Licensing Digital Equipment and Dedicating Commercial Grade Items are Combined to Address Commercial Grade Digital Equipment. 3-2

Figure 3-2 Equivalent Level of Assurance for Nuclear Grade and Commercial Grade Digital Equipment 3-5

Figure 4-1 Commercial Grade Item Dedication in the Context of the Upgrade Process 4-3

Figure 6-1 ESFAS Architecture Using Multiple PLCs 6-20

LIST OF TABLES

Table 4-1 Critical Characteristics Matrix for Digital Equipment 4-6

Table 4-2 Assessment of "Built-in Quality" for Commercial Digital Equipment..... 4-12

Table 6-1a Simple Indicator Critical Characteristics - Physical..... 6-3

Table 6-1b Simple Indicator Critical Characteristics - Performance..... 6-4

Table 6-1c Simple Indicator Critical Characteristics - Dependability 6-5

Table 6-2a Critical Characteristics for Indicator With Contact Output - Physical..... 6-7

Table 6-2b Critical Characteristics for Indicator With Contact Output - Performance..... 6-8

Table 6-2c Critical Characteristics for Indicator With Contact Output - Dependability 6-9

Table 6-3a Multi-Function Controller Critical Characteristics - Physical 6-14

Table 6-3b Multi-Function Controller Critical Characteristics - Performance 6-15

Table 6-3c Multi-Function Controller Critical Characteristics - Dependability..... 6-16

Table 6-4a ESFAS Programmable Logic Controller Critical Characteristics - Physical..... 6-27

Table 6-4b ESFAS Programmable Logic Controller Critical Characteristics - Performance..... 6-28

Table 6-4c ESFAS Programmable Logic Controller Critical Characteristics - Dependability 6-30

1

INTRODUCTION

Nuclear utilities are seeing an increasing need to use commercial digital equipment when replacing or upgrading their instrumentation and control systems. However, many utilities have been hesitant to use such equipment in safety systems because of questions related to a number of outstanding technical and licensing issues. This section provides background on the current situation and describes the purpose and scope of this guideline document.

1.1 Background

Because of growing problems with obsolescence and increasing maintenance costs, nuclear utilities are replacing or upgrading their existing instrumentation and control (I&C) systems. Analog technology was predominant when plants were designed and built. However, preferred replacement solutions typically apply digital technology due to its ready availability and potential for performance and reliability improvements. In many cases, mature commercial products offer practical solutions, because of their reasonable cost, greater flexibility, and demonstrated reliability.

In contrast, products developed strictly for nuclear applications are less often being viewed as the preferred choice, for a number of reasons. The base of qualified suppliers and products has dwindled as market conditions have led many suppliers to discontinue their nuclear quality assurance (10 CFR 50 Appendix B) programs. The nuclear qualified products that are available or could be developed by the remaining suppliers tend to offer limited functional flexibility and limited operating history. Also, purchase prices tend to be high because development costs are borne by a small user base. Additionally, some suppliers have reduced the level of technical support for their products. These factors have led to increasing interest in using commercial products as replacements.

In the late 1980's, the industry developed an approach for procuring and using commercial grade items for safety-related applications. The approach uses special tests, vendor assessments, and other methods to confirm that the commercial item has adequate quality and once dedicated will perform its intended safety function. This process, called "commercial grade item dedication," has been very successful for mechanical and electrical equipment. However, the commercial dedication process was not developed with software-based equipment in mind, and there has been little

experience to date in applying these methods to equipment that contains computers and commercially developed software.

The use of digital technology in general has raised new design and licensing questions, apart from whether the equipment was developed under 10 CFR 50 Appendix B or as a commercial product. Issues include the use of software and the potential for common cause failure resulting from software errors, the effects of electromagnetic interference (EMI) on digital computer-based systems (e.g., different frequency ranges), and the use and control of equipment for configuring computer-based systems. The most notable of these concerns is the potential for software errors that could lead to common cause failures of redundant trains of safety system equipment.

The industry and NRC have agreed on a framework for addressing these digital issues, described in EPRI TR-102348 (see References in Section 7). The approach emphasizes consideration of the effects of potential failure modes in ensuring equipment adequacy, and this applies regardless of whether nuclear grade or commercial grade equipment is used. For software, it stresses the importance of a systematic, well-documented development effort as part of assuring adequate quality. A number of standards and guidelines are available that can be used to conduct a software development effort for a nuclear safety-related application. However, commercial products contain pre-existing software that was developed to varying commercial standards, often through a more evolutionary than structured or pre-planned process, and with less documentation than would be required under an Appendix B program. Assurance of quality for these devices comes in part from their application experience and the maturity of the software achieved through its ongoing development and operating history. The need to demonstrate a level of assurance for commercial grade items equivalent to that provided by a nuclear qualified (10 CFR 50 Appendix B) development effort has been well established, both in the regulations (10 CFR Part 21) and in recent standards and guidelines (IEEE 7-4.3.2, EPRI TR-102348). However, agreement on the specific approach that should be used for evaluating commercial digital products, developing the needed assurance, and accepting the items for safety-related service, has been lacking.

The Electric Power Research Institute (EPRI) formed a utility working group to address this need. The overall goal of the working group was to assist utilities in using commercial, off-the-shelf digital equipment in nuclear power plants. The group's specific objectives were to produce guidelines that are practical, cost-effective and technically defensible; promote industry use of the guidelines; and gain regulatory support for the approach.

1.2 Purpose

The purpose of this document is to provide guidance on the evaluation and acceptance of commercial grade digital equipment for nuclear safety applications. Specifically, guidance is provided for:

- Determining technical and quality requirements, and identifying critical characteristics of commercial digital equipment to be used in safety systems,
- Identifying appropriate methods for verifying the critical characteristics, accepting digital products from commercial vendors and dedicating them for use in nuclear safety applications, and
- Maintaining the dedication basis to ensure that it remains valid over the operating lifetime of the equipment in the plant.

The guidance in this document is intended for use by utilities or by other organizations who perform dedication of commercial grade equipment which ultimately is supplied to utilities.

The approach taken in developing this guidance is based on the conclusions reached by the working group that: (1) the existing process for commercial grade dedication can, with appropriate supplemental guidance, be applied to digital equipment, and (2) supplemental guidance provided for digital-specific issues should be consistent with the existing framework established for design and licensing of digital upgrades. Accordingly, this document supplements and is consistent with existing industry guidance contained in:

- EPRI NP-5652, "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications,"
- EPRI TR-102348, "Guideline on Licensing Digital Upgrades," and
- IEEE 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

Also, the guidance in this document is consistent with the requirements of applicable federal regulations including 10 CFR 50 Appendix B, which contains quality assurance criteria for nuclear plants, and 10 CFR Part 21, which defines commercial grade items and the dedication process. This guidance also is consistent with NRC Generic Letters 89-02 and 91-05, which provide clarifications and guidance on commercial grade item dedication.

The guidance given here provides a framework and a roadmap showing how the methods in NP-5652 can be applied to digital equipment, and how the technical and regulatory issues associated with the use of commercial digital equipment can be addressed consistent with TR-102348 and IEEE 7-4.3.2. With this guidance utilities will

be better prepared to evaluate commercial digital equipment, determine whether it is adequate for its proposed use, and if it is, apply existing procedures for commercial grade item dedication to accept the equipment. This should help utilities to: (1) take advantage of good commercial design practices and the application experience of proven commercial products, (2) assure adequate safety and reliability with the use of commercial products, and (3) adequately address the technical and regulatory issues associated with the use of commercial digital equipment.

1.3 Scope

This document is intended primarily to address the application of commercial grade digital equipment in safety systems. The guidance also may be used, at the discretion of the utility, when using commercial digital equipment in other applications. The document is written primarily for existing nuclear power plants, but the guidance also can be applied as appropriate for new plants designs, e.g., advanced light water reactors.

The guidance in this document applies to small- and large-scale applications of commercial digital equipment, ranging from use of a relatively simple digital meter or indicator to the installation of a more complex digital controller or control system. It applies when procuring new commercial digital equipment to replace existing analog or digital equipment. It also can be applied in cases where commercial digital equipment already installed in the plant needs to be evaluated to determine if it can be upgraded (in place) to a safety-related classification.

This guidance applies to commercial grade instrumentation and control equipment that uses microprocessors and associated software or firmware. It also applies to mechanical or electrical components that contain digital equipment (e.g., commercial switchgear containing embedded microprocessors). It can be applied, where appropriate, to devices that use application-specific integrated circuits (ASICs) to perform some or all of their functions. The guidance also applies to dedication of replacement parts for a piece of equipment when those parts contain digital components such as microprocessors.

The guidance given here discusses all aspects of the dedication of commercial grade digital equipment, including hardware, software and systems aspects. However, in areas where adequate guidance already exists, this document refers the reader to other guidance documents.

The guidance in this document does not specifically cover the dedication of services. When commercial grade services services (services from a contractor or supplier that does not have a 10 CFR 50 Appendix B quality assurance program) are to be procured related to use of digital equipment, refer to EPRI NP-5652 for guidance.

This document is **not** intended to be used as a detailed "how-to" manual. The lists and examples given here were constructed to illustrate specific points regarding application of the guidance. They are not necessarily all-inclusive. Differences in the equipment or the application may require different critical characteristics, acceptance criteria, and verification methods from those shown in the examples.

1.4 Content of This Guideline

Section 2 provides definitions for key terms used in the guideline.

Section 3 provides an overview. It introduces the basic problem faced when applying commercial digital equipment in a safety application—obtaining adequate assurance the device will perform its intended safety function. It also describes the processes that are presently used for design and licensing of digital equipment and for performing commercial grade item dedication.

Section 4 describes how the existing processes for design, licensing, and commercial grade item dedication can be used together to evaluate and accept commercial digital equipment for use in safety applications.

Section 5 addresses the problem of maintaining the dedication basis to ensure that it remains valid over the operating lifetime of the equipment.

Section 6 provides examples that illustrate application of the guidance in Sections 4 and 5. The examples range from a meter replacement up to a large-scale Engineered Safety Features Actuation System (ESFAS) upgrade.

Section 7 contains a list of documents that are referenced in this guideline, and which provide supporting information and guidance.

2

DEFINITIONS AND TERMINOLOGY

This section provides definitions for key terms as they are used in this guideline. When the definition is taken from another document, the source is noted in brackets ([ ]).

Architecture. When referring to a system or a piece of equipment, the organizational structure of the system or equipment, including the collection of hardware and software components and their interfaces. When referring to software, the organizational structure of the software, including the collection of software units or components and their interfaces. [Adapted from ANSI/IEEE 610.12-1990]

ASIC. An Application-Specific Integrated Circuit (ASIC) is a customized integrated circuit designed to implement a particular signal processing or logic function. An ASIC may include analog or digital circuits or both. It can range in complexity from a simple static logic array to a complex, multi-chip device that may include a microprocessor and other interfacing circuits.

Basic component. A structure, system, or component, or part thereof that affects it safety function 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 10 CFR 100.11. Basic components are items designed and manufactured under a quality assurance program complying with 10 CFR 50, Appendix B, or commercial grade items which have successfully completed the dedication process. [10 CFR 21, 1995]

Commercial grade equipment. See "Commercial grade item."

Commercial grade item. A structure, system, or component, or part thereof that affects its safety function, that was not designed and manufactured as a basic component. [10 CFR 21, 1995]

Commercial grade item dedication. 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 functions and, in this respect, is deemed equivalent to an item designed and manufactured under a 10 CFR Part 50, Appendix B, quality assurance program. [10 CFR 21, 1995] Note that a commercial grade item that is part of

a basic component, but which does not affect its safety function, does not require dedication per 10 CFR 21.

Computer. Used broadly in this document to refer to any device that includes digital computer hardware, software (including firmware), and interfaces. [Derived from IEEE 7-4.3.2-1993] A microprocessor, together with its software and interfaces, is considered to be a type of computer.

Computer program. A combination of computer instructions and data definitions that enable computer hardware to perform computational or control functions. [ANSI/IEEE 610.12-1990] This includes configuration files, "ladder logic" programs, and other similar data or instructions.

Configuration item. An aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process. [ANSI/IEEE 610.12-1990]

Configuration management. A discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements. [ANSI/IEEE 610.12-1990]

Control flow. The sequence in which operations are performed during the execution of a computer program. [ANSI/IEEE 610.12-1990]

Critical characteristics. 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. [10 CFR 21, 1995]

Data. A representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means. [ANSI/IEEE 610.12-1990]

Data flow. The sequence in which data transfer, use, and transformation are performed during the execution of a computer program. [ANSI/IEEE 610.12-1990]

Dedicator. Used in this document to refer to the dedicating entity: the organization that performs the dedication process. Dedication may be performed by the manufacturer of the item, a third-party dedicting entry, or the licensee itself. The dedicating entity is responsible for identifying and evaluating deviations, reporting defects and failures to comply for the dedicated item, and maintaining auditable records of the dedication process. [10 CFR 21, 1995]

Dependability. As used in this document, a broad concept incorporating various characteristics of digital equipment, including reliability, safety, availability, maintainability, and others. [Adapted from NUREG/CR-6294]

Digital equipment. Equipment containing one or more computers.

Electromagnetic compatibility (EMC). The ability of equipment to function satisfactorily in its electromagnetic environment without introducing intolerable disturbances to that environment or to other equipment. [IEC 801-3-1984]

Electromagnetic interference (EMI). Electromagnetic disturbance which manifests itself in performance degradation, malfunction, or failure of electrical or electronic equipment. [IEC 801-3-1984]

Firmware. Software that resides in read-only memory. [Adapted from IEEE 7-4.3.2-1993] An example is software that has been loaded (or "burned") into programmable read-only memory (PROM, EPROM, EEPROM).

Hardware. With respect to a digital computer, the physical equipment used to process, store, or transmit computer programs or data. [ANSI/IEEE 610.12-1990] In general, the term encompasses analog circuitry as well as digital.

Human-machine interface (HMI). Any interface between the instrumentation and control system or equipment and the plant personnel including operators, maintenance technicians, and engineering personnel (e.g., display or control interfaces, test panels, configuration terminals, etc.)

Like-for-Like Replacement. The replacement of an item with an item that is identical. [EPRI NP-5652]

Microprocessor. See "Computer."

Nuclear grade equipment. As used in this guideline, basic components designed and manufactured under a quality assurance program complying with 10 CFR 50, Appendix B.

Regression testing. Selective retesting of a system or component to verify that modifications have not caused unintended effects and that the system or component still complies with its specified requirements. [ANSI/IEEE 610.12-1990]

Robustness. As applied to digital equipment its ability to function correctly in the presence of invalid inputs or stressful environmental conditions. This includes the ability to function correctly despite some violation of the assumptions in its specification.

Safety related. See "Safety systems."

Safety systems. Those systems that are relied upon to remain functional during and following design basis events to ensure (i) the integrity of the reactor coolant pressure boundary, (ii) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (iii) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the 10 CFR Part 100 guidelines. [IEEE 603-1991]

Software. Computer programs, procedures, and data pertaining to the operation of a computer system. [Adapted from ANSI/IEEE 610.12-1990] This includes software that is implemented as firmware.

Software tool. A computer program used in the development, testing, analysis, or maintenance of a program or its documentation. Examples include comparator, cross reference generator, compiler, decompiler, driver, editor, flowcharter, monitor, test case generator, and timing analyzer. [IEEE 7-4.3.2-1993] Configuration software used to develop and load a configuration "program" into an instrument or controller, such as a programmable logic controller (PLC), would be considered a software tool.

System integration. The process of combining software components, hardware components, or both into an overall system. [ANSI/IEEE 610.12-1990]

System testing. Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. [IEEE 7-4.3.2-1993]

Traceability. (1) The degree to which a relationship can be established between two or more products of the development process, especially products having a predecessor-successor or master-subordinate relationship to one another; for example, the degree to which the requirements and design of a given software component match. (2) The degree to which each element in a software development product establishes its reason for existing; for example, the degree to which each software design feature or element references the requirement that it satisfies. [Adapted from ANSI/IEEE 610.12-1990]

Traceability matrix. A matrix that records the relationship between two or more products of the development process; for example, a matrix that records the relationship between the requirements, the design, and the testing of a given software component. [Adapted from ANSI/IEEE 610.12-1990]

Unit. (1) A separately testable element specified in the design of a computer software component. (2) A logically separable part of a computer program. (3) A software component that is not subdivided into other components. *Note:* The terms "module," "component," and "unit" are often used interchangeably or defined to be sub-elements

of one another in different ways depending upon the context. The relationship of these terms is not yet standardized. [Adapted from ANSI/IEEE 610.12-1990]

Unit testing. Testing of individual hardware or software units or groups of related units. [ANSI/IEEE 610.12-1990]

Vendor. As used in this document when referring to commercial grade digital equipment, the organization that holds information on one or more of the following: the design, design development process, testing, operating history, error reporting, and quality assurance for the equipment. For an instrument or controller, this is often the original equipment manufacturer.

Verification and validation (V&V). The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements. [ANSI/IEEE 610.12-1990] Note that the activities involved in verification and validation are equivalent, for digital systems, of activities that have traditionally been performed for design verification and acceptance testing of other types of equipment used in nuclear safety-related applications. See IEEE 7-4.3.2-1993 for expanded definitions of the individual terms "verification" and "validation."

Watchdog timer. A timer that must be reset on a repetitive basis, or it will time out and take a prescribed action (e.g., actuate a relay contact, display a message, initiate a switchover to a redundant processor, etc.). Watchdog timers can be implemented in software or hardware, and are often provided as a diagnostic or fail-safe feature to monitor and detect failures in computer-based systems.

3

OVERVIEW

This section provides an overview of the approach taken in this guideline for addressing digital issues within the established commercial grade item dedication process, as shown in Figure 3-1. The section introduces the basic problem faced when applying commercial digital equipment in a safety application—obtaining reasonable assurance that the device will perform its intended safety function. This section also describes the processes that are currently used for design and licensing of digital equipment and for performing commercial grade item dedication. Section 4 discusses how these processes can be used together to evaluate and accept commercial digital equipment for use in safety applications.

The following questions are answered in this section:

- What are the differences between nuclear and commercial grade digital equipment that affect the level of assurance for their use in safety applications? What supplemental activities would be necessary with a commercial grade digital product to obtain equivalence with equipment developed under a 10 CFR 50, Appendix B, quality assurance program? (Section 3.1)
- What standards and guidelines are used for design and licensing of nuclear grade digital equipment, giving us assurance that it is adequate for safety applications? (Section 3.2)
- What process and methods are used by the industry in procuring and "dedicating" commercial grade equipment for safety applications? (Section 3.3)

3.1 The Problem: Obtaining an Adequate Level of Assurance with Commercial Digital Equipment

As stated in 10 CFR Part 21, the goal of dedication is to "provide reasonable assurance that a commercial grade item...will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under a 10 CFR Part 50, Appendix B, quality assurance program." Thus the judgment that an adequate level of assurance has been reached is based on achieving equivalency to nuclear grade equipment (equipment developed under an Appendix B program).

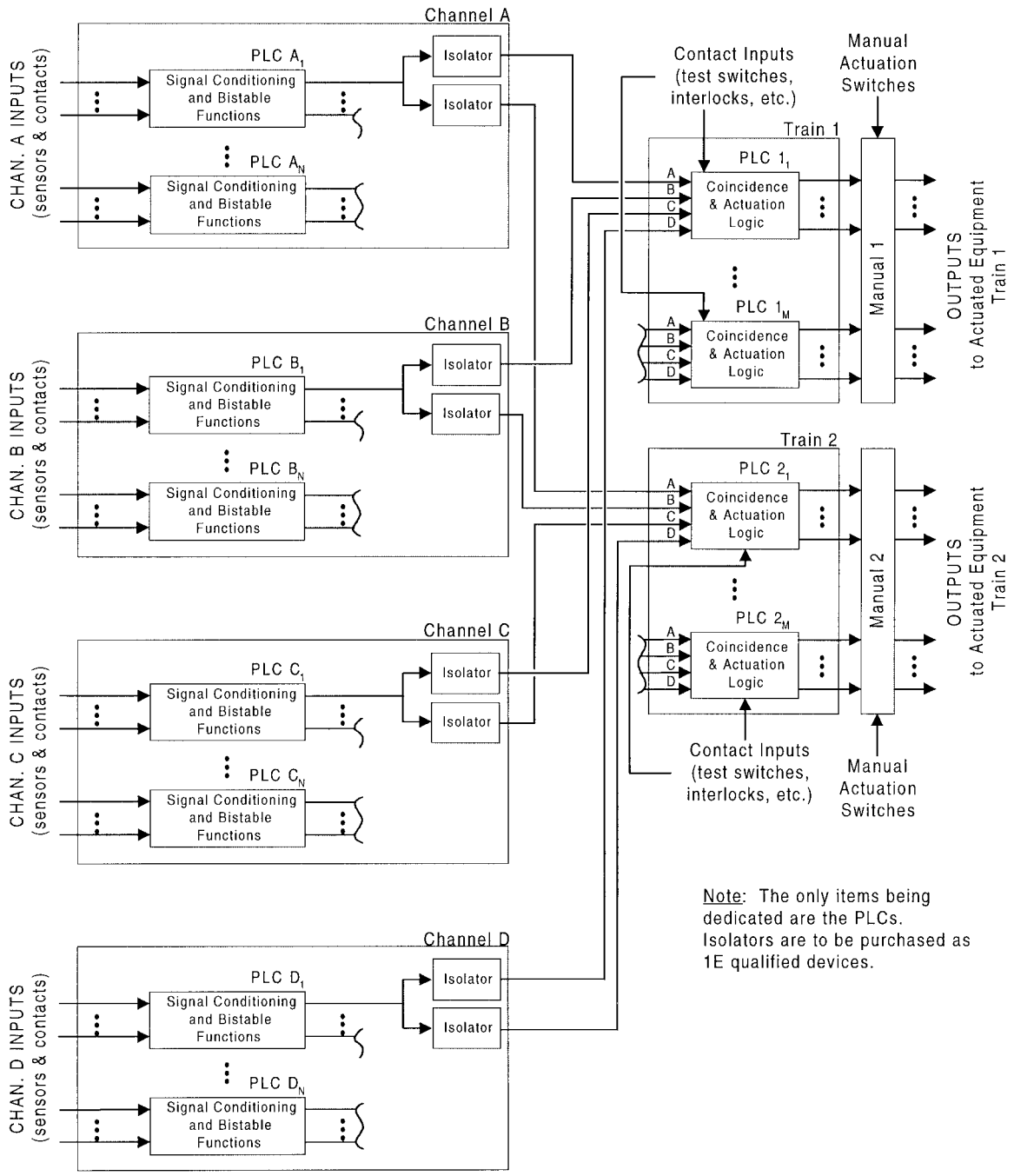

Figure 3-1 Overview: Approaches for Licensing Digital Equipment and Dedicating Commercial Grade Items are Combined to Address Commercial Grade Digital Equipment.

Figure 3-2 contrasts the assurance-building elements used for nuclear grade equipment with those used to establish equivalent assurance for a commercial grade digital item. The relative contributions of the various elements shown in the bars of Figure 3-2 were chosen somewhat arbitrarily to illustrate the basic concept. In practice, the contributions can vary widely depending on the particular application, vendor, and product being evaluated.

Assurance for Nuclear Grade Equipment

The bar on the left side of Figure 3-2 addresses equipment that has been developed specifically for nuclear service. In this case, a significant part of the assurance comes from the use of an approved vendor who has a 10 CFR 50 Appendix B quality assurance program. However, this is not sufficient by itself to reach the needed level of assurance. The utility reviews the design of the equipment, and the vendor's development process and quality assurance program. For digital equipment, this includes evaluating the vendor's programs for software configuration control, verification and validation, and testing.

Standards such as IEEE 7-4.3.2-1993, ASME NQA-1a Subpart 2.7, and other software engineering standards and guides typically are consulted. The guidance in EPRI TR-102348 is used in addressing digital system issues and to support licensing, including the 10 CFR 50.59 evaluation. Failure analysis techniques are used to identify the important failure modes for the system in which the device is to be installed, and to examine the equipment design and the vendor's process for addressing potential failure modes and abnormal conditions or events (ACEs), per IEEE 7-4.3.2 and TR-102348. If the device has been applied previously (it is not the first of its kind), its operating experience may be reviewed to determine whether it has been satisfactory. The utility may perform reviews of the vendor’s design and QA practices. Finally, when the equipment is received the utility performs receipt inspections and acceptance tests, follows its own quality assurance program and QC practices in configuring and installing the device, and performs further testing after installation to ensure that the equipment is operating satisfactorily and will perform its safety function. This entire process is documented and retained in plant records.

Equivalent Assurance for Commercial Equipment

The right-hand bar in Figure 3-2 illustrates how an equivalent level of assurance can be achieved with commercial grade equipment. The level of assurance must be at or above the level reached for the nuclear grade equipment. With a commercial item, we begin with the vendor's commercial practices for product design, development and quality assurance. Because the vendor does not have a 10 CFR 50 Appendix B quality assurance program, the process that was followed in development and verification of the product may not have included all of the elements of an Appendix B program, and

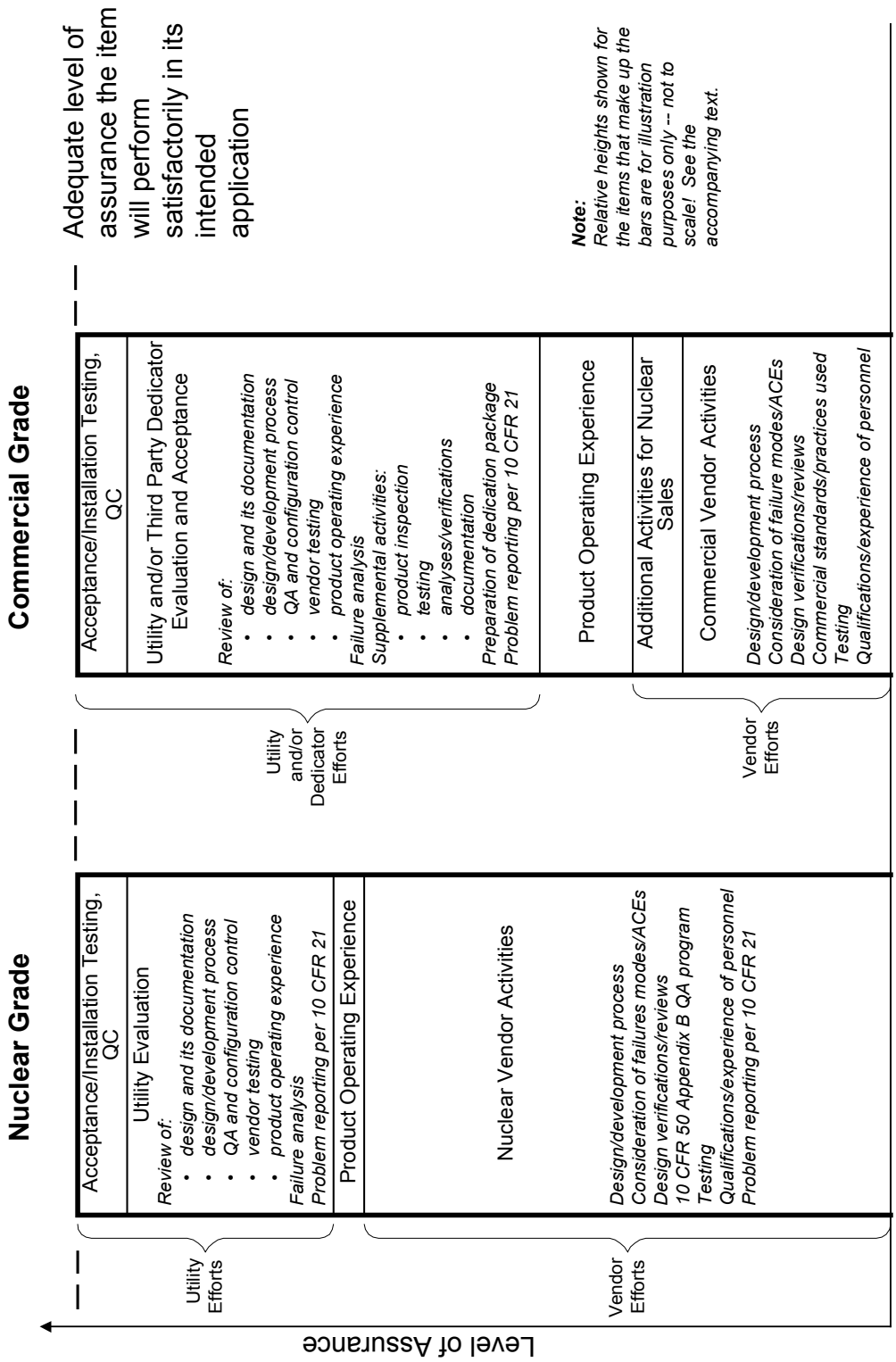

Figure 3-2 Equivalent Level of Assurance for Nuclear Grade and Commercial Grade Digital Equipment

documentation of the process may be lacking. The vendor's commercial practices may follow established commercial quality standards (e.g., ISO-9000), the elements of which are similar to a 10 CFR 50 Appendix B program. The utility may request that some additional activities be undertaken (e.g., additional testing or documentation); however, because nuclear power is a small part of most commercial vendors' markets, additional vendor efforts are likely to be quite limited.

For a commercial product, documented operating history of the equipment can be an important factor in providing confidence in the product. This experience may have been gained through applications in industries other than nuclear power, and may represent a much larger experience base than could be obtained with a device used only in nuclear applications. It is here that one can take advantage of the field experience and product shakeout that has occurred with widely-used, mature commercial devices. However, the experience must be shown to be relevant to the planned nuclear applications, in addition to being sufficient in terms of the number of units and length of time in service, and successful.

Additional activities will be required by the dedicator to reach an adequate level of assurance for a commercial grade item. An example would be additional testing needed to supplement the vendor's tests and build confidence in the device and its functionality, or to examine its response to specific conditions or abnormal events. Additional reviews or analyses may be needed (e.g., review of the device design and analysis of its failure modes), depending on the extent of reviews and verifications performed by the vendor during product development. Additional documentation may need to be produced, for example, in areas where it is evident that some process steps were performed by the vendor but not adequately documented. It is important to note that these supplemental activities by themselves do not add to or improve the quality of the commercial grade item. Their purpose is to help confirm and document the commercial grade item's quality.

The last element shown on the bar for reaching the needed level of assurance for a commercial grade item is the utility's final acceptance and installation testing, and quality control during installation. Again, the entire process is documented and retained in plant records.

Supplemental Effort and Cost

For commercial grade items the vendor's activities may contribute a smaller portion of the assurance as compared to nuclear grade equipment. As a result, the efforts by the utility or dedicator must provide a larger portion of the assurance. The amount of supplemental activity required and the associated cost can vary widely, depending on:

- the safety significance and economic risk associated with the specific application (this sets the overall level of assurance needed)

- how rigorous are the vendor's development and quality assurance practices
- the maturity of the commercial device
- the complexity of the device — the more complex the device, the greater the effort to develop adequate confidence it will meet the requirements of the application, particularly with regard to potential failure modes.

The utility must on a case-by-case basis estimate how much will have to be done to supplement the vendor's process and documentation, and then determine the cost-effectiveness of pursuing dedication (as opposed to buying from a vendor with an Appendix B program). Also, there are cost tradeoffs involved in choosing between available commercial devices. It may be more cost effective to select a somewhat higher priced item if the vendor of that device has a better process and will require less costly supplemental activities by the utility.

Demonstrating vs Adding Quality

It is important to reiterate a point made earlier. The efforts performed by the utility or dedicator do not add product quality; they seek to help confirm that the commercial product already has adequate quality. If a product has a critical shortcoming, dedicating it may not be possible at any cost.

3.2 Existing Guidance on Design and Licensing of Digital Systems

Guidance is currently available for design and licensing of digital systems for safety applications. Some of the key documents are listed below. These industry and NRC documents address the issues and concerns that have been raised with the use of digital, software-based equipment in safety applications.

Industry Guides/Standards	NRC Guidance
EPRI TR-102348, "Guideline on Licensing Digital Upgrades"	Generic Letter 95-02, endorsing EPRI TR-102348
IEEE 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"	Regulatory Guide 1.152 Rev. 1, endorsing IEEE 7-4.3.2-1993

The EPRI licensing guideline, TR-102348, emphasizes the use of failure analysis and examination of system-level effects to assess the significance of failures in digital equipment. This remains an important focus when evaluating commercial digital equipment.

IEEE 7-4.3.2 and EPRI TR-102348 both address dedication of commercial grade digital equipment, emphasizing that the fundamental requirement is to obtain an adequate level of confidence in the commercial device. As stated in the EPRI guideline and reinforced in Generic Letter 95-02, this typically involves making an engineering judgment which needs to be documented.

Appendix D of IEEE 7-4.3.2 provides additional guidance on commercial grade item dedication. It discusses the definition of functional and performance requirements, requirements related to behavior under abnormal conditions and events (ACEs), and verification of these for both hardware and software. It also discusses the need to evaluate the commercial software development process and the operating experience of the commercial device to obtain adequate confidence in the device being dedicated. NUREG/CR-6421 discusses a standards-based approach for the evaluation of commercial digital equipment. However, none of these documents describes the relationship between the existing methods for commercial dedication and the issues that should be addressed for software-based equipment.

This guideline is intended to help fill that gap, showing how digital issues can be addressed within the established commercial grade item dedication process. In doing so, the guideline focuses primarily on digital-specific issues and criteria. Guidance for other types of equipment is provided in other referenced documents.

3.3 Existing Guidance on Commercial Grade Item Dedication

Guidance on commercial grade item dedication has been developed and used by utilities for a number of years. Key documents are listed below. These guidelines have been applied successfully in dedicating many different kinds of commercial grade items for nuclear safety applications.

Industry Guidance	NRC Guidance
EPRI NP-5652, "Utilization of Commercial Grade Items in Nuclear Safety Related Applications"	Generic Letter 89-02, conditionally endorsing EPRI NP-5652
EPRI NP-6406, "Guidelines for the Technical Evaluation of Replacement Items for Nuclear Power Plants"	Generic Letter 91-05, providing additional NRC guidance
EPRI TR-102260, "Supplemental Guidance for the Application of EPRI Report NP-5652"	

NP-5652 is the primary source of guidance on commercial dedication, and has formed the basis for many utilities' commercial dedication programs, along with clarifying

guidance provided by the NRC in Generic Letters 89-02 and 91-05. NP-5652 defines the basic process for commercial dedication: a technical evaluation, definition of "critical characteristics for acceptance," and use of any of four acceptance methods to verify the characteristics. The four methods are:

Method 1 — Special Tests and Inspections
Method 2 — Commercial Grade Survey of Supplier
Method 3 — Source Verification
Method 4 — Acceptable Supplier/Item Performance Record

NP-6406 provides detailed guidance for technical evaluation of replacement items. This includes determining whether a replacement item is an equivalent or like-for-like replacement, or if it is sufficiently different that a design change is required. It also includes guidance on defining safety-related functions and design requirements from which critical characteristics are identified.

TR-102260 supplements NP-5652, giving more clarification and guidance that builds on both NP-5652 and NP-6406. Also, NRC Inspection Procedure 38703 can be used as a source of guidance on commercial grade item dedication.

Digital equipment utilizing software presents new challenges in commercial dedication. However, the same basic approach still applies. Key elements of the dedication process are:

- An up-front technical evaluation to define the requirements for the device
- Selecting from these a set of critical characteristics for acceptance
- Applying the methods described in NP-5652 (as endorsed by Generic Letter 89-02 and supplemented by Generic Letter 91-05) to verify the critical characteristics.

With digital equipment, there are new critical characteristics and additional verification activities that need to be performed. For the dedication to be successful, these activities must achieve the required level of assurance for the commercial device, as shown in Figure 3-2. Typically, this requires the use of more than one of the methods described in NP-5652 — no one method (e.g., testing per Method 1, or review of performance history per Method 4) will suffice by itself. For many digital devices, Methods 1, 2 and 4 will be needed.

4

EVALUATION AND ACCEPTANCE

This section describes how the existing processes for design, licensing, and commercial grade item dedication can be used together to evaluate and accept commercial grade digital equipment for use in safety applications. It provides guidance for identifying and verifying critical characteristics for commercial grade digital equipment.

4.1 The Process: A Combination of Design and Procurement Activities

Figure 4-1 shows a flow chart of the overall upgrade process when commercial grade digital equipment is involved. The center column and right side of the chart show the design and licensing processes outlined in EPRI TR-102348 for digital upgrades. The plant change process is shown in the center column[1] . Licensing is shown at the lower right, interacting with the change process (illustrated by the gray bars). Failure analysis, shown at the upper right, is a key element in addressing digital issues as described in TR-102348. This holds true for both nuclear and commercial grade equipment. Failure analysis interacts heavily with the other design and licensing activities.

The left side of the chart shows what traditionally have been largely procurement activities: technical evaluation of replacement items, and dedication of commercial grade items for use as replacements.

The design and licensing processes (TR-102348) and the procurement processes for technical evaluations and commercial grade item dedication (NP-6406 and NP-5652) must work together to support the evaluation and acceptance of commercial grade digital equipment. In fact, as illustrated by the gray bars in Figure 4-1, a considerable amount of interaction is required between design and procurement activities when dealing with commercial grade digital equipment. There are several reasons for this:

- Some of the activities that occur as part of the design process are also part of or directly support the dedication of commercial grade digital items (e.g., vendor evaluations and component testing)

[1] The example activities, listed in the boxes for each of the upgrade process steps, have been modified from those shown in TR-102348 to illustrate some of the activities specifically related to the use of commercial grade digital equipment.

- Failure analysis supports dedication as well as design and licensing (10 CFR 50.59) — in fact, the failure analysis may identify some of the critical characteristics, and it provides information that assists in evaluating and verifying critical characteristics. It is important to understand the failure modes of the commercial device and their impact on the system failure modes. The results of the failure analysis can affect system design, procurement and dedication activities, and licensing activities in support of the change.

- Applying digital expertise in evaluating the equipment is critical, but procurement personnel may not have this expertise, particularly for early digital upgrades at the plant. They may need to rely on people in the design organization or outside sources for the requisite expertise. Many utilities have found that the procurement and design staffs must work hand-in-hand to reach sound decisions on applying commercial grade digital equipment in safety applications.

Figure 4-1 is intended to be generic, describing the types of design, licensing and procurement activities involved with any change that includes commercial grade digital equipment. It is intended that the reader will be able to relate this generic process to the utility's specific practices for organizing, assigning responsibilities, and setting timelines for digital upgrades and commercial grade item dedication activities.

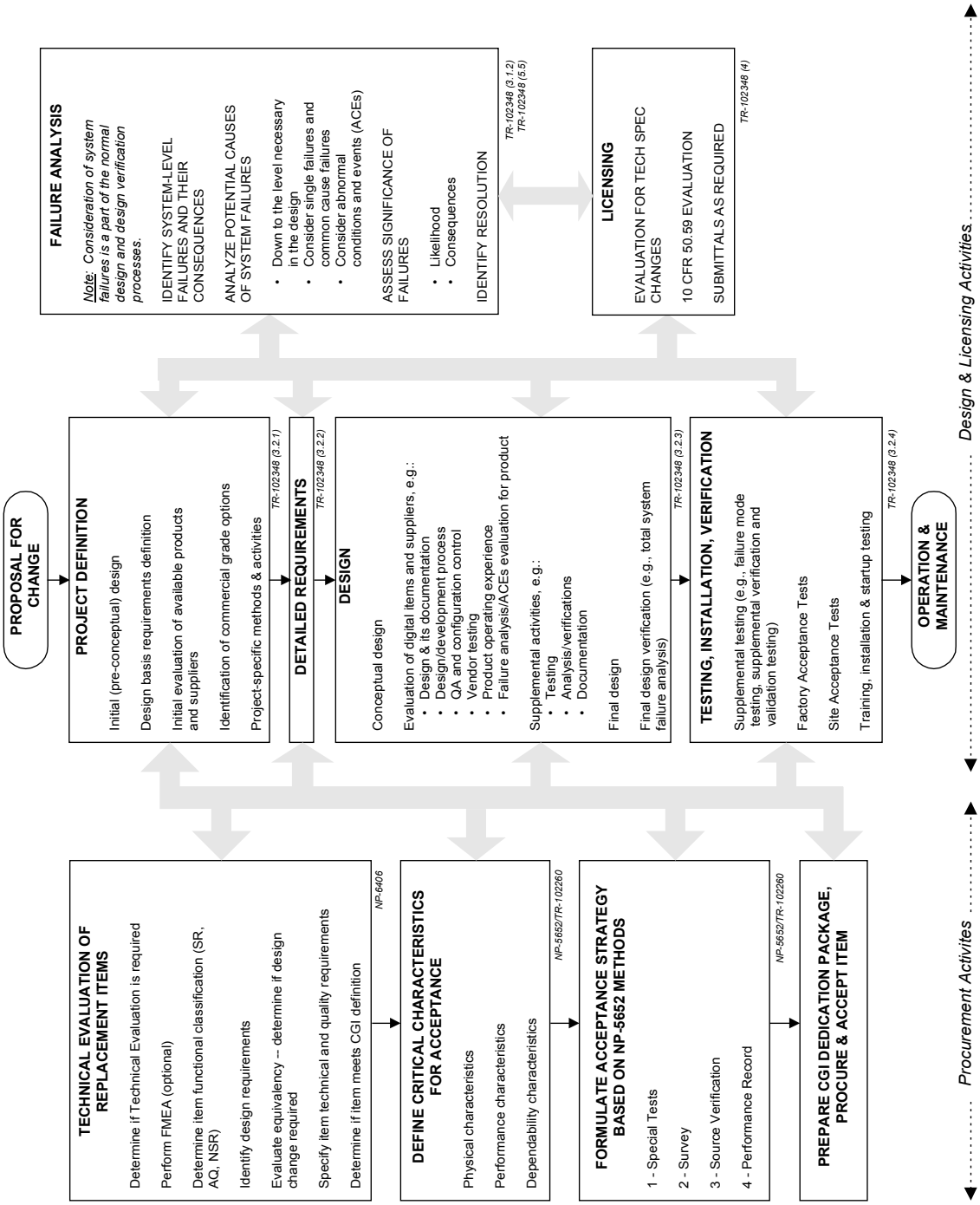

Figure 4-1 Commercial Grade Item Dedication in the Context of the Upgrade Process

4.2 Guidance on Defining and Verifying Critical Characteristics

Critical characteristics are 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. Translation of design requirements into critical characteristics for a commercial grade item is a key element in the dedication process. It is the link between the technical evaluation, which defines requirements, and the acceptance process, which verifies critical characteristics. Thus, a complete definition of requirements, including hardware, software, human-machine interface, quality and reliability requirements, is an important prerequisite for dedication of a commercial grade item. It is especially important for digital equipment, where experience has shown that many of the problems that occur are due to inadequate definition of requirements. For software-based equipment, in addition to design requirements for the intended functions and anticipated failure modes, it is particularly important to identify requirements related to unused, and unintended or prohibited functions.

For mechanical and electrical equipment, where commercial dedication originally was applied, most of the critical characteristics fall into the category of *physical* or *performance* characteristics, describing physical properties such as dimensions and material properties of a metal part, or functional properties such as the opening time of a circuit breaker. These types of characteristics also apply to digital equipment. In addition, a third type of critical characteristics, referred to in this guideline as *dependability*, becomes significantly more important when dedicating digital equipment including software.

It should be pointed out that placing critical characteristics into three categories is done here for convenience only. From the standpoint of commercial grade item dedication, there is one set of critical characteristics, and each of these must be verified regardless of what type of characteristic it is. The three categories are used in this guideline to help the reader understand what types of attributes may represent critical characteristics for digital equipment and the different methods of verification that may be used for each. The names of the categories (physical, performance, and dependability) were chosen simply to be descriptive of the characteristics. The names have no formal significance in themselves.

Table 4-1 shows a "critical characteristics matrix" that lists typical critical characteristics and provides examples of acceptance criteria and verification methods that can be used in verifying them. The matrix covers each of the three categories of critical characteristics:

Physical characteristics. These include physical characteristics of the hardware such as size, mounting, and other characteristics similar to those for mechanical, electrical, and analog electronic equipment. The criteria and the verification methods for these are, for the most part, the same for digital equipment as they are for analog. The matrix points

out some differences in the area of part identification owing to the need to verify software or firmware revision. Most of these characteristics are verified using inspection and measurement, which fall under Method 1 in EPRI NP-5652. Note that while this guideline is concerned primarily with the digital-specific aspects, many of the critical characteristics of the device involve the analog/solid state/mechanical aspects. Some examples of these are included in the matrix.

Performance characteristics. These include the functionality required of the device (the "must-do" functions) and performance related to this functionality (e.g., response time). They also include environmental requirements related to the needed performance (e.g., meeting accuracy requirements over a specified range of ambient temperatures). The acceptance criteria and verification methods for these again are similar to those for analog equipment. However, this category also includes characteristics related to failure management and "must-not-do" functions. For example, based on a failure analysis the utility may require specific behavior of the device under certain abnormal or faulted conditions. Acceptance criteria might include items such as detection of classes of failures, and "preferred" or fail-safe failure modes to be entered under prescribed circumstances (e.g., a specific output state required on loss of power or signal input). Verification methods include testing and design reviews, supported by failure analysis and reviews of operating history. These activities can involve Methods 1 (Tests and Inspections), 2 (Commercial Grade Survey), and 4 (Supplier/Item Performance Record) of EPRI NP-5652.

Dependability[1] characteristics. This is the category in which dedication of digital equipment differs the most from that of other types of components. It addresses attributes that typically cannot be verified through inspection and testing alone and are generally affected by the process used to produce the device. A key issue is that hardware failures are typically associated with fabrication defects, aging and wear-out, but software does not wear out. If there is a problem in the software that degrades the dependability of a device, it reflects a design error that was built into the device, or a mismatch between the application requirements and the device design.

In traditional dedications of mechanical and electrical equipment, dependability issues have been treated within the supplier's QA program and have been delineated in the commercial grade survey or source inspection plan. Due to the increased importance of

[1] The term "dependability" is used in various ways within the software and safety communities. In this document it is used broadly to include a number of characteristics of digital equipment such as reliability, availability, built-in quality, and other related characteristics (see the definition in Section 2).

Table 4-1
Critical Characteristics Matrix for Digital Equipment

Critical Characteristics for Acceptance	Acceptance Criteria	Methods of Verification	Application of Methods
Physical Product/part identification: • Model/part number • Firmware revision number • Software revision level • Hardware version (e.g., module or circuit board revision level) Physical characteristics of hardware, e.g.: • Size • Mounting Physical characteristics of device interfaces, e.g.: • Power • Signal • Data communications • Human-machine interfaces	Product/part identification must match the purchase requirements to support verification that the item received is the item specified, including both hardware and software. Criteria for other physical and interface characteristics are based on the requirements of the intended application(s).	Hardware part identification is handled the same as for other equipment (*Method 1*). For firmware, need to address whether the vendor changes the part number when firmware revision changes; if not, firmware revision must be verified separately. Firmware revision may be checked by simple part number verification (*Method 1*), given proper marking and knowledge of vendor's controls on the process of loading (burning) the firmware memory (*Method 2 or 3*). For software not encoded in firmware, verification of correct version can be more involved. Other physical characteristics are typically verified by inspection and measurement (*Method 1*).	When procuring multiple units in a batch, some characteristics may be verified only on a sample rather than doing a full inspection on each one, depending on the complexity of the item and the particular characteristics. For characteristics that are verified only on a sample basis, there should be a sufficient understanding of the design and manufacturing process, and the factors that influence those characteristics to ensure that sampling is adequate. The basis should be documented.
Performance Required functionality, e.g.: • Input processing • Specific functions or algorithms required • Output signal requirements • HMI functionality • Test and diagnostic functions — on-line and off-line	Functional and performance criteria based on the requirements of the intended application(s).	Most functional and performance characteristics are verified by testing (*Method 1*). Some may be verified in part by design review, e.g., checking the design for EMI protection features (*Method 2*), in addition to EMI testing (*Method 1*). Failure analysis can support the definition and verification of some performance characteristics.	The dedicator typically reviews tests that were performed by the vendor or a third party, and runs supplementary tests as part of the dedication. Some characteristics may be verified through special stress or "challenge" testing performed by the vendor or dedicator (e.g., tests of performance under conditions of

Table 4-1 (continued)
Critical Characteristics Matrix for Digital Equipment

Critical Characteristics for Acceptance	Acceptance Criteria	Methods of Verification	Application of Methods
Performance requirements related to the required functionality, e.g.: • Response time • Accuracy • Range • Stability • Data throughput rate • Interfaces including power, signal and data communication • Effectiveness of HMI Environmental conditions (harsh or mild) related to the required functionality and performance, e.g.: • Temperature • Humidity • Seismic • EMI/RFI susceptibility and emissions, and ESD		See EPRI NP-5652 Appendix F for guidance on verification of seismic and environmental characteristics.	high data rates or calculation burden)[1]. Some tests can be run on only one or a sample of items, while others may need to be performed for each individual item procured, depending on the complexity of the item and the specific characteristics that need to be verified. For characteristics that are verified only on a sample basis, there should be a sufficient understanding of the design and the factors that influence those characteristics to ensure that the sampling is adequate (e.g., is the characteristic determined solely by the basic design and thus can be checked on only one or a few units, or is it subject to small variations in manufacturing or assembly processes for which there is less control and thus a greater number

[1] The performance of digital equipment can be highly dependent on factors such as signal sampling rates and cycle times for real-time processes. For example, overall response time of a device can depend on the characteristics of input filters, the sample rate used in reading the conditioned input signals, and the cycle time for real-time processing of the inputs and algorithms required. The cycle time for some devices changes depending on the complexity of the configuration or the specific algorithms. Verification of adequate response time for a protective action (e.g., actuation of a contact output in response to certain input conditions) may require evaluation of a worst-case stack-up of all the factors affecting the response time, for all devices and processors involved from input to output. For control functions a similar evaluation may be required in order to verify adequate stability and control system response. Anti-aliasing filters affect response time; on the other hand, inadequate protection against signal aliasing can affect accuracy of the instrument. Depending on the complexity of the device and the functions it performs, verification of characteristics such as response time, accuracy, stability, etc., may require gaining an understanding of the design of the device and how it processes the inputs and determines outputs, for example, via a survey (*Method 2*) in addition to testing (*Method 1*).

Table 4-1 (continued)
Critical Characteristics Matrix for Digital Equipment

Critical Characteristics for Acceptance	Acceptance Criteria	Methods of Verification	Application of Methods
Behavior under specific abnormal or faulted conditions: • Response to specific abnormal conditions and events (ACEs) • Fail-safe characteristics			of units must be tested). Characteristics that are not part of the vendor's published specifications for the device bear special scrutiny, as they may not be as well controlled by the vendor's processes as those that are in the vendor specifications.
Dependability Reliability and maintainability related to the required functionality Built-in quality including: • Quality of design • Quality of manufacture • Failure management • Compatibility with human operators, maintainers Configuration control and traceability of: • Hardware • Software • Firmware (aspects of both hardware and software configuration control) • Problem reporting	Criteria for reliability, availability and maintainability should be derived from the requirements of the intended application(s). Specific criteria may be established such as numerical criteria for reliability or availability of required functions, or maintainability criteria including software. If numerical criteria are used, the method of demonstration should be specified (e.g., hardware reliability prediction using classical methods, or statistical analysis of failure rate data from field experience). Basic criterion for built-in quality is equivalence to the quality of a device developed and applied under a 10 CFR 50 Appendix B program. Judgment of equivalent quality is based on a combination of: • Design and design review processes, including software life cycle, V&V, etc. • Design documentation • Configuration management • QA program and practices • Software requirements definition and requirements traceability • Consideration of failure modes and ACEs in design and verification	Reliability: Review vendor reliability calculation/testing methods and results. Review operating history data. Review and assess design. Perform reliability analysis. (*Method 2*) Review of vendor processes and documentation (*Method 2 or 3*): • Design, development and verification processes • Quality assurance program and practices • V&V program and practices Design reviews -- architecture review, code reviews, walkthroughs, use of analytical techniques, etc. (*Method 2*) Failure analysis, at the system level and of the commercial grade item itself Comparison of device's failure modes to needs of the application Review of product operating history (from vendor, users, user groups, industry reports, INPO, etc.) (*Method 4*): • Documented (records, traceable)	The number and extent of verification activities required depend on the complexity and safety significance of the device. Supplemental activities may be required such as additional testing, verifications or analyses, and documentation. Many of the required characteristics can be verified once for a given type or model of equipment and the verification would not have to be repeated for each application of that device in the plant. This requires verification that the vendor's configuration management and quality control practices assure that the same item (with the same verified characteristics) is received with each new procurement. Also, if the device is to be applied in a more critical application, additional verification activities may be needed.

Table 4-1 (continued)
Critical Characteristics Matrix for Digital Equipment

Critical Characteristics for Acceptance	Acceptance Criteria	Methods of Verification	Application of Methods
	• Qualifications and experience of personnel involved in design and verification activities • Product operating history • Testing by the vendor or dedicator Minimum criterion for configuration control and traceability is that these be sufficient to support use of operating history data and to ensure the item delivered can be traced back to the documents reviewed as part of acceptance. Additional criteria may apply if the dedicator wishes to procure more of the same item in the future. As a minimum, problem reporting must be sufficient to support use of product operating history and to allow dedicator to carry out 10 CFR 21 responsibilities. Specific criteria should be established (e.g., on coverage, timeliness, reporting to the right organization or department).	• Sufficient (units, years in service) • Successful (error tracking shows good performance and device including software is stable) • Relevant (same or similar hardware/software configuration, functions used, operated similarly, etc.) Configuration control: review vendor configuration management program and practices. Examine actual practices, records. (*Method 2 or 3*) Problem reporting: review vendor procedures and practices. Assess performance record with previous customers (*Method 2*). Enter into contractual agreement. Assess maintainability of dedication.	

these built-in attributes to a digital device, this document has defined these attributes as critical characteristics to ensure that they are adequately addressed and documented during the dedication process. Although this may be viewed as a departure from traditional procurement and dedication practices, the end result is considered compatible with current industry practices.

The dependability attributes, which include items such as reliability and built-in quality, are generally influenced strongly by the process and personnel used by the manufacturer in the design, development, verification, and validation of the software-based equipment. For software-based systems, high quality is best achieved by building it in, following a systematic life cycle approach from requirements through implementation, with verification and validation steps and appropriate documentation for each phase of the life cycle. Hence, understanding the vendor's development process can be very useful in developing confidence in the dependability of a product.

The dependability of a digital device also can be heavily influenced by designed-in elements, including robustness of the hardware and software architectures, self-checking features such as watchdog timers, and failure management schemes such as use of redundant processors with automatic fail-over capabilities. Evaluation of these attributes requires that the dedicator focus on more than just the development and QA processes. It may require gaining an understanding of the specific software and hardware features embodied in the design, and ensuring that they are correct and appropriate in light of the requirements of the intended application. Accordingly, a survey team may need to include specialists who understand the device design, the software, and the system in which it will be applied, in addition to quality assurance and programmatic issues.

The dependability category captures those critical characteristics that must be evaluated to form an appropriate judgment regarding built-in quality of a software-based device. It also includes characteristics related to problem reporting and configuration control. Verification of these characteristics typically involves a survey of the vendor's processes (Method 2), and review of the vendor performance record and product operating history (Method 4). Source inspections (Method 3) may be used to verify certain hardware quality characteristics during manufacture, or to ensure quality of changes made to software as part of a particular procurement. Source inspections would not be used in verifying built-in quality of pre-existing software, because the software development has already occurred.

The critical characteristics in the dependability category, including the "built-in quality" characteristic, are somewhat different from those in the other categories because they are less tangible and quantifiable than, for example, a part number or a physical dimension. A commercial product may be judged to have sufficient quality, even if its development process lacked some of the rigorous steps of modern software engineering and/or some formal documentation. Reaching a reasonable level of assurance of quality of a

commercial grade digital item typically involves making a judgment based on a combination of the product development process and its documentation, operating history, testing, review of design features such as failure management, and other factors noted in the critical characteristics matrix, Table 4-1.

Table 4-2 provides more detail on attributes that can be evaluated in assessing built-in quality. Note that these are examples only, and they are not all-inclusive. See also NUREG/CR-6421, NUREG/CR-6294 and EPRI TR-104159 for lists of attributes related to quality of commercial grade digital equipment.

The dedicator must determine which activities are appropriate for each application. In general, the choice and extent of activities undertaken to verify adequate quality, and the specific criteria applied in making the assessment, depend on the safety significance and complexity of the device.

Safety significance depends on the function of the device and the consequences of its failure, and includes consideration of backups or other means of accomplishing the safety function. This includes consideration of the cumulative effects of upgrades to systems and equipment that provide diverse backup functions, especially in regard to preserving integrity of the intended diversity. Complexity includes the complexity of the device (e.g., overall architecture, number of functions, inputs and outputs, internal communications among processors or modules, and interfaces with other systems or devices) and complexity of the software.

It is important to remember that when the final set of critical characteristics has been identified, all of these characteristics must be verified including physical, performance and dependability characteristics.

The examples in Section 6 illustrate the selection and verification of critical characteristics for several example cases, ranging from a simple meter replacement up to a large-scale ESFAS upgrade.

Table 4-2
Assessment of "Built-in Quality" for Commercial Digital Equipment

Activities Used in Assessment of Item Quality	Examples of Design Factors That Can be Evaluated in Assessing Item Quality
Review of the design, its documentation, and hardware and software implementations	Design and documentation: • Completeness • Accuracy and consistency with actual design • Overall system design and software architecture: • Simplicity • Determinism of program execution, control flow and data flow • Internal consistency • Adequacy to support needed functionality • Unneeded features and their impact on the required functionality • Error handling capabilities, built-in protective features, ability to handle expected and unforeseen errors and ACEs • Human factors and the HMI • Protection against HMI-induced and other errors Software implementation: • Structure of code • Adherence to accepted coding practices Hardware implementation: • Use of good manufacturing practices • Quality of components used
Review of the design/ development process and its documentation, as it was applied for the item being evaluated	Life cycle used for product development, verification and validation • Consistency with accepted standards and guidelines (e.g., IEEE standards, EPRI TR-103291) Adequacy of software/hardware requirements: • Completeness • Correctness • Clarity Traceability from system requirements and design through software requirements, software design, code, and validation testing Design reviews and verifications: • Extent and coverage of reviews and analyses (design reviews, code walkthroughs and inspections, use of analytical tools) • Independence of reviewers and verifiers Systematic application of lessons learned from problems experienced with earlier versions of the product

Table 4-2 (continued)
Assessment of "Built-in Quality" for Commercial Digital Equipment

Activities Used in Assessment of Item Quality	Examples of Design Factors That Can be Evaluated in Assessing Item Quality
Review of qualifications and experience of personnel involved in design and verification	Individuals: • Training in areas related to design or verification responsibilities • Experience in similar projects • Familiarity with specific tools, languages, etc., used in design Organization: • Experience in developing similar products • Third-party certifications as they relate to organizational capabilities
Review of vendor QA program and practices, including SQA	Documented QA program: • Consistency with 10 CFR 50 Appendix B and relevant standards (e.g., IEEE) Vendor program certifications (e.g., ISO 9000, European certifications) Application of QA program to item being procured: • How strictly the program was adhered to for this product, degree of buy-in by personnel involved • How well documented, how formal, approvals required
Review of vendor configuration control program and practices	Documented configuration management program: • Consistency with relevant standards and accepted practices (e.g., IEEE) Vendor program certifications (e.g., ISO 9000, European certifications) Application of configuration management program to item being procured: • How strictly the program was adhered to for this product • How well documented, from initial development through changes and releases • Control over sub-vendors • Control over distributors or suppliers through which the procured items pass Vendor and product track record for control of changes and versions, and notification of changes, especially in repair

Table 4-2 (continued)
Assessment of "Built-in Quality" for Commercial Digital Equipment

Activities Used in Assessment of Item Quality	Examples of Design Factors That Can be Evaluated in Assessing Item Quality
Failure analysis	Consideration of ACEs in system design and verification: • Potential failure modes of hardware and software specifically identified • Formal or informal hazard or ACEs analyses • How early in the process, and degree to which these guided design and verification Predictability of failure modes of the device
Review of vendor testing	Functional and performance testing Environmental testing including EMI/RFI Extent of software verification testing (e.g., module, line, or branch coverage) Extent of validation testing (e.g., static, dynamic, random) Extent of challenge testing (e.g., tests specifically designed to uncover failure modes) Documentation of testing
Review of product operating history	Documented: • Records indicating specific models and software/firmware versions installed, when, and where • Formal or informal problem reports, description of problem and follow-up action Sufficient: • Number of units in service • Number of years of service Successful: • Error tracking shows good performance • Error rate has stabilized, no critical errors, software stable other than feature changes Relevant: • Same or similar software/hardware configurations, and functions or options used • Device installed and operated in a manner similar to the planned application • Similar environmental conditions • Similar run times

4.3 Additional Guidance

This section gives additional guidance on evaluation and acceptance of commercial digital items, expanding on the information given in Sections 4.1 and 4.2.

Application to Different Types of Changes

The process outlined in Figure 4-1, and the guidance given in Section 4.2 for defining and verifying critical characteristics, apply to a variety of situations where commercial digital equipment is used. These include:

- Small-scope changes, such as replacement of a single component (ranging from a single integrated circuit to a complete controller or recorder) that is no longer available with a newer model. The technical evaluation of the replacement item (upper left corner of Figure 4-1) determines whether the change is an equivalent or like-for-like replacement, or the new device is sufficiently different that a design change is required. *Note:* If the old device uses analog technology, and the new one is digital or software-based, the replacement typically will result in a design change, invoking the plant modification or upgrade process (shown in the center of Figure 4-1). Also, for digital-to-digital upgrades, if the new device has new or enhanced functionality (e.g., via a change to the firmware) compared to the old one, it is not a like-for-like change.
- Larger-scale changes, such as upgrading an entire control or monitoring system with new equipment that includes commercial digital devices
- Installation of a brand new digital system or component in a safety-related application—in this case there is no replacement (only original design), but any new commercial devices that perform safety functions need to be dedicated.

Timing of Activities in the Process

It is beneficial to identify early in the process (e.g., in the project definition phase—see Figure 4-1), based on a preliminary definition of requirements, whether a commercial grade digital item might be involved in the change and what options should be considered, including candidate vendors and products. This typically includes comparing the application requirements to the published specifications for available commercial products. If a commercial digital item may be involved, this can affect what detailed requirements are imposed on the rest of the process. It also can affect the project schedule, for example, ensuring that sufficient time is allotted for reviews, commercial grade surveys, or special tests.

Also, it can be beneficial to set up screening criteria for initial evaluation of vendors and their products, before committing to a commercial grade survey. This allows weeding out any products or vendors that are unlikely to make it through the dedication process. It provides some confidence before investing much effort. Examples of items that might be checked in this initial screening are whether the vendor will support a commercial grade survey, and commit to problem reporting.

The point at which a commercial grade device is finally "accepted," i.e., the dedication is complete, varies. In some cases, certain critical characteristics are not verified until after installation and final testing, so the dedication package cannot be closed until that point. Some applications require the release to the plant of partially dedicated commercial grade items where post-installation testing is necessary to complete the dedication. (Controls should be established to ensure that these items are controlled, tracked, and not placed into service or declared operable until all of the critical characteristics have been verified.) In other cases, all of the critical characteristics are verified through reviews, analyses and tests prior to installation. Post-installation testing may still be required prior to declaring the device or system operable (e.g., demonstrating successful performance of normal surveillance tests).

Technical Reviews and Expertise Required

The process of evaluating and accepting commercial digital equipment requires a multi-disciplinary approach—applying knowledge of digital systems and their failure modes, real-time measurement and control issues, software quality assurance, HMI, maintenance, training, and procurement activities such as audits and surveys. Qualifications of the personnel doing the reviews and verifications must be appropriate for the activities being performed.

Reviews of the overall device design, software architecture, and control and data flows have proven to be very useful in judging the acceptability of commercial digital equipment. Such reviews are needed in order to: (1) determine what aspects of the vendor's processes to concentrate on, (2) focus the failure analysis on areas of most concern, (3) determine how complex the device and the software are, which sets the levels of scrutiny for many aspects of the assessment, (4) look for potential failure modes related to how both the device and the system in which it is to be installed are structured and how the software performs its tasks, and (5) understand the implementation of built-in diagnostics, and what failures they cover and don't cover.

A commercial grade survey (Method 2 of EPRI NP-5652) can address many of the critical characteristics, covering the design and architecture review as well as programmatic reviews. Compensating the vendor for time spent in supporting a survey, and entering into appropriate agreements for protecting vendor proprietary data, can help overcome

reluctance on the part of some commercial vendors to get involved in commercial grade vendor surveys.

It is important to examine the effects of user interactions, and the potential for unintentional or unauthorized reconfiguration or other failures to occur through use of the human interface. This is a potential problem area for any digital equipment, but it can be particularly troublesome for commercial grade digital equipment because such equipment is designed to be flexible and easily reconfigurable, and it may have built-in modes and features that could be entered accidentally and could impact the safety function.

Who and Where to Survey

For many digital items, verification of the critical characteristics requires going to the original manufacturer or developer of the device. The original developer in some cases is one or more levels removed from the organization that actually supplies the item to the utility, but it is the developer who has the information needed to support a commercial grade vendor survey. Also, there may be a sub-vendor who manufactures some parts or assemblies. The dedicator should gain an understanding of the entire path the commercial item follows from its original manufacture, through distributors and other third parties who may at some time have custody of the item, and finally to the utility as the end user. Configuration control is of particular concern as the item makes its way through this chain. The dedicator should determine how the required level of configuration control is maintained through this process.

Iteration on Requirements and Critical Characteristics

Definition of a complete set of requirements for digital equipment is a difficult process, regardless of whether it is commercial. It is often an iterative process, during which both the requirements and the design evolve and become more complete. This affects the determination of critical characteristics, which are needed to support dedication.

As system requirements are decomposed to obtain requirements on the particular device, some requirements initially may be defined on the basis of system level requirements — characteristics required of the commercial item in order to provide reasonable assurance that the system can perform its intended safety function. However, as more becomes known about the component and the way it will be used within the system, requirements based primarily at the system level can be supplemented or replaced with requirements defined at the component or subcomponent level.

For example, if operator action is planned as a backup in the event of certain failures of a device, then immediate operator notification of those failures may become a requirement. Or it may be discovered during a survey and critical review of a device that protection

against certain failure modes is best provided by use of an optional feature offered by the vendor to drive an external relay (which could then drive a visual indication or alarm) based on the status of an internal watchdog timer. The design team may conclude that provision of this feature is a requirement and thus should be represented as a critical characteristic in its own right.

Changes to the system design also can result in changes to the requirements, and thus the critical characteristics for a component within the system. For example, if based on the results of a survey or design review an external watchdog device is added to protect against possible silent failures of a component, some requirements will effectively shift to the watchdog. Note, however, that at the system level the critical characteristics necessary to preserve the safety function have not changed.

In summary, the requirements and the resulting list of critical characteristics for a device may change as the design and dedication activities proceed. However, two important points should be kept in mind: 1) All critical characteristics must be verified, so each of the critical characteristics should represent a requirement that must be met to assure that the device will perform its safety function (other design characteristics may be beneficial or needed for some other reason, but would not represent critical characteristics for acceptance); and 2) the set of critical characteristics that is ultimately derived must be complete in covering all requirements needed to provide reasonable assurance the device will perform its safety function (see Section 3.1 and Figure 3-2).

Requirements on the Dedicator

The process of performing commercial grade item procurement and dedication activities is itself a safety-related process and, as such, must be controlled and performed in accordance with a quality assurance (QA) program that meets the requirements of 10 CFR 50 Appendix B. This applies to the dedicating entity whether it is the utility or a third-party dedicator. Typically, if a third-party dedicator is used, the utility audits and qualifies the third-party dedicator. The utility should invoke the requirements of 10 CFR Part 21 and 10 CFR 50 Appendix B in the procurement documents for the third-party dedication services, even if the dedicator is verifying only a portion of the critical characteristics.

Dedicating for Multiple Applications

Standardizing on a few types of digital devices and applying them in multiple applications in the plant can make economic sense. For example, performing a commercial grade survey once to cover multiple applications of a chosen device can be cost-effective. As a starting point, this could involve comparing the requirements for the anticipated applications to the design specifications used by the vendor. However, note

that if a device was dedicated for one application, this does not by itself qualify the device for use in other applications. The specific requirements for the new applications should be checked carefully, as they can lead to new or different critical characteristics and acceptance criteria. For example, more stringent time response requirements may imply the need for more scrutiny of sampling delays and other time response factors. Also, the safety significance should be compared to that of the previous applications. The failure analysis should be revisited to ensure that it adequately covers the new application. Device failure characteristics that are acceptable in one application may not be acceptable in another.

It is important to remember that 10 CFR 50 Appendix B requires the use of quality controls *commensurate with the importance to safety*. This depends on the specific application, unless the original dedication was performed such that it covers all applications (and all functions needed to support those applications) including applications of the highest safety significance.

It is also important to check the cumulative impact of multiple changes or upgrades on diversity (e.g., as required by 10 CFR 50.62 for ATWS) or backups that have been relied upon for defense in depth. Use of the same digital device or equipment in multiple locations or multiple systems can have the effect of reducing diversity and defense in depth, and this should be evaluated. See EPRI TR-102348 for more discussion on diversity and defense in depth.

Documenting Engineering Judgment

As stated a number of times in this guideline, the process of obtaining reasonable assurance that an item of commercial digital equipment will perform its safety function, and therefore can be dedicated for use in a safety-related application, often involves making engineering judgments. The basis for these judgments should be documented and retained as part of the dedication records. The documentation should be sufficient to allow the dedication process, and the basis for the engineering judgments used in the dedication, to be reviewed. It also should be sufficient to allow a comparably qualified individual to reach the same conclusion.

5

MAINTENANCE OF A COMMERCIAL DEDICATION

The utility is responsible for maintaining the validity of a commercial grade item dedication for as long as the dedicated device remains in service. Proper configuration control and change management are key to maintaining the integrity of the dedication. Processes to accomplish this for electrical and mechanical components are mature at all nuclear utilities. For digital equipment, a few issues specific to digital equipment warrant special attention. This section provides guidance on addressing these issues.

5.1 Product Changes Including Software/Firmware Revisions

The utility's configuration control procedures should recognize and track software (and firmware) revisions in addition to hardware changes. The revision level and description of the installed software should be maintained in equipment or parts databases. Purchase orders for replacement digital equipment or spare parts should reference the qualified (dedicated) revision levels, with a requirement that the vendor notify the utility of any changes so their impact can be assessed before new revisions are received in purchased replacements. Changes would be assessed under the utility's procedure for technical evaluation of replacement items (see Figure 4-1). Particular attention should be paid to potential changes in features or characteristics required in the utility's application that are outside the vendor's published specifications for the device. These may not be as closely controlled by the vendor's processes as those that are within the published specifications.

To support detection and evaluation of changes, the utility should confirm that the vendor has an adequate configuration control program, with the necessary controls to ensure that the software/firmware revision level actually installed in purchased replacements is controlled and traceable to design change documentation. The utility should understand the vendor's criteria and process for changing revision designations on both hardware and software components, and make an assessment of whether the processes are adequate in light of the utility application. This is typically evaluated in a commercial grade survey performed as part of the original dedication.

The most likely change scenario will involve enhancements or corrections that result in new software revision levels. Depending on the agreement between the utility and the vendor, the utility may be notified when the new revision is available, when new equipment is ordered, or when equipment is sent to the vendor for servicing. The utility should obtain a written description of the changes, with accompanying revisions

to the software development documents. Also, if the vendor performs maintenance or repairs to the equipment on-site, the utility should ensure that the software is not automatically updated to a new revision level without prior evaluation. Before implementing any change, the utility should use its procedures for technical evaluation of replacement items, evaluate the change against the criteria that formed the basis for the original dedication, and determine if a design change is required. The utility's design and modification control procedures should be followed to implement the change and update the configuration control databases and documents as appropriate. Note that regression testing may be necessary to re-validate the modified system.

Alternatively, the utility may elect not to update its software if the installed software is judged to be adequate without the new revisions. This decision should then be reviewed when subsequent software revisions are evaluated, to assess the cumulative effects of all the relevant changes. Decisions on whether to accept revisions involves striking a balance between the need to minimize expense of reviewing and implementing successive changes to the software, and the need to stay relatively current in order to ensure continued vendor knowledge and support of the installed version.

5.2 Operating Within the Bounds of the Original Dedication

Care should be taken to ensure that a commercially dedicated device is not operated in a configuration that is outside the bounds of the original dedication. The dedication package should clearly define the critical characteristics and acceptance criteria applied in verifying them, and it should document the conditions and assumptions under which the characteristics were verified. For example, if only certain configurations or modes of operation of a device were verified, this should be clearly indicated. Changes that occur later to the installed system, or changes in how the system or component is operated, may impact the critical characteristics for the application. These should be evaluated against the acceptance criteria used in the original dedication, or, if appropriate, the acceptance criteria should be revised. The utility's design controls (Appendix B, Criterion III) and modification procedures should evaluate proposed changes in critical design characteristics. All assumptions, both documented and implied, in the original determination of the critical characteristics and acceptance criteria should be considered when making these evaluations.

5.3 10 CFR 21 Reporting

The utility bears a responsibility for reporting of defects and nonconformances per 10 CFR Part 21. Typically, a commercial grade item is designed for use in a variety of applications; the vendor is not involved in the specifics of each application and is not in a position to judge the safety significance of a defect. The utility can make this

assessment, once made aware of the defect. The utility should arrange to be notified by the vendor when defects are discovered. This can be accomplished through a contractual arrangement or by other means if suitable. The utility should also take adequate steps to ensure that the notification will actually reach the appropriate people within the utility.

The utility should confirm, usually through a commercial grade survey, that the vendor's processes will adequately support the utility's needs in regard to newly discovered defects. Should a defect be discovered in the field, even in non-nuclear applications, there should be a high probability that the vendor will become aware of it. Once notified, the vendor should have a process for dispositioning the defect. This can include activities such as recreating the defect, root cause analysis, developing and implementing a fix, and appropriate V&V, including regression testing. The defect handling process should include a reliable mechanism for notifying the utility as to the status of the investigation. A separate reporting mechanism, added just to serve the nuclear utility, may be adequate if it can be shown to have sufficient reliability.

The 10 CFR 21 issues should be addressed before a commitment is made to purchase the subject equipment. It is recommended that the utility negotiate with the vendor a standing customer notification agreement for reporting of defects on systems or components that are installed at the utility's site(s), or at other sites.

10 CFR 21 also requires that the dedicator maintain auditable records of the dedication process.

5.4 Third Party Dedicators

When an outside organization performs a commercial dedication, acting as an intermediary between the equipment manufacturer and the utility, the utility should take appropriate care to assure the success of the dedication, including its maintenance. This can involve assessing the qualifications, experience, and long term viability of the third party dedicator. As part of this, the utility should consider possible contingency plans, should the organization become unable to continue maintaining the commercial dedication. Both the utility and the third party dedicator have 10 CFR 21 reporting responsibilities. If the contractual arrangements that address change and defect notifications are between the third party dedicator and the equipment manufacturer, the utility, at its option, may establish a mechanism to transfer the reporting so that it goes directly to the utility. Or there may be conditions under which all information associated with the dedication should be transferred to the utility.

5.5 Long-Term Support Issues

If maintenance of the software in a commercial digital device is to be performed by the utility itself or contracted to a third party, the utility should procure the tools and associated design and development information (compilers, test tools, configuration logs, test reports, etc.) that will be needed. If the utility contracts with the original vendor for maintenance, the maintenance agreement should specify what materials need to be kept by the vendor. These should be the same as if they were performing their own maintenance, and these items should be reviewed at procurement.

In some cases, special agreements between the vendor and the utility may be needed. For example, if the commercial supplier elects to discontinue its support for a product, it may be appropriate to transfer all records regarding the product design and maintenance to the utility. It may be prudent for the utility to obtain at the time of procurement an escrow and/or first right of refusal for the appropriate design information.

6

EXAMPLES

This section provides examples intended to illustrate how the guidance in Sections 4 and 5 can be applied for items of varying complexity and safety significance. The examples begin with a simple indicator and conclude with an Engineered Safety Features Actuation System (ESFAS) upgrade, illustrating how the level of effort required for the dedication activities increases as the complexity and safety significance of the item increase.

Because the intent in these examples is to illustrate the entire process from selection of a commercial device through evaluation and final acceptance, the examples show cases in which the dedication ultimately is successful. However, it is important to remember that not all commercial items can be successfully dedicated. Evaluation of a commercial grade item using the guidance in this document will lead to rejection of the item if reasonable assurance cannot be demonstrated, or if the utility concludes that providing such assurance is not economically feasible. Also, keep in mind that most real projects involve tradeoffs and iteration on both requirements and design. Think of each of the examples given below as describing the end product of a process that may have encountered a number of bumps and taken several turns before finally coming to the successful conclusion shown here.

6.1 Simple Indicator

This example illustrates a case in which simplicity and testability of the commercial device and its function in the plant, coupled with widespread successful operating history, provide adequate assurance without the need for a commercial grade survey or detailed review of the device's internal design and development process.

The utility is performing an upgrade in which an existing analog indicating device or meter, used as a Reg. Guide 1.97 Category 1 indicator, is to be replaced with a microprocessor-based device. The function of the device is to indicate to control room operators the value of a single variable. Two of these meters are used to provide redundant indication for the variable. The redundant instrument loops are qualified, independent, and separated. A commercial, off-the-shelf digital indicator from an established manufacturer is chosen as the candidate replacement device because it provides the needed functionality, is readily available, and is widely used. It is a single-function device with no programmable or software configurable features. (A fixed 4-20 ma input is used. Only the faceplate and an internal DIP switch setting are changed for

use of the same meter in applications with different ranges of engineering units.) Comparison of the application requirements to the vendor's specifications indicates that the requirements are within the vendor-specified performance limits. Thousands of these indicators have been in service for several years in a number of industries (pharmaceutical, chemical process, etc.), and they have a reputation for reliability.

The utility follows the design process and licensing guidance provided in EPRI TR-102348, and uses the guidance in EPRI NP-5652 and station procedures for planning and performing the commercial dedication. Design requirements for the indicator are identified based on the intended application. The utility also performs a failure analysis that provides information on important failure modes for the application. Based on this information, critical characteristics for the meter are identified as shown in Table 6-1.

The utility procures three indicators and performs the inspections, tests, and reviews described in Table 6-1. For this device and application, verification of many of the physical and performance critical characteristics is straightforward; they are successfully measured or tested on receipt. In the dependability category, verification of the critical characteristics is more subjective and, in this case, the acceptance criteria reflect the fact that the device is simple, is not software configurable, and has only one function, which can be thoroughly tested.

Because of the simplicity and testability of the device, and its successful and relevant operating history, it is concluded that a detailed survey and associated visit to the vendor's facility are not required[1]. Testing is the primary means of verification in this case, supplemented by review of the device's operating history. Because the device has only one function, and unit conversion and scaling are accomplished without software changes, all the operating history is considered relevant to the planned application. The design is very stable; this device represents the third generation in a family of nearly identical indicators, all of which are digital; the changes made in the last generation affected only the faceplate, and the latest model has been operating successfully in many applications for about a year.

The failure analysis finds that, because of its functional simplicity, the device has only a few different external failure modes that encompass all the failure modes of the internal components. The device does not automatically actuate any plant equipment. Behavior of the indication under anticipated abnormal conditions (e.g., loss of input signal) can

[1] Although this example illustrates a case in which no survey is required, this does not mean that there would be no interaction with the vendor. No formal credit is taken in the dedication for the vendor's development or QA processes. However, prior to selecting the device for the application the utility or dedicator typically would contact the vendor to obtain information on the design of the device, how it was developed and where it has been applied, and an overview of the vendor's QA and configuration management programs.

be verified by testing. Confidence that there is a sufficiently low probability of any other unexpected failures of significance (e.g., silent failures that could give incorrect readings) is based on the utility testing of the device, the relevant operating history, and the normal periodic checks and calibrations that are performed on the instrument. In addition, the indicated variable can also be read or inferred using other instruments available to the operators.

Based on these results, the meters are installed and a commercial dedication package is completed documenting the critical characteristics, acceptance methods, and activities used to dedicate the device, including the basis for engineering judgments made. In this case, the simplicity and testability of the indicator, coupled with its demonstrated stability and reliability in many similar applications, prove key to establishing reasonable assurance that the device will perform its safety function.

Table 6-1a
Simple Indicator Critical Characteristics - Physical

Physical Critical Characteristic	Acceptance Criterion	Method of Verification
Configuration • Model number • Software revision number • Dimensions • Mounting	 Vendor model # Vendor software revision # LxWxH Front panel mount with mounting clips	Receipt inspection verifies these characteristics. Note that because a survey has not been performed, detailed information on the vendor's configuration control practices and software version tracking has not been obtained. However, the utility records the software (firmware) revision number for the units that are received and tested, so as to trigger a re-evaluation if different revision levels or part numbers are received in future procurements.
Interfaces • Input signal • Input impedance • Power • Bargraph and digital display	 4-20 mADC Per utility specification Per utility specification 6″ bargraph with 1% resolution 4-digit numeric (requirements per utility specification)	Receipt inspection tests

Table 6-1b
Simple Indicator Critical Characteristics - Performance

Performance Critical Characteristic	Acceptance Criterion	Method of Verification
Functionality • Accuracy • Range • Response time	 Per utility specification 0-100% (4-20 ma) operating range Per utility specification	 Utility's receipt inspection tests (performed for all procured indicators, not just a sample)
Environmental Compatibility • EMI • Seismic • Temperature	 Per utility specification (e.g., using EPRI TR-102323) Per location response spectra Per utility specification based on mounting location (mild environment)	Third-party test lab report for one or a small sample of the indicators in a lot that are tested; the utility inspects all procured indicators to verify homogeneity of the lot and to ensure that the tested items are equivalent to those not tested, for the characteristics being verified.
Behavior under abnormal/faulted conditions • Loss of signal • Loss of power • Signal over/under range	Detectable by operator when reading the indicator	Receipt inspection tests

Table 6-1c
Simple Indicator Critical Characteristics - Dependability

Dependability Critical Characteristic	Acceptance Criterion	Method of Verification
Built-in quality • Quality of design & manufacture	Inspection and test results meet their acceptance criteria Visual inspection shows use of good commercial manufacturing practices Successful and relevant product operating history These taken together demonstrate adequate quality of the device	Inspection and testing by utility Review of extent, relevance, and success of operating experience with the specific model to be procured[1].
• Failure modes and failure management	Failure modes are adequately addressed based on failure analysis and testing. (Note: Failure analysis is also used to help determine whether unreviewed safety questions exist per 10 CFR 50.59 -- see EPRI TR-102348 and NRC Generic Letter 95-02.)	Failure analysis identifying failure modes and assessing their significance. Review of product operating history to help verify absence of specific critical failures[1]. Challenge testing designed to test for possible critical failure modes in normal operation (operation over entire range including slow and fast sweeps plus steady-state readings) and under abnormal conditions (e.g., degraded power supply voltage, out-of-range input, noisy signal, etc.)
Problem reporting	Vendor has error-reporting procedures and will provide reporting to utility.	Agreement with vendor on error-reporting procedures
Reliability	Successful operating history	Review of product operating history[1] for demonstrated reliability.

[1] Review of the product operating history in this example is relatively straightforward. Discussions with the vendor indicate that the firmware has been stable over the last year in which many units have had successful experience. The functional simplicity of the device facilitates establishing relevance of this operating experience. A significant fraction of the units use the same internal switch settings as those to be used here. Selected users are contacted to confirm that their use of the device is similar to the utility's intended application (continuous service, periodic readings taken, similar environment, no problems with silent failures).

6.2 Indicator With Contact Output

This example illustrates a step up in complexity and safety significance as compared to the simple indicator in Example 6.1. In this case an existing level indicator is to be replaced with a new microprocessor-based device. The indicator is on the reactor building sump level. In addition to the indication function, the device also has a contact output that performs a control function. Its purpose is to start a pump when the level rises to a preset value. The pump transfers contents of the sump to radwaste tanks for processing. If the indicator fails to take the control action to start the pump, the level could rise above its limits, causing a spill of radioactive water.

The replacement indicator that is chosen is from the same vendor and the same product line as the simple meter in the previous example. However, in this case the indicator includes a contact output to perform the control function. Because of the additional functionality, complexity and safety significance of this case as compared to the simple meter, the utility concludes that additional critical characteristics apply and more verification actions are needed. In particular, because the indicator now performs an automatic control action that has both safety and economic consequences, the utility decides that greater scrutiny of the device's design, its internal architecture, and the vendor's QA program is needed. To support this, a commercial grade survey is performed. This involves a visit to the vendor by a team of people having expertise in digital systems, real-time measurement and control issues, software quality assurance, manufacturing quality control, and other areas needed to support verification of the critical characteristics addressed by the survey.

The critical characteristics and verification activities for this example are shown in Table 6-2. Those that are added or changed from the simple meter example of 6.1 are shown in italics.

Based on the results of these activities, the meter is procured and installed and a commercial dedication package is prepared that documents the basis for the dedication. As in the case of the simple indicator, the evolutionary development of the device, and the relevant operating experience demonstrating its stability and reliability, contribute substantially to the dedication. The reviews performed as part of the commercial grade vendor survey provide the additional information needed to assure that the device will perform its indication and control functions satisfactorily.

Table 6-2a
Critical Characteristics for Indicator With Contact Output[1] - Physical

Physical Critical Characteristic	Acceptance Criterion	Method of Verification
Configuration • Model number • Software revision number • Dimensions • Mounting	 Vendor model # Vendor software revision # LxWxH Front panel mount with mounting clips	Receipt inspection
Interfaces • Input signal • Input impedance • Power • Bargraph and digital display • *Setpoint adjustment* • *Contact output*	 4-20 mADC Per utility specification Per utility specification 6″ bargraph with 1% resolution 4-digit numeric (per utility specification) *Per utility specification* *Per utility specification*	Receipt inspection tests

[1] Italics indicate differences from the simple meter example of Table 6-1.

Table 6-2b
Critical Characteristics for Indicator With Contact Output - Performance

Performance Critical Characteristic	Acceptance Criterion	Method of Verification
Functionality for level indication • Accuracy • Range • Response time	 Per utility specification 0-100% (4-20 ma) operating range Per utility specification	*Vendor certifications (subject to survey)* and utility's receipt inspection tests (performed for all procured indicators, not just a sample)
Functionality for contact output • *Setpoint adjustability* • *Hysteresis* • *Response time*	*Per utility specification*	*Vendor certifications (subject to survey) and utility's receipt inspection tests*
Environmental Compatibility • EMI • Seismic • Temperature	 Per utility specification (e.g., using EPRI TR-102323) Per location response spectra Per utility specification (mild environment)	Third-party test lab report for one or a small sample of the indicators in a lot that are tested; the utility inspects all procured indicators to verify homogeneity of the lot and to ensure that the tested items are equivalent to those not tested, for the characteristics being verified.
Behavior under abnormal/faulted conditions • Loss of signal • Loss of power • Signal over/under range	Detectable by operator when reading the indicator	Receipt inspection tests

Table 6-2c
Critical Characteristics for Indicator With Contact Output - Dependability

Dependability Critical Characteristic	Acceptance Criterion	Method of Verification
Built-in quality • Quality of design & manufacture	*Vendor maintains a documented QA program covering design and manufacture. QA program addresses key areas including, as a minimum:* • *QA staff and organization definition* • *QA plan and procedure* • *Specific software QA requirements* *Evidence that QA program was applied in the production (at least the hardware manufacture) of the procured item(s)* Documented product operating history These factors taken together demonstrate adequate quality of the device	*Commercial grade survey*[2]*, including:* • *Review of vendor QA Manual and check of actual QA practices, including degree to which QA program was applied in the design and production of the item(s) to be procured.* • *Review of vendor procedures and practices for digital system/software development. Supplemental documentation prepared by utility or vendor where necessary.* • *Review of device design and software architecture, particularly with respect to potential for unexpected failures.* • *Review of vendor testing.* Review of extent, relevance, and success of operating experience with the specific model to be procured[3].
• Failure modes and failure management	Failure modes are adequately addressed based on failure analysis. (Note: Failure analysis is also used to help determine whether unreviewed safety questions exist per 10 CFR 50.59 -- see EPRI TR-102348 and NRC Generic Letter 95-02.)	Failure analysis identifying failure modes from the system standpoint, and assessing their significance. *Review of device design and software architecture to identify important internal failure modes, diagnostic features provided and their coverage, and impact of failures on the intended functionality of the device (focus on contact output).* Review of product operating history to verify absence of specific critical failures[3]. Challenge testing designed to test for possible critical failure modes in normal operation

[2] *A documented (for example, on file) survey by this utility or another utility may be used, if it is verified that the previous survey provides adequate coverage of the specific critical characteristics for this application including information needed on the important failure modes of the device.*

[3] Review of the product operating history in this example is relatively straightforward. *The survey confirms that there is a feedback process in place by which field experience is recorded.* The firmware has been stable over the last year in which many units have had successful experience. The functional simplicity of the device facilitates establishing relevance of this operating experience. The vendor confirms that a significant fraction of the units use the same internal switch settings as those to be used here, *and the contact output feature is used in many of the applications.* Selected users are contacted to confirm that their use of the device is similar to the utility's intended application (continuous service, periodic readings taken from indicator, similar environment, *contact used for automatic control function,* no problems with silent failures).

Table 6-2c (continued)
Critical Characteristics for Indicator With Contact Output - Dependability

Dependability Critical Characteristic	Acceptance Criterion	Method of Verification
		(operation over entire range including slow and fast sweeps plus steady-state readings) and under abnormal conditions (e.g., degraded power supply voltage, out-of-range input, noisy signal, etc.).
Configuration control	*Vendor has an adequate configuration control program.*	*Review of configuration control program during vendor survey*[2].
Problem reporting	Vendor has error-reporting procedures and will provide reporting to utility.	*Review of error-reporting procedures during vendor survey*[2]
Reliability	*Demonstrated reliability and availability based on test, analysis, and/or operating history.*	*Review of vendor test report or analysis.* Review of product operating history for demonstrated reliability.

6.3 Multi-Function Controller

This example represents a further step up in complexity as compared to the meters in the previous two examples. Also, this example illustrates a case in which a multi-purpose, highly configurable device is used to perform a specific set of functions, based on software configuration developed by the utility for the application.

Because of obsolescence and difficulty in obtaining spare parts, the utility concludes it must replace an existing pneumatic control system for heating, ventilation and air conditioning (HVAC) of a switchgear room. A commercial, microprocessor-based, multi-function controller is selected to replace the pneumatics. The particular device is chosen based on its ability to provide both closed-loop control and switching functions necessary for controlling the HVAC system. Also, it includes an integral pneumatic output that can control existing air-operated dampers. Comparison of the performance requirements of the application to the vendor's specified performance indicates that the required performance is within vendor-specified limits.

Because the room contains safety-related (Class 1E) switchgear, the HVAC control system is safety-related. As a result, the controller has to be dedicated for use in this application.

The basic functions required of the HVAC controller are listed below:

1. Monitor the temperature of air in the switchgear room, and the temperature of the outside air (used for ventilation and cooling in the Winter).
2. Provide two modes for control of the switchgear room temperature, and automatically switch between the two modes based on the outside air temperature. The two control modes are:
   - Winter (outside air cold): Provide proportional-integral-derivative (PID) control of the switchgear room temperature by modulating existing dampers, controlling the mix of inside and outside air used for ventilation.
   - Summer (outside air warm): Provide on-off control of the air conditioning compressor to hold temperature in the switchgear room within the control limits, keeping the outside air damper fixed at a 10% opening.
3. Respond in a prescribed (safe) manner to abnormal or faulted conditions postulated for the controller.

The replacement controller provides for user configuration of the control strategy, through software interconnection of pre-encoded function blocks stored in programmable read-only memory (PROM). The application-specific configuration is stored in nonvolatile memory, to prevent loss of data should an electrical power interruption occur. Data entry keys and alphanumeric displays needed for

configuration and local operation of the controller are located on the faceplate of the unit.

The utility develops the configuration to be loaded into the controller to implement the HVAC control application. The configuration is developed under the utility's Appendix B quality assurance program, following procedures established for development, verification and validation of safety-related software. A Software Requirements Specification is developed that defines the functional requirements for the controller software. The configuration is developed to these requirements, and critical characteristics are defined for the controller's built-in firmware based on these requirements. Also, a failure analysis is performed to examine possible failure modes and their effects on the switchgear HVAC control function. This includes consideration of abnormal conditions and events (ACEs) as outlined in IEEE 7-4.3.2-1993.

The critical characteristics identified for the controller and the associated verification activities are shown in Table 6-3. Because of the additional complexity of the application, and the use of a multi-function device that is "software configured" for the particular application, the activities involved in dedicating the controller are more involved than those presented in the previous examples.

A commercial grade vendor survey is performed to check the vendor's quality assurance program and software development process. This involves several days at the vendor's site, during which time the team gains access to files and interviews key personnel; the utility pays the vendor for this support. The survey gets into more detail in a number of areas, as compared to the previous example. For example, it includes a thread audit in which a selected "thread" is followed through the entire process, checking the documentation and traceability from requirements through design, coding and testing. The audit checks the actual practices being followed by the vendor, as well as the written program. In cases where documentation required by the vendor's program and expected by the utility is missing or incomplete, the vendor corrects these deficiencies and ultimately provides a complete set of documentation with the delivered units.

The survey team also reviews the design of the controller, and the software architecture including real-time task management, and program control and data flows. The implementation of diagnostics and error detection features such as watchdog timers are specifically reviewed. Samples of the software code are reviewed to check adherence to established coding practices and to support the thread audit. Documentation of the product operating history is reviewed, including product failure reports. The vendor is found to have an effective feedback mechanism for reports from the field, and a strong corrective action program. Review of the product defect database finds that, with about 1500 units in the field, there have been no software-related deficiencies reported in the life of the controller.

The survey also provides an opportunity to examine the vendor's design and quality assurance organizations, and to assess the qualifications and capabilities of personnel involved in the design, manufacture and support of the product.

Vendor testing is reviewed, including evidence of unit testing (testing of individual software components) performed during development, verification and validation of the controller software. Special tests are performed by the utility to supplement the vendor testing, and to validate the specific configuration developed for this application. The special tests include functional testing (traceable to the Software Requirements Specification), tests of the controller's response to anticipated abnormal conditions (e.g., testing for safe behavior on loss of power and various input failure conditions), and challenge testing that examines behavior under a variety of abnormal conditions and events, including combinations of input transients, and errors in use of the operator interface.

In addition, to help address concerns regarding the potential for undetected or unannounced failures, the utility programs the controller to display a continuously flashing symbol on the front panel display anytime the control program is executing. This provides operators with the ability to detect at a glance whether the controller is functioning or the program or processor is halted. (Operating practices at the plant include periodic checks of the switchgear room by a roving operator.) Operator training is developed that includes instruction on the use of this "heartbeat" indicator in verifying operability of the controller. Also, it is confirmed that other independent indications and alarms are available that will alert operators to take necessary manual actions in the event of a controller failure not previously detected, and the operators will have the time and manual control capabilities required to take manual action and restore cooling to the switchgear room.

The controller is accepted and a dedication package is prepared, documenting the critical characteristics, verification methods employed, and the basis for the judgments made in accepting the controller. In summary, the utility concludes that the controller will perform satisfactorily in its intended application, based on a number of factors including:

- The survey finds that the vendor followed a systematic development process with a reasonable level of documentation which, although not fully in compliance with 10 CFR 50 Appendix B, is considered adequate.
- The survey also finds that the vendor's configuration management program and error reporting schemes are strong and meet the utility's criteria.
- The failure analysis, review of the product's design and diagnostic features, and special testing show good coverage of the device's likely failure modes; the added "heartbeat" indication provides additional assurance that any unexpected failures

would be detected, and there are operator backups available in case of controller failure.

- The successful operating history, gained largely in non-nuclear industry applications, is found to be relevant since the planned application in the nuclear plant is typical of its use elsewhere.
- The utility controls the development, installation and maintenance of the application-specific configuration of the controller under its Appendix B quality assurance and configuration management programs.
- All critical characteristics are adequately verified through the combination of the survey, tests and inspections, and review of the product's performance record.

The controllers are entered into the utility's tracking system for dedicated commercial equipment. This includes placing the firmware as well as the hardware under configuration control so that any future purchases for replacements or spares will include reference to the dedicated firmware revision level and requirement for notification of any changes made so the utility could evaluate whether to accept, and perhaps re-dedicate, the revised product. Also, the vendor agrees to provide reports to the utility of any errors or problems with the device that may be discovered by the vendor.

Table 6-3a
Multi-Function Controller Critical Characteristics - Physical

Physical Critical Characteristic	Acceptance Criteria	Method of Verification
Configuration • Model number • Software revision number • Case type, dimensions • Mounting	 Vendor model # Vendor software revision # NEMA 4X, LxWxH per utility specification Per utility specification	Receipt inspection
Interfaces • Pneumatic supply air connection • Electrical power • Input signals • Input impedance • Pneumatic output • Contact output • Front panel interface (HMI)	Per utility inspection	Receipt inspection and testing verifies correct interface/connection types, input impedance, HMI features, etc.

Table 6-3b
Multi-Function Controller Critical Characteristics - Performance

Performance Critical Characteristic	Acceptance Criteria	Method of Verification
PID control capabilities, e.g.: • PID adjustable ranges • Anti-reset windup • Auto/manual control capability • Bumpless transfer capabilities • Program cycle time • Data sampling rate • Signal conditioning, anti-aliasing, etc.	Per utility specification , including decomposition of requirements on system stability to define requirements on PID adjustability, digital sampling rate and cycle times, and characteristics of signal conditioning circuits as they affect stability, based on system stability analysis.	Primarily through special tests by the utility of the configured controller. Also, review of vendor literature, review of design during commercial grade survey (PID function block in particular), and review of vendor testing of PID control capabilities.
Switching control capabilities, e.g.: • Setpoint adjustability • Hysteresis • Response time	Per utility specification	Review of switching control functions in vendor literature and from reviews during commercial grade survey; review of vendor testing; special tests by utility of controller configured for the specific switching functions of this application.
Human-machine interface performance, ease of use (including use during operation, configuration, maintenance and troubleshooting)	Per utility specification, covering operational requirements, configuration capabilities, maintenance and troubleshooting, and general human factors criteria	Review of vendor literature, review of design and operation during commercial grade survey, special testing by utility, and human factors evaluation by utility engineering and operations.
Environmental compatibility: • EMI • Seismic • Temperature • Humidity	Per utility specification (e.g., using EPRI TR-102323) Per location response spectra Per utility specification Per utility specification	Third-party test lab report
Behavior under abnormal/faulted conditions, e.g.: • Loss and re-gain of power • Loss of one or more signal inputs • Input signal over/under range • Loss of supply air	Per specific utility requirements regarding fail-safe conditions for the controller.	Review of vendor testing, review of design and software architecture during commercial grade survey, plus special tests performed by the utility to examine behavior under expected abnormal/faulted conditions, verifying safe response of controller.

Table 6-3c
Multi-Function Controller Critical Characteristics - Dependability

Dependability Critical Characteristic	Acceptance Criteria	Method of Verification
Built-in quality: • Quality of design and manufacture	Vendor maintains a QA program that generally is in compliance with a recognized standard (e.g., ISO 9000). QA program addresses key areas including, as a minimum: • QA staff and organization definition • QA plans and procedures • Specific software QA requirements Evidence that the QA program was applied in the production (at least hardware manufacture) of the procured item(s). Vendor presently follows a digital system/software development process that includes: • Software development plan and organization • Documented design requirements, including software requirements • Requirements traceability • Documented software design descriptions • Documented V&V plan • Validation test reporting Evidence that the digital system/software development process has been followed for latest revisions of the software.	Commercial grade survey[1], including: • Review of vendor QA program against relevant standards • Review of vendor procedures and practices for digital system/software development, V&V, and testing. Supplemental documentation prepared as necessary. • Thread audit to check actual practices for QA and software development and control • Check of degree to which QA program and software development process were applied in the design and production of the item(s) to be procured • Review of controller design, software architecture including real-time task management, and implementation of diagnostics and error detection such as watchdog timer features • Samples of the software code reviewed to check adherence to established coding practices and to support the thread audit Review of extent, relevance, and success of operating experience with the specific model of controller to be procured[2].

[1] A documented (for example, on file) survey by this utility or another utility may be used, if it is verified that the previous survey provides adequate coverage of the specific critical characteristics for this application, including information needed on the system design and software architecture, and the important failure modes of the device.

[2] Review of the product operating history for the controller is somewhat more involved than it was for the meter in the previous examples. The survey confirms that there is a strong program in place to record feedback from the field on any problems in service. The firmware has been stable over the recent operating history in which many units have been operating in a number of different applications. No software-related failures have been reported. Because the controller is a multi-purpose device, establishing relevance of the operating history involves determining that many of the other applications of the controller use the same function blocks as for the planned application. In this case, the function blocks are standard PID control and switching functions; based on discussions with the vendor and selected users of the controller, it is established that there is significant operating history for applications using these functions.

Table 6-3c (continued)
Multi-Function Controller Critical Characteristics - Dependability

Dependability Critical Characteristic	Acceptance Criteria	Method of Verification
	Documented product operating history showing product stability, reliability, and freedom from critical software-related errors or failures in similar applications. These factors taken together demonstrate adequate quality of the device.	
• Failure modes and failure management	Failure modes are adequately addressed based on failure analysis. (Note: Failure analysis is also used to help determine whether unreviewed safety questions exist per 10 CFR 50.59 - see EPRI TR-102348 and NRC Generic Letter 95-02.)	Failure analysis identifying important failure modes from the system standpoint, and assessing their significance. Review of the device design and software architecture, performed as part of the commercial grade survey, identifies important internal failure modes and diagnostic features provided, including items such as watchdog timers, and assesses the impact of failures on the system. Failure analysis determines that there are independent alarms that will alert operators if switchgear room temperature goes out of bounds due to controller failure, and there will be sufficient time for operators to act using manual control capabilities. Review of product operating history to verify absence of specific critical failures[2]. Review of vendor testing, and performance of special challenge tests designed to test for possible critical failure modes in response to abnormal conditions (e.g., degraded power supply voltage, noisy signal, power and signal transients, combinations of input signal failures, HMI errors, etc.). Programming of the device to display a "heartbeat" indication as long as the control program is executing provides additional assurance that controller failures will be detected.

Table 6-3c (continued)
Multi-Function Controller Critical Characteristics - Dependability

Dependability Critical Characteristic	Acceptance Criteria	Method of Verification
Configuration control	Vendor has a configuration control program that includes: • Documented plan and procedures • Baseline maintenance • Change control Error-reporting process	Review and audit of configuration control during vendor survey[1].
Problem reporting	Vendor has established error-reporting procedures and will provide reporting to utility	Review error-reporting procedures during vendor survey[1].
Reliability	Demonstration of adequate reliability and availability for the specified environmental conditions	Review of vendor test report or analysis. Review of product operating history for demonstrated reliability[2].

6.4 ESFAS Upgrade Using PLCs

In this example a number of programmable logic controllers (PLCs), purchased from a commercial vendor, are used in an Engineered Safety Features Actuation System (ESFAS) replacement. This illustrates a case in which complexity of the commercial digital device (the PLC) and high safety significance of the application (ESFAS) lead to a significantly higher level of effort required to evaluate and dedicate the devices as compared to the previous examples. In general, more interaction is required among the utility, the designer/integrator of the replacement system, and the commercial vendor in this example. Also, this example is a case in which multiple copies of the dedicated commercial device are to be used to perform different functions within a system, so the dedication must consider multiple configurations and different functions to be performed by the PLC.

Background

The ESFAS performs a number of safety-related functions, including actuation of safety injection (emergency core cooling), main steam line isolation, containment isolation, containment spray, and other functions such as purge and vent isolations. For each function, one or more plant parameters are monitored and checked against a setpoint in a bistable device. There are four channels of bistables, with associated signal conditioning. The bistable outputs are fed to two trains of actuation logic, corresponding to the two trains of mechanical equipment (pumps, valves, etc.) that carry out the associated safety function.

A large portion of the system is to be replaced because the existing equipment used for signal conditioning, bistables and logic functions is obsolete, and spare parts are difficult to obtain. The new system design retains the same basic architecture, but uses PLCs to perform the signal conditioning and bistable functions (four channels), and additional PLCs to implement the coincidence logic (two trains). As shown in Figure 6-1, multiple PLCs are used in each bistable channel and each actuation train, with each PLC performing its own set of ESFAS functions. Physical separation and electrical isolation are maintained among the bistable channels, and between the two actuation logic trains. However, the same make and model of PLC is used throughout the new system (all channels, both trains). Different configurations are used at each location as necessary for the different functions to be performed by the PLCs. The system includes capability to manually actuate each of the ESFAS functions, using switches that can be operated independent of the PLCs and based on indications that are also independent of the PLCs.

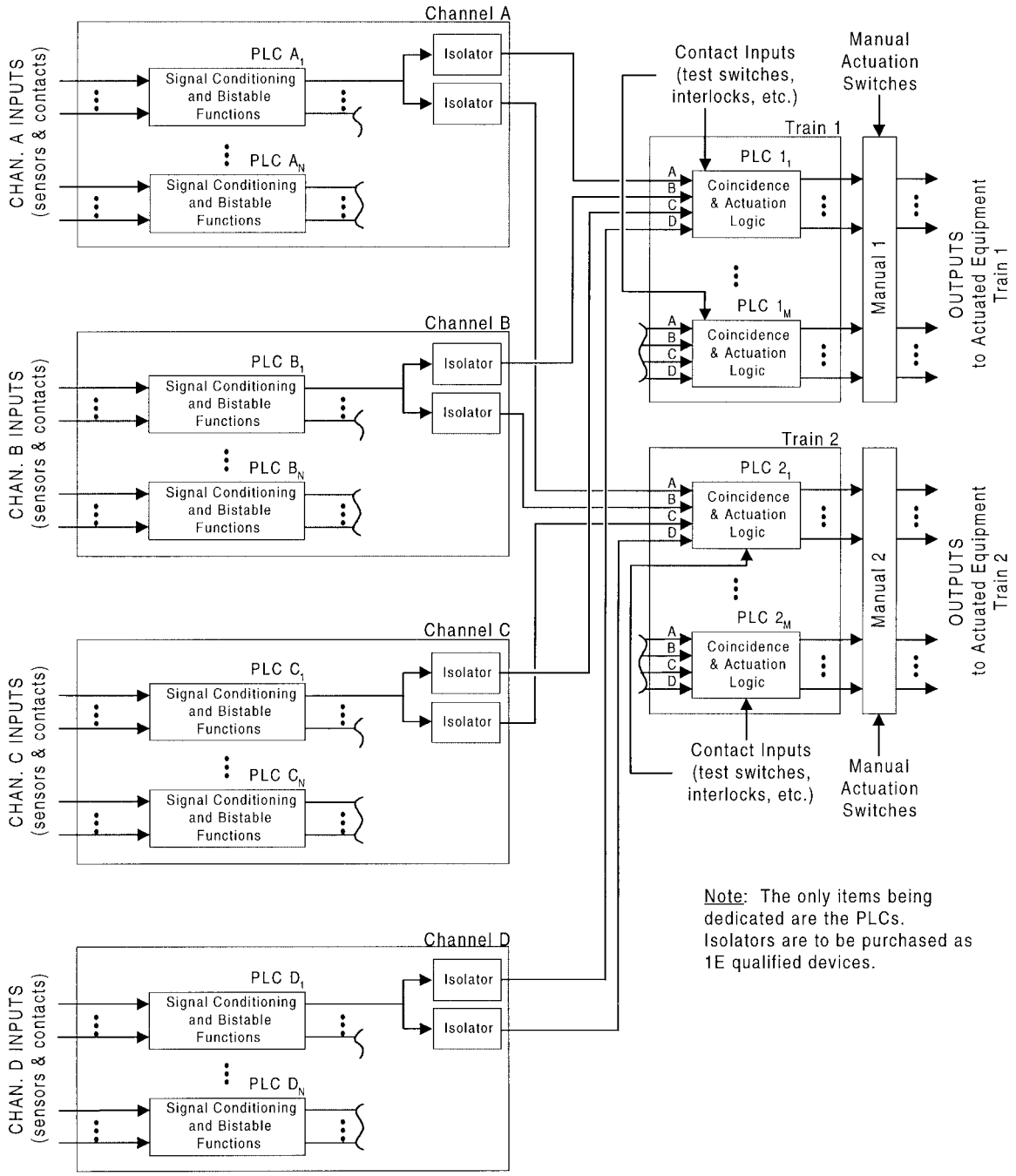

Figure 6-1 ESFAS Architecture Using Multiple PLCs

Upgrade Design and Choice of PLC

The utility follows the design and licensing guidance provided in EPRI TR-102348. Design basis requirements for the ESFAS system are identified, and these are used to define specific design and qualification requirements for the system upgrade. It is concluded that commercial PLCs would be the best choice for performing the signal conditioning, bistable, and coincidence logic functions required for ESFAS. Also, the versatility of the PLC makes it attractive for anticipated future applications, both safety-related and nonsafety-related. Requirements for the ESFAS PLCs are derived from the system requirements and the specific functions required at each location in the system.

The initial choice of PLC make and model is based on what was already in use in a non-safety application in the plant. Review of the vendor literature for that controller indicates that the PLC would likely meet the necessary functional and quality requirements for the safety-related applications. However, when a commercial grade vendor survey is performed, including an attempt to review the details of the controller design and its development, it turns out to be very difficult to obtain the necessary information to support the reviews. Also, the vendor's practices for support of the product do not include appropriate assurances that the utility would be notified of any software or firmware changes when they occur. The vendor's normal practice when repairing a unit is to install the latest update of the firmware and not to provide detailed information that would be required by the utility to evaluate the effect of the changes on the dedication for ESFAS. The vendor is not interested in making special arrangements for the utility or third-party dedicator in this regard, due to the small market involved. As a result, the utility concludes that this PLC would not be acceptable to them for this application.

A broader look at the available devices and their published specifications, plus a more in-depth screening of the vendors, identifies a particular model that appears to meet the requirements. The PLC is widely used in the process industries and manufacturing plants and it has a good reputation for quality. Initial information on the vendor's development and QA processes looks good, and the vendor is cooperative and willing to share detailed information needed to support the dedication (as long as appropriate agreements are put in place for protection of proprietary information, and with compensation for the vendor's additional efforts beyond what would normally be provided for a commercial application). The project proceeds with this PLC.

The chosen PLC uses a backplane with plug-in module arrangement. Different input, output, and power supply modules can be plugged in and the unit can be "programmed" or configured using a portable configuration device or a personal computer (PC) via a plug-in connection. A PC-based software tool is provided that allows development of ladder logic and many other functions supported by the PLC's

built-in software. The development of the required logic based on the functional requirements, the use of the software tool to prepare the PLC application programs, and the loading of the programs into the PLCs and subsequent verifications and testing are all performed by the integrator and/or the utility under a 10 CFR 50 Appendix B program and under strict configuration control. Because the output of the software tool as loaded into the PLC can be verified independently, and the tool is not connected to the PLC during operation in the plant (the PLC would be taken out of service during any re-configuration activity), the use of the tool is examined as part of dedicating the PLC but the tool itself does not require dedication. The PLC, its hardware and the embedded operating software (firmware) do require dedication for the ESFAS application.

The PLC is considered a more complex device to dedicate when compared to the equipment in the previous examples. Several factors contribute to this assessment. For example: the PLC can be provided in many different configurations, using multiple modules that intercommunicate via the backplane; configuration of the PLC involves setting up several different data files; the device can be programmed to perform many different functions, and its programming can include use of internal variables, register and bit manipulations, etc.; and the PLCs to be used in ESFAS have a greater number of inputs and outputs than the devices previously considered.

Identification and Verification of Critical Characteristics

Critical characteristics are identified based on the safety-related functions of the PLC. Examples of the critical characteristics identified are shown in Table 6-4. Acceptance criteria and verification methods are also listed in the table.

In this case the commercial grade vendor survey is a central part of the dedication. The survey requires extensive interaction with the PLC vendor. Initial contact is made and information obtained to prepare for the survey. Then a one-week visit (typical for a relatively complex device like this one) is made to the manufacturer's site where the bulk of the survey information is collected and evaluation performed. This includes evaluation of the vendor's QA program, digital system development process, verification and validation practices, configuration management program, and problem reporting procedures. In addition, a detailed critical design review of the PLC hardware and software architecture is performed, including evaluation of real-time task processing and robustness of failure management provisions.

The utility sees potential for other applications of the PLC beyond ESFAS, and plans to standardize on the use of this model PLC, saving on maintenance and training costs. All of the anticipated configurations of the PLC are identified prior to the survey (ESFAS and other known future applications), so the review of design, operating experience, testing, and other verification activities covers all of the expected

applications. Some of the future applications will use configurations that differ from those needed for ESFAS. By expanding the survey to cover a few additional modules and configurations offered by the vendor, the utility is able to cover these additional applications without much added cost. Then, when those modifications go forward the utility will have the survey information needed to support the dedication of the PLC for applications that are safety-related, and to satisfy the utility's survey requirements for digital equipment applied in critical non-safety systems.

Results of the survey verify that the vendor has a strong, formal program for software quality assurance including procedures for software development, verification and validation, configuration management, and deficiency reporting and correction. However, much of the base software for the controller is "legacy" or pre-existing software, developed over a period of time prior to implementation of the present software quality assurance program. The survey plan is tailored to reflect this, calling for performance of additional activities, or placing particular emphasis on activities that provide an evaluation of the legacy code. For example, because of the lack of formal documentation, additional emphasis is placed on interviews with key vendor personnel to obtain information on the legacy software design, its development and application history. Also, evaluations are performed to examine the suitability of the legacy code for use in this application (e.g., comparison of its original design requirements and use with those of the present application, the process used in porting the code to the present hardware platform, and what evaluations have been performed by the vendor to examine effects of re-using the legacy code, including effects on device failure modes).

The survey finds that the legacy software has evolved as it has been used in successive versions of the controller, following a software development process that contained the same basic elements as the present program but was less formal, without much documentation of the process or results of the software verification and validation activities that were undertaken. (For example, peer reviews of software were performed but not documented.) At the same time, this legacy software has gathered a great deal of operating experience in field applications, and it has matured as the vendor has incorporated lessons learned from each design evolution. This includes experience gained with the legacy software operating on the same platform as the units that are to be procured.

Changes to the software are now made under the present formal SQA program, following written procedures that require error tracking and regression testing as part of verifying all changes. Discussions with the software developers and quality assurance personnel indicate good familiarity with the SQA procedures and thorough knowledge of the PLC system and software, including a good understanding of those aspects of the design that the utility considers critical to the intended applications. Inspections of the actual documentation for recent changes and additions to the software, for the specific PLC model being dedicated, show that the vendor has been

thorough in implementing the SQA program for both changes and new development. The documentation is complete except for minor, non-critical omissions.

The vendor's configuration management practices receive particular scrutiny during the survey, as this has proven to be a recurring problem area with digital equipment. In addition to reviewing the written procedures, actual practices followed for configuration control are checked, looking for documentation and control of baselines, rigid control over changes made to software and the burning of PROMs (firmware), ability to re-create specific versions of the software, and configuration control during controller maintenance and refurbishment activities, both in the factory and by field technicians on-site. The vendor's program is judged to be sound and, more important, the performance-based survey shows it is followed closely in practice, for both legacy code and new software development.

For any PLC units sent in for repair, and for all new units, the vendor's normal practice is to install the latest revision of the firmware. Although the utility prefers to be able to obtain, at its option, the firmware version that has been dedicated, the vendor is not interested in making special arrangements to accommodate this. However, the vendor will provide reporting to the utility on all changes made to the firmware, including detailed information to help the utility evaluate the effects of any changes on its application and the dedication basis. Also, the performance-based survey finds that the vendor assigns a new firmware revision number for essentially all changes made to the software, even minor ones, and thorough regression testing is performed for the changes.

The firmware revision number is clearly identified in the unit, and it also can be displayed using the software configuration tool. In addition, the utility's practice is to include the firmware revision number with the model/part number of the PLC as part of the item's formal description in the utility's materials management system. The firmware revision is then included on any purchase order used to procure one of these devices. This practice ensures that any discrepancy between the as-delivered firmware revision and the firmware revision that was dedicated will be flagged in any future procurements. Any identified discrepancy would require evaluation by the utility using established procedures for evaluating replacement items. This would include evaluation of the effects of using one or more repaired PLCs, which have the new firmware, with PLCs having the earlier firmware revision level, within the ESFAS system. In this case, because the PLCs interface only through discrete, wired signal connections as opposed to the use of digital communication links or networks, evaluation of the use of multiple PLC firmware revision levels within the system would be relatively straightforward. (Evaluation of a system that uses digital communications among PLCs would be similar, but more complicated because of the more complex communications and related failure modes.)

Review of the operating history for the PLC includes review of data from the vendor, who has a formal program for recording feedback from field applications of the controller, evaluating the problems and defining corrective actions. Experience with the specific modules and controller configurations planned for the utility applications is checked as described in Table 6-4. Selected users are contacted to obtain first-hand information on experience with the equipment and the vendor's support.

A failure analysis is performed, starting early in the design process, to identify any potential vulnerabilities in the design of the overall upgrade, to support licensing activities for the modification, and to identify specific failure modes of concern for the PLCs. Allocation of functions to the different PLCs within a channel or train is based in part on the results of this analysis. The results also help focus the evaluation of the PLC design and the failure analysis for the PLC itself, which includes FMEA and other ACEs type evaluations. Review of the PLC's internal self-testing and fault detection capabilities, performed as part of the failure analysis and the vendor survey, identifies a number of internal faults that are detected by the PLC. The PLC operating software sets internal variables or register flags when these faults are detected, but these flags must be read by the application program in order to bring this information out of the device to alert operators or maintenance personnel. This finding leads to some additional requirements on the programming of the PLCs, and impacts other aspects of the modification (e.g., wiring of specific PLC outputs to indicators and alarms).

The design team also considers the option of adding a separate, hardware-based watchdog around each PLC, that would continuously monitor a periodic signal driven by the PLC application program to detect any silent failure that causes the PLC to stop processing the application. However, in this case it is concluded that such a feature is not required; the internal diagnostics have a high degree of coverage of internal failures, and the implementation of the onboard watchdog timers is sufficiently robust (protects against the failure modes of interest) that these features, combined with the fact that the ESFAS circuits are functionally tested every month and there is manual backup capability, provide adequate protection against such failures.

The failure analysis considers the possibility of a software-related common cause failure to occur that could disable the redundant PLCs and prevent an automatic actuation of an ESFAS function. The likelihood of such a failure is considered very low based on the review of the software development process, the successful operating history of the controller in similar applications, knowledge of the device design and failure management provisions, monthly surveillance tests that check functionality of the system, and extensive testing performed by the vendor and the utility/integrator to support the dedication. However, because of the potential safety significance if such a failure were to occur, the utility performs a defense in depth evaluation to determine whether the existing defense in depth (e.g., operator actions using the manual actuation capability) would provide adequate protection for design basis events. The evaluation,

using best-estimate methods, concludes that the existing manual capability could be used to adequately mitigate the design basis accidents of concern, with a high degree of confidence.

Conclusion

The utility concludes that the chosen PLC is acceptable for the ESFAS applications. Acceptance is based on a number of factors that are summarized below (see Table 6-4 for details):

- The formal, well-documented processes followed by the vendor for digital systems and software development, verification and validation, configuration control, and error reporting; although not fully in compliance with 10 CFR 50 Appendix B, the differences in the development process are primarily in completeness of documentation
- The operating history shows very good performance, with many units in service in various applications in a number of different industries; a significant number of the units in service use the same modules in the same or similar configuration to that planned for the ESFAS application; the vendor has a good track record for support, is proactive in addressing potential problems, has a solid configuration management program and follows it, and is cooperative in supporting the dedication effort
- A critical review of the device's overall architecture, hardware and software design, real-time task management, and failure management shows a good design that has evolved over the years of experience gained by the vendor and does not show any critical weaknesses that would affect its dependability in service
- The failure analysis indicates that the failures of concern for the ESFAS safety functions or for plant availability are adequately addressed in the design of the PLC's failure management features and in the provisions for operator or maintenance personnel notification provided in the upgrade design; a defense-in-depth analysis shows that there is adequate defense in depth via manual actuation independent of ESFAS to adequately mitigate the design basis accidents
- The utility and system integrator provide adequate control over the development, installation and maintenance of the application program and other configuration data for each installed controller, under an Appendix B quality assurance and configuration management program; the application programs are reviewed against the dedication package to ensure that the programming is within the bounds of the dedication (e.g., no special constructs or programming features are used that were not considered in the dedication)
- All critical characteristics are adequately verified through the combination of the survey, tests and inspections, and review of the product's performance record

A dedication package is prepared that documents the critical characteristics, verification methods employed, and the basis for the judgments made in accepting the controller for the ESFAS applications. The package identifies each specific application within ESFAS and the particular configuration of PLC that is dedicated for that application.

The controllers are entered into the utility's tracking system for dedicated commercial equipment, for each specific application within ESFAS. This includes placing the firmware, the software tool used for PLC configuration and programming, the application programs, and the hardware under configuration control. Also, information from the survey and other dedication activities is retained to support possible future applications of the controller.

Table 6-4a
ESFAS Programmable Logic Controller Critical Characteristics - Physical

Physical Critical Characteristic	Acceptance Criteria	Method of Verification
Configuration • Model number • Software revision number • Case type, dimensions and mounting	Vendor model # for main unit plus model/part numbers for each module to be procured and dedicated Vendor software revision # for each unit/module containing software or firmware Case type, dimensions and mounting per utility specification for each hardware configuration to be dedicated. Also, assembly per utility specification (e.g., holddown or positive locking of plug-in modules is in accordance with spec, consistent with seismic evaluation)	Receipt inspection for each unit/module received (or assembly received if pre-assembled by manufacturer)
Interfaces • Electrical power • Grounding and shield termination provisions • Number and type of inputs • Input impedance (with and without power) • Number and type of outputs • Output characteristics (e.g., current drive/sink capability) • Programmer (software configuration) interface • Front panel interface (HMI)	Per utility specification for each hardware configuration to be dedicated	Receipt inspection and testing for each unit received verifies correct interface/connection types, HMI features, etc. Some characteristics are verified by special testing on one unit of each model (e.g., test to verify maximum output current capability as part of design verification) along with review of vendor design information and vendor testing.

Table 6-4b
ESFAS Programmable Logic Controller Critical Characteristics - Performance

Performance Critical Characteristic	Acceptance Criteria	Method of Verification
Signal conditioning, bistable, and logic functions required for the application, e.g.: • Input signal filtering including anti-alias filters • Bistable logic functions required • Bistable setpoint adjustability • Bistable hysteresis • Combinatorial logic functions required • Timing and latching functions • Blocking and inhibit functions • Output isolation	Per utility specification for each PLC configuration	Verified through a combination of: • Review of PLC design including input module filters, anti-alias protection, implementation of bistable (comparator) and other required logic functions • Review of documented vendor testing for these features • Tests performed by the utility and/or integrator of the configured controllers, verifying proper functionality (tests verify application programming as well as PLC function) • Site acceptance testing for the integrated system
Response time including: • Time for signal conditioning and bistable units to produce bistable trip output in response to valid input • Time for logic units to produce actuation output in response to appropriate combination of bistable or other valid inputs	Per utility specification, based on required overall response time as used in safety analysis (limiting case may be used so that a single criterion is applied to all units for simplicity)	Review of PLC system design, including input sample rate, processing time, and total cycle time including output propagation and covering worst-case combination of times for each series PLC from sensing to actuation. Final verification via testing of integrated system.
Human-machine interface performance and ease of use, including use during: • operation (e.g., indications provided for status, fault indication, etc.) • configuration (ease of use, protection against mis-configuration, security features, etc.) • maintenance and troubleshooting (e.g., diagnostic information provided, clarity of information, etc.)	Per utility specification, covering operational requirements, configuration capabilities, maintenance and troubleshooting, and general human factors criteria	Detailed review of design and operation of the PLC during commercial grade survey, special testing by utility and/or integrator, and human factors evaluation by utility engineering and operations.

Table 6-4b (continued)
ESFAS Programmable Logic Controller Critical Characteristics - Performance

Performance Critical Characteristic	Acceptance Criteria	Method of Verification
Environmental compatibility: • EMI	Per utility specification (e.g., using EPRI TR-102323 or other suitable method)	Vendor testing, detailed review of hardware design and EMI protection features, laboratory testing of controller susceptibility and emissions in configurations that mimic as close as possible the installed configurations, and post-installation testing. This is coupled with specific practices followed in installation and wiring of power and signal cables and in grounding configuration for the ESFAS application. The dedicator notes that for another application a localized survey or map might be needed to characterize the EMI environment, if the application gives rise to potentially high EMI susceptibility through an unusual combination of sources, physical separation, grounding configuration and shielding approach (per EPRI TR-102323).
• Seismic	Per response spectra chosen to envelop all planned application locations	Third-party laboratory testing plus review of hardware and mounting design, including assembly and positive locking of plug-in components
• Temperature	Per utility specification, covering all planned application requirements	Vendor and/or third-party laboratory testing, plus review of reliability analysis assumptions regarding temperature
Behavior under abnormal/faulted conditions, e.g.: • Loss of power to one or more modules • Failure of an I/O module • Loss of one or more signal inputs • Short and open circuit of input or output • Input signal over/under range	Per specific requirements regarding fail-safe conditions for each application of the controller.	Review of vendor testing, detailed review of controller design and hardware/software architecture during commercial grade survey, failure analysis including FMEA for the controller, plus special tests performed by the utility to examine behavior under expected abnormal/faulted conditions, verifying safe response of controller.

Table 6-4c
ESFAS Programmable Logic Controller Critical Characteristics - Dependability

Dependability Critical Characteristic	Acceptance Criteria	Method of Verification
Built-in quality • Quality of design and manufacture	Vendor maintains a QA program that generally is in compliance with a recognized standard (e.g., ISO 9000). QA program addresses key areas including, as a minimum: • QA staff and organization definition • QA plans and procedures • Specific software QA procedures (e.g., ISO 9000-3) Evidence that the QA program was applied in the production of the procured item(s) hardware and recently developed software. Vendor presently follows a digital system/software development process that includes: • Software development plan and organization • Documented design requirements, including software requirements • Requirements traceability • Documented software design descriptions • Documented V&V plan • Validation test reporting Evidence that the digital system/ software development process has been followed for latest revisions of the software; for older, mature software (“legacy” software) produced prior to existence of this	Commercial grade survey, including: • Review of vendor QA program against relevant standards • Review of vendor procedures and practices for digital system/software development, V&V, and testing for each module/unit to be procured, and how these processes have evolved. Supplemental documentation prepared as necessary. • Thread audit to check actual practices for QA and software development and control • Check of degree to which QA program and software development process were applied in the design and production of the item(s) to be procured • Check of degree to which experience with previous designs has been factored into each succeeding design, evolving to a mature process and product • Review of controller design, software architecture including real-time task management, and implementation of diagnostics and error detection such as watchdog timer features • Review of software coding procedures or guidelines used in development • Samples of the software code reviewed to check adherence to established coding practices and to support the thread audit

Table 6-4c (continued)
ESFAS Programmable Logic Controller Critical Characteristics - Dependability

Dependability Critical Characteristic	Acceptance Criteria	Method of Verification
	program, evidence that a process was used that addresses essentially the same elements as the present process (though perhaps not as well documented). Documented product operating history showing product stability, reliability, and freedom from critical software-related errors or failures in similar applications. The items listed above, taken together, demonstrate adequate quality of the device.	• Review of operating experience with the specific controller modules and configurations to be procured[1] , including review of: Extent: number of units in service for each specific module to be used (main unit, I/O modules, power supply modules, etc.), and how long they have been in service; also, number of PLCs with the specific configurations[2] to be used in the planned applications • Relevance: types of applications, physical environment, operational environment, functions performed, specific software features used, size of application program • Success: vendor's data on problems and error rates; for specific applications; user's program for problem reporting and tracking (does vendor know it when failures occur? are they evaluated? etc.); experience

[1] Because of the relative complexity of the programmable logic controller, the variety of configurations in which it can be used, and the high safety significance of the planned ESFAS application, the review of product operating history for the PLCs is more extensive than it was for the previous examples. The survey confirms that the vendor uses a formal program to record feedback from the field via field returns or problems reported with the PLCs in service. There is good tracking and closure of the problem reports in a centralized database, with documentation of the nature of the problems encountered, the impact, and corrective actions taken. The survey team reviews problem reports and change records for hardware and software changes made to address the problems. All outstanding problem reports are reviewed, and none are judged to be critical. Vendor data indicate that the firmware has been stable over the recent operating history, in which many units have been operating in a number of different applications. There are no outstanding critical software failure reports. Because the PLC can be configured with different modules (I/O, power, etc.), establishing relevance of the operating history involves determining that many of the other applications of the controller use the same modules as for the planned application, and several use essentially the same configuration. The operating environment for many of the installed units is judged to be similar to that of the planned utility applications, and the utility will not be using any unusual or recently-developed modules or functions.

[2] Determining the number of units and specific modules in service helps determine the extent of the operating history for the PLCs. However, it is also important to determine the extent of experience with the particular configuration of modules to be used in the ESFAS application. There can be differences in the way in which the modules intercommunicate, differences in what portions of the PLC's operating software are exercised, and other differences depending on the particular configuration of modules (e.g., number and type of input/output modules communicating with the main unit). Review of the PLC's overall architecture, hardware and software design can help determine the important attributes of the configuration that need to be verified through field experience.

Table 6-4c (continued)
ESFAS Programmable Logic Controller Critical Characteristics - Dependability

Dependability Critical Characteristic	Acceptance Criteria	Method of Verification
		• with training of personnel, both maintenance and engineering; nature and cause of problems/errors encountered; support provided by vendor, both proactive and reactive; experience with software updates and information provided by vendor on same • Documentation: vendor's recording of problem/error reports, and their coverage of units sold and information needed to evaluate experience
Failure management	Continuous, built-in self-testing is provided that will detect as a minimum: • memory failures • internal communication failures (e.g., communication between I/O modules and main processor) • internal fuse failures • power failures to modules • processor halt (main or other processor, e.g., I/O) Alarms and other indications of failure conditions are provided per utility specification. Testability supports technical specification requirements for periodic surveillance testing. Failure modes important to the ESFAS system safety functions and plant availability are adequately addressed based on the failure analysis and evaluation of defense in depth.	Review of the PLC design, hardware and software architecture, and real-time task management, performed as part of the commercial grade survey, and an FMEA performed by the vendor, identifies important internal failure modes, evaluates self-test and diagnostic features provided in the design, including items such as watchdog times, and assesses the impact of failures on the PLCs functions. This includes evaluation of potential abnormal conditions and events (ACEs) per IEEE 7-4.3.2. System-level failure analysis for the ESFAS identifies the most important failure modes for the PLC from the standpoint of the system's safety functions and effect on plant availability. Each of these is evaluated specifically, using information from reviews above, to determine potential causes and likelihood of occurrence, and ensure that these failures are adequately addressed in the design. Review of product operating history to verify absences of specific critical failurs. Review of vendor testing, and performance of special challenge tests designed to test for possible critical failure modes in response to abnormal conditions (e.g., degraded power supply voltage,

Table 6-4c (continued)
ESFAS Programmable Logic Controller Critical Characteristics - Dependability

Dependability Critical Characteristic	Acceptance Criteria	Method of Verification
	(Note: Failure analysis is also used to help determine whether unreviewed safety questions exist per 10 CFR 50.59 - see EPRI TR-102348 and NRC Generic Letter 95-02.)	noisy signal, power and signal transients, combinations of input signal failures, HMI errors, configuration errors, etc.). The failure analysis and evaluation of backups in event of PLC failure (defense in depth evaluation) identifies capability to manually actuate each of the ESFAS functions that normally would be actuated automatically by the PLCs. The manual actuation capability could be used in the unlikely event of common cause failure of redundant PLCs (the four bistable channels, or the two actuation trains) and, on a best-estimate basis, adequately mitigate the consequences of the pertinent design basis accidents analyzed in the FSAR.
Configuration control	Vendor has a formal configuration control program and uses it over the life cycle of the software. Program includes: • Documented plan and procedures • Baseline maintenance • Change control • Control of firmware during initial manufacture and maintenance or refurbishment activities, including protection against introduction of software viruses • Control of development tools • Error-reporting and corrective action process	Review of configuration control program against appropriate standards during vendor survey, and inspection of actual practices and implementation of program for samples of the software used in the PLC to be procured (including both legacy and new software)
Problem reporting	Vendor has established error-reporting procedures, with sufficient coverage to ensure that problems potentially affecting any of the critical characteristics for the PLC will be reported, and vendor agrees to provide this problem reporting to the utility.	Review of error-reporting procedures, coverage of potential errors, and track record in implementing procedures, as part of vendor survey.
Reliability and availability	Hardware reliability/availability analysis has been performed that demonstrates adequate reliability and availability for the expected environmental conditions.	Review of vendor's reliability and availability analysis including data and assumptions used, and any supporting tests performed. Review of product operating history for demonstrated reliability

7

REFERENCES

1. ANSI/IEEE 610.12-1990, "IEEE Standard Glossary of Software Engineering Terminology."

2. ANSI/IEEE 730-1989, "Software Quality Assurance Plans."

3. ANSI/IEEE 828-1990, "IEEE Standard for Software Configuration Management Plans."

4. ANSI/IEEE 830-1984, "IEEE Guide to Software Requirements Specification."

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

6. ANSI/IEEE 1016-1987, "IEEE Recommended Practice for Software Design Descriptions."

7. ANSI/IEEE 1028-1988, "IEEE Standard for Software Reviews and Audits."

8. ANSI/IEEE 1063-1987, "IEEE Standard for Software User Documentation."

9. ASME NQA-1a-1995, Subpart 2.7, "Quality Assurance Requirements of Computer Software for Nuclear Facility Applications," American Society of Mechanical Engineers.

10. EPRI NP-5652, "Utilization of Commercial Grade Items in Nuclear Safety Related Applications," 1988.

11. EPRI NP-6406, "Guidelines for the Technical Evaluation of Replacement Items for Nuclear Power Plants," 1989.

12. EPRI TR-102260, "Supplemental Guidance for the Application of EPRI Report NP-5652," 1994.

13. EPRI TR-102323, "Guide to Electromagnetic Interference (EMI) Susceptibility Testing for Digital Safety Equipment in Nuclear Power Plants," 1993.

14. EPRI TR-102348, "Guideline on Licensing Digital Upgrades," 1993.

15. EPRI TR-103291, "Handbook for Verification and Validation of Digital Systems," 1994.

16. EPRI TR-104159, "Experience with the Use of Programmable Logic Controllers in Nuclear Safety Applications," 1995.

17. IEC 880-1986, “Software for Computers in the Safety Systems of Nuclear Power Stations.”

18. IEEE 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.”

19. IEEE 7-4.3.2-1993, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”

20. ISO 9003-3-1991, “Quality Management and Quality Assurance Standards - Part 3: Guidelines for the Application of ISO 9001 to the Development, Supply and Maintenance of Software.”

21. NRC Generic Letter 89-02, “Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products,” 1989.

22. NRC Generic Letter 91-05, “Licensee Commercial-Grade Procurement and Dedication Programs,” 1991.

23. NRC Generic Letter 95-02, “Use of NUMARC/EPRI Report TR-102348, ‘Guideline on Licensing Digital Upgrades,’ in Determining the Acceptability of Performing Analog-to-Digital Replacements Under 10 CFR 50.59,” 1995.

24. NRC Inspection Procedure # 38703, “Commercial Grade Dedication,” 1996.

25. NUREG/CR-5930, NIST 500-204, “High Integrity Software Standards and Guidelines,” 1992.

26. NUREG/CR-6421, “A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications,” 1996.

27. NUREG/CR-6294, “Design Factors for Safety-Critical Software,” 1994.

28. Title 10 of the Code of Federal Regulations, Part 21, “Reporting of Defects and Noncompliance,” 1995.

29. Title 10 of the Code of Federal Regulations, Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants.”